ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Міністерство внутрішніх справ України

ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Збірник матеріалів
Всеукраїнського науково-практичного семінару
24 листопада 2017

Дніпро 2018

УДК 004.78 + 330.47
ББК 65.9(4УКР)-98

Рекомендовано до друку рішенням Науково-методичної ради Дніпропетровського державного університету внутрішніх справ (протокол № 6 від 15 лютого 2018)

СКЛАД ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

Фоменко А.В.	к.ю.н, полковник поліції, ректор *(голова)*.
Бахчев К.В.	перший проректор, полковник поліції *(заступник голови)*.
Рижков Е.В.	к.ю.н, доцент, завідувач кафедри економічної та інформаційної безпеки *(заступник голови)*.
Косиченко О.О.	к.т.н, доцент кафедри економічної та інформаційної безпеки *(відповідальний секретар)*.

ЧЛЕНИ ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

Наливайко Л. Р.	д.ю.н, професор, заслужений юрист України, проректор.
Вишня В.Б.	д.т.н, професор, професор кафедри економічної та інформаційної безпеки.
Краснобрижий І.В.	к.ю.н, доцент кафедри економічної та інформаційної безпеки.
Гавриш О.С.	викладач кафедри економічної та інформаційної безпеки.

П78 Використання сучасних інформаційних технологій діяльності національної поліції України: матеріали всеукраїнського наук.-практ. семінару, м. Дніпро, 24 листопада 2017 року – Дніпро: ДДУВС, 2017. – 195 с.

У збірнику представлено виклад доповідей та тез, наданих на всеукраїнський науково-практичний семінар «Використання сучасних інформаційних технологій діяльності національної поліції України», який відбувся на базі кафедри «Економічної та інформаційної безпеки» Дніпропетровського державного університету внутрішніх справ 24 листопада 2017 року.

Опубліковано в авторській редакції

УДК 004.078
ББК 65.9(4УКР)-98

ЗМІСТ

Вдосконалення навчального процесу з урахуванням сучасних тенденцій інформатизації структурних підрозділів національної поліції

Рижков Е.В.
завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент

Процес реформування правоохоронного відомства безумовно повинен встановлювати нові стандарти для інформаційного забезпечення Національної поліції. Підходи десятирічної давнини не сумісні з намаганнями держави наблизити результативність діяльності поліцейських до загальноєвропейських стандартів. І в цьому плані є певні позитивні зрушення: розробляються та опрацьовуються нові підходи щодо забезпечення інформаційної безпеки існуючих в МВС інформаційних систем; прослідковується запровадження інформаційно-аналітичних продуктів у діяльність різноманітних підрозділів Національної поліції; поступово розширюється коло суб'єктів, яким надана можливість використання інформаційних можливостей Національної поліції на базі планшетних пристроїв. Так, після патрульної поліції такими суб'єктами стали слідчо-оперативні групи відділів поліції та дільничні офіцери поліції (на прикладі м. Дніпро).

Проте, вкрай негативною залишається ситуація із забезпеченням вищих навчальних закладів Міністерства спеціалізованими інформаційними продуктами та подовженням заборони на їх підключення до існуючої Інтегрованої інформаційно-пошукової системи.

В умовах цієї заборони та тотального дефіциту програмного забезпечення навчальних закладів системи МВС з боку центрального органу науково-педагогічні колективи вимушені вишукувати варіанти вирішення проблем забезпечення навчального процесу аматорськими підходами з тим, щоб не обмежуватись навчально-методичними матеріалами презентаційного характеру.

Саме з цією метою у Дніпропетровському державному університеті внутрішніх справ фахівцями кафедри економічної та

інформаційної безпеки розроблена та використовується інформаційно-технічна платформа, яка покладена у основу проекту «Лінія-102».

В рамках проекту реалізовано повний замкнутий цикл відпрацювання навчальних фабул від отримання первинної інформації про правопорушення до винесення судом відповідного вироку. Безумовною перевагою проекту є його практична спрямованість. За сучасною методикою рольової гри курсанти, студенти та працівники Національної поліції набувають практичних навичок, вивчають та поглиблюють теоретичний матеріал. Максимальна наочність та наближеність до реальних умов підвищує їх мотивацію до навчання здобувачів вищої освіти, сприяє підготовці мотивованого педагога із нестандартним творчим мисленням. Комплексність у вирішенні навчальних задач сприяє розумінню взаємодії між собою різних суб'єктів правоохоронної, правозастосовної та судової практики.

Таким чином, в університеті вперше в системі МВС із використанням інформаційно-технічної платформи створено Навчально-інтерактивний комплекс з підготовки здобувачів вищої освіти та практичних працівників Національної поліції, який передбачає повний замкнутий цикл опрацювання інформації про протиправні діяння від її надходження на лінію 102, збору доказової інформації в рамках кримінального провадження до розгляду матеріалів у судовому засіданні в рамках реалізації правозастосочної, правоохоронної та судової функції та створено інноваційну педагогічну методику для навчальних закладів зі специфічними умовами навчання.

Слід відмітити, що в процесі роботи в цьому напрямі за університетом закріплені авторські права та отримано деклараційний патент на корисну модель «Система управління нарядами мобільної патрульної служби» (висновок МЕРТ України №12898/ЗУ/17 від 06.06.2017).

Після апробації проекту на рівні університету 26-27 жовтня 2017 року серед вишів МВС було організовано міжвузівський тренінг. За його результатами отримано позитивну реакцію представників команд-учасників та керівництва навчальних закладів. Так, наприклад, від керівництва Львівського державного університету внутрішніх справ на адресу університету надійшов лист з проханням про використання в навчальному процесі набутого нами досвіду з проведення «Лінії-102», функціонування її інформаційно-технічної платформи та методичного забезпечення.

В свою чергу, маємо намір за підтримки до Департаменту персоналу, організації освітньої та наукової діяльності МВС України запропонувати використання як мінімум інформаційно-технічної платформи, а в ідеалі – «Лінії-102» у повному обсязі у всіх навчальних закладах міністерства.

Плануємо підключити до співпраці представників Національної академії прокуратури через дистанційну он-лайн участь їх представників у діловій грі на етапах відпрацювання роботи слідчо-оперативної групи та виконання функції прокурора на досудовому розслідуванні та у суді.

Перспективним напрямом експлуатації інформаційно-технічної платформи є подальша розробка і імплантація у проект додаткових сегментів практичної спрямованості, а саме: аналітичних програмних продуктів, що дозволять оптимізувати діяльність оперативних та слідчих підрозділів, пошукових методик отримання необхідної інформації та напрацювання оптимальних алгоритмів діяльності.

Разом з тим, наряду з позитивними напрацюваннями науково-педагогічних колективів навчальних закладів, вважаємо неперспективною існуючу практику відокремлення навчальних закладів системи МВС від темпів та якості інформаційно-технічного забезпечення практичних підрозділів Національної поліції. Керівництво Міністерства повинно враховувати в політиці розвитку те, що функціонал спеціалізованих кафедр, де викладаються дисципліни інформаційно-технічного спрямування, повинен відповідати сучасним вимогам якісної професійної підготовки офіцерів поліції. Слід повернутися до позитивної практики централізованого забезпечення державних навчальних закладів зі специфічними умовами навчання. В нашому випадку – інформаційно-технічними ресурсами.

Використання інформаційних технологій в діяльності Національної поліції України та проблемні питання забезпечення інформаційної безпеки

Свириденко С.В.
т.в.о. начальника Управління інформаційно-аналітичної підтримки ГУНП в Дніпропетровській області
Слісаренко І.В.
заступник начальника управління - начальник відділу адміністрування інформаційних систем Управління інформаційно-аналітичної підтримки ГУНП в Дніпропетровській області

Запорукою ефективної роботи та функціонування будь-якої державної установи, чи системи державних органів влади в умовах сьогодення є, насамперед, збір, класифікація, аналіз великого обсягу інформації та швидке прийняття рішень за результатами її обробки. Саме це в умовах сучасного, динамічного, високоінформативного світу є одним з найважливіших чинників успіху.

Національна поліція України, як центральний орган виконавчої влади, що служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку, як ніхто інший потребує постійного впровадження сучасних інформаційних технологій, для забезпечення високої ефективності роботи кожного поліцейського, надання швидкого доступу до інформаційних банків даних Національної поліції, сприяння повному збору інформації безпосередньо на місці події, здійснення аналітичної і превентивної діяльність, що має на меті зменшення кількості скоєних кримінальних та адміністративних правопорушень.

Таким чином, розуміючи вищезазначені фактори в роботі органів поліції, інформаційні підрозділи Національної поліції України за останні декілька років досягли значних результатів в сфері інформатизації та автоматизації роботи поліцейського.

На теперішній час створено швидкісну єдину цифрову відомчу телекомунікаційну мережу (ЄЦВТМ) НПУ, що поєднала у собі всі без винятку підрозділи поліції України, та, в свою чергу, стала платформою для подальшого розвитку впровадження та використання інформаційних технологій.

Всі існуючі в підрозділах поліції автоматизовані обліки, що були накопичені роками, сьогодні об'єднані в єдину загальну реляційну базу даних з доступом через веб-інтерфейс - інформаційний портал Національної поліції України. Це дозволяє створити загальне інформаційне середовище роботи поліцейського та забезпечити отримання вичерпної наявної інформації із всіх існуючих інформаційних підсистем на звичайному робочому місці, що підключене до ЄЦВТМ. На теперішній час в підрозділах поліції ГУНП в Дніпропетровській області зареєстровано 3 327 активних користувачів інформаційного порталу НПУ. Система дозволяє здійснювати централізоване ведення існуючих обліків, пошук за визначеними реквізитами, пошук через майстер-запитів із використанням всіх наявних реквізитів конкретної підсистеми, формувати велику кількість різноманітних звітів для подальшого використання у службовій діяльності поліцейських.

На базі інформаційного порталу НПУ розбудовується єдина система управління нарядами поліції, а саме групами реагування патрульної поліції та слідчо-оперативними групами територіальних підрозділів ГУНП, автопатрулями патрульної поліції та поліції охорони.

Завдяки використанню програмного забезпечення LIS-M реалізована інтеграція в існуючу інформаційну систему мобільних та планшетних пристроїв з використанням закритої 2G/3G мережі оператора мобільного зв'язку. Є можливість здійснювати не лише доступ до інформаційних ресурсів Національної поліції України, а й, використовуючи технологію GPS, визначати місцезнаходження зазначених пристроїв та відображати їх на карті єдиної дислокації підрозділів поліції області для більш ефективного управління. Також, підключені та відповідним чином зареєстровані в системі планшетні пристрої, забезпечують можливість введення інформації в інформаційні підсистеми, завантаження відео та фотоматеріалів що, в свою чергу, сприяло впровадженню в практичну діяльність підрозділів поліції спрощеного порядку розгляду заяв і повідомлень без ознак кримінальних правопорушень, зниженню навантаження на дільничних офіцерів поліції, покращенню якості збирання первинних матеріалів працівниками патрульної поліції безпосередньо за місцем виклику.

Більш ефективному використанню планшетних пристроїв у територіальних підрозділах поліції, нажаль, заважає слабкий розвиток інфраструктури зв'язку за технологією 3G в Дніпропетровській області за межами великих міст, але це питання часу.

На етапі розбудови створення єдиного call-центру викликів, що надходять на спецлінію «102» з всієї території Дніпропетровської області. Встановлено и налаштовано кластер серверів з програмним забезпеченням «CallWay», що з використанням єдиного цифрового потоку дзвінків Е1 та відповідного телекомунікаційного обладнання дозволяє вже сьогодні здійснювати обслуговування викликів, які надходять з території м. Дніпро, м. Кривий Ріг, Новомосковського та Синельниківського районів, а це приблизно 1600 викликів на добу. Реалізація єдиного call-центру дозволить забезпечити контроль над питанням якості та своєчасного реагування підрозділів поліції на повідомлення громадян про скоєння правопорушень, забезпечить стовідсоткову реєстрацію зазначених подій та з технічного боку окрім якісного цифрового каналу зв'язку, архівацію виклику з відповідним приєднанням цього запису до картки «102» у відповідній підсистемі інформаційного порталу.

Вивчається питання об’єднання та використання у службовій діяльності підрозділів поліції вже існуючих місцевих систем відеоспостереження. Мета такого об’єднання - створення єдиного програмно-апаратного комплексу з інтеграцією його з вже існуючими банками даних поліції, що надало би можливість в автоматичному режимі здійснювати аналітичну обробку відеопотоків, які надходять, з метою виявлення правопорушень, реагування на надзвичайні події, у тому числі й техногенного характеру, розкриття кримінальних правопорушень. Програмні платформи Milestone systems та Hewlett packard IDOL на теперішній час розглядаються, як можливі варіанти реалізації зазначеного питання.

Безперечно, слід зазначити, що у сучасних умовах розвитку інформатизації підрозділів Національної поліції України надзвичайного значення набувають питання забезпечення належної інформаційної безпеки при опрацюванні даних, які, відповідно до Закону України «Про Національну поліцію» збираються та зберігаються у відомчих інформаційних ресурсах.

З одного боку повсякденне виконання службових та функціональних обов’язків поліцейського потребує від нього використання відомчих інформаційних ресурсів, власником яких є держава, та які містять персональні дані громадян і охороняються відповідно до вимог чинного законодавства. З іншого боку, наприклад, слідчі підрозділів Національної поліції обов’язково повинні мати доступ до всесвітньої інформаційної мережі Інтернет для внесення необхідних

даних до Єдиного реєстру досудових розслідувань. За аналогічних умов забезпечується доступ поліцейських структурних підрозділів ГУНП до єдиних та державних реєстрів, володільцем яких є Міністерство юстиції України.

Викладене створює передумови для несанкціонованого втручання сторонніх осіб у роботу відомчих інформаційних ресурсів за допомогою шкідливого програмного забезпечення (комп'ютерних вірусів), що розповсюджується через всесвітню інформаційну мережу Інтернет.

Найбільш істотним за останній час фактом такого втручання були події травня-червня поточного року, пов'язані із розповсюдженням шкідливого програмного забезпечення «Petya.A».

На теперішній час не існує дієвого технічного рішення питання вичерпного розділу різних інформаційних систем в одній автоматизованій системі, забезпечення персоніфікації доступу до відомчих інформаційних ресурсів. Так, слід зазначити, що на даний час, проводяться організаційні заходи, спрямовані на запобігання витоку службової інформації, зокрема:

- всі користувачі під особистий підпис попереджаються про неприпустимість у будь-який спосіб поширювати інформацію, яка їм стала відома у зв'язку із роботою з відомчими інформаційними ресурсами;

- розроблено та запроваджено процедуру надання атрибутів доступу до відомчих інформаційних ресурсів, що унеможливлює їх несанкціоноване отримання;

- проводиться моніторинг активності користувачів, за результатами чого перевіряються підстави опрацювання ними інформаційних запитів.

Нажаль, слід зазначити, що викладені заходи є недостатніми та в повній мірі не забезпечують необхідний рівень інформаційної безпеки.

На завершення свого виступу хотів подякувати за запрошення та можливість зазначити існуючі проблемні питання інформаційної безпеки в підрозділах Національної поліції України з метою їх подальшого фахового обговорення, визначення шляхів вирішення та етапів практичної реалізації відповідних заходів.

Використання програмного забезпечення IBM i2 analyst's notebook у аналітичній діяльності

Тишлек Д.П.
начальник управління захисту економіки в Дніпропетровській області Департаменту захисту економіки Національної поліції України.
Мазур Ю.В.
старший оперуповноважений в ОВС відділу оперативно-аналітичного забезпечення Управління захисту економіки в Дніпропетровській області Департаменту захисту економіки Національної поліції України.

На сьогоднішній день у нашому житті практично не залишилось галузей в суспільстві, де не використовуються інформаційні технології, комп'ютеризовані комплекси тощо. Всі ці системи оперують певними масивами даних, які рано чи пізно виникає необхідність аналізувати. І якщо у деяких сферах (фінансового, технічного характеру тощо) існують такі механізми, якими хоча б частково можна автоматизувати аналіз інформації, то в частині кримінального аналізу таких механізмів обмаль.

У рамках наданих повноважень працівники Управління здобувають достатній масив даних, що містить інформацію про злочинну діяльність як окремих суб'єктів, так і організованих злочинних груп. У зв'язку з чим надважливим на сьогодні є застосування аналітичних інструментів, які б надали можливість оперативно опрацьовувати високооб'ємні дані, а також виконувати автоматизовані аналітичні функції. Одним із таких інструментів є кримінальний аналіз.

Кримінальний аналіз – встановлення та передбачення зв'язків між даними про злочинну діяльність та іншими, потенційно з ними пов'язаними даними з метою їх використання у розробленні тактичних та стратегічних засад з протидії злочинності. Кримінальний аналіз, можна розглядати як специфічний вид інформаційно-аналітичної діяльності, яка полягає в ідентифікації і якомога точному визначенні внутрішніх зв'язків між інформаціями (відомостями, даними), що стосуються злочину, та будь-якими іншими даними, отриманими з

різних джерел, і їх використанням в інтересах ведення оперативно-розшукової діяльності, досудового розслідування та їх аналітичної підтримки.

У ході кримінального аналізу забезпечується цілеспрямоване збирання/здобування, упорядкування, фіксація, аналіз та оцінка кримінальної інформації, її представлення (візуалізація), передача та реалізація.

У країнах Європейського Союзу, США та інших країнах світу провадження кримінального аналізу є загальнообов'язковим для всіх правоохоронних органів та відіграє досить вагоме значення у попередженні та розкритті злочинів. Його зміст, правила та процедура чітко визначено та врегульовано у правовому відношенні. Це, зокрема стосується ведення оперативно-розшукової діяльності, слідства та розгляду кримінальних справ у суді.

Відповідно кримінальним аналізом займаються і такі міжнародні структури як Інтерпол та Європол.

Кримінальний аналіз в сфері протидії економічній злочинності досить складний процес. Здебільшого, аналізу піддаються відомості про учасників та переможців тендерних процедур, схеми руху грошових потоків через банківські установи, схеми виведення грошових коштів за межі держави, у тому числі на офшорні рахунки, дані про перетин кордону вантажем, транспортом тощо.

Враховуючи великі об'єми інформації, на все це необхідно витратити велику кількість часу, до того ж результати, отримані з різних програм матимуть різні формати, дані з яких потім дуже складно аналізувати та приводити до одного цілого.

На сьогодні одним з найкращих аналітичних продуктів є програмне забезпечення IBM i2 Analyst's Notebook, яке дозволяє опрацьовувати великі об'єми розрізненої інформації та видавати результат у наглядному вигляді в найкоротший термін.

IBM i2 Analyst's Notebook – це візуальне аналітичне середовище, яке дозволяє максимально ефективно використовувати величезні обсяги інформації, накопичені державними службами та підприємствами, дозволяє аналітикам швидко зіставляти, аналізувати і наочно представляти дані з різних джерел, скорочуючи час на пошук важливої інформації в складних даних. IBM i2 Analyst's Notebook надає актуальні і дієві аналітичні засоби що допомагають виявляли, передбачати, запобігати і припиняти злочинну, терористичну і шахрайську діяльність, у тому числі у сфері економіки.

За допомогою IBM i2 Analyst's Notebook можна:

- швидко систематизувати розрізнені дані в єдине узгоджене подання.

- визначити ключових осіб, подій, зв’язків і закономірностей, які не завжди можна виявити іншими способами.

- отримати розуміння структури, ієрархії і способів дій злочинних організацій.

Вказана програма пропонує безліч можливостей для створення різних схем і має в своєму розпорядженні додаткові функції для роботи з великим об'ємом інформації, а саме:

• Різні об'єкти зображуються графічно: іконками і лініями зв'язку, що підсилює вироблене схемою враження.

• У будь-який момент можна змінити розташування і зображення об'єктів схеми.

• Раніше створені схеми (або об'єкти схеми) можна перекопіювати і на їх основі створити нові схеми.

• Схеми можна створювати автоматично.

• Можливість для складання складних аналітичних схем.

• Для виділення знаходиться на схемі інформації, можна змінити колір об'єктів і ліній зв'язку, шрифт і колір тексту, збільшити розмір об'єктів.

• На схему можна додати відеокліпи, аудіозаписи та документи. Карту, план приміщення і т.п. можна використовувати як об'єкт фону схеми, завдаючи на нього необхідні іконки і зв'язку.

• Можливість створення шаблонів (templates), що дозволяють дотримуватися єдиного стилю при створенні схем.

• Пропонує набір функцій для аналізу зображеної на схемі інформації тощо.

Внесення інформації до схеми надає змогу її візуалізувати, вказати типи та якість зв’язків, час подій, що допомагають у аналізі інформації з різних джерел. Крім того вбудований у вказаній програмі імпорт інформації зі структурованих джерел (наприклад імпорт файлу у форматі Excel, текстового файлу), допомагає отримати та відобразити у схемі великий об’єм зв’язків, які можливо фільтрувати та організовувати для подальшого аналізу.

За допомогою встановлення додатку iBridge з його подальшим налаштуванням можливий імпорт інформації безпосередньо до схеми з баз даних Oracle та інших.

Методичні рекомендації щодо використання програмного забезпечення IBM i2 analyst's notebook (версія 8.9.5) для аналізу імпортованих файлів у форматі «EXCEL». департамент захисту економіки, 2016

1. Analyst’s Notebook Пособие © i2 Ltd © Real Systems
2. https://www.ibm.com/support/knowledgecenter/ru/SS3J58/com.ibm.i2.anb.doc/analysts_notebook_welcome.html

Безупинне комп'ютерне навчання, як складова якісної підготовки фахівців у системі навчальних закладів МВС України

Вишня В.Б.
професор кафедри економічної та інформаційної безпеки ДДУВС, доктор технічних наук, професор

Одним з найважливіших досягнень 20-го сторіччя вважається створення персонального комп'ютера. По впливу цієї події на розвиток людства його порівнюють з відкриттям писемності. Підвищення ефективності використання сучасних комп'ютерних засобів на благо людини і суспільства – задача, що постає зараз не тільки перед вченими в галузі комп'ютерних наук, але і перед науково-педагогічним складом вищих навчальних закладів. Навряд чи в кого викликає сумнів той факт, що серйозна базова комп'ютерна підготовка випускника вузу багато в чому запоруку майбутнього успіху його в професійній діяльності.

Позиція діяльності керівництва країни і МВС України базується сьогодні на тім, що майбутнє України в інтеграції в Європейську співдружність через обов'язкове оволодіння населенням країни іноземними мовами і загальною комп'ютерною грамотністю. Тільки в такий спосіб ми можемо скористатися інтелектуальним і технічним надбанням ведучих західних країн і познайомити їх з нашими досягненнями. Тому нам не перешкодить визначитися, як ми готуємо наших курсантів і студентів в галузі комп'ютерних знань і чи відповідає це задачам сьогоднішнього дня.

У Дніпропетровському державному університеті внутрішніх справ курсанти і студенти, для одержання кваліфікації «бакалавр», навчаються 8 семестрів. Однак, тільки в двох семестрах з 8-ми вони проходять

навчання користуванню комп'ютером на профілюючій кафедрі (економічної та інформаційної безпеки). Причому курсанти опановують навичками роботи з комп'ютером (Windows, Far, Word, Excel) на першому курсі, а на третьому - тобто практично через два роки, вивчають спеціальні додатки використання комп'ютерних засобів (інформаційно-комп'ютерні системи в діяльності органів внутрішніх справ, в економіці, комп'ютерні мережі). Студенти, і того гірше, вивчають ці дисципліни тільки на першому курсі.

Дані дисципліни дають майбутнім правоохоронцям і юристам загальне представлення про можливості персональних комп'ютерів, локальних і глобальних комп'ютерних мереж, початкові навички роботи з ПК. І це все. У той же час, у рамках поставлених перед вузами нашої системи задачі, випускники зобов'язані бути такими користувачами комп'ютерної техніки, які чітко усвідомлюють, що персональний комп'ютер – це обов'язковий і дуже надійний супутник у їхній професійній діяльності.

Чому ж у нас цього поки не виходить. Не тому, що ми їх погано готуємо. Просто в будь-якій справі, у тому числі й у комп'ютерному навчанні, повинна бути системність. Не можна курсантів і студентів учити роботі з комп'ютером уривками. І тут нам на допомогу може прийти організація у вузі безупинного комп'ютерного навчання, яке реалізована в ряді провідних технічних вузів країни.

Суть такого навчання полягає в тому, що в тих семестрах, у яких не ведеться базова комп'ютерна підготовка профілюючою кафедрою, інші кафедри навчального закладу підключаються до неї через систему завдань, що вимагають використання комп'ютерних засобів і вже наявних у курсантів (студентів) знань.

Стосовно до наших умов це може бути видача завдань кожному курсанту (студенту), що вимагають пошуку необхідних документів у мережі Internet чи «Ліга», статистичної обробки даних, побудови таблиць, графіків і діаграм, що характеризують тенденції в правоохоронній діяльності Національної поліції. Багато курсових робіт стали б від цього більш привабливими, несли науково-дослідний характер.

Важливим елементом програми підготовки фахівця є ознайомлювальна і навчальна практики. У рамках безупинного комп'ютерного навчання завдання на практику повинні включати питання, що змусять курсантів звернутися до автоматизованих інформаційних систем (АІС), що реалізованих на базі сучасних

комп'ютерних засобів. Однак у цьому випадку важливо уникнути формалізму. Необхідно, щоб поставлені завдання були не просто виконані, а виконані самими курсантами (студентами). А цього можна досягти лише у випадку, коли при захисті завдань викладачі будуть вимагати знання не тільки по суті виконаного завдання (професійні знання), але і по способах, прийомам і умінням його виконання (базові комп'ютерні знання). Відповіді на останні питання не повинні вважатися другорядними і враховуватися нарівні зі знанням основного предмета.

Так, ми усвідомлюємо, що це може виявитися складним для ряду викладачів, зажадають знань і умінь самому вирішити поставлену задачу за допомогою комп'ютерних засобів. Можливо, прийдеться декому і підучитися.

Однак, щоб вирішувати цю задачу сьогодні варто згадати, що на кожній кафедрі є науково-педагогічні кадри, які добре володіють ПК і працюють в комп'ютерних мережах. Вони і могли б узятися за це діло, не чекаючи підготовки інших співробітників. До підготовки завдань на практику і перевірки отриманих знань (звітів) могла б підключитися профілююча кафедра (економічної та інформаційної безпеки) за умови виділення (перерозподілу) для цієї мети відповідного навчального навантаження.

З метою підвищення рівня комп'ютерної підготовки співробітників Національної поліції всі кандидати на керівні посади МВС України повинні здавати екзамен з комп'ютерній грамотності. З цією метою при Управлінні інформаційно-аналітичного забезпечення Головного управління Національної поліції в Дніпропетровській області кілька років потому була створена комісія для прийому цих іспитів, розроблена програма необхідних умінь і знань для кандидатів, що пройшла рецензування в нашому університеті.

Тому, для того, щоб наші випускники гідним образом виглядали в територіальних органах, вважаємо за необхідне перевірку підсумкових (вихідних) знань по комп'ютерній підготовці включити в державні іспити, підключивши до цього фахівців базової кафедри університету. Для цієї мети достатнім буде рішення Вченої Ради університету, що визначає глибину й обсяг контролю.

Ми усвідомлюємо, що реалізація програми безупинного комп'ютерного навчання не є простою справою, вона зажадає мобілізації зусиль багатьох співробітників, служб і кафедр університету. Але у випадку її здійснення, ми одержимо відчутні результати, за які нам будуть вдячні наші випускники й практичні підрозділи Національної

поліції, куди вони підуть працювати, виконаємо задачу щодо підвищення практичної складової навчання, поставлену перед нами керівництвом університету і МВС України.

Аналіз об'єктів викрадень, систем і засобів захисту вантажів на залізницях

Вишня О.В.
кандидат юридичних наук, доцент
Скорик Т.М.
курсант 3 курсу факультету підготовки фахівців для органів досудового слідства ДДУВС

Залізничний транспорт, як одна з головних галузей економіки, призначена задовольняти потреби населення та суспільного виробництва в перевезені вантажів. Сьогодні на долю "Укрзалізниці" випадає біля двох третин усього вантажообігу в країні. Величезні матеріальні цінності, зосереджені на транспорті, вимагають надійної охорони їх від злочинних посягань.

Разом з тим в оперативній обстановці, що склалася за останні роки на залізничному транспорті відмічається тенденція зростання злочинності, у тому числі, і найбільш небезпечних злочинів – викрадань вантажів.

Для працівників підрозділів поліції, що борються с цими злочинами, важливим стає придбання необхідних знань відносно структури і системи функціонування процесу перевезення вантажів на залізницях, рухомого складу, його використання та тощо. Зокрема для швидкого і кваліфікованого розслідування і розкриття викрадань вантажів слідчі повинні мати знання основ комерційної і вантажної роботи, знати правила здійснення операцій по прийому, відправленню, видачі вантажів, а також обов'язки працівників залізничного транспорту і клієнтури, що приймають участь в операціях [1, 182].

Для перевезення вантажів сьогодні використовується різний вид рухомого складу (криті вагони, піввагони, платформи, цистерни, ізотермічні та спеціальні вагони).

У критих вагонах перевозять тарні, штучні, насипні та інші вантажі, що піддаються атмосферним впливам [2, 228]. Ці вагони мають двоє дверей з зовнішніми запорами і чотири бічних люки, що

зачиняються зсередини. Спеціальні криті чотиривісні вагони з дверима, що самоущільнюються, дозволяють робити механічне завантаження і вивантаження насипних вантажів. На даху знаходиться чотири люки. Вантаж, що надходить через них, тисне на двері, притискаючи їх до стійок. При вивантаженні спочатку відкривається поміщений у міждверному просторі люк, через який висипається вантаж, а потім – двері [3, 4].

До критих вагонів також належать цільнометалеві вантажні вагони типу УМГВ, обладнані для двох'ярусного перевезення легкових автомобілів.

Збирально-роздавальні вагони призначені для перевезення дрібних відправлень у супроводі вагарів-роздавальників, для яких виділено спеціальне службове відділення [4, 98]. Для дрібних відправлень без вагарів-роздавальників використовуються криті вагони, розділені всередині на секції. У кожній секції міститься вантаж, призначений до визначених станцій, потім вони пломбуються [5, 249-250].

Піввагони [6, 208] використовуються для перевезення, головним чином, навалочних вантажів (кам'яне вугілля, кокс, руда і рудні концентрати мінеральні будівельні матеріали). Вони обладнані високими бортами з торцевими дверима і нижніми розвантажувальними люками, що зачиняються гофрованими металевими відкидними кришками з замикаючими пристроями. Цей тип вагонів найбільш підданий для нападу з метою викрадання вантажу.

У разі навантаження у такі вагони вантажів, що містять дрібні фракції, відправник повинен вжити заходи щодо запобігання видуванню та просипанню дрібних часток вантажу під час перевезення, особливо у випадках навантаження вище рівня бортів вагона (із "шапкою"). Поверхня вантажу у всіх випадках розрівнюється і ущільнюється. Для цього відправник може використовувати механізовані установки та інші пристрої [6, 209].

З метою забезпечення збереженості вантажу на його поверхню може наноситися маркування або застосовуватися покриття плівкою (емульсією) чи інше закріплення верхнього шару вантажу.

У разі навантаження у піввагони вугілля вище рівня його бортів "шапка", після ущільненню вантажу, в поперечному розрізі повинна мати форму трапеції з висотою не більш 300 мм над обв'язаним брусом кузова півагона. Це дуже важлива вимога до перевезення такого виду вантажу, бо дозволяє при огляді вагона по зовнішньому вигляду вантажу елементарно зробити висновок про наявність викрадань. На жаль,

залізниці не завжди можуть зажадати від відправників обов'язкового виконання цієї умови незважаючи на те, що вугілля є об'єктом постійного викрадання, а перевезення вугілля за своїм об'ємом складає значну частину вантажообігу на залізничному транспорті [7, 194].

Певні вимоги встановлені і до завантаження вагона мінерально-будівельними вантажами [6, 209].

На платформах перевозять великовагові, довгомірні, громіздкі вантажі (лісоматеріали, металеві труби та інше). Платформи мають відкидні металеві або дерев'яні борти з замикаючими пристроями, а також торцеві і бічні гнізда [3, 4].

Цистерни використовуються для транспортування рідких та наливних вантажів. Вони обладнані верхніми, нижніми або універсальними зливальними приладами. До числа рідких вантажів, що перевозяться в цистернах, відносяться більш 300 найменувань. Тому весь парк цистерн поділяється на три основні групи [7, 217].

До першої з них відносяться цистерни, що призначені для транспортування нафти та продуктів її переробки. Нафтопродукти поділяються на світлі (бензин, керосин, дизельне паливо), темні (сира нафта, мазут, масла та мастила, моторне паливо) та бітуми [7, 216]. Бітуми, що є останніми продуктами перегонки нафти, та інші особливо в'язкі вантажі транспортуються в бункерних піввагонах, що мають двійні металеві стінки та труби, по яким пропускається підігрітий пар для нагріву поверхні внутрішніх стінок та слою вантажу, що до них прилягає. Треба відмітити, що бункерні піввагони та цементовози відносяться то типу спеціальних вагонів [3, 5].

До другої групи належать цистерни для перевезення хімічних вантажів, зокрема зрідженого газу, кислот, отрути. Останні транспортуються в цистернах, не обладнаних зливальними пристроями.

Третя група – спеціальні, для перевезення харчових продуктів (спиртові, винні, молочні) та спеціалізовані цистерни, для транспортування рослинної олії, патоки та інше.

З точки зору збереження вантажів від викрадання правоохоронні органи цікавлять лише цистерни першої та третьої груп.

Ізотермічні вагони призначені для перевезення швидкопсувних продуктів [7, 235-236]. На час перевезення вантажу в ізотермічних вагонах підтримується відносно постійні температура та вологість повітря, нормальна його циркуляція та вентиляція.

В залежності від роду вантажу всі ізотермічні вагони поділяються на універсальні і спеціалізовані. Універсальні вагони дозволяють

перевозити усі масові швидкопсувні вантажі в теплому, охолодженому чи замороженому стані. Спеціалізовані – призначені для перевезень окремих вантажів (молоко, вино, жива риба).

В даний час випускаються цільнометалеві ізотермічні вагони зі сталевим зовнішнім і дерев'яним внутрішнім обшиванням рефрижераторного типу, які транспортують вантажі автономними вагонами або у складі секцій (5 або 12 вагонів). Але зустрічаються ще також старі вагони з дерев'яними кузовами та внутрішнім обшиванням. Усі ці вагони мають одні двері, льодозагрузний люк з ґратами, металеві льодові кишені з решетуванням, розташовані в торцевих стінках або під стелею [3, 5]. Про приклади викрадання з таких вагонів буде наведено нижче.

Окремим видом перевізних засобів, що призначені для транспортування дрібних партій вантажів без тари, у первинному вигляді чи упакуванні в полегшеній тарі є контейнери [7, 102-103].

Контейнери завантажуються безпосередньо на складі відправника і перевозяться до одержувача без вивантаження. Двері контейнера обладнані замком шпінгалетного типу і пристроєм для опломбування. Опломбування здійснюється тільки після замикання дверей.

Перевозяться контейнери на залізничних платформах, рідше, у піввагонах. Забороняється вантажити контейнери разом з іншими вантажами, а також відправляти піввагони чи платформи з неповним комплектом контейнерів.

Відносно вантажів, то на залізничному транспорті вони перевозяться насипом, наливом, навалом, кількістю місць [1, 183]. Насипні вантажі (жито, пшениця, овес, насіння олійних та бобових культур, зернові відходи та відходи переробки зерна, комбікорми) перевозять без упакування у критих вагонах з дверними загородженнями (щитами) або дверми, що самоущільнюються, а також у спеціалізованих вагонах для зерна (вагони-зерновози) [2, 229; 7, 199]. Сучасні вагони-зерновози типа "Хопер" мають на даху 4 завантажувальні люки, а в нижній частині кузова – 6. Час розвантаження вагона 5-6 хвилин без затрат ручної праці [7, 200]. Можливість викрадання частину вантажу з такого вагону за зовсім обмежений час є дуже спокусливим для злочинців, які практикують з викраданням саме цих вантажів.

Наливні вантажі (нафта, бензин, кислоти, молоко та інше), а також зріджені гази перевозяться у цистернах про які йшла мова вище. Навалювальні вантажі (руда, вугілля, ліс, кокс та інше) транспортуються без кількості місць та упакування. За кількістю місць, без тари,

перевозяться такі штучні вантажі, як верстати, автомобілі, автопричепи, сільськогосподарські машини, трактори та інше [3, 6].

З метою контролю збереженості вантажів після завантаження криті вагони (у тому числі ізотермічні), цистерни і контейнери пломбуються свинцевими пломбами або запорно-пломбувальними пристроями ЗПП (пломба в єдиній конструкції з пристроєм для блокування) залізниці, якщо завантаження здійснено залізницею, або відправника вантажу, коли завантаження здійснювалося ним [7, 61; 8, 203; 9, 8-9]. ЗПП призначений для одночасного запирання і пломбування вагонів і контейнерів, належить до групи охоронних технічних засобів одноразового використання. Накладені на вагони та контейнери ЗПП і пломби за своєю конструкцією мають унеможливлювати зняття їх із вагона (контейнера) без порушення цільності [8, 203]. Справні ЗПП і пломби свідчать про те, що у запломбований вагон доступу не було і вантаж в ньому доставлено в тій кількості, в якій він був на станції, де навішені ЗПП чи пломба.

ЗПП і пломби накладаються [8, 204]:

- на критому вагоні (універсальному) – на накладках дверей з кожного боку по одному ЗПП або одній пломбі;
- на критому вагоні для перевезення легкових автомобілів –по одному (одній) з двох боків вагона на запірних пристроях торцевих дверей;
- на рефрижераторному вагоні заводу “Дессау” і автономному рефрижераторному вагоні – по одному (одній) з кожного боку вагона на дверях, обладнаних натискною плитою і важелем запірного пристрою;
- на рефрижераторному вагоні Брянського машинобудівного заводу – по одному (одній) з кожного боку вагона на дверях, обладнаних нижніми вушками для пломбування;
- на цистерні – по одному (одній) на кришці верхнього завантажувального люка, за винятком випадків, коли особливий порядок пломбування передбачено правилами перевезення окремих видів вантажів;
- на вагоні-хопері для зерна – сім: три на штурвалі і по одному (одній) – на кришці кожного завантажувального люка;
- на контейнери всіх типів – по одному (одній) на рукоятку, розташовану зліва на правій половині дверей.

Якщо вагон у верхній частині дверей обладнано додатковими пристроями для пломбування, ЗПП накладаються лише на основні пристрої для пломбування, а на додаткові встановлюється закрутка;

якщо такий вагон пломбується свинцевими пломбами, то вони накладаються і на додаткові пристрої. ЗПП чи навісною пломбою скріплюється замикаючий пристрій на дверях вагона. Відповідно до діючих вимог перед пломбуванням дверні накладки зміцнюються закрученнями з термічно обробленого дроту. Закрученням повинні бути охоплені дверна накладка і вушко стійки вагона таким чином, щоб його не можна було зняти без інструмента. Коли вантажі перевозяться в критих вагонах об'ємом кузова 106 і 120 кубічних метрів, обладнаних дверною засувкою, дротове закручення не застосовується [4, 61; 10, 184].

Пломбу затискають лещатами для пломбування. Категорично забороняється відправлення зі станцій завантаження вагонів і контейнерів з нечіткими відбитками встановлених знаків на пломбах, а також з неправильно навішаними пломбами [10, 15].

Пломби відправника повинні мати такі знаки: найменування відправника вантажу, станції, залізниці (скорочене), номер лещат для пломбування; пломби залізниці - найменування станцій, залізниці (скорочене), контрольні знаки і номер лещат. Контрольний знак пломби на кожному вагоні має бути різним. ЗПП, накладені на вагони і контейнери, повинні мати наступні данні: товарний знак Укрзалізниці, скорочене найменування залізниці відправлення, товарний знак підприємства-виробника ЗПП, найменування ЗПП (Варта Універсал-М), остання цифра року виготовлення ЗПП, контрольний знак (семизначний) [8, 204-205].

Відкриваючи вагон чи цистерну, посадові особи знімають ЗПП або пломбу, розірвав посередині петлю, обгорнену навколо вушка дверної накладки. Дротове закручення повинно зніматися спеціальними ножицями. Перебивати її зубилом, молотком чи іншими предметами заборонено.

Для оперативних працівників та слідчих поліції, що ведуть боротьбу зі злочинними посяганнями на вантажі, має значення знання структури і системи функціонування процесу перевезення вантажів на залізниці, зокрема, зведень про основні технологічні операції при прийомі і відправленні вантажів, їх документальне оформлення.

Основним документом при впроваджені на залізниці автоматизованої системи контролю вантажоперевезень шляхом розбудови вагоконтрольних пунктів є натурний листок потягу,. що передається у напрямку руху потягу. *Натурний листок потягу (Форма ДУ-1)* складається на станції формування і прямує до станції сортування або станції призначення, і являє собою схему вантажного потягу. В ньому

шляхом відповідних шифрів позначені номери вагонів у порядку розташування у потягу; типи вагонів, вага вантажу в кожному вагоні; найменування залізниць й пункти призначення; наявність пломб; вагони, супроводжувані воєнізованою охороною, провідниками відправника вантажу чи вантажоодержувача [1, 184]. За цими даним слідчий може встановити, де в складі потяга знаходився вагон у передбачуваний момент здійснення викрадання, де розташовані гальмові площадки, стрілки воєнізованої охорони.

1. Вишня О. В., Вишня В. Б. Об'єкти вантажоперевезень і боротьба з викраданням вантажів на залізницях/ Вісник Львівського інституту внутрішніх справ. –2003. –№ 1. –С.182-187.

2. Правила перевезення вантажів навалом і насипом/Довідник вантажовласника. –Дніпропетровськ: Вид-во Придніпровської залізниці, 2002. –С.228-234.

3. Федоров Ю. Д., Соболев Б. П. Осмотр места происшествия при кра- же грузов из подвижного состава. –Ташкент: ВШ МВД СССР, 1973. – 43с.

4. Правила перевезення вантажів у супроводі провідників відправників (одержувачів)/Довідник вантажовласника. – Дніпропетровськ: Вид-во Придніпровської залізниці, 2002. –С.97-101.

5. Правила перевезення вантажів дрібними відправками/Довідник вантажовласника. –Дніпропетровськ: Вид-во Придніпровської залізниці, 2002. –С.249-253.

6. Правила перевезення вантажів у вагонах відкритого типу/Довідник вантажовласника. –Дніпропетровськ: Вид-во Придніпровської залізниці, 2002. –С.208-227.

7. Шрамов А. А., Шубко В. Г. Организация грузовых и пассажирских перевозок и коммерческой работы. -М.: Транспорт, 1987. - 399с.

8. Правила пломбування вагонів і контейнерів/Довідник вантажовласника. –Дніпропетровськ: Вид-во Придніпровської залізниці, 2002.–С.203-205.

9. Должностная инструкция приемосдатчику груза. –М.: Транспорт, 1989.–49с.

10. Статут залізниць України/Довідник вантажовласника. – Дніпропетровськ: Вид-во Придніпровської залізниці, 2002. –С.7-34.

Інтернет і розвиток вільного інформаційного обміну

Гавриш О.С.
викладач кафедри економічної
та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

В кінці XX - початку XXI ст. перехід до постіндустріальної епохи, для якої характерний вільний інформаційний обмін, висунув ряд завдань щодо інтелектуальної власності, і вони вимагають якнайшвидшого рішення. Пов'язано це, перш за все, з протиріччям взаємодії двох систем: інституту інтелектуальної власності, вже сталого протягом кількох десятиліть, і глобальною мережі Інтернет, яка на теперішній день є однією з ключових технологій, найбільшою мірою сприяє процесу переходу світової спільноти до вільного інформаційному обміну [1].

В цілому, основна функція Інтернету — це передача інформації в усіх її видах, всі інші функції цього комунікаційного каналу випливають з неї. Відповідно, особливості економічних відносин, що виникають у процесі використання Інтернету, безпосередньо пов'язані з передачею інформації. У XXI ст., коли інтелект стає вирішальним фактором суспільного розвитку, а плоди людського розуму (так званий "Інтелектуальний капітал") розглядаються як один з основних об'єктів економічного обороту, право інтелектуальної власності є серйозним стимулом для наукової, творчої, дослідницької діяльності і служить одним з двигунів науково-технічного прогресу.

Поява такого засобу передачі інформації, як Інтернет, відкрило нові перспективи для використання результатів людської думки і обміну ідеями, дало можливість користувачеві Мережі, з одного боку, донести свої ідеї творчі напрацювання до інших людей, а з другого - отримати доступ до продуктів творчої діяльності всієї світової спільноти. Щомиті в світі з'являються мільйони нових файлів, які успішно завантажуються в Мережу. Сотні тисяч доларів заробляють інформаційні стрічки на поширенні фактів у ЗМІ, Інтернет-бібліотеки реалізують інформацію в електронних книгах, музикальні портали транслюють і продають композиції, фотобанки торгують ілюстраціями. Світові бренди Microsoft, Yahoo, Apple, Google рахують свої нематеріальні активи мільярдами

доларів - їх високотехнологічні інтелектуальні продукти продаються по всьому світу. Сила-силенна домашніх сторінок користувачів пропонують "творчі" послуги за гроші. Найпоширеніші з них можна без зусиль відшукати в пошуковій системі: "Пишемо сценарії, книги, статті на замовлення, продаємо фотографії, знімаємо відеоролики, створюємо гімни, девізи, назви для компаній, розробляємо дизайн сайтів і т.д. Все це дозволяє однозначно стверджувати, що інтелектуальна власність вийшла в Інтернет.

Створилася парадоксальна ситуація: з одної сторони, є право інтелектуальної власності (право власності є основою ринкової економіки), а з іншого боку, є необхідність широкого поширення інформації.

Протиріччя в системі охорони прав інтелектуальної власності в Інтернеті.

В Інтернеті є ряд об'єктів правової відповідальності: поширення фактів подій та пригод в світі, робота журналістів з видобутку і публікації актуальної інформації зі сфери політики, економіки, соціального розвитку та ін. Згідно із законом, авторське право не поширюється на відомості про факти. Авторським правом охороняється лише форма, в якій ці відомості підносять (за умови, якщо форма носить оригінальний і творчий характер).

Ті, для кого новий текстовий контент - єдиний канал для залучення інвестицій, намагаються максимально обмежити себе від протиправних дій користувачів. Для захисту інформаційних продуктів, що публікується на стрічках новин, найбільші інформагентства попереджають: "Інформація" рейтер (www.reuters.com) є інтелектуальної власністю "Рейтер" і його інформаційних провайдерів. Будь-яке копіювання, передрукування чи наступне поширення інформації, в тому числі вироблене шляхом хешування, кадрування або з використанням аналогічних засобів, суворо забороняється без попередньої письмової згоди з боку "Рейтер". Логотип "Рейтер" і сферичний логотип "Рейтер" є зареєстрованими товарними знаками групи компаній "Рейтер" в усьому світі".

Істотно змінилися взаємодії відносини між володарем інтелектуальної власності та її споживачами. якщо роль посередника між автором і публікою традиційно виконував видавець, то тепер її здійснюють організації, що управляють майнові правами на колективній основі, і організатори колективної творчості — власники мережевих ресурсів. У той же час одне з досягнень сучасного людства - це

проголошення прав на доступ до інформації та знанням. Громадські інтереси вимагають перегляду традиційної авторської монополії, і в першу чергу на наукові твори. Обмеження доступу до інформації суперечить також нормам законодавства, зобов'язаннями перед міжнародним співтовариством сприяти подоланню інформаційного розриву і забезпечення рівного доступу до інформації.

З правової точки зору, феномен Інтернету укладений в одну просту річ: даний універсальний майданчик зовсім не захищає правовласників від крадіжки безкоштовного, на перший погляд, контенту (змісту). Так, залишаються економічно і юридично беззахисними перед беззаконням власники домашніх сторінок і комерційних сайтів, фотографи, журналісти, програмісти, музиканти, поети, письменники і інші користувачі, що публікують свої авторські роботи.

У Західній Європі та США законодавство в цій сфері більш розвинене, ніж у нас (досить згадати хоча б Digital Millenium Copyright Act в США). Але злагоджено працюючої законодавчої системи, наприклад, такою, яка є щодо товарних знаків, патентів та інших "класичних" об'єктів інтелектуальної власності, за кордоном також немає. Поки що, це загальна для всього світу проблема.

Зрозуміло, що відсутність норм, які б враховували особливості Інтернету, і його слабка контрольованість дозволяють безкоштовно використовувати інтернет-ресурси, що знаходяться в вільному доступі, і в багатьох випадках безкарно ухилятися від економічної та правової відповідальності.

Має місце безпрецедентне протиріччя і складність регулювання відносин власності в Інтернеті. Однак необхідно встановити баланс між інтересами творців інтелектуальних результатів і суспільства.

Концептуальна основа прав власності в Мережі.

Інтелектуальна власність в сучасному світі є найважливішим економічним ресурсом. У період трансформації сучасного суспільства і його переходу в постіндустріальну епоху пріоритетне значення починають купувати не природні ресурси і навіть не власне високотехнологічне виробництво, а інтелектуальний капітал і, відповідно, права на володіння і розпорядження тим чи іншим інформаційним ресурсом, значна частина якого зосереджена в мережі Інтернет. Саме тому інтелектуальна власність в Інтернеті повинна

перебувати під захистом авторського права і розглядатися як нематеріальний актив її власника (автора).[2]

Йде становлення інституту інтелектуальної власності в Мережі як комплексу економічних, соціальних, правових і культурних феноменів. Феномен інтелектуальної власності в мережі Інтернет - це комплекс відносин, який повинен будуватися на основі системи договірних зобов'язань.

Економічна складова відносин суб'єктів і об'єктів простору Інтернету полягає в праві володіти і розпоряджатися тим інтелектуальним капіталом, яким є інформаційні ресурси, розміщені в Мережі. Цей вид власності потребує чіткого визначення та нормативному оформленні.

Об'єкти авторсько-правової охорони в мережі Інтернет як об'єкти комерційного інтересу диференціюються залежно від того, на якому етапі дані об'єкти пов'язані з використанням Інтернету - на етапі створення або на етапі поширення тієї чи іншої інформації.

Інтелектуальна власність в Інтернеті стає основою великого сегмента "електронної комерції" - сегмента "творчого" бізнесу, що обумовлює необхідність створення нових форм економічних відносин між користувачами Мережі та правовласниками тих чи інших інтернет-ресурсів.

Таким чином, в Інтернеті формуються економічні взаємини нового типу в області інтелектуальної власності, отже, потрібні практичні пропозиції щодо захисту авторських прав на матеріали, розміщені в мережі Інтернет, необхідна розробка способів запобігання несанкціонованому використанню інтелектуальної власності в Інтернеті.

1. Еволюція індустріального суспільства у другій половині XIX — на початку XX ст. [Електронний ресурс]. – Режим доступу: http://pidruchniki.com/1142052042301/politekonomiya/evolyutsiya_industrialnogo_suspilstva_drugiy_polovini_xix_pochatku

2. [Електронний ресурс]. – Режим доступу: http://intellect21.cdu.edu.ua/wp-content/uploads/2011/12/Захист прав інтелектуальної власності в Україні.pdf

Хмарні технології в науковій та педагогічній діяльності.

Каблуков А.О.
доцент, к.т.н., доцент Запорізького державного медичного університету
Страхова О.П.
викладач Запорізького державного медичного університету

Актуальність застосування нових інформаційних технологій продиктована, перш за все, педагогічними потребами в підвищенні ефективності навчання та наукових досліджень. Сьогодні без використання сучасних інформаційних технологій не може ефективно працювати жодний освітній заклад. При цьому зміст і розвиток власної IT-інфраструктури при кожному освітньому центрі обходиться дуже дорого. З кожним роком рівень даних витрат все більше і більше зростає. Вузи витрачають великі суми на комп'ютерну техніку, телекомунікаційне обладнання та програмне забезпечення. Крім вищевказаних витрат значні фінансові вкладення потрібні і для підтримки високого рівня професіоналізму викладачів і фахівців з IT технологій.

"Хмарні обчислення" (Cloud computing) є хорошою альтернативою класичній моделі навчання. Головним її плюсом можна вважати істотну економію коштів освітньої установи, в якому вони використовуються. Адже в цьому випадку комп'ютерна інфраструктура і інформаційні сервіси надаються як послуги "хмарного" провайдера. Документи, електронні листи, програми та інші дані учасників освітнього процесу зберігаються на віддалених серверах провайдера. При цьому для установи немає необхідності утримувати власну дорогу IT-інфраструктуру і переплачувати за обчислювальні ресурси, які в більшості випадків не задіяні на повну потужність. Єдине, чим необхідно забезпечити викладачів та учнів з використанням хмарних технологій, - це доступ до мережі Інтернет.

В даний час існує безліч постачальників хмарних рішень. Такі великі компанії як Amazon, Google, Microsoft і т.д. пропонують значні знижки освітнім установам, за рахунок чого вони отримують доступ до хмарних сервісів практично безкоштовно.

Надійність, доступність і легка масштабованість є ключовими перевагами хмарних технологій. Виникає питання чи може в найближчому майбутньому велика частина освітніх послуг надаватиметься на базі хмарних обчислень?

Для відповіді на це питання треба розглянути і оцінити всі переваги і недоліки використання хмарних обчислень в сфері освіти, а також надати практичні рекомендації щодо застосування хмарних обчислень в процесі навчання в вузах.

Використання хмарних обчислень в галузі освіти має багато позитивних сторін. Особливо значущими з них можна вважати наступні переваги:

• Економічні переваги. Використання хмарних технологій не вимагає капітальних витрат на створення і обслуговування власних центрів обробки даних, закупівлю серверного та мережевого обладнання , а також дорогого програмного забезпечення для створення власної IT-інфраструктури.

• Масштабованість (еластичність). Завдяки еластичності хмарних сервісів, у освітнього закладу є можливість поступово нарощувати обсяг послуг, що використовуються в навчанні.

• Доступність. Хмарні сервіси доступні протягом всього часу. Це зручно для викладачів і учнів, оскільки вони можуть реалізувати можливості з навчання практично в будь-який час і не залежати від локальних інформаційно-освітніх ресурсів установи.

• Задоволення потреб кінцевих користувачів Користувачам зручно, коли дані доступні з будь-якого місця, де є Інтернет і з будь-якого пристрою, будь то персональний комп'ютер, смартфон або планшет. Користувачам не потрібно піклуватися про резервних копіях, дані безпечно зберігаються в "хмарі". Стандартний офісний пакет поставляється навчальним закладам.

• Концентрація на ключових завданнях. У будь-якій сфері освіти головне завдання освітніх установ - концентрація зусиль на освіті та дослідженнях. При використанні хмарних технологій скорочуються витрати на розгортання і підтримку використовуваних в роботі додатків, задіяних в освітньому процесі.

Але хмарні технології мають і мінуси:

• Відсутність очного спілкування між учнями та викладачем. Тобто всі моменти, пов'язані з індивідуальним підходом і вихованням, виключаються.

• Необхідність постійного доступу до джерел інформації. Потрібна хороша технічна оснащеність, але не всі бажаючі вчитися мають комп'ютер і вихід в Інтернет.

• Студенти відчувають недолік практичних занять.

• Відсутній постійний контроль за студентом, який є потужним спонукальним стимулом в навчанні.

• Навчальні програми і курси можуть бути недостатньо добре розроблені через те, що кваліфікованих фахівців, здатних створювати подібні навчальні посібники, на сьогоднішній день не так багато.

Аналіз вищевикладеного дозволяє зробити висновок про те, що використання хмарних інформаційних технологій в педагогічній діяльності навчальних закладів підвисить ефективність їх роботи в науковій та педагогічній галузях.

Висновок. Використання хмарних інформаційних технологій в педагогічній діяльності в навчальних закладах МВС, є однією з перспективних завдань для вузів міністерства внутрішніх справ України.

1. Склейтер Н. Облачные вычисления в образовании: Аналитическая записка/ Пер. с англ. Институт ЮНЕСКО по информационным технологиям в образовании.-Москва, 2010. - 12 с.

2. Алексанян Г. А. Сервисы Google в организации самостоятельной деятельности студентов СПО [Текст] / Г. А. Алексанян // Молодой ученый. — 2012. — №9. — С. 263-266.

3. Диск Google : страница доступа к облачному сервису хранения данных. URL: https://drive. google.com/.

4. Риз Дж. Облачные вычисления : пер. с англ. СПб. : БХВ-Петербург, 2011.

5. Шевчук М. В., Шевченко В. Г. Возможности технологии облачных вычислений при организации учебных виртуальных рабочих мест // Информатика и образование. 2012. № 10. С. 73–75.

Практика електронного судового провадження в кримінальному процесі Англії

Каланча І.Г.
аспірантка кафедри кримінального права, процесу та криміналістики ПВНЗ «Європейський університет», прокурор Київської місцевої прокуратури №2, м. Київ

Протягом останніх років провідні країни світу активно впроваджують електронне (віртуальне) судочинство, засноване на всебічному використанні сучасних інформаційних технологій в процесі відправлення правосуддя.

В Англії та Уельсі Королівською прокурорською службою використовується система управління провадженнями «Compass», що раціоналізує роботу прокуратури, допомагаючи їм провести заздалегідь визначений набір завдань. «Compass» виконує всі дії з інформацією та документами, пов'язаними з реєстрацією провадження (кейс-файлу» («case-file»)), його розподілом, результатом слухання, та остаточним доопрацюванням. «Compass» також надає співробітникам стандартні попередньо відформатовані шаблони документів. Сформована поліцією справа передається прокурору у вигляді кейс-файлу. Після початкового розгляду кейс-файлу, при встановленні прокурором підстав для розгляду справи, в суді магістрату проходить перше слухання. Якщо обвинувачений визнає себе винним, справа завершується в «Compass». Якщо ні, справа призупиняється до подальшого розгляду, а «Compass» автоматично генерує запит до поліції на повний файл. Коли повний кейс-файл отримано, «Compass» генерує для прокурора нове завдання, щоб дозволити повний огляд файлу [2, с.35].

Серед описаної електронної процесуальної процедури необхідно звернути увагу на: зберігання провадження у форматі кейс-файлу («case-file»), що утворює єдину «точку» генерування, обробки та передання інформації у кримінальному проваджені а також встановлення режиму доступу до електронних відомостей відповідно до процесуальних повноважень: електронні завдання («e-tasks»), які є ефективним шляхом усунення паперового документообігу, що актуально для кримінального судочинства України. Стандартні попередньо відформатовані шаблони документів також розглядаються як складова електронного документообігу, однак уже як підсистема формування електронних

документів замість паперових. Також практика судів Англії щодо використання лише електронного файлу кримінального провадження для першого судового слухання (актуальна паралель з підготовим судовим засіданням в кримінальному процесі України), в перспективі може бути застосована при вдосконаленні електронного кримінального судочинства України як така, що сприяє дематеріалізації процесуальної процедури.

Важливим елементом електронних кримінальних процесуальних процедур є система обміну даними кримінального правосуддя - Criminal Justice System Exchange (далі - CJS Exchange). Це захищений центральний комп'ютер, який скеровує захищені матеріали проваджень та інформацію про окремих осіб між суб'єктами кримінального правосуддя. Він працює *як механізм маршрутизації*, який доставляє інформацію туди й назад з судів чи інших установ, що беруть участь в кримінальному переслідуванні. Поліція відправляє свій первісний матеріал до CJS Exchange, який направить його до прокуратури (через «Compass») та суду (через «Libra» - система управління провадженнями суду). У свою чергу, суди направляють результати судових справ назад на CJS Exchange, що скеровує їх в поліцію. Починаючи 2007 року CJS Exchange поступово розширюється, поєднуючи електронні системи поліції, прокуратури, судів, пенітенціарної системи, а також надає інформацію агентствам, компаніям і представникам громадськості, з якими вони взаємодіють у здійсненні кримінального судочинства [2, с.36-38]. Таким чином, CJS Exchange забезпечує інтероперабельність відокремлених електронних систем органів кримінальної юстиції Англії. В Україні на сьогодні аналогічна ситуація в частині електронних кримінальних процесуальних правореалізаційних засобів, що обумовлює необхідність впровадження аналогічного механізму маршрутизації.

В судах Англії передбачається створення «цифрових залів судових засідань». Застарілу «паперову» систему замінять цифрові екрани, на яких захист і обвинувачення зможуть представляти докази, у тому числі з камер відеоспостереження, інші відео і аудіо докази. Часто вчинювані незначні правопорушення, розглядатимуться не в залах судових засідань традиційних магістратів, що звільнить останні для більш серйозних проваджень. Системи на кшталт «Track My Crime», яка дозволяє потерпілим перевірити хід їх справи он-лайн, планується розширити, щоб створити прозору систему кримінального правосуддя [1, с. 1]. Запровадження аналогічної системи відстеження руху провадження актуальне для України.

Очевидним компонентом в електронному суді є електронний варіант подання доказів. Часто, свідок зможе анотувати частину електронних доказів, що можуть бути збережені за допомогою технологічного обладнання і є складовою частиною доказової бази однієї зі сторін. Це дозволяє сторонам подавати певні документи в електронному вигляді, одержувати електронні повідомлення про терміни, забезпечуючи доступ до поточних тематичних реєстрів, а також дозволяє дізнаватись про порядок порушення справи чи винесення рішень. Верховний суд Англії та Уельсу також активно впроваджує механізми процедури електронного подання судових справ [3, с.3]. Електронний варіант подання доказів є важливою складової електронного кримінального провадження та потребує розробки в Україні з використанням досвіду Англії в даному питанні.

1. Criminal justice system to go paperless by 2016 with «digital courts» / Information Daily Staff Writer. URL: http://www.theinformationdaily.com/2013/06/28/criminal-justice-system-to-go-paperless-by-2016-with-digital-courts

2. Fabri Marco. Some European and Australian e-Justice services. 2012. Project: «Rethinking Processual Law: Toward CyberJustice». 70 p.

3. Mark Dillon, David Beresford. Electronic Courts And The Challenges In Managing Evidence: A View From Inside The International Criminal Court // International Journal For Court Administration. June 2014. – P. 1-8.

Витік інформації в каналах мобільного зв'язку

Карпуков Л.М.
доктор технічних наук, професор, завідувач кафедри Запорізького національного технічного університету
Лізунов С.І.
кандидат технічних наук, доцент, професор Запорізького національного технічного університету

У сучасних умовах електронне перехоплення розмов, що ведуться по стільниковому телефону, стало широко розповсюдженим явищем. Так, наприклад, у Канаді, за статистичним даними, від 60% до 80% радіообміну, що ведеться за допомогою стільникових телефонів,

випадково або навмисно, прослуховуються сторонніми особами. Електронне перехоплення стільникового зв'язку не тільки легко здійснити, воно, до того ж, не вимагає великих витрат на апаратуру, і його майже неможливо виявити. Мобільні стільникові телефони, особливо аналогові, є самими уразливими апаратами з боку захисту переданої інформації.

Принцип передачі інформації такими пристроями заснований на випромінюванні в ефір радіосигналу, тому будь-яка людина, настроївши відповідний радіоприймальний пристрій на ту ж частоту, може почути кожне ваше слово. Для цього навіть не потрібно мати особливо складну апаратуру. Розмова, що ведеться зі стільникового телефону, може бути прослухана за допомогою програмувальних сканерів зі смугою прийому 30 МГц, здатних здійснювати пошук у діапазоні 860-890 МГц. Для цієї ж мети можна використовувати й звичайні сканери після їхньої невеликої модифікації. Перехопити розмову можна навіть шляхом повільного перенастроювання УКХ-тюнера в телевізорах старих моделей у верхній смузі телевізійних каналів (від 67 до 69), а іноді й за допомогою звичайного радіотюнера. Нарешті, таке перехоплення можна здійснити за допомогою персонального комп'ютера.

Чим технічно складніше мобільний телефон, тим більше шпигунських функцій можна задіяти: візуальне панорамне фотографування; відеозйомка й акустичний контроль у радіусі до 10 метрів; прослуховування всіх вхідних і вихідних телефонних розмов, смс й електронної пошти; визначення місце розташування об'єкта з точністю до кілька метрів; дистанційне включення мікрофона з відстані в десятки тисяч кілометрів; дистанційне прослуховування розмов через мікрофон телефону, навіть якщо основна батарея вийнята (для сучасних смарт телефонів).

З розвитком технології мобільного зв'язку й появою смарт телефонів і комунікаторів, що поєднують функції телефону й комп'ютера, реалізація спеціальних функцій лягла й на операційні системи, які використовуються в мобільних технологіях. На жаль, такий значний перерозподіл спеціальних функцій з апаратної частини на програмну привів до того, що досвідчені програмісти стали її влучно використовувати й створили цілий ряд так званих «spy» (шпигунських) телефонів на базі серійних мобільних телефонів.

При такому відкритому полі діяльності стало можливим створення недорогих хибних базових станцій (таких як «пастки» IMSI), які займаються активацією мікрофона на мобільному телефоні за

допомогою помилкових дзвінків або смс. Наприклад, в інформації про нову послугу хибного оператора, зовсім непримітної на перший погляд, може міститися код активації мікрофона мобільного телефону для наступного прослуховування розмови й приміщення. Визначити, що включився мікрофон практично дуже складно й зловмисник спокійно може чути й записувати не тільки розмови по телефону, але й розмови в приміщенні, де перебуває мобільний телефон.

Спеціальний пристрій, що називається IMSI-catcher (тобто ловець IMSI, унікального ідентифікатора International Mobile Subscriber Identity, прописаного в SIM-карті), прикидається для мобільних терміналів, що знаходяться поблизу, справжньою базовою станцією стільникової телефонної мережі. Ця діра в безпеці GSM була внесена в архітектуру системи цілком навмисно на вимогу спецслужб - для організації перехоплення й моніторингу без відома компаній-операторів мобільного зв'язку. Тому, як тільки мобільний телефон приймає IMSI-catcher як свою базову станцію, цей апарат-ретранслятор може деактивувати включену абонентом функцію шифрування й працювати зі звичайним відкритим сигналом, передаючи його далі справжньої базової станції. Як свідчать фахівці, у цей час на ринку немає жодного GSM-телефону, який би активно попереджав власника про примусово відключену функцію шифрування. Зате в продажі вистачає нині апаратів, у яких функція шифрування в явному вигляді взагалі не реалізована.

Крім цього, з’явився новий продукт від тайської компанії Vervata - програма FlexiSPY. Як стверджує виробник, це «перша у світі комерційна шпигунська програма, створена спеціально для стільникових телефонів». Тепер з'явилася можливість 24 години на добу й сім днів у тиждень контролювати всі аспекти використання даного стільникового телефону, причому з будь-якого комп'ютера, підключеного до Інтернету. Телефон сам буде регулярно зв'язуватися із сервером компанії й передавати на нього всю інформацію. На дислокацію телефону, що прослуховується, по регіонах і країнам світу обмежень немає: сервіс FlexiSPY працює скрізь. Активувавши послугу, можна прослуховувати дзвінки, читати всі вхідні й вихідні SMS, переглядати call hystory з переліком повної інформації (дата, час, тривалість дзвінка, номер абонента), фіксувати виходи в Інтернет через GPRS, нарешті - дистанційно активувати мікрофон цього телефону, навіть коли його не використовують.

Отже, захист інформації в каналах мобільного зв’язку стає актуальною проблемою, що потребує негайного вирішення як з технічного боку, так і в правовому полі.

Оцінка фінансової безпеки підприємства

Кокарєв І.В.
доцент ДДУВС, канд. екон. наук, доцент
Тютченко С.М.
здобувач ДДУВС

Забезпечення стабільності результатів діяльності підприємства, досягнення цілей, що відповідають інтересам власників та суспільства в цілому, неможливі без розробки та проведення відповідної стратегії суб'єкта господарювання, яка визначається наявністю надійної системи його фінансової безпеки. Важливим елементом управління фінансовою безпекою підприємства є об'єктивне і своєчасне визначення її рівня, що дозволить своєчасно виявити проблеми у фінансовому стані та виправити їх без загрози втрати фінансової стійкості та платоспроможності у майбутньому.

Рівень фінансової безпеки підприємства визначається наступними групами показників:

– оцінка рівня фінансової безпеки як складової економічної безпеки підприємства;

– оцінка рівня фінансової безпеки на основі визначення фінансового стану підприємства;

– оцінка рівня фінансової безпеки на основі інтегральних показників.

До першої групи відносяться наступні функціональні складові: бюджетна безпека, грошово-кредитна, зовнішньоекономічна, банківська, страхова, фондова, інвестиційна. Для кожного конкретного підприємства використовуються лише ті елементи фінансової безпеки, які відповідають його виду економічної діяльності.

Ряд дослідників пропонують оцінювати фінансову безпеку підприємства на основі визначення та оцінки загального стану фінансової діяльності підприємства, а саме: горизонтальний, вертикальний, порівняльний, інтегральний аналізи та аналіз фінансових коефіцієнтів. Комплексно оцінити фінансовий стан підприємства та стан його фінансової безпеки можливо, використовуючи наступні групи показників: майнового стану, ліквідності та платоспроможності,

дебіторської та кредиторської заборгованостей, ділової активності, рентабельності підприємства та фінансової стійкості [1, 2].

Із всієї множини фінансових коефіцієнтів експертами було виділено найбільш значимі, які б не дублювали одне одного і найбільш повно характеризували стан фінансової безпеки підприємства [3]. Кожен з них має нормативне значення.

По-перше, показники майнового стану: коефіцієнт зносу основних засобів (⩽ 0,5).

По-друге, показники ліквідності та платоспроможності: коефіцієнт абсолютної ліквідності (0,2 – 0,5); коефіцієнт загальної ліквідності (⩾1).

По-третє, показники дебіторської та кредиторської заборгованостей: залежність від дебіторської заборгованості (⩽0,4); залежність від кредиторської заборгованості (⩽0,4).

По-четверте, показники ділової активності: коефіцієнт оборотності власного капіталу; коефіцієнт оборотності активів.

По-п’яте, показники фінансової стійкості: коефіцієнт незалежності (автономії) (⩾0,5); коефіцієнт самофінансування (>1); коефіцієнт фінансової стійкості (⩾0,75).

По-шосте, показники прибутковості (рентабельності): рентабельність загальних активів (>0,05); рентабельність необоротних активів (>0,1); рентабельність оборотних активів (>0,1); рентабельність власного капіталу (>0,15); рентабельність інвестицій (>0,1).

Отже, проаналізувавши фінансову звітність підприємств та розрахувавши коефіцієнти, можна сформувати інтегральний показник оцінки стану фінансової безпеки підприємства. Він формується із суми бальних оцінок коефіцієнтів за кожною групою показників. Розрахованим значенням показників оцінки фінансової безпеки підприємства присвоюється відповідна бальна оцінка рівня показника від одного до п’яти. Виділяють п’ять станів фінансової безпеки підприємства: оптимальний, високий, середній, низький та кризовий.

Здійснені розрахунки дають змогу оцінювати стан фінансової безпеки підприємства загалом та в розрізі окремих груп.

Проте оцінка фінансової безпеки підприємства не може зводитись до простого аналізу фінансового стану підприємств. Про високий рівень фінансової безпеки можуть свідчити такі критерії як: технологічна незалежність підприємства, висока ефективність менеджменту підприємства, ефективність його організаційної структури, високий рівень кваліфікації персоналу підприємства та його інтелектуального

потенціалу, якісна правова захищеність усіх аспектів діяльності підприємства, забезпечення захисту інформаційного середовища підприємства, комерційної таємниці та досягнення високого рівня інформаційного забезпечення діяльності усіх його служб та підрозділів, забезпечення безпеки персоналу підприємства, його капіталу, майна та комерційних інтересів.

Отже, дуже важливим при оцінці фінансової безпеки підприємства є поєднання традиційних та нетрадиційних методів. Нетрадиційні методи базуються на оцінці рівня розвитку та управління, оцінці ризиків та ринкової вартості підприємства.

Таким чином, діагностика фінансової безпеки підприємства дозволить з мінімальними втратами часу та максимальною ефективністю приймати управлінські рішення. Адже, за сучасних економічних умов оцінка рівня фінансової безпеки є невід'ємною частиною управління підприємством. Вона дає можливість керівництву та менеджерам підприємств ефективніше вирішувати проблеми забезпечення фінансової безпеки, обирати ефективні шляхи мінімізації фінансових втрат.

1. Бланк И.А. Управление финансовой безопасностью предприятия / И.А. Бланк. – К. : Ельга, Ника-Центр, 2014. – 784 с.

2. Кириченко О.А. Вдосконалення управління фінансовою безпекою підприємств в умовах фінансової кризи / О.А. Кириченко, І.В. Кудря // Інвестиції: практика та досвід. – 2009. – № 10. – С. 22-26.

3. Орлова В. В. Моделі оцінки рівня фінансової безпеки підприємства / В. В. Орлова // Моделювання регіональної економіки. Збірник наукових праць. – Івано-Франківськ : Плай, 2016. – №1(7). – С. 89-96.

Деякі організаційно-психологічні напрямки забезпечення кібербезпеки у державі.

Косиченко О.О.
доцент кафедри економічної та інформаційної безпеки
Дніпропетровського державного університету
внутрішніх справ, кандидат технічних наук.

Останнім часом ми часто зустрічаємося із подвійним відношенням до питання інформаційної безпеки. З одного боку, хвилі надмірної паніки, відчутні після великих кібератак, з іншого боку - надмірно легковажне відношення. Дані різних опитувань, проведених в останні роки, як правило, указують на низьку культуру безпеки в організаціях. Мова при цьому йде тільки про технічні заходи захисту інформації, як про малу увагу до освіти. І це незважаючи на те, що ці ж дослідження акцентують увагу на тому, що деякі із самих вражаючих по масштабом кібератак відбулися саме в результаті недостатньої інформованості персоналу.

Так що те, наскільки серйозно та або інша компанія ставиться до корпоративної культури кібербезпеки, сильно відрізняється: співробітники однієї організації можуть проходити безліч тренінгів і одержувати всілякі вказівки, у той час як співробітники іншої фірми можуть знати, що в принципі правила кібербезпеки важливі, але вирішувати реальні проблеми вони будуть самостійно. Для керівників сьогодні важливе розуміння і основ, і питань, пов'язаних з конкретним використанням технологій. Але отут є складність: поняття "основи" постійно розширюється. Представникам бізнесу доводиться адаптуватися до постійно зростаючого списку технологій. Потрібно одночасно думати, наприклад, про захист девайсів від неавторизованого застосування та від атак шкідливих програм, про збереження систем у в робочому стані, про захист конфіденційної інформації, про захист персональних даних, про безпечне використання мереж, про безперебійне створення резервних копій даних на випадок втрати, крадіжки або поломки обладнання. Це аж ніяк не вичерпний список нових кіберзагроз. Причому кожна з погроз небезпечна одночасно для обладнань самого різного типу. Наприклад, ще кілька років назад віруси були реальною проблемою тільки для десктопів і ноутбуків. Зараз нам доводиться побоюватися їхнього проникнення в смартфони, планшети

та в інші гаджети. Багато із цих проблем стосуються не тільки корпоративних систем, але рядових користувачів. Багато з перелічених погроз спрямовані безпосередньо на приватних користувачів: фішинг, спрямований на одержання доступу до конфіденційної інформації; шкідливі програми, які цілком успішно використовують системи кінцевих користувачів як засіб відправлення спама або запуску атак проти інших мішеней, і так далі. Знання тих самих основ може допомогти забезпечити захист людини – і як індивідуального користувача, і як співробітника на робочому місці. Так що, поліпшуючи освіту у сфері безпеки та підвищуючи поінформованість про проблеми, ми вирішуємо кілька проблем. В інтересах кожної компанії мати персонал, який би сам міг забезпечувати свою безпеку. Тоді працівники будуть краще справлятися із захистом власних систем і даних.

Ключовий спосіб навчання персоналу – через зіткнення з погрозами, які можуть виникнути з найбільшою ймовірністю. Проте, навчити співробітників точно розпізнавати погрози різної природи неможливо. Інший підхід – переконатися, що співробітники знають, які об'єкти особливо коштовні та важливі, і усвідомлюють необхідність їх захисту. У деяких організаціях мова може йти про документи, системи, дані — для них використовують інформаційні класифікації начебто "конфіденційно" або "секретно". Маркування вказують на необхідність працювати з такою інформацією особливим способом. Коли співробітники досить інформовані про цінність даних, з якими мають справу, вони куди частіше замислюються про свої дії, перш ніж ділитися доступом до даних.

Важко назвати основні погрози для компаній, не перераховуючи в остаточному підсумку той самий список потенційних проблем, з якого ми почали. Опитування звичайно називають найпоширенішими погрозами ті, що пов'язані зі шкідливими програмами, фішінговими повідомленнями, у цілому із проблемами, що випливають із необхідності для бізнесу працювати з зростаючим обсягом даних. Однак найбільш шкідливими та впливовими стають разові погрози, наприклад погрози з боку самого персоналу. Також важливо не випускати з уваги погрози, що виникають у результаті випадкових подій – збоїв систем, порушень у роботі обладнання. Адже збиток у таких випадках може бути настільки ж масштабним, як і у випадку цілеспрямованих атак зловмисників.

Кіберзагрози прийнято ділити на внутрішні й зовнішні. Найчастіше увага керівників компаній зосереджена на зовнішніх погрозах, – наприклад, на протидії атакам хакерів, на захисті від

шкідливих програм (такі атаки широко висвітлюються в ЗМІ). Проте навмисні погрози зсередини компанії – шахрайство, неавторизований доступ, крадіжка даних – не менш небезпечні. Вони можуть бути замасковані. До того ж деякі внутрішні погрози виникають у результаті ненавмисних дій або недостатньої поінформованості співробітників. Деяких з подібних ризиків можна уникнути саме за рахунок більш якісного навчання персоналу. Інша група ризиків, пов'язаних із внутрішніми погрозами, вимагає не стільки освіти співробітників, скільки налагоджених систем моніторингу, чітких алгоритмів виявлення інцидентів кібербезпеки.

Існує величезна необхідність навчання звичайних користувачів, інакше ми просто виявимося в ситуації повної уразливості всіх громадян. Якщо приватні користувачі не будуть знати, як себе захистити, вони ненавмисно можуть збільшити ситуацію й для себе, і для інших, у тому числі для бізнесу. Наприклад, якщо моє обладнання не захищене й заражається шкідливим програмним забезпеченням, а потім починає атакувати інші системи як частини "ботнету", це означає, що проблема вже не винятково моя. Недостатня безпека мого обладнання фактично впливає на інших.

Є базові правила, які повинні бути відомі всім. Їх можна розглядати як мінімально необхідний рівень знань у сфері кіберінформаційної грамотності. Молоді користувачі можуть одержати основні знання в рамках традиційної системи освіти. Для користувачів, які вже пройшли всі стадії освіти, методики навчання можуть варіюватися. Наприклад, у Великобританії працює портал *Get Safe Online (www.getsafeonline.org)*, він дає ради як приватним користувачам, так і представникам бізнесу. Сайтів такого рівня якості в Україні практично немає.

Держава повинна турбуватися про інформаційну безпеку, тому що проблеми в цій сфері впливають на схильність громадян злочинам різного виду. Держава повинна взяти на себе контролюючу роль: якщо кожний громадянин захищений, його поведінка не шкодить усім іншим. Гарна аналогія - контроль держави за безпекою на дорозі. Наявність правильних вказівок захищає не тільки окремого водія, але пішоходів та водіїв.

Можливі методики проведення аналізу інформації о злочинних проявах, отриманої з відкритих контентів мережі інтернет

Краснобрижий І.В.
к.ю.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

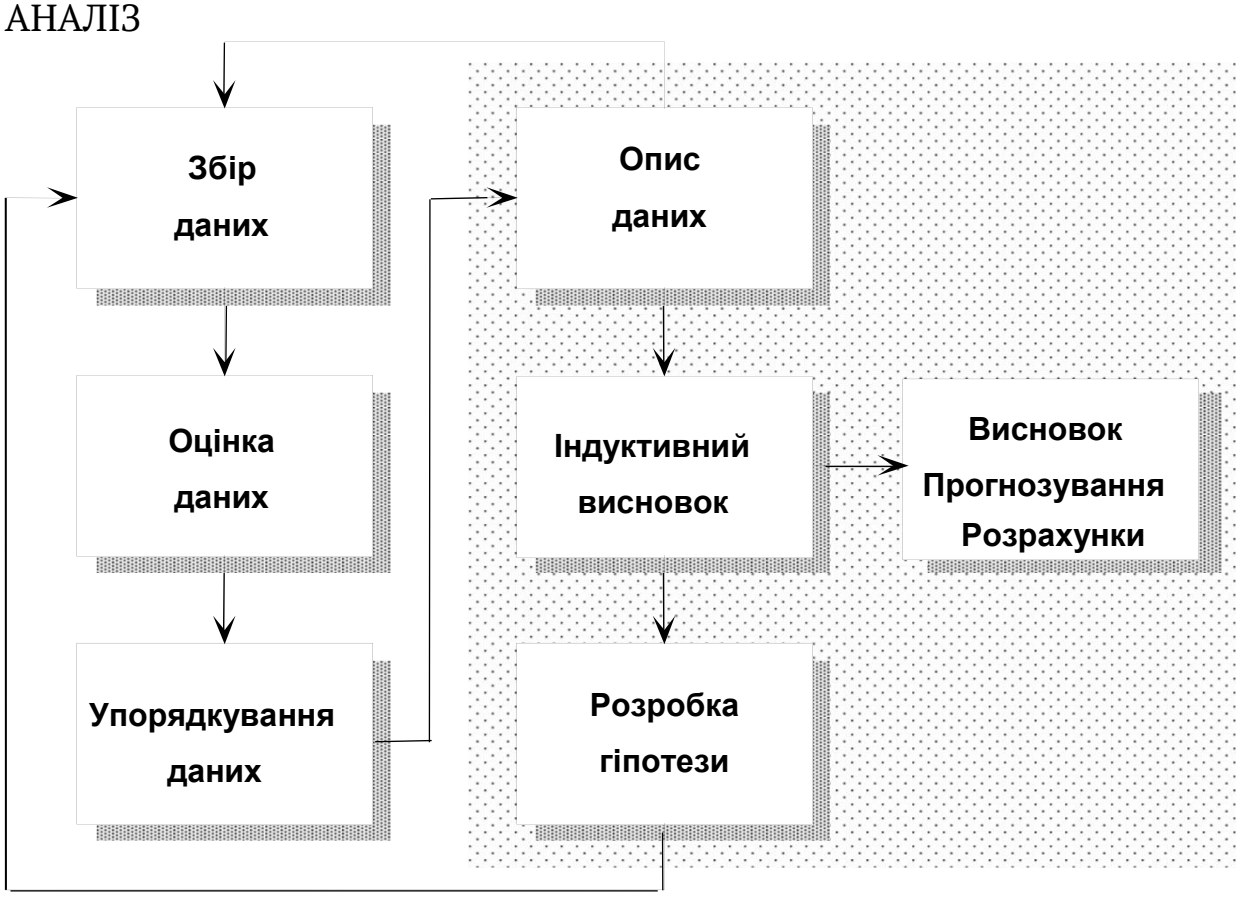
На теперішній час, у зв'язку з переведенням значної кількості інформаційних масивів у цифрову форму та надання доступу до більшості цієї інформації через глобальну інформаційну мережу (Інтернет), стає можливим отримати цілі пласти логічно зв'язаної інформації, що цікавить різноманітні фізичні чи юридичні особи. У даної статті ми розглянемо роботу з інформаційними ресурсами, що виконують державні правоохоронні органи з метою попередження та розкриття різноманітних злочинних проявів.

Як вже вказувалось, інформацію в мережі Інтернет на юридичних та фізичних осіб можливо отримати в доволі великих обсягах. Отримання цієї інформації здійснюється за допомогою різноманітних методик [1, с. 111-115] здійснення пошуку, а також засобів [1, с. 110, 111, 114-122], що дозволяє здійснювати пошук в напівавтоматичному, чи навіть в автоматичному режимі. Як приклад програмних засобів для автоматизації пошуку інформації можемо навести такий програмний комплекс як IBM i2 analyst's notebook [2] з підключеними програмними модулями SocialGrabber4i2 2.0 [3].

Основним призначенням SocialGrabber4i2 2.0 є отримання даних із соціальних мереж для аналізу явних і прихованих зв'язків між різними об'єктами дослідження, що дозволяє визначити приховані спільноти, організовані злочинні групи і виявити ключові об'єкти і лідерів груп. Програмний модуль IBM i2 iBase [4] дозволяє вилучати інформацію з різних баз даних, а також імпортувати ці бази даних гуртом. Інші джерела, які можливо використовувати для пошуку більш-менш достовірної інформації, у цій статті ми приводити не будемо бо вони гідні окремого розгляду.

Але отримання даних це лише початковий етап роботи з інформацією. Наступний етап називається аналіз. Аналітичний етап процесу починається з отримання відповідних даних і їх організації у формі, що дозволяє розуміти їх значення. Даний етап, опис даних,

сприяє виявленню відсутньої інформації і допомагає направляти подальші заходи по збору даних на отримання відсутніх даних. Їм також утворюється основа для вживання індуктивного висновку з метою розробки однієї або більш гіпотез про ключові аспекти злочинної діяльності. Гіпотези апробовуються повторенням збору, оцінки, впорядковування, опису даних і індуктивного циклу обґрунтовування. Кожного разу при повторенні циклу, він все сильніше націлюється на конкретні види інформації, необхідної для підтвердження або спростування гіпотези, що веде до формування висновку з високим рівнем надійності (мал.№1).



мал. №1

Кінцева мета справжнього процесу полягає в забезпеченні даного висновку – висновку, прогнозування або розрахунків, на основі яких можна діяти з упевненістю [5, с. 662, 663].

В якості висновку слід зауважити, що нині проблема не у відсутності потрібних інформаційних даних, а у здатності інформаційних підрозділів навіть фізично обробляти інформаційні потоки, а також знаходити необхідну інформацію в базах даних, тому використовуючи спеціальне програмне забезпечення для отримання та першочергової аналітичної обробки отриманих даних правоохоронні органи набагато покращать ефективність своєї діяльності. Ще я вважаю

за необхідне інтенсифікувати підготовку майбутніх поліцейських та провести додаткові практичні курси з практичними працівниками правоохоронних органів в сфері пошуку та аналітичної обробки інформаційних ресурсів з різноманітних джерел.

1. Застосування комп'ютерних технологій в Національній поліції : навч. посіб. / І.В. Краснобрижий, С.О. Прокопов, Е.В. Рижков – Дніпро : ДДУВС, 2017. – 161 с.
2. https://www.ibm.com/us-en/marketplace/analysts-notebook
3. http://www304.ibm.com/partnerworld/gsd/solutiondetails.do?solution=51450&expand=true&lc=ru
4. https://www.ibm.com/us-en/marketplace/data-management
5. Підвищення кваліфікації слідчих, рамкова програма співробітництва для Вірменії, Азербайджану, Грузії, Республіки Молдова, України й Білорусії, спільний проект Європейського Союзу та Ради Європи «Посилення імплементації європейських стандартів прав людини в Україні», 2017. – 659 с.

Можливості створення та використання відео-презентацій у педагогічній діяльності.

Краснощок В.М.
доц., к.т.н. доцент кафедри інформаційних технологій та кібернетичної безпеки НАВСУ

Розвиток більшості галузей науки та народного господарства визначають інформаційні технології, серед яких особливого значення набувають інтерактивні технології. Технології електронного навчання дають, по-перше, можливість отримувати практико-орієнтовану освіту, оскільки електронний контент регулярно коригується як тими хто вчить, так і тими хто навчається, доповнюється «свіжою» інформацією з професійних сайтів і блогів; по-друге, технології дозволяють вибудовувати індивідуальну траєкторію навчання. Тим хто навчається надається можливість самостійно вивчати навчальні дисципліни за електронними курсами, «відвідувати» віртуальні семінари, брати участь

у вебінарах, дивитися лекції в режимі онлайн або в записі, а також виконувати контрольні роботи в електронному середовищі.

В даному аспекті особливого значення набувають відео-уроки, по яким зручно вивчати дисципліни, які вимагають точної послідовності при роботі с технічними приладами.

Для створення відео-презентацій використовують різні програми обробки відео та фото файлів. Однією з найбільш зручних таких програм є програма для нелінійного видеомонтажу Pinnacle Studio, яку випускали компанія Pinnacle Systems, Avid Technology та пізніше «Corel». Програма дозволяє монтувати відео будь якої складності на професійному рівні [1].

Для отримання «початкового матеріалу» для монтажу кінцевого відео часто необхідно виконати якісь дії на комп'ютері та пояснити їх виконання. Одного опису послідовності виконання дій буває замало. Для наочної демонстрації виконання певних дій на комп'ютері використовують наступні програми[2]:

1. Ezvid – програма дозволяє розділяти засняте відео та вставляти текс між цими частинами. Відео на можна відразу експортувати у файл, але можна завантажити його на YouTube прямо з програми. Для геймерів є опція "Ігровий режим" для запису ігрового процесу.

2. BlueBerry FlashBack Express Recorder. BB (коротко від BlueBerry) FlashBack Express Recorder дозволяє робити одночасно запис з екрана монітора та з веб-камери. Після завершення запису буде створений файл FBR, який можна редактувати у вбудованому редакторі.

3. Screenr – програму можна використовувати без її інсталяції, для цього вона використовує Java. Можна записувати не весь екран, а лише його частину. Максимальне відео – 5 хв. Відео зберігається у власний аккаунт. Потім відео можна експортувати в MP4-файл або завантажити на YouTube.

4. CamStudio – програма дозволяє включати відображення курсора, записувати аудіо самих програм або з мікрофона (чи взагалі без звука), робити записи користувача до відео. Можна вибрати область запису чи вікно програми. Є можливість налаштувати швидкість запису, наприклад 1 кадр в секунду (для створення ефекта timelapse), чи 30 кадрів в секунду для плавного відео.

5. Rylstim Screen Recorder – дуже маленька програма, що дозволяє швидко зробити скрінкаст - записати всі дії на екрані комп'ютера. Інтерфейс програми розташовано в одному вікні, що складається з декількох блоків – вибору активного монітора для

захоплення, активації функції виділення кліків миші, варіанти використовуваного кодека і FPS. Після вказівки директорії для збереження кінцевого файлу можна приступати до задачі запису відео. Головні переваги програми – її простота і повна безкоштовність.

1. Молочков В.П. Pinnacle Studio Plus. Основы видеомонтажа на примерах / В.П. Молочков – Киев: БХВ-Киев, 2007 – 336 с. – Рос. мовою.
2. http://www.coolwebmasters.com/video/3339-win-screen-recording-softwares.html – coolwebmasters – онлайн журнал для профессиональных веб-дизайнеров и разработчиков.

Деякі проблеми, що виникають у слідчого Національної поліції України при веденні єдиного реєстру досудових розслідувань

Кудінов В.А.
кандидат фізико-математичних наук, доцент,
професор кафедри інформаційних технологій
та кібернетичної безпеки Національної
академії внутрішніх справ

Досудове розслідування в Україні розпочинається з моменту внесення відомостей до Єдиного реєстру досудових розслідувань (надалі – ЄРДР). Він розпочав своє функціонування одночасно з надбанням чинності Кримінальним процесуальним кодексом (далі – КПК) України – з 20 листопада 2012 року [1]. Реєстр – це створена за допомогою автоматизованої системи електронна база даних, відповідно до якої здійснюється збирання, зберігання, захист, облік, пошук, узагальнення даних, які використовуються для формування звітності, а також надання інформації про відомості, внесені до Реєстру.

ЄРДР утворено та ведеться відповідно до вимог КПК України з метою забезпечення: 1) єдиного обліку кримінальних правопорушень та прийнятих під час досудового розслідування рішень, осіб, які їх учинили, та результатів судового провадження; 2) оперативного контролю за додержанням законів під час проведення досудового розслідування; 3) аналізу стану та структури кримінальних правопорушень, вчинених у державі.

Правову основу роботи ЄРДР складають: Конституція України; КПК України; Кримінальний кодекс України; низка відомчих наказів [2-5] тощо.

Держателем Реєстру є Генеральна прокуратура України. Реєстраторами Реєстру є: прокурори; слідчі органів прокуратури, поліції, безпеки, органів, що здійснюють контроль за додержанням податкового законодавства.

Розглянемо деякі проблеми, що виникають у слідчого Національної поліції України при веденні Єдиного реєстру досудових розслідувань, а саме:

1. Вихід з ЄРДР здійснюється автоматично через 10 хв. після початку роботи в ньому, незважаючи на те, чи було зареєстровано кримінальне правопорушення чи тільки велась робота по даному питанні, а також при здійсненні інших дій.

2. При реєстрації кримінального правопорушення досить часто при натисканні на пункт «реєстрація» з'являється інша вкладка, що унеможливлює реєстрацію. Після цього слід по новому здійснювати реєстрування та заповнення всіх вкладок.

3. Роздрукування «Форми № 2» про особу правопорушника при заповненні відповідного підменю «правопорушник» відбувається від 5 до 8 хв., що не є досить комфортним, тому як в одному кримінальному провадженні може бути досить велика кількість епізодів (об'єднані).

4. Підменю «наслідки досудового розслідування» та «завдані збитки» слід об'єднати в одне підменю і визначити одну картку для друку. Для заповнення цих двох вкладок та роздрукування двох карток (форми 1.1 та 1.2) необхідно досить велика кількість робочого часу в разі, коли в одному кримінальному провадженні об'єднано декілька кримінальних правопорушень (епізодів).

5. Цікавим моментом є внесення відомостей про правопорушника. Так, зокрема, в разі внесення відомостей про правопорушника у вкладці «правопорушник», слідчий повинен роздрукувати відповідну форму 2, що відноситься до відділу статистика. Однак, досить часто вносяться відомості про правопорушника, але не нажимається поле «Повідомлення про підозру». Таким чином, нібито статистичні дані підвищуються, рівень злочинності падає, проте на практиці особу правопорушника не повідомлено про підозру і він не набуває статусу підозрюваного, строки досудового розслідування не збігають.

6. Досить важливим і проблемним питанням залишається підменю «фільтр кримінальних правопорушень»: неможливо здійснити фільтр закритих кримінальних проваджень, а також інших здійснених процесуальних дій за певний період часу при роботі з ЄРДР слідчому.

7. Важливим моментом в роботі з ЄРДР виступає роздрукування різноманітних карток при здійснені певних процесуальних дій. Так, з точки зору практики і економії робочого часу, відділу статистики слід також отримати відповідні ключі для роботи з ЄРДР, тому що слідчий при реєстрації кримінального правопорушення витрачає досить велику кількість часу та паперу на роздрукування карток по зареєстрованим заявам. За одне чергування в складі СОГ може бути зареєстроване близько двадцяти кримінальних правопорушень.

Вважаємо, що вирішення зазначених проблем дозволить удосконалити роботу слідчого Національної поліції України з Єдиним реєстром досудових розслідувань.

---

1. Кримінальний процесуальний кодекс України // Відомості Верховної Ради України. – 2013. – № 9-10, № 11-12, № 13 – ст. 88. *Верховна Рада України*. URL: http://zakon3.rada.gov.ua/laws/show/4651-17.

2. Про затвердження Положення про порядок ведення Єдиного реєстру досудових розслідувань: Наказ Генеральної прокуратури України № 139 від 06.04.2016.

3. Про затвердження Змін до Положення про порядок ведення Єдиного реєстру досудових розслідувань: Наказ Генеральної прокуратури України № 147 від 22.05.2017.

4. Про затвердження Порядку надсилання інформації про осіб у кримінальних провадженнях та електронних копій судових рішень щодо осіб, які вчинили кримінальні правопорушення: Наказ Генеральної прокуратури України, Державної судової адміністрації України № 82/108 від 14.08.2014.

5. Про затвердження Порядку взаємодії Генеральної прокуратури України та Міністерства внутрішніх справ України щодо обміну інформацією з Єдиного реєстру досудових розслідувань та інформаційних систем органів внутрішніх справ: Наказ Генеральної прокуратури України, Міністерства внутрішніх справ України № 115/1046 від 17.11.2012.

Мистецтво розробки когнітивних тестових завдань

Кулешник Т.Я.
викладач Львівської Національної академії мистецтв, начальник ІОЦ
Кулешник О.І.
старший викладач Львівської Національної академії мистецтв

Валідність тесту – це відповідність, змістовність та корисність певних висновків, зроблених за результатами тесту. Валідація тесту – означає процес накопичення доказів на підтвердження цих висновків (стандарти освітнього та психологічного тестування AERA/APA/NCME).

Когнітивність тесту – це достатність для прийняття рішення [1].

Когнітивні тести, що використовуються в освіті та навчанні – це інструменти вимірювання, які складають основу для прийняття рішення.

Автори тестових завдань повинні постійно пам'ятати про два важливі запитання, які визначають якість тестового завдання: яка мета тесту, для якого я пишу тестове завдання і чи зміст цього тестового завдання відповідає такій меті?; чи формулювання цього завдання і його технічне представлення такі, що воно однозначно і надійно визначить підготованих і непідготованих кандидатів?

Необхідно зазначити, що є дві важливі теми для правильного розуміння того, що слід робити і чого не варто робити при розробці хороших тестових завдань: це план тесту і психометричні характеристики тестів, що входять до тестових завдань [2].

Як будинок не можливо збудувати без плану – так і тест слід складати виключно на основі плану тесту. План тесту – це відображення мети тесту, визначення знань та вмінь, які потрібно оцінити, очікуваний рівень засвоєння, типи і кількість тестових завдань, які повинні бути у тесті для прийняття, на підставі критеріїв якості тестів, достатньо обґрунтованого (валідного) рішення. Такі критерії якості, що є достатніми для прийняття рішення, роблять тести когнітивними.

Для правильного планування тестів в першу чергу потрібно визначити вимір змісту, або перелік тем на основі яких будуть створюватися тестові завдання. Ці теми, в свою чергу, можуть розподілятися на основні категорії та підкатегорії.

Наступним є вимір поведінки, або розумових операцій (ще називають “виміром навиків” чи “виміром поведінки”). Розумові процеси, що відбуваються в мозку того що тестується, складають другий вимір умовної тестової матриці.

Під час розробки описів когнітивних сфер використовувалося чимало теорій для розробки відповідного поведінкового виміру. Одна з найперших теорій – таксономія Блума, де тестові завдання діляться на шість різних категорій: знання, розуміння, застосування, аналіз, оцінка та синтез. Проте на практиці дуже складно здійснити цей розподіл.

Зараз все частіше простежується тенденція використання лише кількох рівнів на відміну від таксономії Блума. Для прикладу, рамки Тесту (FCAT) загальної оцінки у штаті Флорида використовують схему для класифікації тестових завдань за двома рівнями: нижчі розумові та вищі розумові рівні (навики).

Ще один типовий приклад перерозподілу категорій Блума – проект TIMSS, великі міжнародні дослідження освітніх досягнень, які було вперше проведено у 1995 році. Тут вимір поведінки складається з трьох категорій: знання, застосування та обґрунтування.

На даний час у США для валідації державних тестів широко використовується схема класифікації “Глибини знань” (DOK), розроблена Норманом Веббом. Це прагматичне поєднання загальних навиків і навиків, специфічних для якогось предмету. Загальна схема у DOK має чотири рівні вимог до розумових процесів, які є однаковими для усіх предметів: просте відтворення, необхідна певна розумова обробка, необхідне складніше/стратегічне розмірковування, необхідне розширене мислення.

Голландський національний інститут освітніх вимірювань, наприкінці 1970-х років розробив схему класифікації, яка базується на теорії роботи мозку при вирішенні завдань, а не на розвитку навиків. У цій схемі використовується операційний вимір Структури інтелекту Гілфорда (SI), як основа для виміру поведінки, що складається з трьох рівнів: відтворення А (“Ra”), відтворення В(“Rb”), продукування (створення) інформації (“P”).

Класифікація тестових завдань у відповідності до змісту та поведінки складає важливу частину процесу підготовки тестових завдань і включення їх в базу завдань, тому усі тестові завдання повинні мати маркування, на яких повинно бути позначено, який зміст та поведінку вони оцінюють.

Тестові завдання бувають двох форматів: із варіантами відповідей (вибір вірної відповіді серед запропонованих варіантів, або selecter response – SR) та розширеними відповідями (відкритих, або constructed response – CR). Формати тестових завдань – це інструмент у руках розробника тесту. Рішення використовувати конкретний формат залежить виключно від питання: який формат найкраще підходить для досягнення мети тексту.

Кожне тестове завдання слід розробляти з дотриманням наступних критеріїв якості тестування [3]:

- Валідність – мета тестування чітка і вписується у Програму тесту; існує класифікація завдань за Програмою; використано релевантні аспекти; відповідає сучасному розумінню предмета; дистрактори відповідей представляють реальні та релевантні помилки і хибні сприйняття;
- Надійність – відсутність недоліків, зокрема: нечітка чи двозначна мова, надто відкрите формулювання, ненавмисні підказки, ключі не розкидані навмання;
- Об'єктивність – відсутність етнічних, релігійних гендерних чи культурних упереджень; відсутність контексту, який може засмутити особу, яка складає тест; відсутність заплутаних запитань; якісна і ефективна система та структура оцінки робіт;
- Ефективність – увесь текст, таблиці і картинки є функціональними; інформація чітко сприймається, є відповідні пояснення;
- Прийнятність – тестове завдання вважається валідним, а його контекст – функціональним та реалістичним; громадськість розглядає це тестове завдання як об'єктивний тест.

Висновки.

Процес створення когнітивних та валідних тестових завдань повинен проводитись з дотриманням критеріїв якості та включати наступні пункти:

1. Вибір контекстного матеріалу.
2. Складання завдання.
3. Перевірка та перегляд завдання автором.
4. Перевірка та рецензування завдання іншим експертом.
5. Апробація.
6. Рецензування третім експертом.

1. Мудрук С. Практичний посібник для розробки тестових завдань. – Львів, 2014.
2. Аванесов В.С. Композиция тестових заданий/ В.С. Аванесов. – М.:Адепт, 1998. – 217 с.
3. Аванесов В. С. Применение заданий в тестовой форме в новых образовательных технологиях / В.С. Аванесов // Школьные технологии. — 2007. — № 3. — С. 146—163.

Етапи розробки валідних тестових завдань

Кулешник Я.Ф.
доцент кафедри інформатики Львівського державного університету внутрішніх справ

Перед тим як почати розробляти тестові завдання потрібно усвідомити, що робити і чого уникати при створенні тестових завдань, за допомогою яких можна створити валідні, надійні, об'єктивні та ефективні тести.

У статті розглянуто наступні питання:

– термінологія, що використовується під час розробки тестових завдань;
– процес розробки тестових завдань;
– формати тестових завдань;
– формати завдань з варіантами відповідей;
– тестові завдання з розширеними відповідями;
– критерії якості когнітивних (достатніх для прийняття рішення) тестів.

У процесі розробки тестових завдань, зазвичай, здійснюються такі кроки [1]:

– відбір контекстуальних матеріалів;
– розробка тестових завдань;
– рецензування тестових завдань і їхній перегляд автором (через деякий час);
– перегляд і рецензування тестових завдань другим рецензентом;
– попереднє тестування;
– перегляд третім експертом.

Розробник тестових завдань на будь-якій стадії повинен без вагань виключити з тексту окремі завдання, забраковані експертами.

Розгляд етапів розробки тестових завдань з варіантами відповідей (вибір вірної відповіді серед запропонованих, або selecter response – SR) розпочнемо з термінології. Зазвичай, тестові завдання розпочинаються з тексту, у якому наведено інформацію, яка повинна тлумачитися і використовуватися при наданні відповідей на тестові завдання. Це називається контекстом, або стимулюючим матеріалом (див. мал. 1).

Частина, у якій міститься реальне запитання, називається основою тестового завдання. Тестові завдання формату SR мають варіанти, з яких вибирається правильна відповідь. Варіант, в якому міститься правильна відповідь, називається ключем. Інші варіанти – це відволікаючі варіанти або дистрактори.

Для тестових завдань з варіантами відповідей, SR часто використовують наступні формати:

– варіанти відповідей, 3-6 варіантів які не повинні бути випадковими;

Малюнок 1. Термінологія завдань із варіантами відповідей (SR)

– підбір, один комплекс подій, характеристик, назв тощо слід підставити/з'єднати з іншим;

– розташування за порядком, комплекс подій, дій. тощо потрібно поставити у правильній послідовності, для прикладу, у хронологічному порядку;

– тест на заповнення (клоуз-тест), коли студент використовує припущення з заданого контексту для того, щоб доставити слова, які зумисне усунуті з тексту.

Для тестових завдань з відкритими запитаннями (constructed response – CR) часто використовують наступні формати:

– коротка відповідь;

– сконструйована відповідь;

– твір/есе/модельна справа.

При розробці тестових завдань необхідно дотримуватися наступних п'яти критеріїв якості:

– валідність;

– надійність;

– об'єктивність;

– ефективність;

– прийнятність.

Завдання мають надавати можливість розробникам тестів приймати валідні рішення, що базуються на результатах тесту. Тобто, індивідуальні тестові завдання повинні перевірити саме те, що від них очікують, і ніщо інше. Кожне завдання, яке пропонується, повинно класифікуватися у відповідності до розділів Плану тесту і бути визначеного формату. Потрібно створювати завдання, які відповідають поточному стану науки і думкам спеціалістів з цього питання, не використовують застарілу інформацію, забезпечують довговічність питання ще на етапі його розробки.

Кожне завдання повинно надійно забезпечувати послідовне розмежування (дискримінантність) слабких і сильних здобувачів вищої освіти. Ключі до запитань повинні бути розкидані навмання серед неправильних варіантів відповідей, щоб випадково не створити систему для вгадування правильної відповіді.

Тестові завдання неповинні містити жодних тендерних, етнічних чи культурних упереджень. Схеми оцінювання робіт повинні бути якісними для того, щоб звести до мінімуму відмінності між оцінками одних і тих же робіт, перевірених різними експертами.

Тестові завдання нададуть якомога більше інформації про кандидата за якомога менший період часу, якщо будуть використані замість звичайного тексту картинки, таблиці та інше. Запитання у тесті не повинні бути заплутаними чи скандальними.

1. Мудрук С. Практичний посібник для розробки тестових завдань. – Львів, 2014.

Сучасні радіозакладні пристрої

Лізунов С.І.
кандидат технічних наук, доцент, професор
Запорізького національного технічного університету
Абраменко Л.О.
слухачка магістратури Запорізького
національного технічного університету

Радіоелектронні закладні пристрої (ЗП) являють собою пристрої, що створюють канал несанкціонованого отримання і передачі в пункт прийому аудіо-, аудіовізуальної або оброблюваної радіоелектронної апаратурою та переданої в мережах зв'язку інформації.

ЗП можна поділити за кількома ознаками:

• радіозакладні пристрої, що випромінюють в ефір;

• закладні пристрої, які не випромінюють в ефір (з передачею перехопленої інформації по мережах зв'язку, управління, електроживлення, сигналізації і т.п.);

• радіозакладні пристрої з перевипромінюванням;

• закладні пристрої з передачею перехопленої інформації по стандартному телефонному каналу.

Також ЗП можна класифікувати за наступними критеріями (рис. 1):

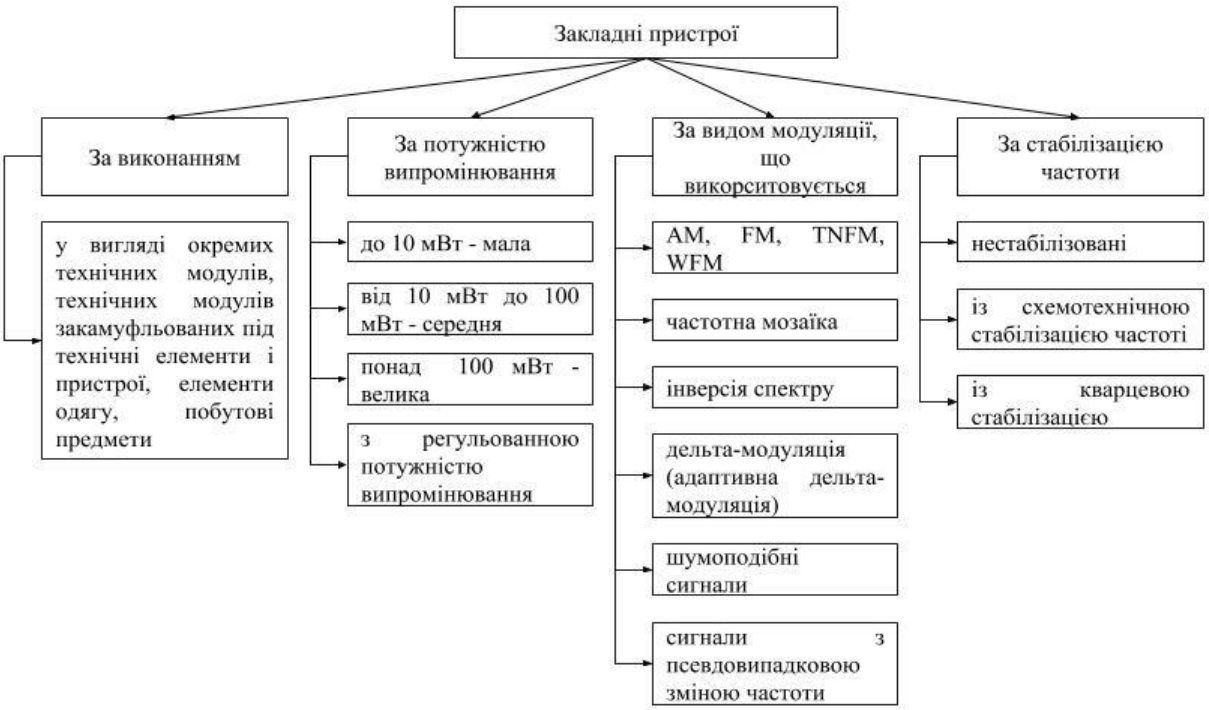


Рис. 1 – Класифікація закладних пристроїв

Для виявлення випромінюючих в ефір радіозакладок необхідно визначити можливий частотний діапазон їх роботи і види модуляції. Як випливає з аналізу існуючих радіозакладних пристроїв (РП), діапазон їх роботи досить широкий і має тенденцію до просування в більш високі частоти. Також існують пристрої із "стрибаючими" частотами. Це істотно ускладнює пошук РП по їх випромінюванням. Серйозне ускладнення в пошуку ЗП викликають і зміни та удосконалення видів модуляції, що використовуються. З'явився принципово новий клас РП з дельта-модуляцією. Крім того, в найбільш професійних радіозакладках використовують такі складні сигнали, як шумоподобні або з псевдовипадковою перестановкою несучої частоти. При кодуванні перехопленої інформації часто застосовується аналогове скремблювання, що змінює характеристики мовного сигналу таким чином, що він стає нерозбірливим.

Пошук таких пристроїв досить клопітка і головне дуже складна робота. Вони можуть бути закамуфльовані або вбудовані в предмети, що знаходяться у приміщенні.

Найбільшого поширення набули радіомікрофони. Цьому сприяв ряд причин. По-перше, простота установки і знімання інформації без необхідності застосування складного обладнання: необхідно лише сам ЗП і приймач для прийому радіосигналів. По-друге, можливість отримання інформації «з перших рук» в режимі реального часу.

Сучасні «прослушки» по радіоканалах мають широке розповсюдження тому що мають:

• невеликі розміри і досить високу потужність;

• високу якість звуку, завдяки багаторівневим мікрофонам;

• тривалий час роботи без підзарядки;

• наявність функції голосової або іншої активації;

• відсутність необхідності оплачувати послуги мобільного оператора для передачі аудіоінформації;

• доступну ціну.

Найсучасніші радіомікрофони, мають габарити не більше чверті олівцевої гумки та здатні протягом року сприймати і передавати на приймальний пристрій, розташований за півтора кілометра, розмову, яка ведеться в приміщенні пошепки. Він відноситься до класу пристроїв типу «клоп». Крім того, вже зараз виробляються "клопи", які можуть записувати перехоплену інформацію, зберігати її протягом доби або тижня, а потім передати її в режимі швидкодії за дуже короткий час, стерти запис і почати процес знову.

Такі пристрої негласного знімання інформації можуть бути вмонтовані, наприклад, в брелки, кулькові ручки, мережеві фільтри, окуляри або годинник, елементи одягу, тощо.

Із зазначеного вище можна зробити висновок, що боротьба із радіозакладними пристроями в сучасних умовах набуває все більшої актуальності.

Окремі питання внесення відомостей до ЄРДР в умовах особливого режиму досудового розслідування

Лисенков М.О.
викладач відділу підготовки прокурорів з нагляду за додержанням законів органами, які проводять ОРД, дізнання та досудове слідство Національної академії прокуратури України
matveilysenkov@gmail.com

Новелою чинного КПК України стала стаття 214, якою запроваджена електронно-процесуальна система Єдиного реєстру досудових розслідувань (далі – ЄРДР, Реєстр) [1].

Із цього часу, захист особи, суспільства та держави від кримінальних правопорушень можливий тільки після реєстрації відповідного провадження до Реєстру.

Проведення ж слідчих (розшукових) дій, окрім огляду місця події, до внесення відомостей в ЄРДР не допускається і може мати наслідком визнання судом таких доказів недопустимими [2].

Так, наприклад, ухвалою Козелецького районного суду Чернігівської області від 15.12.2016, закрито кримінальне провадження стосовно Велігоши О.Ю. та неповнолітнього Ганкевича О.О. за ч. 3 ст. 185 КК України. Під час судового розгляду встановлено, що слідчим усупереч вимогам ч. 3 ст. 214 КПК України окремі слідчі дії здійснювалися до внесення відомостей в ЄРДР, що призвело до визнання здобутих доказів недопустимими [3].

Разом з тим, чинним кримінальним процесуальним Законом передбачені окремі випадки, коли слідчі дії можуть проводитися до внесення відповідної інформації у ЄРДР.

Так, за ч. 3 ст. 214 КПК України, у випадку виявлення ознак кримінального правопорушення на морському чи річковому судні, що перебуває за межами України, можливо одразу розпочати проведення слідчих (розшукових) дій.

Запровадження такого окремого процесуального інституту пояснюється технічними особливостями функціонування електронно-процесуальної системи ЄРДР, необхідністю використання інтернет-мережі або засобів мобільного радіозв'язку з метою внесення відомостей до Реєстру, що, інколи, зробити складно або, взагалі, не можливо.

Вважаємо, що аналогічний процесуальний інститут необхідно запровадити щодо кримінальних проваджень, розслідування яких здійснюється в умовах воєнного, надзвичайного стану або у районі проведення антитерористичної операції, адже в умовах бойової обстановки життю та здоров’ю учасників провадження загрожує постійна небезпека, тому слідчому та прокурору необхідно проводити першочергові слідчі дії максимально оперативно у стислий термін. Однак, законодавча вимога щодо обов’язковості внесення даних до ЄРДР, а, інколи, і фізична неможливість це зробити (відсутність електричної енергії, доступу до інтернет-мережі чи мобільного радіозв'язку), збільшує час початку проведення таких дій.

На нашу думку, в умовах особливого режиму досудового розслідування, внесення відомостей до Реєстру про прийняті процесуальні рішення, а саме: визначення місця проведення досудового

розслідування (ч. 4 ст. 218), повідомлення про підозру (ч. 4 ст. 218), зупинення досудового розслідування (ч. 4 ст. 280), відновлення досудового розслідування (ч. 3 ст. 282), оголошення розшуку підозрюваного (ч. 2 ст. 281), закінчення досудового розслідування (ст. 283), здійснення спеціального досудового розслідування (ч. 6 ст. 297-4) може відбуватися при першій можливості.

Вбачається за доцільне внести зміни до Положення про порядок ведення Єдиного реєстру досудових розслідувань, затверджене Наказом Генерального прокурора України від 06.04.2016 року № 139, зазначивши, що здійснення досудового розслідування в особливих умовах є підставою для внесення до Реєстру прийнятих процесуальних рішень при першій можливості.

Враховуючи викладене, також, пропонуємо змінити ч. 3 ст. 214 КПК України, передбачивши можливість здійснення слідчих (розшукових) дій у кримінальному провадженні до моменту внесення відомостей у ЄРДР у випадку особливого режиму досудового розслідування в умовах воєнного, надзвичайного стану або у районі проведення антитерористичної операції.

---

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 року 4651-VI [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/4651-17.

2. Столітній А.В. Початок досудового розслідування: правова природа, регламентація та межі прокурорського нагляду / А. В. Столітній // Право і суспільство. - 2015. - № 4 (3). - С. 200-206.

3. Справа № 734/4131/15-к від 15.12.2016 // Єдиний державний реєстр судових рішень. [Електронний ресурс]. – Режим доступу: http://www.reyestr.court.gov.ua/Review/63445265.

Дослідження захищеності закритих Wi-Fi мереж

Лізунов С.І.
кандидат технічних наук, доцент, професор
Запорізького національного технічного університету
Вовкостріл А.І.
слухачка магістратури Запорізького
національного технічного університету

Дослідження бельгійського університету KU Leuven знайшли серйозні недоліки WPA2-протоколу, що забезпечує захист сучасних захищених мереж Wi-Fi. Зловмисник, який знаходиться в зоні дії жертви, може використовувати ці недоліки та застосовувати для атаки на повторну установку ключів (KRACK). Таким чином, може бути викрадена конфіденціальна інформація, що вважалась раніше захищеною: номери кредитних карток, паролі, повідомлення чату, електронні листи, фотографії і т.д. [1]

Зловмисник може розшифрувати всі дані, що передає жертва, використовуючи повторну установку універсального ключа шифрування. При криптографічному рукостисканні не гарантується безпека одноразового використання параметрів, що пов’язані з використовуваним ключем. Зловмисник при перехваті ключа шифрування компрометує жертву переустановкою вже використовуваного ключа. Зв’язані параметри (інкрементний номер пакету що передається (nonce) та номер пакету що приймається (лічильник повторів)) скидаються до початкового значення.[1,2]

Коли новий клієнт приєднується до мережі, він виконує чотиристоронне рукостискання для узгодження нового ключа шифрування. Як тільки ключ встановлено, він буде використовуватись для шифрування нормальних фреймів даних з використанням протоколу шифрування. Так як повідомлення можуть бути втрачені чи скинуті, точка доступу повторно передає повідомлення про підтвердження сеансу, якщо воно не отримало відповідного пакета для підтвердження. Тому клієнт може отримувати це повідомлення декілька разів. Зловмисник може змусити повідомлення некоректно скидатися, в результаті чого клієнт отримує його і перевстановлює той самий ключ шифрування та скидає інкрементний номер пакету передачі (nonce),

отримуючи лічильник повтору, що використовується протоколом шифрування. Таким чином, викликаючи навмисне повторне використання, пакети можуть бути відтворені, дешифровані та/або підроблені. Цей метод можливий для використання в атаці групового ключа, PeerKey, TDLS і узгодження швидкого переходу BSS.[1,2]

Дешифрування потоку можливе тому, що атака перевстановлення ключа приводить до відновлення nonce (також відомих як номери пакетів чи вектори ініціалізації) до початкового значення. Тобто один і той же ключ шифрування використовується із повторюваним декілька разів значенням nonce. Це призводить до того що всі протоколи WPA2 повторно використовують кеш-потік при шифруванні пакетів.

Можливість дешифрування пакетів може бути використана для дешифрування пакетів TCP SYN, що дозволяє зловмиснику отримати порядкові номери TPC з'єднання та захопити його. Після цього зловмисник може не зважати на використання WPA2 та виконати найбільш розповсюджену атаку на мережі Wi-Fi: внесення шкідливих даних в незашифровані HTTP-з'єднання (вводити вимагання чи шантаж, тобто шкідливе програмне забезпечення на сайти, що відвідує жертва).[1]

В небезпеці знаходяться жертви, що використовують протокол шифрування WPA-TKIP чи GCMP замість AES-CCMP.

Проти цих протоколів шифрування можливе не тільки розшифрування, а й підробка та введення пакетів, так як ці протоколи використовують повторне використання nonce. GCMP використовує один і той же ключ аутентифікації в обидві сторони зв'язку, тому ключ може бути відновлено. Як рішення цієї проблеми, підтримка GCMP на даний момент розвертається під назвою Wireless Gigabit (WiGig) та очікується її прийняття в найближчі декілька років.

Напрям, в якому пакети можуть бути дешифровані чи підроблені, залежить від атаки на рукостискання. Якщо спрощено атакувати чотиристоронне рукостискання, зловмисник може дешифрувати і підробити пакети, відправлені клієнтом. Коли атака відбувається на рукостискання Fast BSS Transition (FT), є можливість розшифрувати і підробити пакети відправлені клієнту. Більшість атак також здатні відновлювати одноадресні, широкомовні чи багатоадресні кадри. [1]

Важливою деталлю є той факт, що наведені атаки не відновлюють пароль від мережі Wi-Fi, не відновлюють будь-які частини нового ключа шифрування що узгодився під час чотиристороннього рукостискання.

На даному етапі розслідування можливість KRACK можна нейтралізувати за допомогою оновлень безпеки пристроїв, які дозволять

встановлювати ключ шифрування тільки раз. Постачальники, чиї продукти протестували дослідники, отримали повідомлення про недоліки ще в липні 2017 року. У серпні до процесу також підключилася координаційний центр CERT-CC, який розіслав повідомлення про вразливості. [1]

Оновлення безпеки гарантують, що ключ встановлюється тільки один раз, що запобігає атаці. Тому користувачі повинні переконатися, що всі пристрої оновлені, а також повинні оновити прошивку маршрутизатора. Що робити, якщо немає оновлень безпеки для мого маршрутизатора або точки доступу, або якщо він не підтримує 802.11r? Домашні маршрутизатори або AP, ймовірно, не вимагають оновлень безпеки. Замість цього, головним чином, корпоративні мережі повинні будуть оновити свою мережеву інфраструктуру.

Є можливість спробувати зменшити атаки на маршрутизатори і точки доступу, відключивши клієнтські функції (наприклад, використовувані в режимах ретранслятора) і 802.11r (швидкий роумінг).[1]

1. Breaking WPA2 by forcing nonce reuse [Електронний ресурс]. – Режим доступу: https://www.krackattacks.com/#demo

2. Mathy Vanhoef, Frank Piessens - Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2.

Аналіз брандмауерів на захищеність

Лізунов С.І.
кандидат технічних наук, доцент, професор
Запорізького національного технічного університету
Верещака М.П.
магістр Запорізького національного
технічного університету

Системи захисту інформації в комп'ютерних мережах повинні забезпечувати цілеспрямовану роботу останніх. Тобто вся інформація повинна бути прихованою і цілісною. В більшості випадків всі мережі офісів і компаній підключаються до всесвітньої павутини.

Для захисту локальних мереж, використовують міжмережеві екрани, які називаються брандмауерами. Даний екран є засобом диференціального доступу. Це означає, що мережа розосереджена на дві половини. Тобто є межа між інтернет-мережею і локальною мережею.

Брандмауери бувають програмними та апаратними.

Для аналізу брандмауерів на захищеність використовують утиліти з сайту www.testmypcsecurity.com, а саме Jumper, DNStester і CPIL Suite (розробка компанії Comodo). Ці утиліти використовують такі ж самі методи, що і шкідливі програми, роботу яких вони симулюють. Під час тестування всі засоби антивірусного захисту повинні бути деактивовані.

Розглянемо утиліти:

- Jumper - дозволяє обійти брандмауер, використовуючи методи «DLL injection» і «thread injection»;
- DNS Tester - використовує рекурсивний DNS-запит, щоб обійти брандмауер;
- CPIL Suite - набір тестів (3 тесту) від компанії Comodo.

Всі ці утиліти потрібно запускати безпосередньо з досліджуваних комп'ютерів, а з зовні потрібно сканувати мережу за допомогою програми nmap.

Апаратні брандмауери використовують для ефективного захисту кожного вузла мережі. До їх недоліків можна віднести те, що вони не можуть забезпечити захист кожної окремої робочої станції, безсилі при атаках всередині мережі, а також не можуть виконувати розмежування інформаційної системи персональних даних.

Програмні брандмауери використовують для захисту всієї мережі в цілому. Їх стандартні настройки не можуть забезпечити максимальний захист від усіх типів загроз, тому правильно налаштовані програмні брандмауери дають більш гарантовану безпеку роботи в мережі.

Для досягнення найбільшої ефективності захист інформаційної системи повинен бути комплексним та включати програмні і апаратні брандмауери, антивіруси і правильні налаштування операційної системи.

Забезпечення конфіденційності даних оперативно-розшукової діяльності та досудового розслідування у локальних мережах на базі ос Windows Server 2012

Лізунов С.І.
кандидат технічних наук, професор ЗНТУ
Лапутько А.В.
співробітник Управління Держспецзв'язку в Запорізькій обл.
Гужва А.А.
слухач магістратури ЗНТУ

Проведення оперативно-розшукової діяльності та досудового розслідування вимагає обробки великого об'єму інформації різних типів. У зв'язку з цим виникає потреба в автоматизації процесів обробки засобами обчислювальної техніки. При цьому дані, що оброблюються, нерідко містять інформацію, несанкціоноване розголошення або модифікація якої може завдати значної шкоди розслідуванню. Це створює цілий ряд проблем, пов'язаних з забезпеченням захисту інформації у локальних мережах органів поліції.

У цій роботі розглядається процес захисту інформації у локальних мережах на базі ОС Windows Server 2012 з використанням вбудованих механізмів захисту (дозволи, групові політики, налаштування окремих компонентів тощо).

Визначено компоненти ОС [1], які найбільш часто використовуються при побудові локальних мереж, та механізми їх захисту. Для кожного компонента описано процес його встановлення, характер оброблюваних даних, та процес налаштування з метою захисту оброблюваних ним даних.

Додатково було розглянуто параметри безпеки групових політик Active Directory [2], які використовуються для обмеження дій користувачів мережі, та розроблено перелік рекомендацій з їх налаштування, виконання яких значно зменшить вірогідність несанкціонованого розголошення або модифікації конфіденційної інформації.

Результатом роботи є набір рекомендацій для мережних адміністраторів. Ці рекомендації можуть бути як виконані напряму, так і використані при формуванні власної політики безпеки.

1. Server Roles and Technologies in Windows Server 2012 R2 and Windows Server 2012 [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://technet.microsoft.com/en-us/library/hh831669(v=ws.11).aspx (дата звернення 12.10.2017) – Назва з екрана.

2. Security Policy Settings Reference [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://technet.microsoft.com/en-us/library/dn452423(v=ws.11).aspx (дата звернення 12.10.2017) – Назва з екрана.

Методики та інструменти аудиту кібербезпеки інформаційних систем.

Махницький О.В.
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

У повсякденному житті часто інформаційна безпека (ІБ) розуміється лише як необхідність боротьби з витоком секретної та поширенням неправдивої і ворожої інформації. Однак, це розуміння дуже вузьке. Існує багато різних визначень інформаційної безпеки, в яких висвічуються окремі її властивості. Під інформаційною безпекою розуміється стан захищеності інформаційного середовища суспільства, що забезпечує її формування та розвиток в інтересах громадян, організацій і держави.

В інших джерелах наводяться наступні визначення:

Інформаційна безпека - це

1) комплекс організаційно-технічних заходів, що забезпечують цілісність даних і конфіденційність інформації в поєднанні з її доступністю для всіх авторизованих користувачів;

2) показник, що відображає статус захищеності інформаційної системи;

3) стан захищеності інформаційного середовища;

4) стан, що забезпечує захищеність інформаційних ресурсів і каналів, а також доступу до джерел інформації.

Існує кілька підходів до тестування кібербезпеки інформаційних систем.

Термін «інформаційна безпека» часто трактується як шифрування інформації. Ця область зазвичай регулюється державними та відомчими нормативними актами. Проблема такого підходу полягає в його статичності. Крім того, вона охоплює лише частину питань, пов'язаних з кібербезпекою. Кожну хвилину хакери працюють над новими прийомами несанкціонованого доступу, а норми і методики перевірки стійкості до кіберзагрозам залишаються незмінними на протязі багатьох років. У зв'язку з цим виникають питання:

Наскільки мережа захищена від несанкціонованого вторгнення ззовні? Наскільки актуальні методології та інструменти аудиту мережевої кібербезпеки? Крім того, в інформаційну безпеку можуть входити питання продуктивності мережевого обладнання: ті чи інші класи мережевих пристроїв повинні не тільки перешкоджати вторгненню ззовні в вашу мережу, а й безперешкодно пропускати корисний трафік, не заважаючи нормальній роботі організації.

Існують інструменти та методики, що дозволяють по-новому поглянути і оцінити ступінь захисту інформаційних ресурсів і мережевих вузлів.

Що є об'єктом тестування (аудиту)? Тестується стійкість мережевої інфраструктури і додатків до широкого спектру кібератак з застосуванням новітніх методик і апаратних засобів. Об'єктами тестування на предмет інформаційної безпеки і стійкості до кібератаки є:

• Периметри інформаційної безпеки

• Критична мережева інфраструктура (магістральні маршрутизатори, комутатори, NAT), в тому числі на об'єктах стратегічного значення

• Центри обробки даних (ЦОД)

• Мережеві додатки і сервіси

• Машинні системи, об'єднані в мережі (IoT - т.зв. «інтернет речей»)

• Роботизовані системи, в тому числі:

- промислові

- військові, включаючи безпілотні системи

• Бортові інформаційні системи (авіоніка) літаків, морських суден, автомобілів і т.д.

Типовими об'єктами для тестів інформаційної безпеки є маршрутизатори, балансувальник трафіковий навантаження, міжмережеві екрани, комутатори, програмно-апаратні комплекси для глибокого аналізу трафіку, що проходить (DPI), ЦОДи, а також різні комбінації включення цих пристроїв.

Існують спеціальні апаратні рішення призначені для аудиту стійкості мережевої інфраструктури і додатків до існуючих і перспективних кіберзагрозам, включаючи: стресове навантаження, різні DDoS-атаки, шкідливий код в загальному трафіку, спам, черви, атаки типу «zero day», атаки із застосуванням технології fuzzing , і т.д.

Випробування на інформаційну безпеку проводяться в лабораторних умовах - тобто нема на працюючої мережі. Для цього використовується досліджуваний пристрій (DUT - device under test), або цілий фрагмент мережі в зборі (SUT - system under test) і спеціальний генератор / аналізатор трафіку, який створює стресову навантаження з корисного і шкідливого трафіку і одночасно аналізує відгук від досліджуваного пристрою або системи.

Переваги даного методу полягає в можливості генерації і аналізу стресового навантаження (трафіка) і одночасному аналізі якості роботи інформаційної системи по різним метрик якості та сприйняття інформаційних сервісів (QoS / QoE).

Апаратне рішення тестової складової - генератор стресового навантаження. Генератор стресового навантаження є спеціальним програмно-апаратним комплексом. Його мета - створити стресовий потік трафіку високої щільності на рівнях L2-L7 (по моделі OSI) і проаналізувати відгук і поведінку досліджуваного об'єкта при різних рівнях навантаження і профілях мережевого трафіку. Пристрій емулює запити великої кількості користувачів з унікальними IP-адресами, а також сервери додатків.

Даний комплекс заходів призначений для тестування на стійкість мережевої інфраструктури і додатків до шкідливого трафіку, включаючи:

- Різні типи DDoS-атак
- Черви
- Fuzzing
- E-mail атаки
- Віруси / Трояни / Malware (такі як Red October і т.д.)
- VoIP-атаки
- Атаки на додатки
- Evaded Attacks / Fragmentation

- Сканування і порушення роботи портів
- Buffer Overflows / Protocol Exploitation
- Генерація flooding-атак з інтенсивністю до декількох мільйонів в секунду
- Комбіновані і багатоступінчасті атаки

• Пошук вразливостей в інфраструктурі і додатках для несанкціонованого проникнення ззовні (хакерський взлом) і zero-day атаки

• Вибір технічних рішень і постачальників

• Розробка засобів інформаційного захисту

• Налаштування політик периметрів інформаційної безпеки (при зміні прошивок, додаванні нових IT-сервісів, оновлення обладнання і т.д.)

Генеруються атаки постійно підтримуються в актуальному стані за рахунок періодичного поновлення бази даних атак.

Крім цього, користувач може створювати власні атаки за допомогою спеціального конструктора атак (Attack Designer). Атаки можуть бути створені як «з нуля», так і шляхом модифікації наявних бібліотек. Для більшої гнучкості реалізована можливість використання pcap-файлів. Як приклад для інструментів для аудиту периметрів інформаційної безпеки можна розглянути:

Генератор хакерських атак, шкідливого трафіку і корисного прикладного трафіку Spirent Avalanche

Генератор стресового навантаження, змішаного і шкідливого трафіку нового покоління Avalanche NEXT

Приклади тестування інформаційної безпеки з використання зазначених вище інструментів:

• Тестування електричного навантаження на і стійкості web-порталу до DDoS-атакам.

• Тестування продуктивності банківської мережевої інфраструктури по можливості підключення банкоматів по каналах IPSec.

• Налаштування політик безпеки і продуктивності периметра інформаційної захисту організації.

• Тестування стійкості SaaS сервісу в ЦОДі.

• Стресовий тестування RADIUS-сервера в core-мережі оператора мобільного зв'язку.

[Електронний ресурс]. – Режим доступу: http://www.lab.pr-group.ru/ITsecurity.html

[Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/w/index.php? search=безпеака+інформації

Інформаційна безпека України в сучасних умовах

Мирошниченко В.О.
к. т. н., доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Інформаційна безпека в XXI столітті виходить на перше місце в системі національної безпеки держави, тому лише та держава може розраховувати на лідерство в економічній, військово-політичній та інших сферах, мати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби.

Інформація постійно ускладняється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас збільшується і уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності й т. ін. Тому Конституцією України забезпечення інформаційної безпеки віднесено до найважливіших функцій держави.

За даними наукових досліджень, система забезпечення інформаційної безпеки України не виконує окремих важливих функцій. Зокрема, неефективними є управління її діяльністю, організаційні зміни, що здійснюються в межах адміністративної реформи, мають несистемний характер, проводяться без попереднього функціонального дослідження органів державної влади. Негативні тенденції розвитку національного інформаційного простору, кризовий стан економіки країни та інші чинники обумовлюють ескалацію загроз, що може призвести (а часом і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру, завдання шкоди юридичним особам та громадянам.

Сучасне впровадження новітніх інформаційних технологій посилює важливість однієї з основних складових системи національної безпеки – інформаційної безпеки, для забезпечення якої необхідний системний комплексний підхід. Проблеми інформаційної безпеки в умовах глобальної інформатизації і розвитку Інтернету набувають стратегічного значення. Тому основними напрямами державної інформаційної політики повинно бути забезпечення інформаційної безпеки України, сприяння міжнародній співпраці в інформаційній сфері та входженню України до світового інформаційного простору [1]. В сучасних умовах рівень розвитку та безпека інформаційного простору країни є системоутворюючими факторами у забезпеченні безпеки, що активно впливають на стан політичної, економічної, воєнної, інформаційної та інших складових національної безпеки держави. Тенденція забезпечення національної безпеки та її складових враховується провідними державами світу та оборонними блоками при модернізації власних стратегій. Прикладами таких документів є: "Стратегія національної безпеки" у США, "Політика національної безпеки" у Канаді, "Стратегічна концепція національної оборони" в Італії. В Україні також проводиться послідовна робота з розбудови інформаційного суспільства. [2]. У прийнятих документах відображені принципи, базові для інформаційного суспільства – це партнерство влади, суспільства і бізнесу, а також відкритість, відповідальність та ефективність самої влади. Реалізувавши Стратегію, Україна стане рівноправним учасником глобального інформаційного суспільства. В умовах формування глобального інформаційного суспільства в сучасних конфліктах з'явилася нова фаза – інформаційно-психологічна війна, яка займає проміжну сходинку між політичною кризою і фазою збройного зіткнення, будучи при цьому "поворотною точкою" від мирної фази до військової. У цій фазі технології інформаційно-психологічного впливу на політичні (в тому числі, міжнародні) конфлікти стають одним з вирішальних чинників і високоефективних інструментів в діяльності по їх політичному вирішенню [3].

На сучасному етапі основними реальними та потенційними загрозами національній безпеці України в інформаційній сфері, стабільності в суспільстві є:

- прояви обмеження свободи слова та доступу громадян до інформації;

- поширення засобами масової інформації культу насильства, жорстокості, порнографії, комп'ютерна злочинність та комп'ютерний тероризм;

- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;

- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації.

Основними напрямами забезпечення інформаційної безпеки та протидії вищезазначеним загрозам для України можна визначити:

- у сфері міжнародної співпраці – інтеграція в міжнародну систему забезпечення інформаційної безпеки і співпраця по запобіганню протиправних дій в інформаційній сфері;
- у сфері оборони – вдосконалення системи моніторингу загроз та їх джерел, своєчасне інформування відповідних суб'єктів влади про стан інформаційного ресурсу і інформаційних систем оборонної сфери; засобів, методів і способів здійснення, спеціальних заходів і заходів інформаційного впливу, системи підбору і спеціальної підготовки користувачів.

Таким чином, інформаційна безпека відіграє провідну роль в забезпеченні життєво важливих інтересів будь-якої країни. Метою її забезпечення є створення розгалуженого та захищеного інформаційного простору, захист національних інтересів держави в умовах формування світових інформаційних мереж, захист економічного потенціалу країни від незаконного використання інформаційних ресурсів, реалізація прав громадян, установ та держави на отримання, поширення та використання інформації.

1. Інформаційна безпека суспільства / А. Суббот // Вісник. - 2015. - № 8. - С. 29-31 . - Режим доступу: http://nbuv.gov.ua/UJRN/viche_2015_8_7;

2. Указ Президента України від 25 лютого 2017 року № 47/2017 «Про Доктрину інформаційної безпеки України»;

3. Указ Президента України від 15 березня 2016 року № 96/2016 «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України».

Телекомунікаційне супроводження професійно-ділової гри «Лінія 102».

Прокопов С.О.
старший викладач Дніпропетровського державного університету внутрішніх справ

На протязі року в Дніпропетровському державному університеті внутрішніх справ проводиться ділова професійна гра «Лінія 102». Вона впроваджена в навчальний процес передвипускних та випускних курсів курсантів факультетів для підготовки фахівців Національної поліції та студентів юридичного факультету університету.

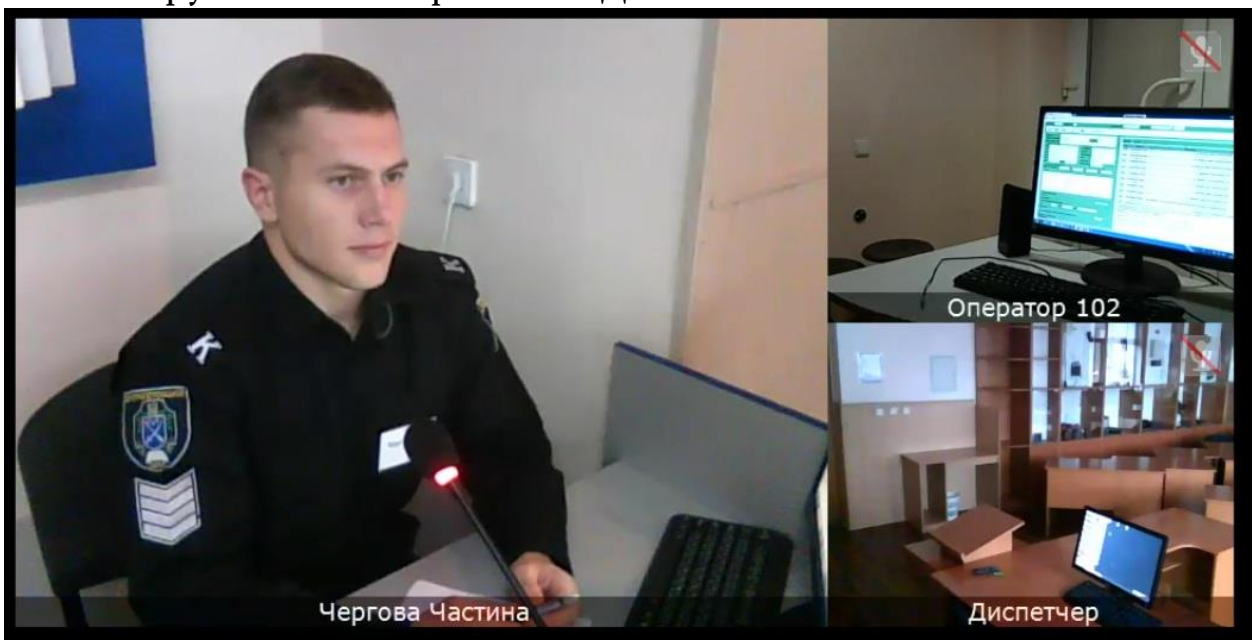
Нещодавно в Дніпропетровському державному університету внутрішніх справ проходив тренінг «Інноватика в освітньому процесі» – професійно-орієнтована ділова гра «Лінія 102», в якому прийняли участь представники всіх навчальних закладів системи МВС. По результатам цього тренінгу було прийняте рішення про впровадження цієї професійно-ділової гри в навчальний процес усіх університетів внутрішніх справ України.

Багато наукових досліджень було присвячено розгляду інформаційної та іншої технічної підтримки професійної гри «Лінія 102», розробленої фахівцями кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ. Розглядались робочі місця інформаційно-технічної платформи супроводження ділової гри [1]. В цій доповіді хотілось приділити увагу розгляду телекомунікаційних можливостей цієї інформаційно-технічної платформи. Інформаційно-технічна платформа надає можливість безперервної передачі відеозображення та акустичного сигналу до умовного штабу тренінгу з найбільш важливих місць проведення рольової гри. Умовно можливо поділити відеопотоки з цих місць на дві групи, а саме, зі стаціонарних навчальних робочих місць, та з мобільних навчальних робочих місць [2] інформаційно-технічної платформи навчань «Лінія 102».

Розглянемо першу групу. Передавання відеозображень та аудіо сигналу зі стаціонарних навчальних робочих місць [3], а саме, оператора 102, диспетчера та начального відділу поліції, в якому розміщені робочі місця чергового відділу, слідчого, оперативного працівника та спеціаліста, здійснюється за допомогою відеокамер які під’єднуються до

комп`ютерів за допомогою USB роз'єму та програмної оболонки "Communication Services". В результаті з відеосервера, який встановлений у штабі, можна побачити все, що відбувається на навчальних робочих місцях та чути, по черзі переключаючи мікрофони на потрібне робоче місце, учасників тренінгу.

Відеозображення проеціюється на великий екран за допомогою мультимедійного проектору. Необхідне робоче місце можна збільшувати для більш зручного спостереження. Див. мал. 1.



Мал. 1

В разі необхідності всі відео потоки можна записувати на електронні носії та проглядати з метою акцентування правильності дій кожного учасника тренінгу.

На другому екрані в штабі «Лінія 102» відображуються події, які відбуваються на території університету, це умовні місця подій, місця проведення слідчо-розшукових дій, затримання підозрюваних та інших дій, які відбуваються під час тренінгів. Передавання відеозображення та звуку здійснюється за допомогою планшетів або смартфонів та програмної оболонки «Скайп», у вигляді як одиночних, так і групових відео конференцій.

На початковому етапі ми використовували можливості 3G стільникового зв'язку, але потім територію університету обладнанали Wi-Fi роутерами, що значно підвищило якість та безперервність передачі відео зображень та звуку до штабу навчань .

Вважаючи, що професійно-орієнтована ділова гра «Лінія 102» буде використовуватися і у інших навчальних закладах системи МВС, ця

доповідь допоможе фахівцям університетів у впровадженні телекомунікаційного супроводження цих тренінгів.

1. Прокопов С.О., Махницький О.В., Гавриш О.С. Інформаційно-технічна платформа інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників Національної поліції в ДДУВС / О.С. Гавриш, О.В. Махницький, С.О. Прокопов // Право і суспільство. – 2017. – № 1. – С. 128–141.

2. Прокопов С.О. Навчальне автоматизоване робоче місце оперативного працівника в інформаційно-технічній платформі інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників національної поліції в ДДУВС / С.О. Прокопов // Юридична наука: сучасний статус, перспективи, інновації: матеріали всеукраїнської науково-практичної конференції (7 грудня 2016) / Редкол.: Краснощок А.В. (гол.ред.) та ін. – Кривий Ріг: КФ ДДУВС, 2016. – 433 с.

3. Прокопов С.О. Навчальне автоматизоване робоче місце патрульного поліцейського в інформаційно-технічній платформі інтерактивного комплексу з підготовки здобувачів вищої освіти та практичних працівників національної поліції у ДДУВС / С.О. Прокопов // Економічна та інформаційна безпека: проблеми та перспективи: матеріали Всеукраїнської науково-практичної конференції (14 квітня 2017 р., м. Дніпро). – Дніпро: Дніпропетровський державний університет внутрішніх справ, 2017. – С. 153-160.

Впровадження нових підходів щодо автоматизації кримінального аналізу у практичній діяльності Національної поліції України

Сеник В.В.
завідувач кафедри інформатики
Львівського державного університету
внутрішніх справ, кандидат технічних наук, доцент
Шишко В.Й.
викладач кафедри інформатики
Львівського державного університету внутрішніх справ
Братичак О.В.
здобувач освітнього ступеня «бакалавр»
факультету №1 Інституту з підготовки фахівців
для підрозділів Національної поліції
Львівського державного університету внутрішніх справ

Вивчення злочинності є необхідною умовою попередження та розкриття злочинів. Науковий підхід до аналізу стану правопорядку і до розробки заходів щодо його укріплення, пізнання закономірностей і ролі суб'єктивного фактору у подоланні антисуспільних явищ забезпечують успіх справи. Нехтування ж науковим аналізом може призводити до прийняття неефективних рішень, і, як наслідок, до можливого нераціонального використання сил та засобів.

Для прийняття ефективних рішень з встановлення правопорядку необхідно, насамперед, мати достовірні і повні дані про стан злочинності, її структуру та динаміку, загальні, часткові причини і умови здійснення правопорушень. Важливо розглядати територіальний та галузевий розріз злочинності, її відмінності за регіонами, галузями і об'єктами народного господарства, визначити місця найбільшої кількості злочинних проявів і стосовно до цього аналізу уточнити умови, які сприяють цим проявам. Зрештою, необхідно критично проаналізувати організацію, засоби і методи проведення аналізу, який до цього часу застосовувався, його ефективність і достатність для протидії злочинності. Безпосередня мета вивчення злочинності – це отримання достовірної інформації про її стан, рівень, структуру, динаміку, причини і умови, що їй сприяють, про ефективність заходів, які направлення на протидію їй. Для того, щоб кримінологічна інформація дійсно

відображала стан та інші характеристики злочинності, вона має відповідати, щонайменше, трьом вимогам: повноті, своєчасності та достовірності. Очевидно, що зробити правильний висновок про стан злочинності можна лише у тому випадку, якщо отриманий достатній обсяг інформації про це явище.

До сьогоднішнього дня вимога повноти кримінологічної інформації не трактувалась за принципом «чим більше, тим краще». За логікою статистичних методів дослідження злочинності великий обсяг інформації, у якому є суттєві та несуттєві дані для пізнання цього явища, призводить не лише до збільшення затрат матеріальних ресурсів і часу, але й ускладнює сам процес аналізу. Окрім того, вимога повноти інформації визначалась «економно», виходячи з конкретних завдань того чи іншого дослідження, за принципом «необхідно – достатньо».

Під час вивчення злочинності практично неможливо отримувати достатньо повну про неї інформацію відразу під час виникнення відповідних фактів чи подій. Для трактування стану злочинності необхідно накопичувати і сумувати дані про злочини за певний, відносно тривалий період часу. Тому важливою та своєчасною буде і така кримінологічна інформація, яка отримана із звітних даних за певний минулий період часу або отримана в результаті дослідження попередньої практики боротьби зі злочинністю.

Сьогоднішні дослідження злочинності, на жаль, не охоплюють усієї сукупності взаємодіючих соціально-економічних факторів, які впливають на злочинність. Усі дослідження спрямовані на дослідження зв’язку між окремими факторами і злочинністю, а це обмежує практичну цінність планування заходів для попередження злочинності та вироблення стратегії і тактики боротьби зі злочинністю.

У процесі проведення кримінологічного аналізу використовуються різноманітні підходи та методи. Від методів, які використовуються, залежать результати досліджень, глибина проникнення у закономірності злочинності. Надійна методика необхідна і під час вирішення проблем організації боротьби зі злочинністю, оцінки ефективності заходів, які застосовуються. Не дивлячись на те, що на даний час накопичено певний практичний досвід проведення кримінологічних досліджень, можна констатувати його обмежені можливості щодо широкого використання в сучасних умовах через інтенсивний розвиток змін як в економічних, соціальних і правових умов життя суспільства, так і через стрімкий розвиток науково-технічного

прогресу, який, зокрема, вимагає використання нових методів і технологій до проведення таких досліджень.

Сучасні дослідники виділяють три підходи до проведення досліджень:

- ймовірнісний – зазвичай з припущенням, що величини, які досліджуються, підлягають розподілу Гауса;
- геометричний – вважається, що дані не підлягають ймовірнісній природі і утворюють у багатовимірному просторі структури з певними властивостями;
- змістовний – припускає можливість досягнення результатів за допомогою методів моделювання.

Перші два підходи реалізуються за допомогою методів прикладної статистики, третій – за допомогою використання технології Data Mining. Ймовірнісний та геометричний підходи припускають той факт, що під час аналізу даних має місце певна модель, як правило лінійна, і мета проведення дослідження – знайти параметри, які б цю модель оптимально задовольняли. Методи ж інтелектуального аналізу даних за допомогою алгоритмів машинного (алгоритмічного) навчання ітеративно підбирають модель, яка певним чином найкраще описує вихідні дані.

У цьому сенсі машинне навчання наближене до непараметричної ідентифікації, яка припускає, що потрібно в ході вирішення визначити модель і дати оцінку її параметрів. Під час цього реалізується конструктивний підхід до побудови моделей, що базується на індуктивної теорії і спирається на ідею можливості опису даних з використанням рядів примітивів на основі їх селекції за певними критеріями. На даний час до методів непараметричної ідентифікації можна віднести методи Data Mining.

Суть і мета технології Data Mining полягає у пошуку у великих обсягах даних неочевидних, об’єктивних і корисних на практиці закономірностей. Неочевидні – це значить, що знайдені закономірності не виявляються стандартними методами обробки інформації або експертним шляхом. Об’єктивних – це значить, що виявлені закономірності будуть повністю відповідати дійсності, на відміну від експертної думки, яка завжди є суб’єктивною. Корисних на практиці – це означає, що висновки мають конкретне значення, якому можна знайти практичне застосування.

Основні завдання, які вирішуються з використанням технології Data Mining [1]:

- *класифікація* – під час якої визначаються ознаки, що характеризують групи об'єктів набору даних, які досліджуються;

- *асоціація* – пошук асоціативних правил, на основі яких відшукуються закономірності між зв'язаними подіями у сукупності даних;

- *послідовність* – пошук тимчасових закономірностей між трансакціями (встановлення закономірностей між подіями, що відбуваються з певним інтервалом часу);

- *прогнозування* – оцінювання пропущених або майбутнє значення цільових числових показників;

- *визначення відхилень* – виявлення і аналіз даних, які найбільше відрізняються від загальної кількості даних; виявлення так званих нехарактерних шаблонів;

- *оцінювання* – зводиться до передбачення неперервних значень ознак;

- *аналіз зв'язків* – пошук закономірностей у наборі даних;

- *візуалізація* – створення графічного відображення даних, що аналізуються;

- *підведення підсумків* – опис конкретних груп об'єктів з набору даних, що аналізуються.

Не дивлячись на те, що на даному етапі розвитку суспільства для аналізу і прогнозування технологію Data Mining використовують переважно комерційні структури, її запровадження у діяльність Національної поліції України дозволить створить передумову для:

– об'єктивного визначення рівня та динаміки злочинності;

– сукупності чинників, що впливають на криміногенну обстановку як в окремих регіонах, так і в державі загалом;

– узагальнення результатів діяльності підрозділів Національної поліції щодо виконання поставлених перед ними завдань.

---

1. Сеник В.В. Перспективи використання технології Data Mining для аналізу та прогнозування стану злочинності / Теорія та практика протидії злочинності у сучасних умовах: збірник тез Міжнародної науково-практичної конференції (10 листопада 2017 року) / упор. О.В. Авраменко, С.С. Гнатюк, І.В. Красницький. – Львів: ЛьвДУВС. – с. 214-215.

Трансформаційне забезпечення економічної безпеки бізнесу

Соломіна Г.В.
кандидат економічних наук, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Виходячи з узагальнення теоретичних засад сутності економічної безпеки, функцій та ролі підприємництва, як сектору національного господарства, є підстави для висновку, що економічна безпека підприємництва є станом захищеності економічних інтересів суб'єктів сектору під час взаємодії з державою, іншими суб'єктами господарювання, елементами інституційного середовища при створенні суспільних благ і послуг. Економічними інтересами є активи, які суб'єкти підприємництва під час або внаслідок взаємодії з державними структурами, іншими економічними агентами можуть втратити та зазнати через це збитків або фінансових витрат, істотного погіршення фінансово-економічного стану і результатів діяльності. Відповідно, метою державного регулювання системи забезпечення економічної безпеки підприємництва є розвиток його суб'єктів, покращення їх економічної ефективності та фінансової стійкості. Основними параметрами при цьому виступають умови господарювання, інституційне середовище, захист права приватної власності, захищеність майна та капіталу, доступ до ресурсів і ринків, відсутність корупції та державна підтримка. Досягнення поставленої мети потребує вирішення комплексу завдань та реалізації функцій безпеки, узгоджених між собою синергетичними властивостями і системоутворюючими елементами, дотримання принципів механізму функціонування та засобів управління. Передумовою належного формування політики економічної безпеки підприємництва з усіма її складовими елементами, спроможної забезпечити необхідну ефективність і життєздатність його суб'єктів є критерії системного підходу [1,с.113-137].

Сучасний стан економічної безпеки підприємництва в Україні можна охарактеризувати як незадовільний: економічні втрати суб'єктів бізнесу здебільшого пов'язані з отриманням дозволів на діяльність, погоджень державних структур, високим рівнем злочинності. Дестабілізують ситуацію також зміни законодавства, недосконалий

захист права приватної власності. Цим проблемам не приділяють необхідної уваги при державному регулюванні системи забезпечення економічної безпеки підприємництва у програмах підтримки підприємництва в Україні. Недоліками державного регулювання в цій площині також є недотримання таких принципів, як додержання балансу економічних інтересів особи, суспільства та держави; своєчасність та адекватність заходів із попередження загроз економічним інтересам суб'єктів бізнесу; недопущення монополізації. Внаслідок недостатньої ефективності стратегічного програмування розвитку підприємництва його показники в Україні ще не досягли рівня розвинених держав, а рівень економічної безпеки підприємництва залишається низьким [2].

Вітчизняна система стратегічного планування розвитку економічної безпеки підприємництва характеризується такими головними недоліками:

1) програми підтримки підприємництва стосуються лише сектору малого бізнесу, отже, не передбачають заходів сприяння розвитку усіх секторів підприємництва;

2) сталий перелік кількісних індикаторів оцінки результативності програмних заходів є неповноцінним;

3) обсяги фінансування програм підтримки підприємництва необґрунтовані, змінюються хаотично як на центральному, так і на регіональному та місцевому рівнях;

4) механізм державного програмування не передбачає належного моніторингу цього процесу [3].

Це об'єктивно доводить необхідність удосконалення стратегічного програмування покращення середовища для цього необхідно сформувати її повноцінний інституціональний базис. Оперативні заходи державної політики формування середовища економічної безпеки підприємництва в Україні необхідно здійснювати за основними напрямками – система оподаткування, ліцензування, державний нагляд у сфері господарської діяльності, інноваційна інфраструктура, фінансово-інвестиційне та техніко-технологічне забезпечення.

Пріоритетними напрямами та завданнями державної політики формування в Україні середовища економічної безпеки підприємництва є:

1) удосконалення інституціонального базису підприємництва;

2) розвиток і реалізація експортного потенціалу підприємств;

3) покращення інвестиційно-інноваційного клімату;

4) зміцнення фінансової, науково-технологічної, виробничої, екологічної безпеки підприємництва [4].

Для ефективного вирішення окреслених стратегічних завдань необхідно створити повноцінний інституційний базис, а операційні програмні засоби реалізації доцільно поєднати з посиленням найбільш загрозливих для безпеки характеристик підприємницького середовища.

1. Франчук В.І. Основи економічної безпеки / В.І. Франчук. – Львів:2008.– 203 с.

2. Моделювання економічної безпеки: держава, регіон, підприємство: Монографія / [за ред. В.М.Геєця]. – Х. : Інжек, 2006. – 240 с.

3. Механізми розвитку підприємництва в умовах посткризового відновлення економіки України: Аналітична доповідь / Д. С. Покришка, Я. А. Жаліло, Д. В. Ляпін, Я. В. Белінська [та ін.]. – К. : НІСД, 2010. – 72 с.

4. Поповіченко Ю. А. Державне регулювання системи забезпечення економічної безпеки сектору малого підприємництва: автореф. дис. к.е.н. за спец. 08.00.03 / Ю. А. Поповіченко;Львівський національний аграрний ун-т.– Львів, 2014. – 20 с.

Оскарження бездіяльності слідчого або прокурора, що полягає у невнесенні відомостей про злочин до ЄРДР

Столітній А.В.
к.ю.н., начальник відділу підготовки прокурорів з нагляду за додержанням законів органами, які проводять ОРД, дізнання та досудове слідство Національної академії прокуратури України
stoleta@ukr.net

Численними є випадки оскарження до слідчого судді у порядку ст. 303 Кримінального процесуального кодексу України (далі – КПК України) бездіяльності слідчого чи прокурора, що полягає у невнесенні відомостей про злочин до Єдиного реєстру досудових розслідувань (далі – ЄРДР), та постановлення слідчим суддею за результатами розгляду таких скарг ухвал про зобов'язання вчинити слідчому чи прокурору певну дію – внести відповідні відомості до ЄРДР.

Проте аналіз положень КПК України свідчить, що така практика не відповідає положенням вказаної норми закону з наступних підстав.

По-перше, правова колізія полягає у тому, що зазначена вище бездіяльність слідчого чи прокурора згідно з вимогами ст. 303 КПК України може бути оскаржена лише на досудовому провадженні, яке за правилами ст. 214 цього Кодексу розпочинається лише з моменту внесення відомостей до ЄРДР [1]. Іншими словами, оскарження такої бездіяльності відбувається поза межами кримінального провадження, тобто по суті не є можливим.

По-друге, мають місце випадки, коли особи оскаржують до слідчого судді зазначену вище бездіяльність слідчого, прокурора, у той час, коли безпосередньо останньому фактично не було доручено вирішувати заяву про злочин. Наприклад, у випадку відмови в тому чи іншому органі поліції працівником чергової зміни в прийнятті такої заяви або коли керівники поліції не уповноважували слідчого приймати по ній рішення у передбаченому ст. 214 КПК України порядку. Прикладом наведеного є справа № 621/2772/15-к від 21.10.2015. Згідно з копією талона-повідомлення, заява скаржника прийнята черговою частиною Зміївського РВ ГУМВС України в Харківській області. В ході судового розгляду встановлено, що розгляд вказаного звернення здійснював дільничний інспектор міліції (який не є слідчим чи прокурором). В судовому засіданні прийняли участь заступник начальника СВ Зміївського РВ ГУМВС України в Харківській області та прокурор, які не є слідчим та процесуальним керівником дії яких оскаржуються. За результатами розгляду скарги судом ухвалено зобов'язати керівника СВ Зміївського РВ ГУМВС України в Харківській області вчинити наступні дії: внести відомості про кримінальне правопорушення до ЄРДР та визначити слідчого, який здійснюватиме досудове розслідування; надати скаржнику витяг з ЄРДР за його заявою [3]. Тобто, суд, розглянувши заяву на дії дільничного інспектора міліції (не слідчого, не прокурора) за участі прокурора (який не є процесуальним керівником) та заступника начальника слідства (який не здійснює розслідування), зобов'язав начальника слідчого підрозділу вчинити певні дії, керуючись при цьому ст. 214, 303, 306, 307 КПК України, які передбачають оскарження рішень слідчого та прокурора.

У зв'язку з відсутністю, на даний час, передбаченого кримінальним процесуальним законодавством правового механізму оскарження поза межами кримінального провадження до слідчого судді бездіяльності, що полягає у невнесенні відомостей про злочин до ЄРДР, на нашу думку, більш правильним, до належного законодавчого врегулювання цього питання, оскаржувати таку бездіяльність у порядку,

передбаченому Кодексом адміністративного судочинства України (далі – КАС України).

До того ж, згідно з вимогами ч. 2 ст. 4, ст. 17 КАС України розгляд усіх публічно-правових спорів, крім спорів, для яких законом встановлений інший порядок судового вирішення, є юрисдикцією саме адміністративних судів (суд загальної юрисдикції, до компетенції якого цим Кодексом віднесено розгляд і вирішення адміністративних справ) [2].

Ураховуючи зазначене, пов'язану із невнесенням відомостей про злочин до ЄРДР бездіяльність органів досудового розслідування та прокуратури як суб'єктів владних повноважень, слід оскаржувати шляхом направлення до адміністративного суду (місцевий загальний суд як адміністративний суд або окружний адміністративний суд – за вибором позивача) адміністративного позову про зобов'язання відповідача прийняти рішення або вчинити певні дії, керуючись при цьому ст. 1, 2, 4, 6, ч. 3 ст. 18, ч. 3 ст. 50, ст. 104, 105, 106 КАС України.

Доцільно зазначити, що відповідно до п. 2 ч. 3 ст. 17 КАС України юрисдикція адміністративних судів дійсно не поширюється на публічно-правові справи, що належить вирішувати в порядку кримінального судочинства. Проте дане обмеження не може стосуватися оскарження бездіяльності, що полягає у невнесенні до ЄРДР відомостей про злочин з наведених вище підстав.

---

1. Кримінальний процесуальний кодекс України від 13 квітня 2012 року 4651-VI; зі змін. і доповн. // База даних «Законодавство України»/ ВР України. URL: http://zakon2.rada.gov.ua/laws/show/4651-17 (дата звернення: 19.10.2016).

2. Кодексом адміністративного судочинства України від 6 липня 2005 року № 2747-IV; зі змін. і доповн. // База даних «Законодавство України»/ ВР України. URL: http://zakon0.rada.gov.ua/laws/show/2747-15 (дата звернення: 19.10.2016).

3. Справа № 621/2772/15-к від 21.10.2015 // Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/ Review/52551326 (дата звернення: 19.10.2016).

Інформаційно-аналітичні заходи щодо визначення маркерів психологічного відбору працівників МВСУ.

Страхова О.П.
викладач Запорізького державного медичного університету
Каблуков А.О.
доцент, к.т.н., доцент Запорізького державного медичного університету

Швидке розуміння ситуації, охоплення усіх аспектів поставленої задачі, адекватне реагування – це ознаки доброї професійної підготовки працівника органів внутрішніх справ.

Відомо, що на якість виконання поставлених перед професійною особою завдань, швидкість відповідних реакцій особи, повноту осмислення поставленого перед нею завдання впливає психологічний стан цієї особи, а саме її ситуативна і особистісна тривожність.

Особистісна тривожність визначається типом вищої нервової діяльності, темпераментом, характером, вихованням і набутими стратегіями реагування на зовнішні чинники. Ситуативна тривожність більше залежить від поточних проблем і переживань. Дуже висока особистісна тривожність прямо корелює з наявністю невротичного конфлікту, психосоматичними захворюваннями [1].

Вивчення особливостей функціонування центральної нервової системи - провідної системи адаптації до факторів середовища – дозволяє оцінити вплив психологічного стану осіб на кінцевий результат їх праці і прогнозувати можливі реакції осіб на обставини що виникають у повсякденному житті і професійних ситуаціях.

Визначення станів тривожності осіб проводиться за допомогою тесту ситуативної та особистісної тривожності «Шкала самооцінки Спілбергера- Ханіна» [1,2]. Це – визнаний об’єктивний метод контролю психологічного стану людей. За допомогою цього тесту можна визначити тривожність, пов'язану з конкретною зовнішньою ситуацією, і тривожність як властивість особистості.

У Запорізькому медичному університеті проведено роботу, результати якої твизначили, що особистісна і ситуативна тривожність будь-якої людини знаходиться в прямій кореляційній залежності від стану її електрошкірних характеристик у певних ділянках, розташованих

на зап'ястках та щиколотках [3].. Поточні проблеми та переживання людини при її роботі впливають на ступінь зміни її функціонального станузмінюючи певним чином показники електрошкірних характеристик цієї особи.

Оскільки рівень особистісної тривожності показав високу кореляцію зі зміною електрошкірних параметрів, а сама особистісна тривожність визначається типом вищої нервової діяльності, темпераментом, характером, вихованням і набутими стратегіями реагування на зовнішні чинники [1], люди з відповідними перерахованими ознаками сильніше схильні до змін функціонального стану. Значні зміни погіршують якість відповідних реакцій особи на виклики професійних ситуацій, що здатно призвести до негативних наслідків як для цієї особи, так і виконуваної нею справи в цілому.

Отже, перевірка електрошкірних характеристик осіб на етапі проведення професійного відбору дозволить уникнути зайвих витрат часу на підготовку осіб що не відповідають професійним вимогам працівників МВСУ, і відповідно зкоригувати напрями професійної підготовки здатних осіб, з метою підвищення їх кваліфікації.

1. Єна А. І. Система професійного психофізіологічного відбору працівників, які виконують роботи підвищеної небезпеки: дис. д.мед. н. / А.І. Єна. – Київ, 2004. –376 с.
2. Судаков К.В. Нормальная физиология. Ситуационные задания и тесты. – М: МИА. – 2006.– 247 с.
3. Страхова О. П. Ситуативная и личностная тревожность студента в эргатической компьютерной обучающей системе / О. П. Страхова // Медична інформатика та інженерія. - 2015. - № 1. - С. 33–38.

Використання сучасних інструментальних засобів взаємодії поліції з населенням

Узлов Д.Ю.
к.т.н, начальник Управління інформаційно-аналітичної підтримки Головного управління Національної поліції в Харківській області
Струков В.М.
доцент, к.т.н, завідувач кафедри інформаційних технологій факультету № 4 Харківського національного університету внутрішніх справ

Проблеми ефективності взаємодії поліції з населенням, оцінки якості діяльності окремо взятих поліцейських, категорій правоохоронців, поліцейських підрозділів і служб різного територіального рівня, включаючи центральний є актуальними в усіх країнах світу. Особливо гостро ці питання постали після того, як Україна взяла курс на входження до Європейського співтовариства і, відповідно, прихильність демократичним принципам роботи правоохоронних органів і європейським підходам до взаємодії з населенням та оцінці діяльності поліції, з огляду на те, що основна функція поліції - сервісна - забезпечення і захист прав і свобод громадян. Зазвичай взаємодія підрозділів поліції з населенням здійснювалося шляхом: прийому заяв громадян в письмовому вигляді в черговій частині або у дільничного інспектора, прийому телефонних повідомлень і заяв в службу 102 і на телефони довіри, а також за допомогою передачі письмових повідомлень через поштовий ящик довіри. Якість роботи підрозділів міліції оцінювалося за кількісними показниками, такими як розкриваємість злочинів, загальна кількість злочинів різного виду, кількість злочинів на душу населення і іншими, які не завжди відображають реальний стан злочинності в регіоні і ефективність діяльності поліції щодо виконання своїх основних соціальних функцій. До того ж ця інформація, як правило, доступна лише вузькому колу керівників. Разом з тим багато і часто говорилося про те, що назріла необхідність переходити до інших способів і механізмів взаємодії з населенням та оцінки діяльності міліції з упором на оцінку населення. Джерелами інформації для населення про діяльність поліції в основному були ЗМІ - періодична преса, радіо, телебачення і в останні роки - інтернет-джерела, які в основному

надають інформацію в тому ж стилі, що і ЗМІ. Ступінь інформованості населення про діяльність поліції - на рівні популізму і говорити про якусь навіть можливості об'єктивної або суб'єктивної оцінки діяльності поліції з боку населення не доводилося. За відсутності повної і об'єктивної інформації про роботу поліції, громадяни просто не мають можливості давати таку оцінку. В цьому контексті представляє безперечний інтерес досвід поліції Грузії з прозорими стінами і перегородками в будівлях і приміщеннях поліцейських підрозділів.

Другим найважливішим моментом в контексті проблеми, що розглядається, є сама можливість здійснити таку оцінку і донести її до споживача, тобто до керівництва конкретного поліцейського підрозділу або відомства. Причому така можливість повинна забезпечуватися якомога простішим, легким і доступним способом, що допускає автоматизовану реєстрацію, зворотний зв'язок з звернулися і подальшу обробку, в іншому випадку вона не буде затребувана.

Авторам не відомі існуючі дотепер кошти і технології взаємодії поліції з населенням, які в повній мірі задовольняють перерахованим умовам.

ІТ-фахівцями Харкова спільно з співробітниками Управління інформаційно-аналітичної підтримки Головного управління Національної поліції в Харківській області розроблено інноваційний підхід, реалізований на сучасних веб-технологіях, у вигляді веб-порталу www.police.kh.ua, який забезпечує можливість переходу поліції до взаємодії з населенням на абсолютно нових, сучасних принципах, що відповідають європейським вимогам.

Портал забезпечує виконання наступних функцій: 1) інформування громадськості про стан злочинності в обслуговуваному регіоні (в даному випадку - в Харківській області), 2) реалізація зворотного зв'язку з населенням.

До першої групи функцій відносяться такі:

• відображення на географічній карті місцевості всіх реєстрованих поліцією злочинів, включаючи розкриті і нерозкриті, із забезпеченням можливості вибору: а) одного або декількох видів злочинів; б) цікавить району (або районів) Харкова або Харківській області; в) цікавить проміжку часу (за останній день, тиждень, місяць та ін;

• відображення на географічній карті місцевості ділянок концентрації всіх реєстрованих поліцією злочинів із забезпеченням можливості вибору: а) одного або декількох видів злочинів; б) певного

району (або районів) Харкова або Харківській області; в) проміжку часу (за останній день, тиждень, місяць та ін.);

• відображення на географічній карті місцевості всіх доступних відеокамер з можливістю перегляду в on-line режимі в реальному часі ситуації в спостережуваному даної відеокамерою (або декількома відеокамерами одночасно) ділянці місцевості;

Ця можливість цікава тим, що дозволяє: а) спостерігати розвиток ситуації під час масових заходів у реальному часі; б) зацікавленим особам (наприклад, родичам) спостерігати ситуацію в реальному часі в місці знаходження спостережуваних осіб (наприклад, дітей або інших близьких родичів);

• відображення на географічній карті місцевості розташування всіх дільничних інспекторів з можливістю перегляду їх контактної інформації та зон їх обслуговування (списку будинків);

• можливість перегляду списку всіх злочинців, які перебувають в даний момент в розшуку, а також осіб, зниклих без вісті;

До функцій реалізації зворотного зв'язку відносяться:

• можливість будь-якому громадянину відправити повідомлення про правопорушення, про яке-небудь небезпечному предмет і ін. по Інтернету з прикріпленням файлу з фотозображенням або відео описуваної події або предмета;

• можливість оцінки ефективності діяльності поліції в режимі інтерактивного опитування (в перспективі).

Кібербезпека як складова частина системи забезпечення національної безпеки України

Байдуж Ю.І.
слухачка магістратури юридичного факультету ДДУВС
Косиченко О.О.
науковий керівник , к.т.н., доцент кафедри економічної та інформаційної безпеки ДДУВС

В умовах глобалізації інформаційних процесів, їх інтеграції в різні сфери суспільного життя, керівництво провідних країн приділяє посилену увагу створенню та удосконаленню ефективних систем захисту власного інформаційного простору від зовнішніх та внутрішніх загроз кібернетичного характеру. Так, у процесі розвитку високих технологій

виникло принципово нове середовище – кіберпростір, що формується із соціальної, технічної, телекомунікаційної, інформаційної, мережево-комп'ютерної складової. Кіберпростір одночасно виступає як суб'єкт та об'єкт впливу. Сучасна успішна геополітика неможлива без стійкого домінування у кіберпросторі. Кіберборотьба набула стратегічного управлінського спрямування. Вона проводиться без міжнародних правових обмежень у просторі та часі і характеризується високою ефективністю щодо досягнення воєнно-політичної мети. Все більш вирішальним чинником досягнення успіху у світовому протиборстві стає інформаційно-технічна дезорганізація систем державного і воєнного управління та інформаційно-психологічна деморалізація населення країн, насамперед складу їх збройних сил.

Під кібербезпекою розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави в кіберпросторі. При цьому важливо визначити, що собою являє кіберпростір, адже кібербезпека є його складовою частиною. Так, кіберпростір - це середа, яка виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем.

Діяльність із формування системи забезпечення національної безпеки України була невід'ємною складовою і чинником державотворчих процесів із початку виникнення незалежної України. Вже в Декларації про державний суверенітет України (16 липня 1990 р.) питання безпеки розглядалися в розділах «Зовнішня і внутрішня безпека», «Міжнародні відносини», «Екологічна безпека». Питання внутрішньої та зовнішньої безпеки аналізуються через призму права України на власні збройні сили, власні внутрішні війська та органи державної безпеки.

Система національної безпеки будь-якої країни базується на концептуальних нормативно-правових документах, у яких викладаються офіційні погляди на роль і місце держави у світі, її національні цінності, інтереси й цілі, способи й засоби запобігання зовнішнім і внутрішнім небезпекам і загрозам. Система кібернетичної безпеки – сукупність узгоджених за завданнями елементів кібернетичної безпеки, які комплектуються та розгортаються за єдиним замислом і планом в кібернетичному просторі для забезпечення кібернетичної безпеки інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем. Розвиток національної системи кібербезпеки повинен супроводжуватись відповідними корективами у

процесі реформування сфери національної безпеки, а функціонування вказаної системи є неможливим без тісної співпраці з приватним сектором.

Кіберпростір характеризується відсутністю кордонів, динамікою і відносною анонімністю. Забезпечення безпеки в кіберпросторі повинно бути організовано на конституційному рівні.

Останнім часом воєнно-політичне керівництво України здійснює комплекс заходів щодо підвищення ефективності та поліпшення координації діяльності своїх силових структур у сфері кібернетичної безпеки. Війна в кіберпросторі спричиняє нові кіберзагрози. Конкретні загрози в кібербезпековому просторі носять розширений, динамічний і глобальний характер, що ускладнює їх виявлення та реалізацію заходів протидії. Глобальність кіберпростору збільшує його потенційні ризики.

Таким чином, в Україні існують наступні загрози інформаційній безпеці: ведення інформаційної війни проти нашої держави; відсутність цілісної комунікативної політики держави, недостатній рівень медіа-культури суспільства. Загрози кібербезпеці і безпеці інформаційних ресурсів: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом.

Причинами виникнення постійних інформаційних загроз, безумовно є використання злочинцями людського фактору та вразливість технічних засобів у різних сферах приватного та державного секторів, які обумовлюють сферу національних інтересів.

З метою протидії цим загрозам необхідним є створення та ефективне функціонування національної системи кібербезпеки як складової системи забезпечення національної безпеки України.

Отже, забезпечення належного рівня кібернетичної безпеки є необхідною умовою розвитку інформаційного суспільства. Очевидною є необхідність створення Національної системи кібербезпеки. Одним із ключових питань організації ефективної роботи якої залишається налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, здійснення координації такої діяльності та забезпечення превентивної та попереджувальної діяльності у кіберпросторі.

Інтернет речей: проблеми безпеки

Безрук Є.А.
студент кафедри захисту інформації
Запорізького національного технічного університету
Брусенський В.Р.
студент кафедри захисту інформації
Запорізького національного технічного університету
Куцак С.В.
науковий керівник, старший викладач кафедри захисту інформації
Запорізького національного
технічного університету

В даному дослідженні розглянуті три ключові вимоги безпеки з акцентом на системи Інтернету речей: автентифікація, конфіденційність, масштабованість.

Інтернет речей (Internet of Things, IoT) - динамічна глобальна мережна інфраструктура з можливістю самонастроювання на основі стандартних і сумісних протоколів зв'язку, де фізичні та віртуальні «речі» мають ідентифікатори, фізичні атрибути, використовують інтелектуальні інтерфейси та інтегруються в інформаційну мережу [1].

З логічної точки зору, система IoT може бути представлена як сукупність спільно взаємодіючих інтелектуальних пристроїв. З технічної точки зору, IoT може використовувати різні шляхи обробки даних, комунікації, технології та методології, ґрунтуючись на їх цільове призначення.

Основні проблеми пов'язані з безпекою IoT:

1. Високий рівень неоднорідності в поєднанні з широкою гамою систем IoT збільшило число загроз безпеки власників пристроїв, які все частіше використовуються для взаємодії людей, машин і речей в будь-який варіації.

2. Традиційні заходи забезпечення безпеки і дотримання конфіденційності не можуть бути застосовані до технологій IoT, зокрема, через їх обмежену обчислювальну потужність.

3. Велика кількість підключених пристроїв породжує проблему масштабованості. У той же час для досягнення визнання з боку користувачів необхідно в обов'язковому порядку забезпечити

дотримання безпеки, конфіденційність і моделі довіри, які підходять для контексту IoT.

4. Довіра (надійність, англ. Trust) – це основна проблема, оскільки IoT-середовище характеризується різними типами пристроїв, які повинні обробляти дані відповідно до потреб і правами користувачів.

5. Проблеми пов'язані з контролем доступу в сценарії IoT.

Для підвищення захищеності IoT використовується:

– Автентифікація. Передбачають використання налаштування користувачем механізму інкапсуляції, а саме протокол прикладного рівня для IoT під назвою - «інтелектуальна служба забезпечення безпеки» (англ. Intelligent Service Security Application Protocol). Він поєднує в собі крос-платформні зв'язку з шифруванням, підписом і автентифікації для підвищення ефективності розробки додатків IoT шляхом створення системи захищеного зв'язку між різними речами.

Підхід, який усуває проблему автентифікації зовнішніх потоків даних з використанням безперервної перевірки автентичності в потоках даних (англ. Continuous Authentication on Data Streams, CADS) [2], тут передбачається наявність постачальника послуг, який збирає дані від одного або декількох власників разом з інформацією автентифікації і при цьому одночасно обробляє запити багатьох клієнтів. Постачальник послуг повертає клієнтам результати запитів, а також інформацію про перевірку, що дозволяє їм перевірити справжність і повноту отриманих результатів на основі інформації автентифікації, наданої власником даних.

– Конфіденційність і цілісність. Існуючі системи управління ключами можуть бути застосовані в контексті IoT. Це дозволяє класифікувати протоколи систем управління ключами (англ. Key Management System, KMS) [3] за чотирма основними категоріями: структура пулу ключів, математична база, механізм взаємодії і структура відкритого ключа.

– Вимоги до обчислювальної потужності. Метод перевірки автентичності і контроль доступу, спрямований на створення ключа сеансу із застосуванням еліптичної криптографії (англ. Elliptic Curve Cryptography, ECC) [4].

– Довіра. Потрібно звернути увагу також на аутсорсинг (використання зовнішнього джерела або ресурсу, англ. Outsourcing) даних. Через велику кількість потокових даних компанії можуть не купувати ресурси, необхідні для розгортання систем управління потоками даних (англ. Data Stream Management Systems, DSMS). Постає

питання довіри: третя особа може діяти зловмисно, наприклад, з метою збільшення свого прибутку. Рішення полягає в тому, що метод прийнятий так, для автентифікації потоку, що клієнти можуть перевіряти цілісність і актуальність отриманих від сервера даних. При цьому метод задовольняє вимогам IoT пристроїв, що характеризуються обмеженими ресурсами з точки зору енергоспоживання, обчислювальної потужності і захисту пристроїв.

Проведений аналіз безпеки інтернет речей показує, що поширення послуг IoT вимагає гарантування автентифікації, масштабованості, конфіденційності, сумісності та відповідності протоколам безпеки. Він проливає світло на напрямки досліджень в області поширення IoT.

1. Internet of Things Global Standards Initiative [Електронний ресурс]: – Режим доступу: http://www.itu.int/en/ITU-T/gsi/iot/Pages/default.aspx.

2. S. Paradopulus, Y. Yang, D. Papadias, Continuous authentication on relational data streams, VLDB Journal, 2010, Vol. 19, №1, pp.161-180.

3. Understanding KMS [Електронний ресурс]: – Режим доступу: https://technet.microsoft.com/ru-ru/library/ff793434.aspx.

4. elliptical curve cryptography (ECC) [Електронний ресурс]: – Режим доступу: http://searchsecurity.techtarget.com/definition/elliptical-curve-cryptography.

Підготовка фахівців для боротьби з кіберзлочинністю в Україні

Бобик М.В.
курсант групи ПС – 541 факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Рижков Е.В.
науковий керівник, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент

В наш час комп'ютерні злочини є поширені оскільки технології розвиваються і люди не сидять на місці. Це залежить від прискореного

розвитку технологій й науки у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Історія навчила нас, що розвиток і прогрес, які приносять людям нові блага та можливості, на жаль, завжди супроводжуються негативними явищами. Також масова комп'ютеризація, і стрімкий розвиток цифрових технологій, які максимально спростили людині всі технологічні та виробничі процеси, полегшили її існування та перевернули уявлення про роботу, кар'єру, дозвілля, фінанси і навіть особисте життя, приховують у собі серйозні небезпеки[1].

Неможливо сьогодення уявити без нових інформаційних технологій ,в потребі яких полягає широке використання комп'ютерної техніки та новітніх засобів комунікації. Більшість функцій суспільства пов'язані з комп'ютерами, інтернет - мережами та комп'ютерною інформацією.

Популярність Інтернету невипадкова, адже він забезпечує цілодобовий доступ до величезної кількості інформації, швидку передачу даних, можливість проведення банківських, торгових, біржових операцій, переказ коштів і багато іншого. Інтернет – це чудовий засіб для зв'язку та спілкування. Для багатьох людей він став цілим світом, віртуальним світом. Як і в реальному світі, так і в віртуальному, де панує комп'ютерна інформація, трапляються, злочини, кіберзлочини. Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем - це далеко не повний перелік подібних злочинів [1].

На сьогодні Україна не стоїть на місці а просувається вперед в підготовці фахівців для боротьби з кіберзлочинністю :

-у березні 2016 року уряд прийняв Стратегію кібербезпеки України, яка має на меті створення національної системи кібербезпеки;

-у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки. Першим етапом його роботи є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки.

-у вересні 2016 року Верховна Рада України у першому читані прийняла закон про основні засади забезпечення кібербезпеки України[3].

- починаючи з 2016 року Харківський національний університет внутрішніх справ здійснює підготовку фахівців з вищою освітою для

підрозділів Національної поліції України, що займаються протидією кіберзлочинності, злочинам у сфері торгівлі людьми та моральності, у міжнародній сфері та транснаціональній злочинності [4].

-17 березня 2017 року відбулося підписання Меморандуму про співпрацю між Державною службою інтелектуальної власності (ДСІВ) та Національною академією внутрішніх справ (НАВС). Одним із перспективних напрямів подальшої співпраці сторони вважають реалізацію Проекту з підготовки фахівців по боротьбі з кіберзлочинністю. Створення на базі Національної академії внутрішніх справ курсів з підготовки правоохоронців за спеціалізацією, що спрямована на захист прав інтелектуальної власності, стане платформою для розробки нової освітньої програми, за якою відбуватиметься навчання правників нової генерації, покликаних захистити інноваційний потенціал України.

До підготовки українських спеціалістів вже висловили готовність долучитися міжнародні експерти урядових та громадських структур, які безпосередньо здійснюють боротьбу з кіберзлочинністю. Курси розраховані на правоохоронців системи МВС, СБУ, фіскально-митних органів і Державної служби спеціального зв'язку, в обов'язки яких входить захист прав інтелектуальної власності, боротьба з кіберзлочинністю[2] .

Отже, на нашу думку просування в розвитку в підготовці фахівців для боротьби з кіберзлочинністю є важливою функцією в Україні, так як з кожним роком суспільство рухається в науці, техніці, збільшуються злочини, кіберзлочини прогресують у всіх сферах суспільного життя.

Тож протидія кіберзлочинності та рівень кібербезпеки на сьогодні одним із пріоритетних напрямків в політиці країни. Але для комплексної боротьби з цією проблемою потрібні спільні зусилля держави, громадян та міжнародної спільноти[3].

1.[Електронний ресурс]. - Режим доступу: https://www.science-community.org/ru/node/16132

2.[Електронний ресурс]. - Режим доступу: http://nk.org.ua/ tekhnologii/pidgotovka-fahivtsiv-po-borotbi-z-kiberzlochinnistyu-ta-piratstvom-93239

3.[Електронний ресурс]. - Режим доступу: https://www.gurt.org.ua/ articles/34602

4. [Електронний ресурс]. - Режим доступу: http://univd.edu.ua/dir/ 589/fakultet--4

Проблеми фінансової та економічної безпеки

Василина О.Н.
здобувач ДДУВС
Махницький О.В.
науковий керівник, старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Фінансова безпека країни — багаторівнева система, яка утворює низу підсистем, кожна з яких має власну структуру і логіку розвитку. Безпека внутрішньої фінансової сфери України визначається досконалістю правової, організаційної та інституціональної бази, а також політичною стабільністю, рівнем ризиків ринкової кон'юнктури, масштабами тіньової економіки та рівнем корупції в державі. Фінансова безпека відіграє важливу роль у економіці в цілому, адже кожен її недолік буде негативно відображатися на підприємствах і населенні. Суб'єктами фінансової безпеки виступають: Держава, населення, підприємства, регіони, та інші. Фінансову безпеку держави визначають такі фактори: - Рівень законодавчого забезпечення функціонування фінансової сфери;- Рівень фінансової незалежності; - Політичний клімат у країні; Загрози фінансовій безпеці України – наявні та потенційно можливі явища і чинники, що створюють суттєву небезпеку національним фінансовим інтересам.

Фінансова безпека підприємства — основна складова економічної безпеки, нормальне її функціонування на підприємстві забезпечує йому економічну стабільність і надає можливості для розвитку інших галузей. Для кожного типу підприємств потрібні свої методи та засоби забезпечення фінансової безпеки, щоб слідкувати за економічною ситуацією, та забезпечувати реалізацію захисних заходів на підприємстві, створюються спеціальні підрозділи служби безпеки. Сучасний світ розвивається дуже швидко і поряд із розвитком медицини, науки, нових технологій, ми можемо побачити виникнення все нових і нових проблем, в тому числі і економічних, через нестабільну економічну ситуацію і збільшення криміналізації населення, питання фінансової безпеки в Україні стоїть особливо гостро.

Головні загрози фінансовій безпеці підприємства:

- Нестабільність економіки;
- Ріст боргів;
- Недостатня кількість коштів на рахунку підприємства;
- Зниження ринкової вартості підприємства;
- Форс-мажорні обставини;

Важливу роль у розвитку підприємства грає професіоналізм менеджменту, його чіткі дії і самовіддача можуть привести підприємство до успіху, але в той же час некомпетентність менеджменту можна віднести до основних загроз.

Фінансова безпека банків: Фінансова безпека банків, це важлива складова економічною безпеки країни, в банках зберігаються як кошти простого населення, так і професійних учасників фінансового ринку, тому заходам що до покращення безпеки банківської системи і приділяється багато уваги. Зараз в Україні склалася така ситуація при якій люди не можуть довіряти банкам, адже велика їх кількість закрилася. Національний банк України, на чолі з Гонтаревою Валерією Олексіївною з початку 2014 року вивели з ринку 81 банк, їх головною ідеєю було зменшення ризиків, та збільшення надійності банків, кожен банк повинен був збільшити свій капітал до 300 мільйонів гривень, якщо банку не вдасться це зробити, його ліквідують. На думку економічного експерта Андрія Новака, таким чином пограбували економічно активну частину українців - представників малого та середнього бізнесу або висококооплачуваних фахівців, в яких на депозитах лежали суми понад 200 тисяч гривень. Тому, вважає Новак, так зване "оздоровлення", яке супроводжується виведенням капіталу за межі України їх власниками, - це елемент не дуже швидкої, але величезною наживи. Взагалі рішення Гонтаревої В.О були дуже спірними, починаючи від політики "вільного плавання" курсу гривні, яка призвела до девальвації, і до методів ліквідації неплатоспроможних банків. Голова Комітету економістів України А. Новак вважає, що саме дії українського уряду та Нацбанку призвели до погіршення економіки, і це знайшло відображення у прогнозі МВФ. А. Новак зазначає: «Погіршення прогнозу МВФ щодо української економіки означає, що МВФ бачить падіння ВВП не лише через війну, а й через дії уряду. Кабмін оголосив політику затягування поясів, тобто замороження зарплат і пенсій, і цим самим він зменшив купівельну здатність українців, що призводить лише до подальшого падіння економіки. А треба діяти з точністю до навпаки: має бути контрольована емісія для підвищення виплат. Щось подібне українська

влада робила у 2000 році, тоді це справді поліпшило економічну ситуацію. В нас емісія є і досить суттєва, але вона витрачається передовсім на рефінансування банків. Тобто маємо не просто погіршення економіки через війну, маємо рукотворну економічну кризу».

1. [Електронний ресурс]. – Режим доступу: http://iac.org.ua/kompleksna-otsinka-ekonomichnoyi-situatsiyi-v-ukrayini-u-2014-2015-rr-chastina-1-zagalna-otsinka-makroekonomichnoyi-situatsiyi/
2. [Електронний ресурс]. – Режим доступу: https://knowledge.allbest.ru/finance/3c0a65635b3bd69a5c43a88521316c36_0.html
3. [Електронний ресурс]. – Режим доступу: https://www.radiosvoboda.org/a/27048902.html

Інноваційні методи підготовки майбутніх правоохоронців

Джараєва А.А.
студентка групи ЮД-642, другого курсу
юридичного факультету ДДУВС
Рижков Е.В.
науковий керівник, завідувач кафедри економічної та
інформаційної безпеки, к.ю.н, доцент

Стрімкий розвиток сучасного суспільства спирається на високорозвинені технології, що висувають чимдалі складніші вимоги до людини як їх суб'єкта. Саме тому початок XXI сторіччя зумовлений переходом від індустріального суспільства – до суспільства інформаційного. Всі ми знаємо, що навколо нас з кожним днем з'являється все більше і більше інноваційних розробків, і здається, що прилади здатні повністю замінити людство! Але чому не скористатися такою можливістю, розвитку та створити тандем штучного інтелекту та людини задля благих цілей: допомоги людям та використовувати це у правоохоронній діяльності.

Але нажаль, людство не може увібрати всю інформацію щодо інновацій у світі яка з'являється з дуже великою швидкістю. Здається що не по днях, а по годинах у світі з'являється щось нове: інноваційні винаходи, нові гаджети, прилади, що виконують певну роботу за людей.

Що потрібно для того, щоб взяти з цієї величезної купи інновацій ті, які реально зможуть використовувати правоохоронці, та відфільтрувати корисні для суспільства від чергових забаганок для розваг? Перш за все, потрібні кваліфіковані фахівці які зможуть виконати фільтрування та навчать цьому майбутніх правоохоронців.

Далі мова піде саме про ці технології, які пройшли це фільтрування, та вже сьогодні використовуються для навчання майбутніх правоохоронців захищати суспільство.[1] По-перше, це повинні бути комплексні методи, які включають в себе елементи інформаційних технологій, тренінги, які допоможуть використовувати їх на практиці.

Прикладом яким, являється оперативно-тактичні навчання "Лінія-102". [2] Це являє собою форму практичного навчання здобувачів вищої освіти. Запроваджується він, як різновид позанавчальної роботи з курсантами та студентами випускних курсів ДДУВС. В процесі навчань, забезпечується міждисциплінарна взаємодія усіх кафедр університету. Метою навчань є саме підвищення практичної складової навчального процесу підготовки фахівців для підрозділі Національної поліції та фахівців юристів. У процесі навчань, учасники засвоюють комплекс практичних заходів працівників різних підрозділів поліції. Інноваційність цих навчань, полягає саме в елементах інформаційних технологій, які вперше використовуються максимально наближено до реальних умов у навчанні: робоче місце чергового забезпечується окремою телефонною лінією, за допомогою 3G протоколу, планшету та мультимедійної апаратури забезпечується відео-зв’язок групи документування зі штабом, патрульна поліція та слідчо-оперативна група забезпечена спеціальними транспортними засобами та засобами зв'язку, робочий кабінет слідчого обладнується спеціалізованим програмно-апаратним комплексом "ЄРДР".

Саме таким способом, учасники навчань закріплюють набуті процесуальні знання на практиці, та навчаються використовувати інноваційні технології у дії, що допомагає засвоїти нові та корисні технології для легшої та продуктивнішої праці.

---

1. Сервіс "102": у Нацполіції розповіли про роботу системи "ЦУНАМІ" та навчання операторів екстреної служби. [Електронний ресурс] - Режим доступу: https://www.5.ua/suspilstvo/servis-102-u-natspoltsii-rozpovily-pro-robotu-systemy-tsunami-ta-navchannia-operatoriv-ekstrenoi-sluzhby-125248.html

2. У ДДУВС розробили комплексно-оперативні заняття «Лінія 102» [Електронний ресурс] - Режим доступу: http://dduvs.in.ua/2016/12/08/u-dduvs-rozrobyly-kompleksno-operatyvni-zanyattya-liniya-102/

Вплив тіньової економіки на безпеку держави

Димитрієва О.Д.
студент 1 курсу
спеціальність «Менеджмент», ДДУВС
Соломіна Г.В.
науковий керівник, к.е.н., доцент кафедри
економічної та інформаційної безпеки ДДУВС

Економічна безпека держави представляє собою захист національних економічних і соціальних інтересів держави і суспільства на основі досягнення стабільного стану економіки; захист їх від впливу несприятливих внутрішніх і зовнішніх факторів. Під останніми розуміють джерела небезпеки та загрози, що пов'язані з інтересами держави та індивідуума.

Найважливішою загрозою економічній безпеці країни є наявність тіньової економічної діяльності, значне збільшення її обсягів, ускладнення її видів. Тому актуальним є питання щодо визначення напрямів впливу чинників тіньової діяльності на економічну безпеку.

Тіньова економіка достатньо стародавнє явище, що виникло з розвитком суб'єктів господарювання. Її складовими є сектори – це структурно-логічний метод поділу тіньової економіки на неофіційний, прихований і підпільний (кримінальний) сектори. Неофіційний (свідомо невраховуваний державою) сектор тіньової економіки – сукупність соціально-нейтральних та соціально-позитивних неоподатковуваних джерел доходів громадян, отримуваних від невраховуваних і неоподатковуваних державою видів економічної діяльності. Щодо прихованої економіки, до якої належить легальна, але офіційно не показана, то тут існує можливість прискореного накопичення капіталу з метою ведення прихованого бізнесу, тому політика у сфері безпеки має спрямовуватися на реформування податкової системи з метою створення більш вигідних умов та реформування системи соціального захисту.

Практика засвідчує, що держава впливає на економічний розвиток, реалізуючи бюджетну, податкову, грошово-кредитну тощо політику. А дослідивши механізми взаємодії тіньової економіки з легальною економікою, можна впевненіше здійснювати політику детінізації. Найнебезпечнішою є підпільна (кримінальна) економіка, яка має злочинний, а відтак, виключно деструктивний характер. Небезпека її розвитку полягає у звужені офіційного сектору економіки, змушеному банкрутстві значної частини підприємств; неконтрольованому поширенні позаправових відносин, корумпованості, захопленні політичної влади кримінальними елементами; формуванні фінансової олігархії; розпаді бюджетної системи, зростанні державного боргу; неконтрольованому переміщенні капіталів за кордон.

Специфічною формою прояву тіньової економіки в Україні останнім часом стало рейдерство – силове захоплення або поглинання підприємств. Мета рейдерства полягає у перерозподілі нерухомості, а тому воно приносить значні прибутки загарбникам.

Ситуація в Україні, відносно рейдерства набула системного та загальнонаціонального характеру. На думку членів Антирейдерського союзу підприємців України, така ситуація стала можливою через бездіяльність законодавчої, виконавчої та судової влади щодо усунення рейдерської загрози та відсутність рішучих дій із захисту прав власників.

Крім рейдерства, виразним виявом підпільної економіки є корупція – одна з найбільших економічних небезпек в Україні. У широкому розумінні корупція є складним соціально – економічним явищем, що виникає в процесі реалізації тіньових економічних відносин між посадовими особами та іншими суб'єктами з метою задоволення особистих інтересів через комерціалізацію суспільних благ і цінностей. У вузькому розумінні корупція – це комерціалізація посадовими особами своїх функціональних обов'язків.

Дослідження тіньової економіки в Україні стає актуальним як з точки зору оцінки ефективності проведення реформ у цій сфері, так і з точки зору становлення відповідного інституту, в частині її адекватності реальним процесам.

Таким чином, процес детінізації економіки потребує постійного вдосконалення законодавчої, організаційної та управлінської бази, що дозволить вийти на новий рівень ведення бізнесу та розвивати міжнародні відносини.

1. Кіржецький Ю. Методичні основи дослідження тіньової економіки в контексті економічної безпеки регіону / Р.Й. Чайковський // Вісник Львівського університету. – 2008. – № 40. – С. 327-330.

2. Тіньова економіка в Україні: причини та шляхи подолання.- Електронний ресурс. - Режим доступу icps.com.ua/assets/uploads/.../t_novaekonom_kaukra_ni.pdf.

3. Тенденції тіньової економіки. - Електронний ресурс. - Режим доступу http://www.me.gov.ua/Documents/List?lang=uk-UA&id=e384c5a7-6533-4ab6-b56f-50e5243eb15a&tag=TendentsiiTinovoiEkonomiki

Проблеми захисту персональних даних користувачів мережі Інтернет

Задоя В.Є.
студентка 2 курсу ЮД-643 ДДУВС
Косиченко О.О.
науковий керівник, кандидат технічних наук, доцент кафедри економічної та інформаційної безпеки ДДУВС

В двадцятому столітті в наше життя увірвалися перші комп'ютери, інформаційні технології, як наслідок тотальне підкорення людей.

На сучасному етапі двадцять першого століття всі сфери суспільного життя охоплені і неможливі без застосування комп'ютерних технологій, мережі «Інтернет», мобільних телефонів, соціальних мереж.

Проблеми захисту персональних даних присвятили свої роботи А. Пазюк, В. Головченко, Л. Чернишевський, П. Макушев, О. Оніщенко, І. Сенюта.

Прогрес має дві сторони: позитивна – полягає в тому, що життя людини з появою нових технологій набагато стало простішим, ми переходимо від тих часів коли для того аби написати або прочитати щось потрібно йти до бібліотеки сідати в читальному залі і переписувати від руки інформацію, яка тобі потрібна, ми можемо спілкуватися з друзями або знайомими які знаходяться за сотні або навіть і тисячі кілометрів, ми можемо вільно купувати, замовляти, продавати будь які товари в Інтернет мережі. Негативна сторона – полягає в тому, що багато правопорушень вчиняється за допомогою мережі Інтернет. На даний момент питання захисту персональних даних активно розглядається як на національному так і на міжнародному рівні. Це викликало велику

кількість кібрзлочинів по відношенню до суб'єктів всіх міжнародних відносин. Це питання зацікавило: ООН, Європейський Союз, Раду Європи, МОН. У перше питання захисту прав особи прозвучало в Загальній декларації прав людини, прийнятої Генеральною Асамблеєю ООН і підписаною 10 грудня 1948р. У декларації йшлося про те, що ніхто не може зазнавати безпідставного втручання в його особисте, сімейне життя, безпідставно посягати на недоторканність його житла, таємного його кореспонденції або на його честь і репутацію. У 1973 р. УРСР ратифікувало ц. декларацію. Згодом у Конвенції про захист прав людини і основоположних свобод, яка набула чинності 11 вересня 1997 р. було зазначено, що «Кожен має право на повагу до свого приватного і сімейного життя, до свого житла і кореспонденції. Органи державної влади не можуть втручатись у здійснення цього права, за винятком випадків, коли втручання здійснюється згідно із законом і є необхідним у демократичному суспільстві, в інтересах національної та громадської безпеки чи економічного добробуту країни, для запобігання заворушенням чи злочинам, для захисту здоров'я чи моралі або для захисту прав і свобод інших осіб».

В ст. 32 Конституції України зазначено, що «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини».

Відповідно до ст. 2 ЗУ «Про захист персональних даних», «Персональні дані - відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована».

Основними ознаками персональних даних є: відомості чи сукупність відомостей; про фізичну особу; фізична особа; ідентифікована або конкретно ідентифікована.

Головною проблемою пов'язаною з мережею інтернет це автоматичний обмін з віддаленими серверами персональними даними. Тобто, під час підключення до мережі, користувач автоматично реєструється в мережі оприлюднюючи в наслідок чого свої персональні данні: IP-адрес, телефонний номер комутованого з'єднання, абонентський телефон. Після відвідування різноманітних сайтів, сторінок особа залишає за собою інформаційний шлейф.

Серед основних порушень в мережі Інтернет є:

1. Доступ до персональних даних за відсутності повноважень, законних підстав і обґрунтованої мети доступу.

2. Розкриття персональних даних для широкого загалу, а також збір надлишкового обсягу даних щодо цілей, для яких вони обробляються в подальшому.

3. Обробка персональних даних в цілях, несумісних з тими, з якими вони були зібрані.

4. Незаконне заволодіння персональними даними, шахрайським шляхом.

5. Використання незаконно зібраних персональних даних з шахрайськими мотивами.

При реєстрації в соціальних мережах обов'язковим є надання таких даних: ПІБ, географічне положення, місце навчання, номери телефонів. Всі ці данні необхідні для створення персональної сторінки. Разом з цим без вказівки цих критеріїв неможливе створення особистого акаунту. Всі ці данні можуть використовуватися без згоди особи, в процесі функціонування сторінки в соціальній мережі. Цієї проблеми можливо уникнути шляхом умисного вказування невірної інформації, але якщо сторінка створюється з метою спілкування чи з іншою метою, обов'язковим критерієм якої є вказання точних відомостей, за якими можливо ідентифікувати особу, тобто тут виникає проблема правова ситуація. Прикладом цього є справа австрійського студента-юриста Макса Шремса. Він спробував з'ясувати стан безпеки його особистих даних, звернувшись до соцмережі Facebook. Він був здивований, коли представники Facebook погодилися надіслати йому більше ніж 1200 сторінок інформації про нього, навіть за умови, що він вже давно видалив свій профіль в цій соцмережі. Для вирішення таких колізій необхідно запровадити:

1. Запровадити в соціальних мережах умову, в якій буде написано, що «Чи згодна особа яка реєструється, що її персональні дані в процесі функціонування сторінки можуть бути використані»

2. Створення державного підрозділу який би контролював неправомірне використання персональних даних в мережі Інтернет.

Отже, підводячи висновок можна сказати, що основною і головною проблемою Інтернету є незахищеність особи, порушення інформаційної безпеки. Це питання га даний момент є відкритим всі вчені намагаються створити багаторівневої і багато суб'єктної системи захисту персональних даних, окрім того необхідно створити правоохоронні

органи які б контролювали дотримання Законів України та міжнародного законодавства стосовно захисту персональних даних.

1. Закон України «Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних http://zakon2.rada.gov.ua/laws/show/2438-17/print1361278834285429

2. Директива 95/46/ЄС Європейського Парламенту і Ради" Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних" від 24 жовтня 1995 року. http://zakon4.rada.gov.ua/laws/show/994_242/print1360150843706940

3. Використовуються рекомендації ARTICLE 29 - DATA PROTECTION WORKING PARTY WP 136 Opinion 4/2007 on the concept of personal data http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_en.pdf

4. Системна інформатизація правоохоронної діяльності : європейські нормативно-правові акти та підходи до упорядкування інформаційних відносин у зв’язку з автоматизованою обробкою даних : посіб. / В. Брижко, М. Швець [та ін.]. – Кн. 2. – К. : ТОВ “ПанТот”, 2006. – 509 с.

5. Права человека и защита персональных данных / А. Баранов. В. Брыжко, Ю. Базанов. – (Финансовая помощь и содействие в издании Харковской правозащитной группы и Национального фонда поддержки демократии (США). – Харьков : Фолио, 2000. – 280 с.

6. Про захист персональних даних : Закон України від 01.06.10 р. № 2297-VI ; із змін. та доп. // Відомості Верховної Ради України (ВВР). – 2010. – № 34. – ст. 481

Психологічна та професійна підготовка майбутніх працівників поліції

Іщук Б.М.
курсант 413 взводу факультету №3
Одеського державного університету внутрішніх справ

Шелехов А.О.
науковий керівник, завідувач кафедри адміністративної діяльності ОВС та економічної безпеки Одеського державного університету внутрішніх справ, к.ю.н. , доцент

Важливим аспектом забезпечення публічного порядку та безпеки, надійного захисту прав і свобод людини від злочинних посягань є діяльність поліцейського. З метою більш результативної роботи органів Національної поліції потрібно забезпечити якісну підготовку безперервну відповідних фахівців (постійний розвиток, вдосконалення своїх знань та навичок). Також варто зазначити, що професійна діяльність поліцейських, майже щодня, пов'язана з виникненням небезпечних та екстремальних ситуацій, а саме, тих, що перш за все, пов'язані з затриманням злочинців, застосуванням примусових заходів, забезпеченням правопорядку під час проведення масових заходів, подоланням наслідків різних життєвих небезпек, стихійних лих тощо, що передбачає необхідність в особливій психологічній та фізичній підготовці майбутніх працівників поліції до дій в таких умовах, тому ця проблема на сьогодення набуває дуже важливого значення.

Проблема кадрової підготовки поліцейських у світлі зазначених реформ набула особливої актуальності і міжнародного характеру. В сучасному демократичному суспільстві поліцейська служба є досить важливою професією і дуже складним видом соціальної діяльності. Невипадково освітній і культурний рівень поліцейських розглядається як основний чинник, що забезпечує прогресивний розвиток поліції, а освіта поліцейських - як потужний резерв підвищення ефективності правоохоронної діяльності [6, с. 56].

Зазначена тема не раз ставала об'єктом наукового пошуку таких науковців, як: Бондаренко Я. Г., Бортнічук П. М., Власенко І. В., Васильєв В. Т., Горпинич Г. Ф., Доценко В. В., Ларіонов С. О.,

Макаренко П. В., Малолєпший С. Б., Мілорадова Н. Е., Пасько О. М., Сергієнко В. В., Сокуренко В. В тощо. Але не усі проблемні питання кадрової підготовки поліцейських в повній мірі знайшли своє відображення в їх роботах, наприклад, це стосується питань психологічної підготовки поліцейського.

Аналіз стандартів навчання поліцейських, які пропонуються Міністерством юстиції США, засвідчив, що до обов'язкових навчальних дисциплін, які вивчаються поліцейськими віднесені: поводження з вогнепальною зброєю, навички самооборони, спеціальна фізична підготовка, тактика патрулювання, перша медична допомога, оформлення процесуальних документів, навички володіння комп'ютером, культурна різноманітність і толерантність, стратегії community policing, управління конфліктами та навички медіації [7].

Особливості розвитку професіоналізму працівника поліції також включає в себе: юридичну освіту, юридичну практику, правову культуру юриста, політичну культуру юриста, моральну культуру юриста, естетичну культуру юриста та психологічні аспекти діяльності, знання психологічних прийомів та особливостей психіки людини.

Наприклад в США, перш ніж вступати на службу або навчання в поліцію кандидати проходять особливий відбір, де визначають рівень готовності особи до отримання почесного звання «поліцейського». Більшість поліцейських органів США приймає на службу кандидатів, які мають середню або вищу освіту. У небагатьох департаментах поліції встановлені вимоги вищої освіти для працівників. Більше того, кандидати до служби в поліції зобов'язані закінчити курси з якої-небудь з наступних дисциплін: правозастосування; відправлення правосуддя; психологія; адвокатура; історія Америки; громадське управління; англійська мова; правові відносини; соціологія; торгове право.

У США випускники академій, прийшовши на службу, проходять сувору й ретельну підготовку, через те що окрім навичок, отриманих у навчальному закладі, поліцейський повинен знати алгоритми, правила, інструкції поводження в екстремальних ситуаціях і повною мірою уявляти собі, як правильно виконувати свою роботу. Тому випускникам академії дають 2 тижні, щоб «призвичаїтися», перш ніж вони пройдуть спеціальний курс «Підготовча програма працівників поліції». За два тижні новачки пристосовуються до нової обстановки, знайомляться з інструкторами наставниками, які готуватимуть їх до практичної роботи [8].

Для того, щоб працівники поліції були готові до екстремальних ситуацій вони повинні засвоїти основні професійні навички. До них відносяться: використання поліцейської техніки, навички спілкування та самоконтролю, а також відповідне володіння спеціальними засобами, вогнепальною зброєю, та вмінням застосовувати фізичну силу [3; с. 64].

Екстремальні умови вимагають від працівника поліції швидких та безкомпромісних дій для відвернення небезпеки або надання невідкладної допомоги собі або постраждалим особам. Міжнародний та український досвід передбачають, що наявність спеціальної підготовки та розвинені навички, не гарантують і не можуть гарантувати виключення факту екстремальності.

Тому, з метою покращення підготовки працівників правоохоронної системи, можна запропонувати такі методи: запозичення зарубіжного досвіду; залучення закордонних спеціалістів; удосконалення нормативної бази з даного питання; поєднання теоретичного навчання з системою тренінгового навчання; використання ситуацій з моделюванням екстремальних ситуацій; збільшити навантаження на теоретичне та практичне освоєння основ першої медичної допомоги, швидкого реагування та мислення в екстремальних ситуаціях; розробка програми стресостійкості працівника поліції в екстремальних умовах та методики зниження реакції тривоги і страху.

Ситуації з використанням моделювання екстремальних ситуацій – це специфічний вид практичної підготовки з оперативно-тактичних, тактичних і тактико-спеціальних навичок, до яких включається і спеціальна фізична підготовка, при якій працівники поліції на тлі єдиної оперативно-тактичної обстановки набувають, закріплюють і поглиблюють теоретичні знання і практичні навички для подальшої оцінки обстановки, прийняття рішення із організації дій у надзвичайних ситуаціях та забезпечення ними в екстремальних умовах, що склалися належного збереження громадського порядку.

При моделюванні конкретних психологічних ситуацій пов’язаних з психологічно напруженою обстановкою, які створюються протягом занять, наближених до реальних умов, відбувається формування і розвиток психологічної готовності працівників поліції до успішного здійснення їх професійної діяльності. Досягається це різними засобами психологічного моделювання: ознайомленням з відеозаписами різних ситуацій, фотографіями місць подій, осіб які постраждали і т.п.; прослуховуванням фонограм із записом звуків, які можуть завдавати

несподіваний і психогенний вплив; переглядом кінофільмів, кінокадрів, які документально відтворюють елементи екстремальних ситуацій; імітацією різних факторів екстремальних ситуацій за допомогою спеціальних засобів (муляжів, трупів, неприємних запахів, макетів місць подій і т.п.); проведенням занять у відповідних часових і кліматичних умовах [4].

Також у якості підготовки, доцільно створити окремий спецкурс поведінки в екстремальних умовах, в який включити практичні тренування, а саме:

- організація дій під час імітації небезпеки на транспорті;
- орієнтування під час виконання службових обов'язків у незнайомій місцевості;
- дії в ситуації пов'язаній з використанням вогнепальної зброї злочинцями;
- виконання вправ в темряві, в сутінках, зі зв'язаними темною або напівпрозорою пов'язкою очима, в засобах індивідуального захисту тощо.

Також можна виокремити декілька основних проблем забезпечення якісної підготовки працівників поліції:

- недосить якісний відбір кандидатів на посади поліцейських;
- відсутність максимально тісної взаємодії з громадськими організаціями та населенням під час навчання поліцейських;
- невелика кількість годин відведених на проведення практичних занять та тренінгів, які спрямовані на закріплення за майбутніми працівниками практичних навичок та адаптація до певних екстремальних ситуацій;
- відсутність у кандидатів, які проходять навчання мотивації та бажання служити закону;
- теоретичні основи не завжди відповідають виконанню певних завдань на практиці.

Враховуючи вищезазначене, можна підвести підсумки, що підготовка майбутніх поліцейських - це дуже складний та багаторівневий процес, який потребує значних змін для покращення готовності працівників поліції до проблем, які їх очікують під час здійснення ними професійної діяльності. Для готовності працівників до дій в екстремальних ситуаціях та покращення виконання службових завдань пов'язаних з небезпекою потрібно:

по-перше, внести до нормативної бази системи МВС поняття екстремальної ситуації, де зазначити певне коло повноважень та

обов'язків громадян і працівників правоохоронної системи при виникненні такої ситуації;

по-друге, зробити акцент на організацію практичних занять для отримання навичок поводження в умовах небезпечних для життя працівників поліції та громадян;

по-третє, проводити тренінги з моделюванням екстремальних ситуацій в різних сферах життєдіяльності та запровадити інтерактивне навчання, яке характеризується переходом до активних форм і методів освіти, що сприяє реалізації компетентнісного підходу, тому що пропонується відтворення предметного змісту професійної діяльності, моделювання систем відносин, характерних для конкретного виду професійної практики, а також проводити психологічну перевірку та підготовку майбутніх працівників до готовності здійснювати професійну діяльність.

1. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР // [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/254к/96-вр

2. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII // [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/580-19

3. Шляхи покращення системи професійної підготовки правоохоронців до дій в екстремальних умовах : зб. матеріалів міжнародної наук.-практ. конф. (м. Харків, 18 груд. 2015 р.) / МВС України, Харків. нац. ун-т внутр. справ. – Харків, 2015. – 168 с

4. Иосифа Ю.Р. // Психологические факторы профессиональной подготовки работников ОВД к действиям в экстремальных ситуациях [Електронний ресурс] – Режим доступу: http://www.info-library.com.ua/libs/stattya/4627-psihologichni-chinniki-profesijnoyi-pidgotovki-pratsivnikiv-ovs-do-dij-v-ekstremalnih-situatsijah.html

5. Юхновец Г.А. Проблемы психолого-педагогического обеспечения деятельности органов внутренних дел: Научные разработки Академии по совершенствованию практической деятельности и подготовки кадров органов внутренних дел //Материалы научно-практической конференции Академии внутренних дел Украины. - Киев, 1994.

6. Жукевич І. Професійна компетентність майбутнього правоохоронця: сутність і складові [Електронний ресурс] / І. Жукевич //

Освіта дорослих: теорія, досвід, перспективи. - 2013. - Вип. 6. - С. 54-60. - Режим доступу: http://nbuv.gov.ua/UJRN/OD_2013_6_7

7. Reaves B. A. State and Local Law Enforcement Training Academies,2006 : Bureau of Justice Statistics Special Report : February 2009, NCJ 222987 : Revised 4/14/09 [Електронний ресурс] / Brian A. Reaves. – U.S.Department of Justice, Office of Justice Programs, [2009]. – 15 p. – Режим доступу: http://www.bjs.gov/content/pub/pdf/slleta06.pdf

8. Система підготовки поліцейських у США [Електронний ресурс]. – Режим доступу: http://police-reform.org

Кіберзлочинність в Україні

Казмерчук К.А.
студентка 1 курсу ЮД-744 ДДУВС
Гавриш О.С.
науковий керівник, викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

На сьогодні не існує загальновизнаного визначення поняття «комп'ютерних злочинів». Та показники поширення цих злочинів швидко збільшуються через постійне розширення сфери застосування комп'ютерної техніки. На цей час кіберзлочини створили особливу загрозу безпеці і складають 35% від загальної кількості вчинених у світі злочинів.

Аналіз даних офіційної статистичної звітності за 2016-2017 рр. свідчить про стабільність кіберзлочинів [1]. Як зазначає начальник кіберполіції України Сергій Демедюк: «Йде зростання кількості злочинів, але й розкриття йде в якихось періодах на 70-75 відсотків». За показниками на 2016 рік у Дніпропетровській області зареєстровано 39 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а на січень-квітень 2017 року – 13. У 2016 році відомство зареєструвало 1018 злочинів по Україні, за січень-квітень 2017 року – 705. За словами Генеральної Прокуратори України на 2016 рік відомство вже розслідувало і направило до суду обвинувальні акти по 501 провадженню, тим часом за січень–квітень 2017 року у 185 провадженнях [2]. «У

минулому році було понад 4 тис. злочинів, і близько 300-400 злочинів ми супроводжуємо, допомагаючи іншим службам, а вже за цей квартал у нас 1000 злочинів вчинено, і 300, які ми супроводжуємо. 1300 лише за цей квартал», - констатує Сергій Демедюк [3].

Звичайно, що як з кожним роком зростає кількість інтернет-користувачів (2008 р. – 1,5 млрд чоловік, 2013 р. – 2,3 млрд осіб, 2015 р. – 3,4 млрд і, за прогнозами фахівців, до 2018 р. доступ отримають до 75% від загальної чисельності населення світу), так і пропорційно зростає кількість злочинів, що скоюють у кіберпросторі. За інформацією Національної поліції України, за 3 квартали 2017 року кількість злочинів з використанням інформаційних технологій зросла в 2,3 рази – 6136 випадків порівняно з 2621 зафіксованими торік. До переліку областей, у яких стрімко зростає злочинність такого характеру, входять Івано-Франківська (505% приросту), Кіровоградська (483%) та Луганська (307%). У Сумській області кількість таких злочинів навпаки зменшилася на 40%, у Харківській – майже на 6%. Не можна не сказати, що Україна увійшла до трійки лідерів з DDoS-атак. За даними антивірусних лабораторій, 12% від усіх атак припадає на Україну.

Задля інтенсивної боротьби з кіберзлочинами були проведені наступні дії:

1. Указом Президента України від 15.03.2016 р. № 96/2016 була затверджена Стратегія кібербезпеки України, метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави [4].

2. Підписання 8 червня 2016 р. Президентом України Петром Порошенком Указу про створення Національного координаційного центру кібербезпеки, який би скоординував роботу суб'єктів національної безпеки і оборони України під час реалізації Стратегії кібербезпеки України.

3. 20 вересня 2016 р. Верховна Рада прийняла у першому читанні Закон України «Про основні засади забезпечення кібербезпеки України» [5].

Сьогодні закони повинні відповідати вимогам, що пред'являються сучасним рівнем розвитку технологій. Однак, в реаліях сьогодення цього не достатньо, повинна проводитися планомірна робота з користувачами щодо підвищення комп'ютерної грамотності та систематична робота з покращенням технічного обладнання захисту.

1. Статистика кіберзлочинності в Україні [Електронний ресурс]. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v
2. Статистика кіберзлочинності в Україні [Електронний ресурс]. – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_vb
3. Сергій Демедюк, керівник української кіберполіції [Електронний ресурс]. – Режим доступу: https://www.ukrinform.ua/rubric-technology/2216404-sergij-demeduk-kerivnik-ukrainskoi-kiberpolicii.html
4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» [Електронний ресурс] : Указ Президента України. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/96/2016
5. Про прийняття за основу проекту Закону України про основні засади забезпечення кібербезпеки України [Електронний ресурс] : Постанова Верховної Ради України. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/1524–19

Принципи застосування інформаційних технологій в діяльності органів внутрішніх справ.

Калюжна А.О.
студентка 1 курсу ЮД-746 ДДУВС
Гавриш О.С.
науковий керівник, викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

На сучасному етапі продовжується процес формування, удосконалення інформаційних технологій та принципів застосування в діяльності органів внутрішніх справ. Для забезпечення успішного вирішення основних завдань Національної поліції України потребує удосконалення правоохоронної діяльності шляхом оптимізації взаємовідносин з іншими суб'єктами життєдіяльності, зокрема, шляхом інформаційної взаємодії. Це обумовлює необхідність дослідження принципів застосування інформаційних технологій, а також удосконалення форм правового регулювання із забезпечення її

реалізації в діяльності поліції та органами публічної влади і громадськістю.

Завдяки, Ст. 25 закону України «Про Національну поліцію», яка називається «Повноваження поліції у сфері інформаційно-аналітичного забезпечення», в ч.2, яка визначає повноваження поліції в рамках інформаційно-аналітичної діяльності, зазначено, що поліція здійснює інформаційну взаємодію з іншими органами державної влади України, органами правопорядку іноземних держав та міжнародними організаціями (п. 4) та вивчає принципи взаємодії.[1] Але слід врахувати недостатній ступінь їх дослідженнях і вивченості. Бо досягнення соціальних цілей за допомогою закономірностей побудови знаходиться /в даний час, на стадії теоретичного осмислення і супроводжується недостатніми інтересами науково-практичних досліджень.

Закономірності інформаційно-технологічного забезпечення діяльності ОВС об'єктивно випливають з групи закономірностей соціального управління, пов'язаних з реалізацією організаційно-технологічних цілей управління. До групи об'єктивних закономірностей інформаційно-технологічного забезпечення в сфері правоохоронної діяльності відносять:

1.Організації інформаційних технологій управління в сфері правоохоронної діяльності обумовленні особливостями об'єкта інформаційного забезпечення. Ця закономірність непрямо випливає із закону необхідної різноманітності. В агрегованому вигляді об'єктом інформаційного забезпечення є система управління ОВС. При більш детальному, предметному розгляді кола об'єктів інформаційного забезпечення виявляється, що їх перелік на 1-2 порядки перевищує відповідний перелік об'єктів управління. Це пов'язано з тим, що зміст інформаційного забезпечення може ставитися до всього процесу управління, до певних його функцій і стадій, методам і формам, до діяльності окремих управлінських ланок, до конкретних видів керованої правоохоронної діяльності, до діяльності конкретних категорій особового складу та окремих співробітників ОВС і військовослужбовців ВВ. І в кожному з цих випадків забезпечують інформаційні технології будуть характеризуватися своєю специфікою та особливостями. Так, інформаційно-технологічне забезпечення загально-управлінських функцій системи ОВС диференціюється на інформаційні технології прогнозування, планування, організації, регулювання і контролю.[2]

2.Безперервність і циклічність інформаційно-технологічного забезпечення процесу управління в сфері правоохоронної діяльності. Ця

об'єктивна закономірність тісно пов'язана з достатньо вивченою закономірністю циклічності, безперервності процесу управління. Інформаційні технології управління ОВС покликані забезпечувати ряд постійно повторюваних взаємопов'язаних операцій зі збирання, зберігання, обробки, передачі та подання інформації, що забезпечує нерозривність управлінських процедур в часі, циклічний перехід від однієї управлінської функції до іншої.

3.Функціональна спеціалізація інформаційних технологій управління ОВС, яка відбувається в міру ускладнення сфери правоохоронної діяльності. Ця закономірність пов'язана з динамікою соціального розвитку та з особливостями прогресу комп'ютерної індустрії. Традиційні загальноприйняті схеми інформаційного забезпечення сфери правопорядку в умовах реформує суспільство все частіше виявляються неефективними і трансформуються в спеціалізовані підсистеми і комплекси. Розуміння цієї закономірності дасть змогу успішно вирішувати питання співвідношення централізації і децентралізації інформаційно-технологічного забезпечення ОВС, створення і функціонування інформаційних технологій, орієнтованих на функціональну специфіку рішення неоднозначних управлінських завдань в різних регіонах країни.[3]

4.Технологічний консерватизм інформаційного забезпечення правоохоронної діяльності в порівнянні з динамічністю і мінливістю процесів управління. Відповідно до практики діяльності ОВС останніх п'яти-семи років, існуючі структури інформаційно-технологічного забезпечення неминуче застарівають, при цьому швидкість старіння характеризується постійним наростанням. Очевидно, що технологічні перетворення повинні бути адаптивні та з кожним роком все більш досконалішими.

Отже, в даному вигляді загально-управлінської принцип об'єктної орієнтації інформаційних технологій тісно пов'язаний з усіма перерахованими вище загально-управлінської принципами побудови і функціонування систем управління та з принципами здійснення процесу управління системи. І для подальшого використання та розвитку необхідно удосконалення, систематичне вивчення інформаційних технологій, різноманітність висококваліфікованих фахівців, які б допомогли в вдосконалені, застосуванні та виведенні інформаційних технологій в діяльності органів внутрішніх справ на належний високий рівень.

1.Інформаціна взаємодія поліції з органами внутрішньої влади [Електронний ресурс] – Режим доступу: https://yandex.fr/clck/jsredir?bu=uniq15107351086001934151&from=yandex.fr%3Bsearch%2F%3Bweb%3B%3B&text=

2. Інформаційні системи органів внутрішніх справ [Електронний ресурс] – Режим доступу: http://stud.com.ua/34590/informatika/informatsiyni_sistemi_organiv_vnutrishnih_sprav

3. Функціональна спеціалізація інформаційних технологій управління ОВС [Електронний ресурс] – Режим доступу: http://stud.com.ua/34592/informatika/informatsiyna_infrastruktura_organiv_vnutrishnih_sprav

4. Система інформаційного забезпечення органів внутрішніх справ (ОВС) України [Електронний ресурс] – Режим доступу: https://studfiles.net/preview/5536057/page:2/

Особливості здійснення рейдерства в Україні

Козій В.С.
студент 1 курсу спеціальність «Менеджмент», ДДУВС
Соломіна Г.В.
науковий керівник, к.е.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

За оцінками експертів, в Україні діє від 35 до 50 професіональних рейдерських груп. Особливість діяльності яких, полягає у захопленні і перерозподілі власності за рамками закону та передбачає використання психологічного тиску, шантажу, підробці документів, підкупі силових структур. Під рейдерські атаки за 2017 рік в Україні вже потрапили 3,7 тисяч суб'єктів господарювання. Річний обсяг перерозподілу сягає від 2 до 3 млрд. доларів США.

Рейдери – це команда висококваліфікованих спеціалістів із захоплення фірми або із перехоплення управління за допомогою навмисне розіграного бізнес-конфлікту. Основна мета рейдерства – приборкання великого бізнесу, великих фірм, підприємств, захоплення значних площ, земельних ділянок, обладнання і нерухомості [1].

Науковці та практики поділяють рейдерів на білих та чорних. Білі рейдери діють методом корпоративного шантажу в рамках чинного

законодавства. Вони є характерними для країн із розвиненою економікою. Таке рейдерство прямо чи безпосередньо із процедурою банкрутства усуває від керівництва неефективний менеджмент, підвищує результативність бізнес-процесів. Початок здійснення захоплення характеризується скуповуванням акцій за порівняно високими цінами (10-15%), щоб ініціювати проведення зборів акціонерів з необхідним порядком денним. Як правило, керівники не йдуть на перемовини, після чого рейдери переходять до чорних дій.

Чорні рейдери для отримання результату використовують кримінальні методи (захоплення, підробка документів, реєстрація компаній на підставних осіб, підкуп силових структур, чиновників, суддів, фізичне усунення). Результати діяльності чорних рейдерів украй негативні, оскільки здійснюється зазіхання і на власність особи, і на інші її основні права, гарантовані Конституцією України (право на життя, здоров'я, честь, гідність). Під час захоплень, чорні рейдери використовують методи скуповування акцій і боргових зобов'язань, ініціюють процедури банкрутства, протиправний доступ до реєстру акціонерів, значне заниження вартості підприємства. Особливий інтерес становлять державні та приватні підприємства, що володіють нерухомістю.

Аналогічну оцінку можна дати й новому для економіки явищу- «гринмейл» – блокування та перешкоджання роботі підприємства внаслідок шантажу з боку власників дрібних пакетів акцій.

Ринок рейдерства в Україні представлений певною кількістю юридичних фірм, структура яких як правило включає: збір та аналіз інформації; юридичну оцінку діяльності суб’єкта підприємництва; розробку безпосереднього поглинання для кожного індивідуально із врахуванням усіх особливостей, включає в себе такі варіанти захоплення: скуповування акцій та проведення додаткової емісії; банкрутство - введення підприємства у стадію нездатності розрахуватися с боргами та кредитами (шляхом «придбання» кредитної заборгованості у бізнес-партнерів, укладання договорів з банківськими та іншими фінансовими організаціями, формування конкурсної комісії); реприватизація- повторна приватизація після повернення в державну власність раніше приватизованого об'єкта; корпоративний шантаж- самостійний високоприбутковий вид бізнесу, що не передбачає здійснення контролю над компанією; додаткова емісія- перехоплення управління для позбавлення небажаного міноритарного акціонера; силове захоплення- перехоплення шляхом залучання силових структур та сфальсифікованого

судового рішення; контроль над менеджментом; фіктивне банкрутство; корупція [2].

Практика показує, що найефективнішим від захоплення рейдерами є захист превентивного характеру. Його стратегічна мета – максимальне підвищення вартості захоплення підприємства для того, щоб зробити атаку нерентабельною, а отже – недоцільною. Відповідно власникові необхідно здійснити заходи, щоб перевести інтерес рейдера із площини корпоративного захоплення на механізм об'єднання та поглинання. Для цього слід провести системну реструктуризацію бізнесу, що дасть змогу створити таку систему володіння і управління найбільш привабливих активів, яка зробить захоплення рейдерами підприємства нерентабельним бізнесом.

До державних способів запобігання рейдерських захватів відноситься діяльність, що спрямована на: встановлення обов’язковості забезпечення дотримання конкуренції, захист прав акціонерів; формування правил і процедур корпоративного управління, які відповідали міжнародно-визнаним принципам та враховували при цьому національні особливості. Результатом діяльності таких груп стала поява в розвинених країнах Кодексів корпоративного управління [3].

1. Рейдерство в Україні – загроза національній безпеці.- Електронний ресурс. - Режим доступу: http://veche.kiev.ua/journal/2105/.

2. Загальні тенденції тіньової економіки в Україні. – Електронний ресурс.- Режим доступу: http://www.me.gov.ua/Documents/List?lang=uk-UA&id=e384c5a7-6533-4ab6-b56f-50e5243eb15a&tag=TendentsiiTinovoiEkonomiki.

3. В Україні за півроку зафіксували 570 нападів та рейдерських захоплень. - Електронний ресурс. – Режим доступу: http://grushevskogo5.com/analytics/reyderstvo-v-ukraini-zagroza-zhittyu-lyudey-ta-ekonomitsi-kraini/.

Кіберполіція та кіберзлочинність в Україні

Коптяєва А.Ю.
студентка 1 курсу ЮД-744 ДДУВС
Махницький О.В.
науковий керівник, старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Кіберполіція — територіальний орган Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, хакерами, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність. Має на меті попередження, виявлення припинення та розкриття кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких, передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем. На жаль на сьогодні комп’ютерні злочини - це одна з найдинамічніших груп злочинців їх чисельність збільшується щогодини [1].

Кіберполіція має певні завдання, щоб досягти конкретні цілі. Наприклад:

1) Реалізація державної політики у сфері протидії кіберзлочинності.

2) Завчасне попередження населення про появу новітніх кіберзлочинів.

3) Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.

4) Швидка реакція на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.

5) Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

6) Залучення до міжнародних операціях та співпраць у реальному часі. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу.

7) Протидія кіберзлочинам [2].

Кіберзлочинність — це злочин через інтернет. Він включає різні види злочинів, які здійснюються завдяки таким ресурсам, як інтернет та комп'ютер. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація будь-яких персон. Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні. Адже ці злочинці можуть анулювати світові рахунки, від цього страждають сотні людей, адже зараз великий відсоток людей зберігає велику суми в банках [3].

Об'єктом кіберзлочинів стає звичайний користувач інтернету будь-якого віку.

Види злочинів [3]:

Кардинг - використання в злочинних операціях реквізитів платіжних карт осіб, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів.

Фішинг - вид шахрайства, при якому до клієнта платіжних систем надсилають повідомлення електронною поштою або повідомленням на телефон нібито від адміністрації або служби безпеки, від банку цієї системи з проханням вказати свої рахунки та паролі для встановлення.

Вішинг - вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний номер, а при розмові запитуються конфіденційні дані власника картки.

Онлайн-шахрайство - несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

Піратство - незаконне розповсюдження інтелектуальної власності в Інтернеті.

Кард-шарінг - надання незаконного доступу до перегляду супутникового та кабельного ТУ. Соціальна інженерія - технологія управління людьми в Інтернет-просторі.

Мальваре - створення та розповсюдження вірусів і шкідливого програмного забезпечення.

Протиправний контент - контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

Рефайлінг - незаконна підміна телефонного трафіку.

Є поради, як не попасти на гачок кіберзлочинців [4] :

1) надійні паролі, а не визначні дати власного життя;

2) встановлювати захист на техніку, такі як блокування, антивірус;

3) перевірка власних облікових записів.

Отже, кіберполіція є головним протистоянням кіберзлочинцям. Є багато методів, які допоможуть уникнути махінацій, головне вчасно ними скористатися. Експерти впевнені: саме хакери в недалекому майбутньому стануть загрозою номер один, змістивши тероризм. Незважаючи на віртуальність злочинів, збиток вони завдають цілком справжній. Нині кіберзлочинність становить для нашої держави більш серйозну небезпеку, ніж ще 5 років тому. Незважаючи на зусилля правоохоронних органів, спрямованих на боротьбу з кіберзлочинами, їх кількість, на жаль, не зменшується, а, навпаки, постійно збільшується. Треба багато сил, знань та фахівців, щоб хоч якось призупинити цей вид злочину. Тому сьогодні особливо важливо переглянути усі існуючі заходи та активно розробляти нові, що принесуть більшу користь та надійніший захист від кіберзлочинців.

1. https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0)
2. https://cyberpolice.gov.ua/Офіційний сайт кіберполіції України
3. Прохоренко В. Кіберзлочинність для України стає актуальним поняттям – НБУ. - //Економічна правда від 26 лютого, 2013року.
4. Комп'ютерна злочинність - К.: Атіка, 2002

Захищеність комунікаторів зв'язку від несанкціонованого доступу

Кохан О.В.
студентка кафедри захисту інформації Запорізького національного технічного університету
Куцак С.В.
науковий керівник, старший викладач кафедри захисту інформації Запорізького національного технічного університету

В наш час все гостріше відчувається необхідність в надійному захисті комунікаторів зв'язку від несанкціонованого доступу. Проблема безпеки інформації зростає з ростом кількості сфер комерційної діяльності, які використовують цифрові методи для передачі даних.

Найбільш важливим в цьому напрямі є захист державної та приватної цифрової інформації, тому що серйозні заходи щодо захисту інформаційної підвищують рівень безпеки держави загалом.

На даний момент є декілька способів захисту від несанкціонованого доступу до даних в комунікативних пристроях:

- необхідність введення пароля з цифр та літер різного регістру;
- необхідність сканування відбитку пальця;
- необхідність сканування сітківки ока.

Способи захисту інформації розміщені у порядку поширеності їх використання.

Нещодавно з'явився метод зламу найпоширенішого способу захисту даних на комунікативному пристрої: зловмисник може отримати доступ до пароля, не отримуючи прямий доступ до комунікатора зв'язку. Для цього йому потрібно у якомусь громадському місці встановити свою точку доступу до мережі Wi-Fi. Користувач повинен самостійно підключитися до цієї мережі, тому зловмиснику потрібно розміщувати точку доступу у такому місці, де дійсно є публічний Wi-Fi. Наприклад, це може бути кафе або парк. Подальший крок цього методу зламу робить його ще більш нетривіальним. Коли користувач, який підключив комунікативний пристрій до Wi-Fi, робить якісь рухи пальцями на екрані свого гаджету, у мережі Wi-Fi відбуваються деякі коливання. Вчені вже розробили алгоритм, який вміє асоціювати коливання у мережі з натисканням на кнопки для вводу пароля. Вірогідність правильного підбору підвищується, якщо власник пристрою вводить той самий пароль неодноразово. Таким чином, алгоритм дає на виході три варіанти пароля, і як показало дослідження вчених [1, 2], один з цих варіантів вірний. За принцип своєї роботи алгоритм зламу отримав назву WindTalker, яку можна перекласти як «той, що розмовляє з вітром».

Якщо замінити або поєднати необхідність вводити пароль з іншими способами захисту доступу до інформації, то важливо буде відмітити, що це також не дає повної гарантії захисту від зламу. Професіонали в галузі хакерів довели, що обманути комунікативний пристрій можливо. Потрібно зробити фотографії достатньо високої якості, які дозволять зробити зліпок з відбитком пальця або сітківки ока. Також відбиток пальця можна отримати з якихось поверхонь, які достатньо добре зберігають відбитки.

Також є альтернативний метод зламу пароля, який можна використати лише у тому випадку, якщо власник комунікативного пристрою носить Smart-годинник, і саме на тій руці, якою вводить

пароль. Метод полягає у тому, що коли користувач вводить пароль, спеціальний алгоритм, який знаходиться у схованому сканері неподалік, асоціює коливання датчиків годинника з натисканням тих чи інших символів на гаджеті, а потім передає результати на пристрій зловмисника за допомогою Bluetooth.

Якщо розглянути методи захисту даних у більш широкому сенсі, то можна виявити два види заходів:

- ті, що має організувати система безпеки пристрою, сервісу або банку, до якого за допомогою комунікативного пристрою підключається клієнт.
- ті, яких має дотримуватись сам власник пристрою.

Для більш надійного захисту у деяких сервісах реалізовані складні методи автентифікації. Серед таких є необхідність вводити цифри (наприклад, якщо це PIN-код), натискаючи на них у інтерфейсі з випадково генерованою послідовністю цифр, що в свою чергу значно зменшує вірогідність підбору паролю за допомогою алгоритму WindTalker [3]. Інші способи для підвищення безпеки доступу до даних вимагають прийняти дзвінок за заздалегідь вказаним номером телефону, або прийняти генерований код доступу через SMS або електронну пошту. Крім того, те що останні два способи захисту зменшують вірогідність зламу доступу, важливо відзначити, що вони ще й ускладнюють доступ для самого власника пристрою.

Проаналізувавши дану проблему, можна сказати, що технології злому розвиваються чи не швидше, ніж методи забезпечення безпеки. Алгоритм злому WindTalker – це спосіб, який не вимагає безпосереднього доступу до гаджету, що набагато полегшує роботу хакерів. Жертвою хакерів може стати практично будь-який власник смартфона, але якщо не користуватися незнайомими загальнодоступними точками доступу Wi-Fi можна уникнути такої участі. Наявність таких зломів вимагає відразу декількох спосіб захисту доступу до даних: необхідно знайти і реалізувати рішення, яке зможе скоротити кількість ітерацій для доступу до своїх даних і при цьому буде мати досить високий рівень захисту.

1. When CSI meets public wifi: Inferring your mobile phone password via wifi signals [Електронний ресурс]: – Режим доступу: https://blog.acolyer.org/ 2016/ 11/10/.

2. Хакеры научились определять PIN-код пользователей по колебаниям сигнала Wi-Fi [Електронний ресурс]: – Режим доступу:

http://it-news.club/when-csi-meets-public-wifi-inferring-your-mobile-phone-password-via-wifi-signals/.

3. Як користувачі самі «зливають» паролі, PIN-коди через Wi-Fi [Електронний ресурс]: – Режим доступу: https://navkolonas.com/archives/21583.

Використання технологій штучних нейронних та капсульних мереж у системах захисту інформації

Кузьменко А.В.
ст. 3 курсу групи РТ-815 ЗНТУ
Матвейчук О.В.
ст. 3 курсу групи РТ-815 ЗНТУ
Корольков Р.Ю.
науковий керівник, старший викладач кафедри захисту інформації, ЗНТУ

Штучні нейронні мережі – це паралельно розподілена система обробки інформації, утворена тісно зв'язаними простими обчислювальними вузлами (однотипними або різними), що має властивість накопичувати експериментальні знання, узагальнювати їх і робити доступними для користувача у формі, зручній для інтерпретації й прийняття рішень.

Штучні нейронні мережі знаходять сьогодні широке застосування у будь-яких галузях. Зокрема, штучні нейронні мережі демонструють надлюдські можливості у задачах розпізнавання обличь і зображень. Роль нейронних мереж буде найбільшою для систем відеоспостереження, аудіо аналітики, забезпечення кібербезпеки, а також для систем управління доступом. Особливу роль нейромережеві технології будуть відігравати в інтеграції та обробці різнорідної інформації від різноманітних типів сенсорів та датчиків. Це дозволить створити інтелектуальні автономні системи безпеки нової якості.

Недоліком сучасних нейронних мереж є потреба у великій кількості даних. Програмне забезпечення для розпізнавання зображень, яке сьогодні використовується Google та іншими, потребує великої кількості прикладів фотографій, щоб навчитись надійно розпізнавати об'єкти у всіх ситуаціях. Це пов'язано з тим, що програмне забезпечення не вміє узагальнювати те, що вивчається у нових ситуаціях, наприклад,

розуміння того, що об'єкт є одним і тим же, якщо дивитися на нього з нової точки зору.

Капсульні мережі направлені на усунення недоліків сучасних систем машинного навчання, які обмежують їх ефективність. В цьому підході використовуються невеликі групи нейронів, які називаються капсулами. В свою чергу, капсули складають шари для ідентифікації об'єктів на відео або зображеннях. Коли декілька капсул в одному шарі приймають однакове рішення, вони активують наступну капсулу, що знаходиться на рівень вище. Цей процес продовжується доки мережа не зможе зробити висновок про те, що вона бачить. Кожна із капсул КМ створена таким чином, що здатна виявляти у зображенні конкретну ознаку і розпізнавати її під різним кутом.

Капсульні мережі потребують менший об'єм даних для навчання та розпізнавання об'єктів у нових ситуаціях. Вони не поступаються звичайним ШНМ у розпізнаванні рукописних символів. КМ пройшли тест на розпізнавання об'єктів, що були зображені з різних ракурсів, та зробили в два рази менше помилок ніж інші мережі.

Проте на даному етапі розвитку КМ поступаються традиційним ШНМ у швидкості обробки даних, що потребує подальшого вивчення та вдосконалення технології капсульних мереж.

Захист WEB-порталів спеціалізованих інформаційних систем Національної поліції України

Мазенко Н.А.
курсант 4-го курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Мирошниченко В.О.
науковий керівник, доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

На теперішній час неабиякий вплив здійснюють не лише соціальні, політичні та економічні течії, а насамперед інформаційний потік інформації. Інформаційний вплив здатен уражувати будь-який пласт не лише суспільства, а й держави в загалом. Впровадження нових

інформаційних систем призвело не лише до підвищення рівня інформаційних технологій, а й до створення нових проблем інформаційного середовища. Важливим напрямком підвищення ефективності функціонування спеціалізованих інформаційних систем Національної поліції (НП) є інтегрування з глобальною мережею Internet. У багатьох випадках завдяки, власне ступеню інтегрування, вирішуються дві основні задачі. По-перше, об'єднуються територіально розподілені підсистеми інформаційних систем (ІС). По-друге, користувачам Internet забезпечується доступ до відкритої інформації ІС. Досить часто при розв'язанні обох задач використовується Web-сайт (Web-портал), який, у свою чергу є провідним серед інших інформаційних систем у мережі Інтернет [1, с.146].

Якщо звернутися до практичної діяльності, то треба зазначити, що функціонування окремого WEB-порталу відіграє свій вплив на функціонуванні усієї інформаційної системи. Основною ланкою WEB-порталу є Web-сервер, який забезпечує доступ користувачів із мережі Internet до Web-сторінок порталу.

Однак, в практиці зустрічаються випадки, коли безпека інформації зазнає впливу негативних уразників. Такими випадками порушення безпеки інформації є:

- блокування інформації (дії, наслідком яких є припинення доступу до інформації);
- несанкціонований доступ (доступ до інформації, що здійснюється з порушенням установлених в ІС правил розмежування доступу);
- витік інформації – результат дій порушника, унаслідок яких інформація стає відомою (доступною) суб'єктам, що не мають права доступу до неї;
- втрата інформації (дія, внаслідок якої інформація в ІС припиняє своє існування для фізичних або юридичних осіб, які мають право власності на неї в повному або обмеженому обсязі);
- модифікування інформації (умисні дії, які призводять до деформації інформації, яка має оброблятися або зберігатися в ІС);
- порушення роботи ІС (дії або обставини, які призводять до спотворення процесу оброблення інформації)

Саме тому керуючий особовий склад підрозділів Національної поліції України під час процесу створення будь-яких WEB-порталів та при цьому визначає операторів, вузли яких будуть використовуватись для налаштування під'єднання до мережі Internet, керуючись при цьому

не лише законами України та іншими нормативно-правовими актами, а й базою даних, що встановлює вимоги забезпечення з технічного захисту інформації (ТЗІ) та передовим практичним досвідом стосовно розроблення новітніх інформаційних методів і процесів захисту інформації [2, с.372]. Будь-який із WEB-порталів може бути розміщений на власному сервері, або ж на сервері, який визнається власністю оператора. На певного власника серверу покладається обов'язок гарантувати власнику інформації певний рівень встановленого захисту, досягається це тим, що функціонування WEB-порталу забезпечується ІС, в якій створюється комплексна система захисту інформації (КСЗІ), яка є сукупністю організаційно-правових та інженерно-технічних заходів, а також програмно-апаратних засобів, які безпосередньо і забезпечують захист інформації [3, с.293].

Нормальне функціонування Web-порталу, під'єднаного до мережі Internet, практично неможливе, якщо не надавати належну увагу кожній проблемі забезпечення його інформаційної безпеки. Найефективніше ця проблема може бути вирішена шляхом застосування комплексного підходу до захисту інформаційних активів порталу від можливих інформаційних нападів. Для цього до складу комплексу засобів захисту порталу повинні входити підсистеми антивірусного захисту, виявлення втручань, контролю цілісності, криптографічного захисту, розмежування доступу, а також підсистема управління. При цьому кожна з підсистем повинна бути оснащена елементами власної безпеки.

1. Кулешник Я. Ф. Основні завдання захисту інформації в операційних системах / Я. Ф. Кулешник, Т. В. Рудий, І. В. Бичинюк, Д. М. Неспляк // Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності органів Національної поліції,– Львів: 2016. – С. 145–148.

2. Захаров В. П. Проблеми інформаційного забезпечення правоохоронних структур: навчальний посібник / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2011. – 372 с

3. Андреєв В. І. Основи інформаційної безпеки: підручник для студентів ВНЗ які навчаються за напрямом «Інформаційна безпека» / В. І. Андреєв, В. О Хорошко, В. С. Чередниченко, М. Є. Ше- лест; за ред. В. О. Хорошко. – К.: ДУІКТ, 2015. – Вид. 2-ге, доп. і переробл. – 293 с.

Правове регулювання забезпечення кібербезпеки в Україні

Манік Ю.А.
курсант Дніпропетровського державного університету внутрішніх справ
Рижков Е.В.
науковий керівник, завідувач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент

За останнє десятиліття значно зросла кількість насильницьких посягань на державні, політичні та економічні інтереси України, які вирують не лише у традиційних сферах збройних суперечок, таких як земля, море і повітря, а й поступово просуваються в новітні простори — інформаційний та кібернетичний [4]. Це визначило політичну необхідність контролю і подальшого регулювання взаємовідносин та дало підстави стверджувати про особливу актуальність процесу створення надійної системи кібернетичної безпеки відсутність якої може призвести до втрати політичної незалежності будь-якої держави світу, тобто до фактичного програшу нею війни невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони [25].

Актуальні питання інформаційної безпеки держави досліджували: А. Марущак, В. Петрик, В. Ліпкан та інші фахівці. Проблемні питання забезпечення кібербезпеки розглядали у своїх наукових працях А.С. Алпеєв [1], В. Бурячок [2], А. Бабенко, В. Бутузов [3], В. Гавловский, В. Голубєв, С. Гнатюк, Д. Дубов [5,6], В. Номоконов, С.В. Мельник [8], В. Петров [9], М. Погорецький, В. Шеломенцев [27] та ін.

Існують різні підходи багатьох науковців до визначення поняття кібербезпеки, під якою вони розуміють стан захищеності життєво важливих інтересів особи, суспільства та держави від зовнішніх і внутрішніх загроз, пов'язаних з використанням ресурсів інформаційно-телекомунікаційних систем, так званого кіберпростору, за наявності якого забезпечуються гарантовані умови для реалізації державної інформаційної політики. Водночас, Указом Президента України від 15.03.2016 р., № 96/2016 була введена в дію постанова Ради національної безпеки і оборони України "Про Стратегію кібербезпеки України", в якій

кібербезпека визначена як стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі. А в Проекті Стратегії забезпечення кібербезпеки України це поняття визначено як стан захищеності критичних об'єктів національної інформаційної інфраструктури та окремих її складових, за якого забезпечується їх стале функціонування та розвиток, своєчасне виявлення, запобігання та нейтралізація кібернетичних загроз в інтересах людини, суспільства, держави". І хоча нова редакція Стратегії національної безпеки вже враховує кібербезпекову проблематику, в Україні все ще відсутня цілісна термінологічна система, що сформувала б єдиний термінологічний апарат у сфері кібербезпеки.

Проблеми, які ускладнюють боротьбу з кіберзлочинами в Україні, насамперед, пов'язані з відсутністю чіткого правового регулювання національної державної політики в сфері кібербезпеки [7, 23, 26]. Також відсутня єдина державна структура з координації протидії кіберзлочинам чи кібератакам, внаслідок чого існує загроза, наприклад, критичній інфраструктурі держави, спостерігається значне зростання комп'ютерного піратства і порушення авторських прав.

Останнім часом розпочалися процеси щодо унормування даної проблеми та пошуку шляхів її вирішення, зокрема через створення відповідних нормативних документів. Україна робить певні кроки у напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю. Нормативно-правову базу у цих сферах діяльності складає: Конвенція Ради Європи про кіберзлочинність [7], ратифікована Законом України від 7.09.2005 року № 2824-IV; Закони України «Про інформацію» [24], «Про основи національної безпеки України» [21], «Про Державну службу спеціального зв'язку та захисту інформації України» [22], «Про телекомунікації» [10], «Про захист інформації в інформаційно-телекомунікаційних системах» [11], «Про доступ до публічної інформації» [12], «Про оборону України» [13], «Про засади внутрішньої і зовнішньої політики» [14], «Про об'єкти підвищеної небезпеки» [15]; Укази Президента України, зокрема про: Доктрину інформаційної безпеки [16], Стратегію національної безпеки України [17] та Воєнну доктрину України [18]; окремі положення Кримінального Кодексу України, окремі Постанови Кабінету Міністрів та Рішення РНБО України.

При цьому ключова роль у забезпеченні кібербезпеки покладається на: 1) Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», який регулює відносини у

сфері захисту інформації в інформаційних, телекомунікаційних та ІТ систем; 2) Закон України «Про Основні засади розвитку інформаційного суспільства України на 2007-2015 роки» [19] у запропонованих змінах до якого указується на необхідність створення національної системи кібербезпеки; 3) запропонований Міністерством внутрішніх справ (МВС) законопроект «Про внесення змін до Закону України «Про основи національної безпеки України» щодо кібернетичної безпеки України» [20], яким має бути запроваджено низку термінів, пов'язаних із кібербезпекою.

Пріоритетним залишається створення та прийняття принаймні Стратегії забезпечення кібернетичної безпеки України, зобов'язання щодо розробки якої Україна вже брала на себе перед закордонними партнерами. Цей документ має визначити зміст основних понять у даній сфері, загрози, принципи та напрями забезпечення кібернетичної безпеки, зокрема заходи з удосконалення держав- ного управління та нормативно-правового поля у сфері кіберзахисту.

Таким чином, можна дійти висновку, що кіберпростір на сьогоднішній день відіграє важливу роль у забезпечення нормального функціонування держав світу і суспільства в цілому. Тому необхідність протидії кіберзагрозам, що можуть нанести шкоду національній безпеці України, потребує створення власної дієвої системи інформаційної безпеки.

1. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность / А.С. Алпеев // Вопросы кибербезопасности : журнал. – 2014. – Вып. № 5(8). [Электронный ресурс]. – Доступный с http://wiki.informationsecurity.club/doku.php/публикации:terminologiya-bezopasnosti-kiberbezopasnost-informatsionnaya-bezopasnost

2. Бурячок В.Л. Кібернетична безпека – головний фактор сталого розвитку сучасного інформаційного суспільства / А.Л. Бурячок // Сучасна спеціальна техніка : зб. наук. праць. – 2011. – № 3 (26). – С. 104-114

3. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія / В. М. Бутузов. – К. : Вид-во КИТ, 2010. – 408 с.

4. Гриняев, С. Н. США развертывают систему информационной безопасности [Електронний ресурс] / С. Н. Гриняев.— Режим доступу: http://www.cnews.ru/security/part3/rus-edu.shtml, 24.05.2010. 55. Ільяшов, О. А. До питання захисту інформаційно-телекомунікаційної сфери від

сторон- нього кібернетичного впливу / О. А. Ільяшов, В. Л. Бурячок // Наука і оборона.— 2010.— № 4.— С. 35–40.

5. Дубов Д.В. Кібербезпека : світові тенденції та виклики для України / Д.В. Дубов, М.А. Ожеван. – К. : Вид-во НІСД, 2011. – 30 с.

6. Дубов Д.В. Стратегічні аспекти кібербезпеки України / Д.В. Дубов // Стратегічні пріорите- ти : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 119-126.

7. Конвенція про кіберзлочинність (набула чинність 01.07.2006) // Верховна Рада України. [Електронний ресурс]. – Доступний з http://zakon4.rada.gov.ua/laws/show/994_575 10. Лук'янчук Р.В. Державна політика у сфері забезпечення кібернетичної безпеки в умовах проведення антитерористичної операції / Р.В. Лук'янчук // Вісник НАДУ : зб. наук. праць. – 2015. – Вип. 3. – С. 110-116.

8. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпе- ки / С.В. Мельник, О.О. Тихомиров, О.С. Лєнков // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., м. Київ, 22 березня 2011 р. – К. : Вид- во НА СБ України. – 2011. – Ч. 2. – С. 43-48.

9. Петров В.В. Щодо формування національної системи кібербезпеки України / В.В. Петров // Стратегічні пріоритети : наук.-аналіт. щокварт. зб. / Нац. ін-т стратег. дослідж. – К. : Вид-во НІСД. – 2013. – № 4 (29). – С. 127–130.

10. Про телекомунікації: за станом на 15.10.2011 р. / Закон, затверджений ВР України, 18.11.2003, № 1280-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур’єр від 24.12.2003, № 243.

11. Про захист інформації в інформаційно-телекомунікаційних системах: за станом на 30.04.2009 р. / Закон, затверджений ВР України 05.07.1994, № 80/94-ВР. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 02.08.1994.

12. Про доступ до публічної інформації: за станом на 09.06.2013 р. / Закон, затверджений ВР України 13.01.2011, № 2939-VI. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2939-17. – Офіц. вид. – К.: Відомості Верховної Ради України від 12.08.2011.

13. Про оборону України: за станом на 01.07.2013 р. / Закон, затверджений ВР України 06.12.1991, № 1932-XII. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/1932-12. – Офіц. вид. – К.: Відомості Верховної Ради України від 03.03.1992.

14. Про засади внутрішньої і зовнішньої політики: за станом на 01.07.2010 р. / Закон, затверджений ВР України 01.07.2010, № 2411-VI. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/ laws/show/2411-17. – Офіц. вид. – К.: Відомості Верховної Ради України від 08.10.2010.

15. Про об'єкти підвищеної небезпеки: за станом на 18.11.2012 р. / Закон, затверджений ВР України 18.01.2001, № 2245-III. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2245-14. – Офіц. вид. – К.: Відомості Верховної Ради України від 13.04.2001.

16. Про Доктрину інформаційної безпеки України: за станом на 08.07.2009 р. / Указ Президента України від 8.02.2009 р., № 514/2009. [Електронний ресурс]. – Режим доступу: http://zakon1.rada. gov.ua/cgi-bin/laws/ main.cgi. – Офіц. вид. – К.: Офіційний вісник України від 20.07.2009.

17. Про Стратегію національної безпеки України: за станом на 12.02.2007 р. / Указ Президента України від 12.02.2007 р., № 105/2007. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/ main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 07.03.2007, № 43.

18. Про Воєнну доктрину України: за станом на 22.06.2012 р. / Указ Президента України від 15.06.2004, № 648/2004. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/ laws/show/648/2004. – Офіц. вид. – К.: Офіційний вісник України від 13.08.2004.

19. Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки: за станом на 09.01.2007р. / Закон, затверджений ВР України 09.01.2007 № 537-V. [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/ laws/show/537-16. – Офіц. вид. – К.: Відомості Верховної Ради України від 23.03.2007.

20. Про внесення змін до Закону України "Про основи національної безпеки України" щодо кібернетичної безпеки України: проект за станом на 06.03.2013 р. № 2483. [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/web proc4_1?pf3511=45998

21. Про основи національної безпеки України: за станом на 20.07.2010 р. / Закон, затверджений ВР України 19 червня 2003 р., № 964-IV. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 30.07.2003, № 139.

22. Про державну службу спеціального зв'язка та захисту інформації: за станом на 07.08.2011 р. / Закон, затверджений ВР України 23 лютого 2006 року, № 3475-IV. [Електронний ресурс]. – Режим доступу:

http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Урядовий кур'єр від 11.04.2006, №68

23. Про Стратегічний оборонний бюлетень України. [Електронний ресурс]. – Доступний з http:// zakon2.rada.gov.ua/laws/show/ 771/2012/print1361272038412688

24. Про інформацію: за станом на 09.05.2011 р. / Закон, затверджений ВР України 02.10.1992, № 2657-XII. [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi. – Офіц. вид. – К.: Відомості Верховної Ради України від 01.12.1992.

25. Руководство по кибербезопасности для развивающихся стран. [Електронний ресурс]. – Режим доступу: http://www.itu.int/ITU-D/cyb/publications/2007/cgd c-2007-r.pdf.

26. Соловйов С.Г. Інформаційна складова державної політики та управління : монографія / С.Г. Соловйов, О.Є. Бухтатий, Ю.В. Нестеряк та ін.; за заг. ред. Н.В. Грицяк; Нац. акад. держ. упр. при Президентові України. – К. : Вид-во К.І.С., 2015. – 319 с.

27. Шеломенцев В.П. Правове забезпечення системи кібернетичної безпеки України та основні напрями її удосконалення / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика) : зб. наук. праць. – 2012. – № 1(27). – С. 312-320.

Попередження та розслідування кіберзлочинів

Мельникова Е.О.
студентка 1 курсу ЮД-748
юридичного факультету ДДУВС
Гавриш О.С.
науковий керівник, викладач кафедри економічної та
інформаційної безпеки Дніпропетровського
державного університету внутрішніх справ

Станом на сьогодні, жертвами кіберзлочинців можуть стати не лише люди, а і цілі держави. За оцінками Інтерполу, темпи зростання злочинності у цій сфері, наприклад, у глобальній мережі Інтернет, є найшвидшими на планеті. Кількість злочинів, що мають прояв у цієї галузі, зростає пропорційно кількості користувачів комп'ютерних мереж. Сьогодні у світі дослідження проблем боротьби зі злочинами в

кіберпросторі приділяється значна увага, що обумовлено об'єктивними процесами розвитку інформаційно-телекомунікаційних технологій і їх впровадженням у різні сфери громадської діяльності. 27.06.2017 о 11:00 проти України було розпочато масові кібератаки з використанням модифікованої для України версії вірусу "wannacry" – "криптолокера".[1] Ця кібератака була наймасштабнішою за всю історію України.

На 2016 рік в Україні було зафіксовано 1018 кіберзлочинів. З яких найбільша кількість здійснювалася у Києві. Проте на 2017 рік ця кількість значно зменшилася – 705. Найбільша кількість – у Чернівецькій області.[2]

Кіберзлочини - вкрай складна і комплексна сфера, тому дослідники шкідливих додатків часто повинні виступати експертами в розглядах високотехнологічних злочинів. Під час розслідування багато індикаторів можуть пролити світло на особистість кіберзлочинця. Деякі частини шкідливого коду можуть включати псевдонім лиходія або бути запрограмовані в «фірмовому стилі». Це може стати відправною точкою в пошуку злочинця. Дослідники використовують псевдоніми, або інші натяки з вірусу, або поштову адресу, асоційований з одним з доменів, які беруть участь в атаці, а потім прочісують спільноти на кшталт Facebook, Twitter, YouTube, вікіпедію та інші джерела користувацького контенту в надії на те, що злочинець десь то використовував ті ж псевдонім або пошту. Безумовно потрібно гармонізувати закони в різних країнах. Злочинці знають, де закони по їх галузі м'якші і що робити, щоб не потрапити на замітку і уникнути арешту.

Попередження кіберзлочинів складається зі стратегій і заходів, спрямованих на зниження ризику вчинення злочинів і нейтралізацію потенційно шкідливих наслідків для приватних осіб і усього суспільства. У більшості випадках стратегії протидії кіберзлочинності є невідокремною частиною стратегій забезпечення кібербезпеки. Обстеження, проведені у більш розвинутих країнах, показують, що більшість індивідуальних користувачів Інтернету нині вживають основні запобіжні заходи.

Хоча в половині країн діють закони про захист даних, які передбачають вимоги відносно захисту і використання персональних даних, проте в деяких – зроблені виключення для цілей розслідувань правоохоронних органів, згідно з якими постачальники послуг Інтернету та постачальники електронних засобів зв'язку зобов'язані зберігати певні дані користувачів упродовж певного терміну.

Фахівці виділяють такі елементи організації діяльності правоохоронних органів у глобальних інформаційних мережах:

– вивчення та оцінка обстановкив мережах;

– здійснення оптимальної розстановки сил і засобів, забезпечення взаємодії;

– управління, планування і контроль; координація дій суб'єктів правоохоронних органів.[3]

Питання пошуку шляхів протидії злочинам з використанням інформаційно-комунікаційних систем уже тривалий час знаходиться у сфері уваги міжнародної спільноти. На даний час Будапештська конвенція є фундаментом для розробки законодавства у боротьбі з кіберзлочинами як для кожної країни окремо, так і для загальносвітового законодавства.

Будапештська Конвенція вимагає від держав:

- криміналізувати атаки на комп'ютерні дані і системи (тобто незаконний доступ, нелегальне перехоплення, втручання в дані, втручання у систему, зловживання пристроями), а також правопорушення з використанням комп'ютерів (підробка і шахрайство), правопорушення, пов'язані зі змістом (дитяча порнографія) та правопорушення у сфері авторських і суміжних прав;

- вдосконалювати законодавство для того, щоб компетентні органи змогли проводити розслідування кіберзлочинів і зберігати електронні докази найефективніше, включаючи термінове збереження комп'ютерних даних, термінове збереження і часткове розкриття даних про рух інформації, обшук і арешт комп'ютерних даних, збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації;

- розширювати міжнародне співробітництво з іншими країнами-учасницями Конвенції через загальні (екстрадиція, взаємна допомога добровільне надання інформації тощо) і спеціальні заходи (термінове збереження та розкриття збережених даних про рух інформації, взаємна допомога щодо доступу до комп'ютерних даних, транскордонний доступ до комп'ютерних даних, створення цілодобових мереж тощо). [4]

Протидіяти кіберзлочину можна, наприклад:

1.Внести зміни до КК України з посиленням відповідальності за злочин у сфері комп'ютерних та інформаційних технологій;

2. Закріплення вимоги щодо обов'язкового проведення двоканальної аутентифікації та обов'язкового online-інформування клієнтів про кожну проведену операцію;

3. Визнавати електронні документи та інші дані у якості доказової бази при розслідуванні кіберзлочинів;

4. чітка регламентація механізмів взаємодії між клієнтом та банком, між банком відправника коштів та банком отримувача коштів у разі несанкціонованого списання коштів клієнта (шляхом внесення змін до Інструкції про безготівкові розрахунки в Україні в національній валюті);

5. Ввести сертифікації електронних платіжних засобів;

Отже, на сьогодні Інтернет-простір є не тільки місцем вивчення злочину та одержання незаконного доходу, а й місцем легалізації такого доходу. При цьому різноманіття видів кіберзлочинів у сукупності з різноманіттям методів відмивання доходів, одержаних від скоєння такого виду злочину, призводять до складності їх виявлення та розслідування. Хоча, дивлячись на статистику зафіксованих кіберзлочинів в Україні, правоохоронні органи покращили методи боротьби з кіберзлочинністю. Про це повідомив радник голови МВС Антон Геращенко.

---

1. [Електронний ресурс] – Режим доступу: http://portal.lviv.ua/news/2017/06/27/naymasshtabnisha-kiberataka-v-ukrayini-gerashhenko-rozpoviv-yaka-meta-virusu-petya

2.Статистика кіберзлочинів, що була надана Генеральною Прокуратурою України. [Електронний ресурс] – Режим доступу: https://dostup.pravda.com.ua/request/statistika_kibierzlochinnosti_v

3.Моделі кіберзлочинів [Електронний ресурс]. – Режим доступу: http://www.masiev.com/articles/informatsionnaja-bezopasnost/modeli-kiberprestuplenij-chast-2.

4.[Електронний ресурс]. – Режим доступу http://mvd.gov.by/main.aspx?guid=1741

Створення єдиної інформаційно-телекомунікаційної системи забезпечення громадської безпеки

Михайська П.В.
курсант Дніпропетровського
державного університету внутрішніх справ
Прокопов С.О.
науковий керівник, старший викладач Дніпропетровського
державного університету внутрішніх справ

Події 2014 – 2015 років на теренах нашої держави пов’язані із суттєвим збільшенням криміногенних загроз громадській безпеці та громадському порядку. Неконтрольований обіг зброї, вибухівки та боєприпасів зумовлюють необхідність формування принципово нових підходів до розв’язання цієї проблеми.

Впровадження сучасних інформаційно-телекомунікаційних систем, апаратних та програмних засобів створило нові унікальні можливості для розвитку системи безпеки в Україні.

З метою об‘єднання для охорони громадського порядку в системі єдиної дислокації слідчо-оперативних груп, чергових частин та підрозділів патрульної служби, підвищення ефективності їх діяльності, скорочення часу реагування на повідомлення громадян про злочини і пригоди, припинення правопорушень та затримання злочинців «за гарячими слідами», покращення контролю за якістю реагування нарядів міліції на злочини та правопорушення, дотримання законності під час виконання службових обов‘язків працівниками поліції створено комплексну автоматизовану систему управління нарядами поліції – «Цунамі».

Центр прийняття повідомлень - служба «102», вирішує завдання з прийняття та реєстрації повідомлень про злочини та події на єдиній інформаційній базі. Автоматизація служби "102" чергової частини Головного управління, дозволила оператору служби заповнювати на персональному комп'ютері формалізовану картку події зі слів заявника. Крім цього, до моменту коли оператор служби "102" підняв трубку телефону, на екран монітора вже надається допоміжна інформація про цей номер, зокрема власника телефонного номеру, географічне місцезнаходження абонента на електронній мапі міста тощо. При

випадковому обриві зв'язку оператор сам може передзвонити абоненту[1].

23 лютого 2016 р. у м. Харкові було презентовано програмно-апаратний комплекс аналітичного супроводу оперативно-розшукової діяльності та підтримки прийняття рішень (RICAS), розроблений співробітниками Управління інформаційного забезпечення ГУ НПУ в Харківській області спільно з місцевими ІТ-компаніями. Протягом 2012-2014 років розроблено інноваційний комплекс аналітичної обробки інформації різних баз даних з виведенням на детальну інтерактивну карту території як об'єктів дослідження, так і результатів аналізу. Система дає змогу виявити логічні відкриті та приховані зв'язки між заданими об'єктами та відобразити їх як у вигляді геоінформації, так і з використанням числового ряду. Можливість відображення на карті рухомих об'єктів дає змогу відстежувати ситуацію в динаміці та, відповідно, забезпечувати адекватну і своєчасну реакцію в потрібному обсязі, зокрема екіпажів рятувальної служби, аварійних бригад комунальних служб, бригад швидкої медичної допомоги.

3 серпня 2014 р. комплекс RICAS був запроваджений в ГУ НПУ Харківської області та кількох структурних підрозділах. Система RICAS вбудовується в службу «102» як додаткова опція аналітичної підтримки та може бути використана в роботі диспетчерської системи управління нарядами патрульної поліції «Цунамі». Відображення на інтерактивній карті підключених камер відеоспостереження і можливість миттєвого доступу до кожної з них як в режимі потокового відео, так і в режимі запису дає змогу відслідковувати як саму подію, так і дії служб реагування, фіксувати обставини правопорушення й у разі потреби використовувати дані як доказову базу в процесі слідства. Використання системи RICAS у тестовому режимі в декількох підрозділах НПУ Харківської області отримало високі оцінки фахівців, і на час презентації можливості цієї системи були випробувані під час розкриття 279 злочинів [2].

Новою віхою в розвитку систем безпеки в Україні став запуск Єдиного аналітичного сервісного центру (UASC) в Маріуполі24 грудня 2016 р.

Унікальна «розумна» система регіональної безпеки побудована на технологіях «смарт-сіті» і допомагає контролювати оперативний стан в області, де ведуться бойові дії, і синхронізувати дії різних служб - поліції, рятувальників, медиків, комунальних служб.

«Розумні» камери здатні розпізнавати номер, модель, марку транспорту, встановлювати, чи знаходиться він в розшуку, крім того, вони можуть розпізнавати обличчя водія і пасажирів автомобіля (за умови, якщо їх візуально можна побачити), виявляти скупчення людей, оцінювати щільність потоку, виявляти нетипове рух транспорту або людини. Все це на відстані 7-8 метрів. В цілому комплекс, який використовується в UASC, виконує близько 700 функцій.

Крім розшуку автомобіля та розпізнавання осіб, система реагує на звуки, наприклад, коли лунає постріл або вибух.

Всього в Маріуполі планується установка 37 таких камер, а по всій області згодом - 120 - в таких великих містах області як Краматорськ, Покровск, Бахмут, Слов'янськ [3].

А з метою створення комплексної системи безпеки м. Києва в закладах освіти, культури, охорони здоров’я, на входах і виходах станцій метрополітену, основних транспортних магістралях і автомобільних мостах через р. Дніпро, в’їздах і виїздах із міста станом на початок 2017 р. вже встановлено понад 3,7 тис. камер відеоспостереження. Під час нещодавнього відкриття міського Центру обробки даних анонсовано встановлення ще 4 тис. смарт-камер і об’єднання останніх разом із майже 100 тис. камер відеоспостереження, що працюють у державних і приватних установах, з уже наявними системами в єдиний загальноміський комплекс відеоспостереження в межах реалізації програми «Безпечне місто», заснованої на єдиній інформаційно-телекомунікаційній платформі, що використовує найновіші технології обробки великих масивів даних.

Для того, щоб ефективно збирати та аналізувати інформацію з усього міста, спеціально створено хмарну платформу загальною потужністю 11 тисяч каналів, яка забезпечує безперервний запис відеоданих. Інтегровані до системи багатофункціональні смарт-камери мають заздалегідь запрограмований сценарій інцидентів і здатні автоматично інформувати ситуаційний центр про небезпеку. Зокрема, завдяки функції розпізнавання державних знаків за допомогою цих камер столичні поліцейські зможуть ефективніше знаходити викрадені автомобілі. Сьогодні система «Безпечне місто» дає дуже багато для аналізу ситуації на дорогах столиці. Наприклад, дає змогу фіксувати в онлайн-режимі порушення правил дорожнього руху і правил паркування, а також контролювати рух смугою для громадського транспорту. Окремі складові частини цієї системи вже розгорнуті в головних управліннях Національної поліції та Служби безпеки України.

На черзі долучення до цієї системи пожежної, рятувальної, медичної, дорожньої та інших комунальних і державних служб [4].

Сектор безпеки і оборони необхідно формувати як цілісну систему, об'єднану єдиним керівництвом.

Комплексне розв'язання проблеми забезпечення охорони громадського порядку та громадської безпеки не повинно обмежуватися встановленням односторонніх систем безпеки, застосуванням засобів зовнішнього контролю (спостереження) та організацією швидкого реагування на правопорушення в окремо взятих населених пунктах України. Необхідно об'єднати кращі системи безпеки на базі новітньої програмно сумісної інформаційно-телекомунікаційної платформи, що використовує найновіші технології обробки великих масивів даних яка б була єдиною для України та придатною для інтеграції з міжнародними системами аналогічного спрямування.

1. Нові проекти реагування на виклики та звернення громадян [Електронний ресурс] // Департамент комунікації Національної поліції України. – 2016. – Режим доступу до ресурсу: https://www.npu.gov.ua/uk/publish/article/2074762.

2. Поліції Харківщини в роботі сприятиме система ricas [Електронний ресурс] // МВС України. – 2016. – Режим доступу до ресурсу: http://mvs.gov.ua/ua/news/700_Policii_Harkivshchini_v_roboti_spriyatime_sistema_RICAS_FOTO.htm.

3. Перший в Україні Єдиний аналітичний сервісний центр запрацював в Маріуполі [Електронний ресурс] // Інформаційне агентство «ОстроВ». – 2016. – Режим доступу до ресурсу: https://www.ostro.org/donetsk/society/news/515859/.

4. Віталій Кличко відкрив Центр обробки даних: «Новітні технології обробки інформації та впровадження програми «Безпечне місто» дозволять створити комплексну систему безпеки у столиці» [Електронний ресурс] // Київська міська державна адміністрація. – 2017. – Режим доступу до ресурсу: http://kievcity.gov.ua/news/46951.html.

5. Сервіс "102": у нацполції розповіли про роботу системи "цунамі" та навчання операторів екстреної служби [Електронний ресурс] // 5 канал. – 2016. – Режим доступу до ресурсу: https://www.5.ua/suspilstvo/servis-102-u-natspoltsii-rozpovily-pro-robotu-systemy-tsunami-ta-navchannia-operatoriv-ekstrenoi-sluzhby-125248.html.

6. Білоус В. В. Стан і перспективи впровадження прогресивних інформаційних технологій у сфері забезпечення громадської безпеки та

громадського порядку / В. В. Білоус. // Судова та слідча практика в Україні. – 2017. – №3. – С. 62–70.

7. Бараненко Р. В. Дослідження особливостей функціонування програмного забезпечення системи централізованого управління нарядами патрульної служби «цунамі» / Р. В. Бараненко. // Юридичний бюлетень. – 2016. – №2. – С. 129–138.

Деякі аспекти фінансової безпеки

Молдаван Л.С.
курсант ПД–732 Дніпропетровського державного університету внутрішніх справ
Кокарєв І.В.
науковий керівник, доцент Дніпропетровського державного університету внутрішніх справ, кандидат економічних наук, доцент

Критеріями для підтримання фінансової безпеки на макрорівні є її складові, а основними стабілізаційними напрямами можуть бути [1, с. 9-10]:

- забезпечення фінансової стабілізації в країні;
- ліквідація нецільового використання бюджетних коштів;
- стабільність національної грошової одиниці;
- зниження дефіциту державного бюджету;
- здійснення бюджетної реформи;
- виконання дохідної частини державного бюджету;
- удосконалення податкової системи;
- розвиток державної фінансової інфраструктури економічної сфери;
- основні напрями детінізації економіки;
- ліквідація заборгованості із заробітної плати ,пенсій, інших соціальних виплат;
- зниження інфляції;
- позитивне зовнішньоторговельне сальдо;
- створення достатнього золотовалютного запасу держави;
- вдосконалення національної банківської системи.

Основу фінансової безпеки держави в цілому складає її бюджетна безпека. Під фінансовою безпекою розуміється такий динамічний стан фінансових відносин, за якого б створювались сприятливі умови та необхідні ресурси для розширеного відтворення економічного росту та підвищення життєвого рівня населення, удосконалення національної фінансової системи для успішної протидії внутрішнім і зовнішнім факторам дестабілізації фінансового стану в державі [2, с.241].

Як свідчать дослідження, за останні роки стан Державного бюджету характеризується в основному як дефіцитний, що спричиняє не лише зниження рівня бюджетної і фінансової безпеки, а й низку інших наслідків для економіки держави [3].

Фінансову безпеку держави визначає також фінансова безпека банківської системи, яка розглядається в двох аспектах [4, с. 338]. По-перше, з позиції фінансових наслідків діяльності комерційних банків для економічної безпеки країни в цілому та окремих клієнтів і контрагентів. По-друге, з позиції недопущення та відвернення явних і потенційних загроз фінансовому стану банківської системи країни на рівні як центрального банку, так і комерційних банків.

До індикаторів безпеки банківської системи належать:

- відношення активів банків до ВВП;
- розмір чистих внутрішніх активів НБУ (обсяг грошової маси та розмір емісій);
- обсяг чистих зовнішніх резервів НБУ;
- частка активів недіючих банків у загальній сумі активів комерційних банків;
- частка іноземного капіталу у сукупному капіталі банківської системи та ін.

Безпека банківської системи в цілому залежить від безпеки окремого банку та навпаки.

Важливою складовою фінансової безпеки держави є інвестиційна безпека, яку визначають як такий рівень національних та іноземних інвестицій (за умови оптимального їх співвідношення), який здатен забезпечити довгострокову позитивну економічну динаміку при належному рівні фінансування науково-технічної сфери, створення інноваційної інфраструктури та адекватних інноваційних механізмів [5].

Таким чином, фінансова безпека держави формується за рахунок її складових, які повинні складати ефективну систему.

1. М. Голомша. Економічна безпека – основа національних пріоритетів // Вісник прокуратури. - №8. - 2006. – С. 9-10.

2. І. О. Ревак Механізм забезпечення фінансової безпеки України: теоретичний аспект // Науковий вісник Львівського державного університету внутрішніх справ.-№2.-2009. – С. 241.

3. Деменок О. В. Бюджетна безпека України як одна з складових фінансової безпеки держави. [Електронний ресурс] / О. В. Деменок. – Режим доступу: http://www.rusnauka.com/7_NND_2009/Economics/43052.doc.htm

4. Барановський О. І. Фінансова безпека [Текст] / О. І. Барановський; Ін- т екон. прогнозування. – К.: Фенікс, 1999. – 338 с.

5. Методика розрахунку рівня економічної безпеки України, затверджена наказом Міністерства економіки України № 60 від 02.03.2007 р. [Електронний ресурс] / Міністерство економіки України. – Режим доступу: http://www.me.gov.ua/control/uk/publish/article?art_id=97980&cat_id=3873

Попередження та розслідування кіберзлочинів

Оболенцева Я.М.
студентка 1 курсу юридичного факультету
Дніпропетровського державного університету
внутрішніх справ
Махницький О.В.
науковий керівник, старший викладач кафедри
економічної та інформаційної безпеки
Дніпропетровського державного
університету внутрішніх справ

У наші дні використання інформаційних технологій не має меж. Віртуальний простір переймає від реального все підряд, у тому числі й злочинність у її нових формах і проявах. Практично кожен чув про кіберзлочинність і, можливо, навіть особисто з нею зіштовхувався. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера і в мережі Інтернет. Об'єктом кіберзлочинів є персональні дані, банківські рахунки, паролі та інша особиста інформація як фізичних осіб, так і бізнесу та державного сектору.

Кіберзлочинність є загрозою не тільки на національному, а й на глобальному рівні.

На сьогодні комп'ютерні злочини - це одна з найдинамічніших груп суспільно небезпечних посягань . Швидко збільшуються показники поширення цих злочинів, а також постійно зростає їх суспільна небезпечність. Це зумовлене прискореним розвитком науки й технологій у сфері комп'ютеризації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки.

Розповсюдження комп'ютерних вірусів, шахрайства з пластиковими платіжними картками, крадіжки коштів з банківських рахунків, викрадення комп'ютерної інформації та порушення правил експлуатації автоматизованих електронно-обчислювальних систем - це далеко не повний перелік подібних злочинів. Дану категорію злочинів називають по-різному: кіберзлочини, комп'ютерні злочини, злочини в сфері комп'ютерних технологій, злочини в сфері комп'ютерної інформації. В літературі найчастіше зустрічаються два терміни: кіберзлочини та комп'ютерні злочини. Оскільки вони використовуються для назви одних і тих самих суспільно-небезпечних діянь, то їх можна вважати синонімами та рівнозначними. Поняття "кіберзлочин" молоде і утворено сполученням двох слів: кібер і злочин. Термін "кібер" має на увазі поняття кіберпростору та інформаційний простір, що моделюється за допомогою комп'ютера. Тобто кіберзлочини – це суспільно-небезпечні діяння, які так чи інакше пов'язані з кіберпростором та комп'ютерною інформацією, що моделюється комп'ютерами. Такі злочини характеризуються наступними особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказу в суді подібних справ, транснаціональною складовою в основному з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного злочину.

Специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, практично не відходячи від "робочого місця", злочини є доступними; оскільки комп'ютерна техніка постійно дешевшає; злочини можна скопіювати з будь-якої точки земної кулі, у будь-якому населеному пункті, а об'єкти злочинних посягань можуть знаходитись за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично-значущу інформацію при виконанні слідчих дій для використання її в якості речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців.

Об’єктом кіберзлочинів може стати будь-який користувач інтернету.

Найпоширенішими видами таких злочинів є:

Кардинг – використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

Фішинг – вид шахрайства, відповідно до якого клієнтам платіжних систем надсилають повідомлення електронною поштою нібито від адміністрації або служби безпеки цієї системи з проханням вказати свої рахунки та паролі.

Вішинг – вид кіберзлочинів, у якому в повідомленнях міститься прохання зателефонувати на певний міський номер, а при розмові запитуються конфіденційні дані власника картки.

Онлайн-шахрайство – несправжні інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку.

Піратство – незаконне розповсюдження інтелектуальної власності в Інтернеті.

Кард-шарінг – надання незаконного доступу до перегляду супутникового та кабельного TV.

Соціальна інженерія – технологія управління людьми в Інтернет-просторі.

Мальваре – створення та розповсюдження вірусів і шкідливого програмного забезпечення.

Протиправний контент – контент, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства.

Рефайлінг – незаконна підміна телефонного трафіку.

Сукупність потреб, задоволення яких забезпечує існування і можливість прогресивного розвитку кожного громадянина, суспільства і держави – це частина національних інтересів, без реалізації яких неможливо забезпечити стабільний стан держави і суспільства, а також нормальний розвиток країни як незалежного суб’єкта міжнародних відносин. Усі інтереси, що захищаються, в інформаційній сфері підрозділяються на інтереси особи, держави, суспільства. Проблема кіберзлочинності нині зачіпає як цілі країни, так і окремих осіб. Інформаційна безпека вже розглядається державами як одне з пріоритетних завдань у сфері національної безпеки та міжнародної політики. При цьому концепція інформаційної безпеки включає як

захист користувачів мереж, так і захист держави у цілому. Однак, оскільки жодна держава не може захистити себе, здійснюючи заходи лише на національному рівні, для комплексної протидії кіберзлочинності необхідні:

– гармонізація кримінального законодавства про кіберзлочини на міжнародному рівні;

– розробка на міжнародному рівні та імплементація в національне законодавство процесуальних стандартів, що дозволяють ефективно розслідувати злочини в глобальних інформаційних мережах, отримувати, досліджувати і представляти електронні докази з урахуванням транскордонності цієї проблеми;

– налагоджене співробітництво правоохоронних органів при розслідуванні кіберзлочинів на оперативному рівні;

– механізм вирішення юрисдикційних питань у кіберпросторі.

На сучасному етапі важливу роль у боротьбі з кіберзлочинністю відіграють спеціалізовані міжнародні угоди (наприклад, Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в області кіберзлочинності для країн Африки (проект ESCWA), однак вони не є за своєю суттю універсальними міжнародними інструментами, незважаючи на те, що деякі з них вийшли за своїм впливом далеко за рамки регіону, в якому вони були прийняті.

Таким чином, кіберзлочинність є порівняно новим видом суспільно небезпечних діянь, проте на відміну від традиційних крадіжок і шахрайства, вона постійно удосконалюється і йде в ногу з технологіями, що у свою чергу ускладнює виявлення та протидію зазначеним протиправним діям. Ефективний контроль за кіберзлочинністю вимагає більш інтенсивного міжнародного співробітництва, ніж існуючі заходи по боротьбі з будь-якими іншими формами транснаціональної злочинності.

1. [Електронний ресурс]– Режим доступу: https://www.gurt.org.ua/articles/34602/

2. [Електронний ресурс] – Режим доступу: https://www.science-community.org/ru/node/16132

3. [Електронний ресурс] – Режим доступу: http://www.anticyber.com.ua/ article_detail.php?id=220

4. [Електронний ресурс] – Режим доступу: https://internationalconference2014.wordpress.com

Інноватика в освітньому процесі: досвід та перспективи

Пацамай М.П.
курсант 402 взводу факультету №1 Одеського державного університету внутрішніх справ
Шелехов А.О.
науковий керівник, завідувач кафедри адміністративної діяльності ОВС та економічної безпеки Одеського державного університету внутрішніх справ, к.ю.н., доцент

Останнім часом поняття «інноватика» досить широко поширилося у всіх сферах людського життя як продуктивний результат науково-технічного прогресу і фактично стало характеристикою ефективності функціонування діяльності. Сьогодні ж інноватика визначає рівень соціального, економічного, технологічного, оборонного, культурного, інтелектуального розвитку країни. Особлива увага приділяється інноваційним процесам у сфері освіті, адже саме від неї залежить якість підготовки, накопичення знань, досвіду та результати практичної діяльності фахівців усіх галузей.

Актуальність теми дослідження полягає у аналізі сучасної інноватики в освітньому процесі, а саме зарубіжного досвіду організації безперервної освіти та її існування в Україні.

Питання інноватики освітніх процесів досліджували такі вітчизняні науковці, як І.Д. Бех, М.В. Кларін, С.В. Красножон, О.І. Крюков, С.М. Луценко, В.І. Міщенко, В.А. Піддубний, О.В. Попова, Ю.І. Приходько, В.М. Телим, А.В. Хуторський та інші.

Вітчизняний науковець Міщенко В.І. зазначає, що організація та забезпечення безперервної освіти є одним з найважливіших завдань сучасного суспільного розвитку, так як безперервність здобуття знань стає основним принципом функціонування освітньої системи в цілому, що передбачає залучення до освітнього процесу людини впродовж усього її життя і є необхідністю задля прогресу людства [1, С. 9]. І ми погоджуємося з ним, адже все життя людина отримує нові знання, навички в результат саморозвитку та впливу соціуму.

Зарубіжний досвід безперервності освіти дає змогу виділити такі форми отримання знань, як формальна, що включає в себе дошкільну, шкільну та вищу освіту, неформальна – освітні курси, клуби, гуртки, народні університети та інформальні – самоосвіта, життєвий досвід [2, С. 126].

На нашу думку безперервність освіти являє собою можливість людини формувати та здобувати необхідний багаж знань у різних галузях відповідно до існуючих особистих потреб та задля суспільних необхідностей. Обов'язковою тут є роль держави, яка повинна всіляко сприяти цьому процесу, адже і в її інтересах мати кваліфікованих спеціалістів з удосконаленими навичками.

У світі ще в середині минулого століття значного розголосу набуло питання безперервної освіти. Так 1965 року на форумі ЮНЕСКО були озвучені загальні положення концепції «безперервної освіти», що ґрунтувалися на людиноцентриській позиції та необхідності створення умов для повного розкриття здібностей людини протягом усього життя. У рекомендаціях ЮНЕСКО неперервна освіта розумілась як глобальний проект щодо реконструкції системи освіти. У Доповіді Міжнародної комісії з освіти зазначалось: «Освіта впродовж життя є багатостороннім діалектичним процесом. У ньому поєднуються неформальні та формальні знання, розвиток вроджених здібностей та набутих навичок. Цей процес потребує зусиль й водночас є радісним через відкриття нового. Як індивідуальний досвід кожного, він є найбільш складним видом соціальних відносин, оскільки стосується одночасно культури, праці і громадськості» [3, С. 5].

У Гамбурзькій декларації 1997 року було сформульовано основні ідеї безперервної освіти дорослих упродовж життя й рекомендації усім урядам країн – вважати освіту дорослих за пріоритетний напрям державної політики. Метою безперервного навчання ж було підвищення кваліфікації, перепідготовка або просування по службі, відкриття нових можливостей щодо нового шансу в житті, задоволення прагнення до знань і удосконалення, покращення професійної діяльності та практичної підготовки [4, С. 223].

Сьогодні структура безперервної освіти багатьох країн (Великобританія, Канада, Польща, Франція, Німеччина) є складовою державної політики у сфері освіти. Створені державні та приватні університети, центри безперервної освіти, які покликані допомогти людям отримати нові спеціальності, що здатні забезпечити матеріально та створити внутрішній комфорт самодостатньої особистості. У Швеції

освітою дорослих займаються народні університети (їх є понад100), у Польщі освіту дорослих організовує не держава, а громадські товариства і організації. Європейські країни намагаються підвищити функціональну грамотність дорослого населення, тобто вміння ефективно виконувати професійні та соціальні функції [5, С.12].

В Європі власні фірми мають, як правило, власні системи підготовки, перепідготовки і підвищення кваліфікації кадрів. Це мережа спеціальних навчальних закладів, які мають сильну матеріально-технічну базу, штати висококваліфікованих викладачів. У ділових колах справедливо говорять у цьому зв'язку про перетворення корпорацій в «інститути безперервної освіти». У сучасних умовах на передній план висувається надзвичайно важлива задача– забезпечити підготовку працівників нового типу(робітника, фермера, менеджера), професійними якостями якого є гнучкість і мобільність, здатність перекваліфікуватися чи навіть змінити професію. Обов'язкові елементи перекваліфікації – солідна загальна підготовка, широка професійна підготовка і високий культурно-технічний рівень, вміння швидко поповнювати свої знання [1, С. 14].

З огляду на сучасні світові тенденції у Концепції гуманітарного розвитку України передбачено створення в державі дієвої системи безперервної освіти, основним завданням якої визначено здійснення якісних змін у системі підвищення кваліфікації та підготовки кадрів відповідно до тенденцій розвитку ринку праці та потребам людини удосконалювати власний освітній рівень протягом усього життя. Значний внесок у забезпечення неперервної освіти населення здійснюють громадські організації, хоча їх фінансування є незначним і епізодичним. Однак такі організації мають кваліфікований штат лекторів та інструкторів, налагоджені постійні контакти з різними соціальними верствами і віковими групами населення, організаціями та установами на всій території України. [4, С. 223]. Та теперішня вітчизняна система безперервності освіти є інституційно роздрібненою, не має достатніх ознак системності, характеризується відсутністю надійних механізмів стимулювання та недостатньо забезпечена фінансово. На наш погляд, вітчизняна система неперервної освіти має охоплювати професійне навчання та підвищення кваліфікації, розширювати сфери наукових знань, задовольняти потреби людей у підвищенні соціально-культурного рівня та пізнавальні потреби. Тому за фаховим спрямуванням це може бути економічна, правова, екологічна, соціальна, історико-культурна освіта тощо.

Отже, сьогодні в Україні приділяється недостатня увага цим проблемам і, зокрема, питанням неперервної освіти дорослих. З метою вдосконалення цього процесу необхідними є розроблення системи заходів для законодавчого визначення та закріплення поняття безперервної освіти у законодавстві, обґрунтування напрямів і джерел фінансування освітніх заходів як державою, так і громадськими організаціями та запровадження дієвих стимулів для освітніх закладів щодо розширення сфер і видів безперервної освіти. Формування та розвиток неперервної освіти в Україні треба розглядати як важливу складову формування громадянського суспільства, елемент економічної та політичної незалежності країни, систему, що сприяє всебічному розвитку та піднесенню добробуту людей. Тож необхідним є розроблення стратегії або концепції розвитку безперервної освіти в Україні, а також координація практичної роботи у цій сфері державних органів, галузевих установ, підприємств і громадських організацій.

---

1 Міщенко В. І. Зарубіжний досвід та вітчизняні актуалітети організації неперервної освіти / В.І. Міщенко // Рідна школа. - 2014. - № 11. – С. 9-16

2. Кремень В.Г. Філософія людиноцентризму в освітньому просторі / В.Г. Кремень // К:. Т-во «Знання». – 2014. – 520 с.

3. Освіта: прихований скарб: Доповідь Міжнародної комісії з освіти XXI століття. – Видавництво ЮНЕСКО. – 1996. – 31 с.

4. Крюкров О.І., Луценко С.М. Інноваційна освіта як один із основних ресурсів модернізації сучасної держави / О.А. Крюков, Луценко С.М. // Педагогіка вищої на середньої школи. – 2015. – Вип. 44. – С. 221-226

5. Швець Є.Я., Швець Д.Є. Формування концепції безперервної освіти «Новому століттю-нову освіту» в умовах європейської інтеграції вищої освіти / Є.Я. Швець, Д.Є. Швець // Гуманітарний вісниу ЗДІА. – 2013. - №55. – С. 5-16

Попередження та розслідування кіберзлочинів

Паєцик К.С.
студентка першого курсу ЮД-743 ДДУВС
Вишня В.Б.
науковий керівник, професор кафедри економічної та інформаційної безпеки ДДУВС, доктор технічних наук, професор

Кіберзлочинність є явищем міжнародного значення. Її рівень перебуває у прямій залежності від рівня розвитку та впровадження сучасних комп'ютерних технологій, мереж їх загального користування та доступу до них. Стрімкий розвиток інформатизації в Україні несе за собою потенційну можливість використання комп'ютерних технологій з корисливих та інших мотивів, що певною мірою ставить під загрозу не лише національну безпеку держави, а й особисті, майнові, немайнові та інші права і свободи громадян.

Проблематика попередження злочинності у сфері інформаційних технологій та кіберебезпеки досить часто обговорюється фахівцями в інформаційній сфері в журналах, на конференціях, круглих столах і засобах масової інформації. Деякі аспекти попередження кіберзлочинності вивчали та обговорювали у своїх статтях С. Битко, В. Бутузов, А. Волеводз, Д. Дубов, Н. Дубова, С. Кльоцкін, В. Мілашев, М. Литвинов, В. Мохор, Т. Тропіна, В. Хахановський та інші.

Станом на сьогоднішній день кількість кіберзлочинців в Україні достатньо невелика. В групі кіберзлочинців розрізняють дві категорії: Люди віком з 15 до 21 років, а також з 21 і більше. Розрізнити ці дві групи можливо по цілі їх злочину. Якщо в першій групі найчастішою метою є просто бешкетництво, то в другій це детально-поміркований злочин, з метою розкрадання або руйнування інформації в інформаційних системах і мережах.

Попередження злочинності складається зі стратегій і заходів, спрямованих на зниження ризику вчинення злочинів і нейтралізацію потенційно шкідливих наслідків для приватних осіб і суспільства в цілому. У багатьох випадках стратегії протидії кіберзлочинності є невід'ємною частиною стратегій забезпечення кібербезпеки. Ефективна

та успішна боротьба з кіберзлочинцями неможлива без детального аналізу образу мислення і особи порушника .

В багатьох країнах створені спеціалізовані підрозділи які виявляють, розслідують, а також вистежують злочинців. Звісно ці ж підрозділи займаються пошуком інформації з цього питання на національному рівні. Таким чином допустимо вважати ці підрозділи головним рушійним механізмом у боротьбі з кіберзлочинністю.

Для боротьби із загрозою кіберзлочинності, яка, безумовно, зростатиме з подальшим розширенням сфери використання інформаційних технологій, надаючи великі можливості для протиправної діяльності як індивідуумам, так і злочинним групам, необхідна постійна міжнародна співпраця. Контролювати кіберзлочинність і боротися з нею на рівні окремої держави практично неможливо.

Виходячи з вищевикладеного, можна зробити висновок, що протидія кіберзлочинності – це частина національних інтересів держави. Кіберзлочинність уже стала великою проблемою для всього світу, і проблема нестримно наростає. Правоохоронні органи намагаються поспіти за нею: законодавці ухвалюють нові закони, поліцейські агентства формують спеціальні підрозділи по боротьбі з кіберзлочинністю. Кіберзлочин як і будь-який інший злочин є не лише правова, але і соціальна проблема. Тому є велика потреба в боротьбі з проблемою яка може в майбутньому повністю поглинути систему інформаційної діяльності.

1. Іванченко О. Ю. / Криміналістична характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні/ 6 с.

2. О. В. Орлов., Ю. М. Онищенко / Попередження кіберзлочинності – складова частина державної політики в Україні. / 7 с.

3. Актуальні питання розслідування кіберзлочинів : матеріали Міжнар. наук.-практ. конф., м. Харків, 10 груд. 2013 р. / МВС України, Харк. нац. ун-т внутр. справ. – Х. : ХНУВС, 2013. – 272 с

Застосування сучасних технологій підрозділами поліції

Пивовар Д.О.
курсант Дніпропетровського
державного університету внутрішніх справ
Прокопов С.О.
науковий керівник, старший викладач Дніпропетровського державного університету внутрішніх справ

У наш час досить багато новітніх технологій, які б значно полегшили розслідування злочинів та за допомогою яких можуть фіксуватися усі процесуальні дії, встановлені Кримінально-процесуальним законодавством. Проте існує багато причин, через які в Україні користуються тією ж технікою, що і 20-30 років тому.

Проблемам розробки та впровадження інноваційних технологій у практичну діяльність правоохоронних органів приділяли увагу у своїх працях вітчизняні та зарубіжні науковці: В. В. Бірюков, В. Ю. Шепітько, Р. С. Бєлкін, В. О. Коновалова, І. Ф. Крилов, М. В. Салтєвський, О. Р. Россинська, М. Л. Цимбал, М. Я. Сегай та ін.

Впровадження новітніх технологій у діяльність слідчого здійснюється за декількома напрямами: 1) розробка та використання нових науково-технічних засобів для виявлення, збирання та попереднього дослідження доказів; 2) пропонування ідей щодо застосування інновацій; 3) запровадження новітніх прийомів, методів, методик проведення слідчих (розшукових) дій та розслідування в цілому [1,с. 91].

Сьогодні більше уваги приділяється розробці ефективних засобів, прийомів, способів, методик для виявлення і дослідження вербальної інформації (одержаної на основі мовного повідомлення),що в свою чергу розширює доказову базу за матеріалами кримінального провадження. На жаль, злочинність також не стоїть на місці і весь час розвивається, тому збільшуються потреби правоохоронних органів у розробці нових технологій, які полягають у роботі з ідеальними слідами. Зазначене завдання може бути вирішене за допомогою впровадження сучасних інформаційних та інноваційних технологій, спрямованих на актуалізацію ідеальних слідів.

Зараз велика увага приділяється впровадженню у слідчу та експертну практику нової методики відновлення сліду пам'яті зовнішності розшукуваної особи з використанням комп'ютерної програми й засобів комп'ютерної графіки з метою побудови фотокомпозиційних портретів зі слів очевидців. Тобто, система «RAIPS-портрет», яка була розроблена в Науково-дослідному інституті вивчення проблем злочинності імені академіка В. В. Сташиса НАПрН України. Зазначена методика, реалізована в системі «RAIPS-портрет», ґрунтується на врахуванні психологічних особливостей сприйняття, пригадування, впізнання та відтворення зовнішності людини й активізації асоціативної пам'яті очевидця при спогаді раніше спостережуваної особи й фіксації суб'єктивного образу у вигляді фотозображення, що дає можливість скласти фоторобот навіть при наявності негативних чинників (погані умови спостереження, емоційний стан потерпілого тощо). Реалізований у системі «RAIPS-портрет» метод відображення у фотороботі ідеального сліду сприяв створенню електронного каталогу складених фотороботів. У процесі складання комп'ютерного фоторобота актуалізація (відновлення) сліду пам'яті зовнішності здійснюється шляхом використання різних способів активізації асоціативних зв'язків. При складанні комп'ютерного фоторобота з використанням системи «RAIPS-портрет» деякі фахівці до технічних прийомів відносять можливість повернення до будь-якого пункту алгоритму (тобто складання словесного портрета, пошук групи схожих портретів, формування групи подібності, побудова, ретушування й збереження фоторобота) і повторне виконання відповідних процедур зі збереженням раніше отриманих результатів.

Для розкриття та розслідування злочинів заслуговує на увагу аналіз можливостей використання інструментального методу – дослідження на поліграфі. Поліграфний пристрій («лай-детектор», «варіограф», «плетизмограф», «детектор неправди») є багатоцільовим приладом, багатоканальним осцилографом для одночасної реєстрації кількох (до 20) різних функцій організму – фізіологічних процесів (дихання, тиску, біострумів тощо), пов'язаних із виникненням у особи емоційного стану при впливі на особу словесних подразників.

Як приклад можна навести статистику за 2000-2006 роки. У 2000 році наказом ГУБОЗ МВС України № 1дск було запроваджено застосування поліграфів у кадровій роботі та оперативно-розшуковій діяльності підрозділів у боротьбі з організованою злочинністю.

У впродовж 2000–2006 років було проведено 1757 опитувань осіб на поліграфі, у тому числі 1020 – під час проведення оперативно-розшукових заходів і 737 – для вирішення питань кадрового забезпечення, зокрема, встановлено причетність близько 230 осіб до вчинення понад 120 злочинів.

Також популярності у іноземних державах набула 3D-візуалізація місця події, яка досягається за допомогою 3D-фотозйомки або за допомогою застосування 3D-сканерів. Результат їх застосування можна охарактеризувати як фотографічну модель. Дана модель досить об'єктивна внаслідок того, що вона відносно точно відображає обстановку події, однак не характеризується гнучкістю, оскільки в ній, як правило, містяться об'єкти як пов'язані, так і ті які не відносяться до події, внаслідок чого може виникнути необхідність у зміні фактичного змісту [2,с. 43].

Як зазначає американське видання «3Ders», поліцейська дільниця в місті Розуел Нью-Мексико нещодавно придбала Faro 3D-сканер, який дозволить слідчим (а потенційно і судам) виробляти 3D-візуалізацію місця злочину – оцифрований панорамний вигляд місця події [3, с. 136].

Поліція стверджує, що інформація буде подаватися з точністю до «пари міліметрів», так що слідчі, судді і журі присяжних буде мати «дуже точне графічне уявлення про те, що являло собою місце події». Вважається, що це буде кроком у бік якісного поліпшення відомих способів фіксації місця події за допомогою стандартної камери, і що з її допомогою можна буде дійсно запобігти можливим помилкам, які іноді допускаються правоохоронними органами. Щоб заощадити гроші, в Балтиморській поліцейській криміналістичній лабораторії техніки перетворили недорогу програму, призначену для ремонту будівель, в інструмент, що наочно демонструє, як відбувалося вбивство, зґвалтування та т.п. Використовуючи «Floor Plan Plus», криміналістична лабораторія на основі ескізів і фотографій з місця події відтворює його на екрані комп'ютера [2, с. 15].

Отже, застосування сучасних технологій органами поліції в Україні залишається відкритим та дискусійним питанням. З одного боку усі можливості дозволяють користуватися інноваціями у кримінальному провадженні, проте з іншого, до цих технологій вдаються лише під час розслідування резонансних злочинів.

1. Шепітько В. Ю. Вибрані твори / Валерій Юрійович Шепітько. – Х. : Апостіль, 2010. – 576 с.

2. Вандер М.Б. / Применение научно-технических средств при расследовании преступлений / Конспект лекций. – СПб., 2000. – 60 с

3. Бирюков В.В. Научные и практические основы использования компьютерных технологий для фиксации криминалистически значимой информации / В.В. Бирюков. – Монография. – Луганск: РИО ЛАВД, 2002. – 230 с.

4. Бірюков В.В. Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування / Автореф. дис… канд. юрид. наук: 12.00.09 / . – К., 2001. – 20 с.

Застосування новітніх інформаційних технологій в навчальному процесі при підготовки фахівців правоохоронних органів України

Питюренко К.Д.
курсант IV курсу факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Краснобрижий І.В.
науковий керівник, к.ю.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

Одним із пріоритетних напрямів інформатизації суспільства стає процес інформатизації освіти, який передбачає використання нових інформаційних технологій. Стрибок у розвитку персональних комп’ютерів як технічних засобів навчання за останній час зробив їх доступними для використання в навчальних закладах. Тому введення комп’ютерних технологій у начальний процес можна описати як необхідний крок у розвитку сучасного інформаційного світу. Підтвердженням цього може служити виникнення цілої низки спеціальних наукових центрів, що безпосередньо займаються проблемами інформатизації й комп’ютеризації освіти .

Особливості використання інформаційних технологій у навчальному процесі розглядали А. Єршов, М. Жалдак, Є. Клементьєва, В. Лавринець, Є. Машбиць, В. Монахов, О. Пєхота, І. Підласий, С. Смирнов та ін.

У науково-технічній літературі інформаційні технології (далі- ІТ) – це системи, що є комплексом програмно-апаратних засобів,

устаткування, які можуть поєднувати різні види інформації і реалізувати діалог між системою та користувчем [1]. У педагогічній літературі під інформаційними технологіями розуміють методологію і технологію навчально-виховного процесу з використанням новітніх електронних засобів навчання й у першу чергу ЕОМ [2].

Використання студентами чи курсантами мобільних пристроїв під час занять дозволяє звернутися до величезного обсягу інформації та перетворити її на знання, що знаходиться у всесвітній мережі, виокремити необхідний матеріал. Проте Л. Толстой зазначав, що знання лише тоді знання, коли здобуті зусиллями думки, а не самою пам'яттю [3].

Використання новітніх технологій та мережі Інтернет для перевірки власних знань або отримання нової інформації під керівництвом викладача підвищує інтерес до навчання, мотивацію до самоосвіти студентів вищих навчальних закладів. Вибір викладачем оптимальних для процесу навчання технологій зумовлюється багатьма чинниками, зокрема: особливості контингенту студентів та курсантів, специфіка навчального процесу, рівень матеріально-технічного забезпечення, завдання навчальної дисципліни. Доцільність упровадження новітніх технологій навчання дозволяє визначити такі напрями застосування інформаційних технологій:

По-перше, використання ІТ у процесі занять для підвищення ефективності навчально-пізнавальної діяльності студентів та курсантів. ІТ доцільно впроваджувати в навчально-виховний процес як на лекційних, так і на практичних та семінарських заняттях. У процесі проведення лекцій дієвим є використання інтерактивної дошки, мультимедійного супроводження, що дозволяє не тільки унаочнити процес навчання, а й максимально збільшити обсяг інформації за обмежений час. На практичних заняттях студенти і курсанти активно застосовують наявні електронні посібники, самостійно створені навчальні матеріали з використанням універсальних інструментальних комплексів для розробки та редагування різного роду навчальних програм.

По-друге, використання ІТ під час самостійної роботи студентів і курсантів створює сприятливі умови для самореалізації , надає можливість кожному обирати послідовність, обсяг оволодіння матеріалом, здійснювати самоконтроль

По-третє, застосування ІТ у навчально-виховному процесі передбачає ретельну підготовку викладача до занять, створення

електронних варіантів лекцій, підготовку мультимедійних презентацій, що значно підвищує ефективність сприйняття навчального матеріалу студентами і курсантами, дозволяє збільшити обсяги інформації для засвоєння на лекції. Сучасні інструментальні засоби відкривають можливості для візуалізації навчальних матеріалів і створення електронних підручників, посібників, практикумів, що активно використовувалися б у начальному процесі. Тому актуальним є питання створення електронних бібліотек з курсами дисциплін, які викладаються в навчальному закладі.

По-четверте, використання у навчальному процесі можливостей інформаційних технологій відкриває перспективи для дистанційного навчання. Так одним із шляхів оптимізації навчання студентів заочної форми може стати розміщення на WEB-сторінках кафедр навчально-методичних матеріалів щодо самостійного вивчення дисциплін.

Негативним моментом використання інтерактивних пристроїв під час заняття є те, що процес роботи з ними відволікає увагу слухачів, та під час пояснення викладачем теми чи проведенні практичного заняття, тобто студент або курсант не засвоїть матеріал у повному обсязі. Необхідно вивчення та впровадження в навчальний процес Інтернет ресурсів, що призводить до необхідності вироблення та розвитку навичок та умінь роботи з ними. Також негативним моментом використання мобільних пристроїв є обмежений час роботи, тобто під час лекції чи заняття в мобільному пристрої може закінчитись заряд, що призведе до автоматичної неможливості виконання завдань чи користування ресурсом студентами [4]

Отже, впровадження інформаційних технологій навчання є пріоритетним напрямом у системи вищої освіти. Виконуючи навчальну, виховну й дослідну функції, зазначені технології можуть застосовуватися як на етапі підготовки до проведення занять, створенні навчально-методичного забезпечення, так і під час навчально-виховного процесу й у поза аудиторній роботі. Використання інформаційних технологій дозволяє створити принципово нову інформаційну освітню сферу, що надає широкі можливості для навчальної діяльності, значно впливає на перерозподіл ролей між її учасниками, підвищує мотивацію, розвиває самостійність, сприяє модернізації традиційної системи навчання.

1. Палагутина М. А. Инновационные технологии обучения иностранным языкам // М. А. Палагутина, И. С. Серповская // Проблемы и перспективы раз- вития образование: Материалы междунар. заоч.

науч.конф. – Пермь: Меркурий, 2011. – С. 156–159. Серія «Педагогічні науки» Вісник КрНУ імені Михайла Остроградського. Випуск 1/2015 (2). 109

2. Щукин А. Н. Обучение иностранным языкам: теория и практика /А. Н. Щукин // Учебное пособие для преподавателей и студентов – М.: Фило- матис, 2006. – 480 с.

3. Толстой Л. Круг чтения. Афоризмы и наставления // Л. Толстой. – М., 2013. – 7 с.

4. Мартиненко С. М. Лекції із загальної педагогіки: навч. посіб. / С. М. Мартиненко, Л. Л. Хорунжа. – 4-е вид., стер. – К.: КМПУ ім. Б. Д. Грінченка, 2005. – 138 с.

Сучасні біометричні технології віддаленого банкінгу

Притула А.О.
студентка кафедри захисту інформації Запорізького національного технічного університету

Нестеров О.І.
студент кафедри захисту інформації Запорізького національного технічного університету
Куцак С.В.
науковий керівник, старший викладач кафедри захисту інформації Запорізького національного технічного університету

Частка безготівкових банківських операцій на ринку фінансових послуг з кожним днем зростає, а разом з нею зростає і кількість злочинів пов’язаних з несанкціонованим втручанням в системи дистанційного (віддаленого) банківського обслуговування (ДБО). Так, за даними Національної поліції щодня в Україні відбувається сотні крадіжок коштів громадян з банківських карт, що в річному еквіваленті перевищує 400 мільйонів гривень.

Різноманіття систем ДБО (найбільш поширені Internet-banking, Mobile-banking та системи «Клієнт-Банк») дає можливість оперативно і зручно надавати клієнтам (користувачам) сотні банківських послуг в будь-який час і в будь-якому місці земної кулі.

Оскільки електронні платіжні системи базуються на використанні телекомунікаційних технологій, то останні є безпосереднім каналом, через який відбувається несанкціоноване, злочинне втручання в процес обробки банківських транзакцій.

В основі захищеної роботи систем віддаленого банкінгу лежить авторизація користувачів – надання певній особі або групі осіб прав на виконання певних дій, а також процес перевірки (підтвердження) даних прав при спробі виконання цих дій. Складовою процесу авторизації є процедура автентифікації – визначення достовірності клієнта банківською установою і надання йому санкціонованого доступу до платіжної системи.

Проведений аналіз показав, що в банківських системах, як правило, застосовуються системи двофакторної автентифікації [1], засновані на одноразових E-mail- або SMS-паролях і різних типах токенів (апаратних криптографічних USB-ключах). Прикладом двофакторної автентифікації є авторизація Google і Microsoft, коли користувач заходить з нового пристрою, крім автентифікації за логіном-паролем, його просять ввести шестизначний (Google) або восьмизначний (Microsoft) код-підтвердження. Сьогодні кілька компаній пропонують системи двофакторної автентифікації, засновані на генерації одноразових паролів (One-Time Password - OTP), в числі яких RSA Security, VASCO Data Security і ActivIdentity.

На сьогоднішній день використовуються такі види автентифікації:

1. Для АТМ (банкоматів, терміналів з використанням банківських карток та операцій без картки): логін; пароль (як постійний, так і одноразовий); номер телефону.
2. Для систем «Клієнт-банк »: логін та пароль; ключ шифрування для цифрового підпису (USB-носій, CD-диск або вбудований пристрій пам’яті).
3. Для Інтернет-банкінгу: логін та пароль(як постійний, так і одноразовий); SMS-повідомлення або телефонний дзвінок; QR-коди [2].

Розробники систем захисту ДБО сподівалися, що введенні ними методи автентифікації зведуть до мінімуму атаки на платіжні системи. Але на практиці значна кількість цих методів є неефективною. Ось декілька вразливих місць в захисті віддаленого банкінгу: крадіжка банківських карт, крадіжка логінів та паролів шляхом підключення шкідливих програм зчитування інформації, підміна (дублювання) SIM-карт.

З огляду на вище сказане, можна стверджувати, що банківські системи потребують додаткового захисту з введенням більш дієвих методів (механізмів) автентифікації. Такі механізми базуються на біометричних технологіях [3].

На сьогоднішній день найбільш поширенішими напрямками біометричної автентифікації є [4]:

– сканування відбитків пальців (Touch ID). Дана технологія частково застосовується в системах Інтернет-банкінгу там, де користувачі використовують комунікатори (сматрфони, ноутбуки або планшетні комп'ютери) з можливістю введення біометричних даних;

– розпізнавання за обличчям та голосом. Метод використовується в сучасних смартфонах (iPhone) для підтвердження входу;

– геометрія рук;

– райдужна оболонка ока.

Біометричні методи захисту інформації в платіжних системах є більш надійними, але дороговартісними. Враховуючи колосальні збитки, які несуть фінансові установи (як грошові та і репутаційні) через несанкціоноване втручання в електронні платіжні системи, додаткові витрати на впровадження біометрії значно б покращили стан захищеності ДБО. А це, в свою чергу, знизило б рівень злочинності в фінансовому секторі держави.

1. Евсеев С.П. Исследование методов двухфакторной аутентификации / С.П. Евсеев, О.Г. Король // Системи обробки інформації. – 2012. – № 2(118). – С. 81-87.

2. Інтернет-банкінг «iFobs» [Електронний ресурс]: – Режим доступу: https://crystalbank.com.ua/korporativnim-klientam/internet-banking-ifobs.

3. Зубок М. І. Безпека банківської діяльності: Навч.-метод. посібник для самост. вивч. дисц . [Текст] / М. І. Зубок, — К.: КНЕУ, 2003. — 156 с.

4. Использование банками биометрических технологий [Електронний ресурс]: – Режим доступу: https://forex-investor.net/ispolzovanie-bankami-biometri cheskikh -tekhnologij.html

Сутність та особливості здійснення рейдерства

Северін М.І.
студент 1 курсу спеціальність «Менеджмент», ДДУВС
Соломіна Г.В.
науковий керівник, к.е.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

Рейдерство, в сучасному розумінні, знищення компанії і перерозподіл її власності та корпоративних прав, з'явилося у США в 60-70-х роках XX століття. Найпершим рейдером, за оцінками спеціалістів, став Джон Рокфеллер, засновник Standart Oil, який різними способами скуповував акції своїх конкурентів для зміцнення і процвітання власного бізнесу ще наприкінці XIX століття.

Вітчизняне рейдерство умовно можна поділяється на два періоди: перший - початок 90-х років до 2000 року (підприємства захоплювали відверто кримінальним шляхом, досить часто із застосуванням фізичного насильства); другий період, започаткований 2000 року, триває донині і характеризується напівзаконним загарбанням підприємств, більш легальними методами боротьби та активним протистоянням рейдерству.

Рейдери - це команда висококваліфікованих спеціалістів із захоплення фірми або із перехоплення управління за допомогою навмисне розіграного бізнес-конфлікту. Умовно їх поділяють на наймані структури, що працюють під егідою великої бізнес-структури, та на «вільних авантюристів» - незалежні команди.

Основна мета рейдерства - приборкання великого бізнесу, великих фірм, підприємств, захоплення значних площ, земельних ділянок, обладнання і нерухомості.

У сьогоднішніх умовах спеціалісти поділяють рейдерів на білих і чорних. Перші діють методом корпоративного шантажу в рамках чинного законодавства. Другі, для отримання результату використовують кримінальні методи (захоплення, підробка документів, реєстрація компаній на підставних осіб, підкуп силових структур, чиновників, суддів і судових виконавців, фізичне усунення невигідних осіб) [3].

Виділяють наступні способи захоплення фінансових установ: скупівля акцій; проведення додаткової емісії; банкрутство; реприватизація; шантаж; силове захоплення; фіктивне банкрутство.

Загальна методологія проведення рейдерського захоплення має наступний вид: *Збір інформації → Атака → Протистояння →* Легалізація рейдера → Результати та підсумки захоплення [1]

Про рівень рейдерства в Україні та його вражаючи масштаби свідчать наступні факти:

- в Україні діє щонайменше 40-50 спеціалізованих рейдерських груп, які складаються з досвідчених юристів та економістів;
- рейдерство набуло в Україні системного характеру. Кількість захоплень сягає 3000 на рік;
- результативність рейдерських атак – понад 90 %;
- за експертною оцінкою, щорічний обсяг сегмента поглинань і злиттів (без приватизації) становить понад 3 млрд. дол. США;
- середньостатистична норма прибутку рейдера в Україні, за експертними оцінками, становить близько 1000%;
- українське рейдерство має відчутну кримінальну складову: протиправні дії чиняться із залученням збройних формувань, а подекуди – навіть співробітників правоохоронної системи [2].

Універсального способу захисту підприємства від рейдерства немає. Утім, шанси рейдера на успішну атаку значно знижуються, якщо власник вчасно вибудує кілька ліній оборони, ретельно структурує систему власності, розробить способи прийняття рішень.

Практика показує, що найефективнішим від захоплення підприємства рейдерами є захист превентивного характеру. Його стратегічна мета - максимальне підвищення вартості захоплення підприємства для того, щоб зробити атаку рейдерів нерентабельною, а отже - недоцільною. Відповідно власникові необхідно здійснити заходи, щоб перевести інтерес потенційного рейдера із площини корпоративного захоплення на цивілізований механізм об'єднання та поглинання. Для цього слід провести системну реструктуризацію бізнесу, що дасть змогу створити таку систему володіння і управління найбільш привабливих активів, яка зробить захоплення рейдерами підприємства нерентабельним бізнесом.

1.Рейдерство в Україні.- [Електронний ресурс]. – Режим доступу.- https://ti-ukraine.org/wp-content/uploads/2016/11/raider_attacks_-_ti_ukraine_ukr.pdf

2. Щорічна аналітична доповідь Президента. – [Електронний ресурс]. – Режим доступу.-http://old.niss.gov.ua/monitor/juli/1.htm.

3. Захист бізнесу від зовнішніх і внутрішніх посягань. - [Електронний ресурс]. –Режим доступу. -http://www.dynasty.lviv.ua/parts/bz/index.php.

Квест як форма активного навчання

Симонова Г.М.
курсант 413 взводу факультету №3
Одеського державного університету внутрішніх справ
Литовських М.О.
курсант 413 взводу факультету №3
Одеського державного університету внутрішніх справ
Шелехов А.О.
науковий керівник, завідувач кафедри адміністративної діяльності ОВС та економічної безпеки Одеського державного університету внутрішніх справ к.ю.н. доцент

Сучасна педагогічна діяльність у більшості вищих навчальних закладах побудована таким чином, що студент за невеликий проміжок часу змушений оволодіти значним обсягом навчального матеріалу. Окрім того, що особа повинна зберегти у пам’яті отриману інформацію, вона зобов’язана вміти нею апелювати та використовувати на практиці. Основною метою сьогоднішнього висококваліфікованого викладача є не лише надання освітніх послуг, а підготовка майбутніх професіоналів до практичної діяльності, надання можливості творчого переосмислення та систематизації отриманих знань та навичок, можливості реалізації здібностей. В арсеналі у такого викладача є багато методик та тактичних схем, які допомагають у вирішенні поставлених завдань. Одним із специфічним та мало використовуваним методом активного навчання є технологія освітніх квестів.

Квест за первинним значенням – це пошук, предмет пошуку, пошук пригод. У міфології та літературі поняття «квест» спочатку тлумачилось як один із способів постановки сюжетної лінії – пригоди героїв до визначеної мети скрізь подолання перешкод. Освітній квест, у

свою чергу, це своєрідна трансформація квесту літературного – педагогічна технологія, яка включає у себе набір проблемних завдань із елементами ролевої гри, для виконання яких необхідні певні ресурси [1].

Іншими словами, освітній квест – проблема, яка реалізує освітні завдання, відмінні від навчальної проблеми елементами сюжету, ролевої гри, що пов'язана із пошуком та винайденням місць, об'єктів, людей, інформації, для вирішення якої використовуються ресурси якої-небудь території чи інформаційні джерела [2].

Освітні квести можуть бути організовані у різних просторах як навчального закладу так і поза його межами. Наприклад, квести в замкнутому приміщенні, в навчальній аудиторії; квести в музеях, усередині будівель, у парках; квести на місцевості (місцеве орієнтування); квести на місцевості із пошуком секретів (геокешинг) та елементами орієнтування (у тому числі GPS) та краєзнавства; змішані варіанти, у яких поєднується й переміщення учасників, й пошук, й використання інформаційних технологій, й сюжет, й легенда.

В залежності від сюжетної лінії квести можуть бути:

1. Лінійними, в яких гра побудована ланцюгом: вирішивши одне завдання, учасники отримують наступне, і так до тих пір, доки не пройдуть увесь шлях.
2. Штурмовими, де усі гравці отримують основне завдання та перелік точок із підказками, але при цьому самостійно вибирають шляхи вирішення завдань;
3. Кільцевими, вони уявляють собою той самий «лінійний» квест, але замкнутий в коло. Команди стартують із різних точок, які будуть для них фінішем [2].

Актуальність використання квестів сьогодні усвідомлюється усіма. Життя показує, що сучасна молодь краще засвоює знання у процесі самостійного добування та систематизації нової інформації. Використання квестів сприяє вихованню та розвитку якостей особистості, які відповідають вимогам інформаційного середовища, розкриттю здібностей [3]. Загалом, квест – це проектна діяльність, яка заснована на синтезі проектного методу та ігрових технологій, та полягає в триваючому цілеспрямованому пошуку, що пов'язаний із пригодами або грою. Вона може мати різні форми реалізації: освітні веб-квести; пригодницькі, або ігрові квести; «живі» квести.

У процесі захисту виконаних завдань по квесту студент може усвідомити, що по кожній дії, задачі, проблемі може існувати декілька точок зору, декілька варіантів вирішення поставлених завдань.

Використання у навчальному процесі квест-технологій сприяє формуванню у студентів інформаційної компетенції, знань та навичок, які сприяють інформаційній діяльності, виховують самоповагу та емоційно-позитивне відношення до себе, цілеспрямованість та наполегливість при досягненні поставлених завдань.

Таким чином, квести у навчальному процесі допомагають вирішити наступні завдання:

1) освітні - залучення кожного в активний пізнавальний процес. Організація індивідуальної та групової діяльності учасників, виявлення умінь і здібностей працювати самостійно по темі.

2) розвиваючі - розвиток інтересу до предмета діяльності, творчих здібностей, уяви учасників; формування навичок дослідницької діяльності, умінь самостійної роботи з інформацією; розширення кругозору, ерудиції, мотивації.

3) виховні - виховання особистої відповідальності за виконання завдання.

Використання квестів у начальному процесі допоможе студентам підготуватися до практичного використання отриманих знань, сформує правильну обробку інформації, сприятиме результативній роботі у команді.

1. Андреева М. В. Технологии веб-квест в формировании коммуникативной и социокультурной компетенции // Информационно-коммуникационные технологии в обучении иностранным языкам. Тезисы докладов I Международной научно-практической конференции. М., 2004..

2. Осяк С.А. Образовательный квест – современная интерактивная технологыя // Современные проблемы науки и образования. – 2015. – № 1-2.; [Электронный ресурс], - Режим доступа: https://www.science-education.ru/ru/article/view?id=20247

3. Эльмуратова Н.А. Квест как современная педагогическая технология [Электронный ресурс], - Режим доступа: http://www.fcdo.ru/index.php/doklady-chlenov-mo/item/771-kvest-kak-sovremennaya-pedagogicheskaya-tekhnologiya

Фінансово-економічна безпека підприємства

Сокол Р.В.
студентка 1 курсу спеціальність «Менеджмент», ДДУВС
Соломіна Г.В.
науковий керівник, к.е.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

Сучасна система управління фінансово-економічною безпекою підприємства повинна: враховувати альтернативні шляхи забезпечення безпеки підприємства, які відповідають конкретній фінансовій політиці підприємства; включати комплекс виважених збалансованих рішень як в області забезпечення інтересів підприємства, так і в управлінні його фінансовою діяльністю.

Сутність категорії «фінансова безпека підприємства» розкривається через фінансовий стан, який характеризується: збалансованістю і якістю інструментів, технологій і послуг; стійкістю до внутрішніх і зовнішніх загроз; здатністю системи забезпечувати реалізацію власних фінансових інтересів, місії і завдань достатніми обсягами фінансових ресурсів; забезпечувати ефективний розвиток фінансової системи [2, с.5].

Фінансово-економічна діяльність підприємства здійснюється з урахуванням умов зовнішнього середовища, якому притаманне зростання рівня невизначеності, що викликані процесами трансформаційного, інтеграційного та глобалізаційного характеру. Внаслідок існування різних загроз, що стосуються різних сфер діяльності підприємства, виникає об’єктивна необхідність розробки та реалізації заходів, щодо вдосконалення економічних механізмів управління його фінансово-економічною безпекою. Об’єктом системи забезпечення фінансової безпеки виступає стабільний фінансовий стан суб’єкта в поточному і перспективному періоді. Об’єктами захисту виступають ресурси: фінансові, матеріальні, інформаційні, кадрові [1, с.329-330]. Суб’єкти управління впливають на об’єкти за допомогою методів управління (певних способів, прийомів, засобів), що поділяються на [3, с.78-80]: організаційно-розпорядчі (адміністративні) методи передбачають прямий вплив на об’єкт управління, базуються на використанні адміністративної влади (накази, розпорядження,

інструкції) та створюють передумови для використання економічних методів. За їх допомогою формується організаційна структура управління фінансово-економічною безпекою, визначаються повноваження та відповідальність посадових осіб, розпорядок роботи, порядок дій у тій чи іншій ситуації та регламентуються інші дії суб'єктів управління фінансово-економічною безпекою. Економічні методи характеризуються непрямим впливом на об'єкт управління через його економічні інтереси та створюють матеріальну зацікавленість у відповідальних осіб за стан фінансово- економічної безпеки підприємства. Вплив суб'єктів управління на параметри діяльності, відбувається через формування фондів економічного стимулювання; використання гнучких моделей заробітної плати. Соціально-психологічні методи базуються на закономірностях функціонування людської психіки та впливають на мотиви соціальної поведінки людини, сутність яких розкривається через співбесіди; підбір кадрів з урахуванням та діагностикою психологічних характеристик працівників; формування сприятливого клімату в колективі; забезпечення перспективного соціального й професійного росту.

Функціонування механізму забезпечення фінансової безпеки має бути спрямоване на досягнення задач: визначення фінансових інтересів суб'єкта господарювання, які потребують захисту; виявлення на ранніх стадіях загроз, як внутрішнього, так і зовнішнього характеру, які не дозволяють реалізувати фінансові інтереси; розробка та реалізація заходів щодо нейтралізації загроз фінансовим інтересам та недопущення можливих фінансових збитків [4, с.340].

Захисту потребує система фінансових інтересів, що включає: достатність фінансових ресурсів; високий рівень інвестиційної та інноваційної активності; нейтралізацію фінансових ризиків [4, с.48]. Досягнення зазначених фінансових інтересів дозволить забезпечити виконання головної мети функціонування – максимізації прибутку. Адже, належний стан фінансової безпеки досягається тільки у випадку узгодженості його фінансових інтересів з інтересами суб'єктів зовнішнього середовища, тому, забезпечення має розглядатися як процес реалізації заходів щодо недопущення (попередження) можливих фінансових збитків у поточному та перспективному періоді. Фінансових збитків підприємство може зазнати, якщо: система управління та менеджмент підприємства неспроможний попередити негативні наслідки виявлених загроз та небезпек; суб'єкти управління фінансовою

безпекою намагаються визначити проблему та розробити подальшу стратегію, але їх дії не призводять до позитивного результату.

При побудові фінансової стратегії для оптимізації рівня фінансових ризиків, підприємство використовує декілька підходів: відмовляється від діяльності, яка містять джерело підвищеного фінансового ризику; здійснювати діяльність з певним фінансовим ризиком, за умови гарантії повної компенсації втрат за рахунок власних джерел; здійснювати діяльність з передаванням відповідальності за фінансовий ризик страховим організаціям.

1. Череп О. Г. Управління фінансово-економічною безпекою підприємств в Україні [Текст] / О. Г. Череп, З. П. Урусова, А. А. Урусов // Вісник ЖДТУ. Серія: Економічні науки. – 2012. – № 3(61). – С. 328-330.

2. Горячева К. С. Механізм управління фінансовою безпекою підприємства: автореф. дис. на здобуття наук. ступеня канд. екон. наук: спец. 08.06.01 «Економіка, організація і управління підприємствами» / К. С. Горячева. – К., 2006. – 17 с.

3. Мойсеєнко І. П. Управління фінансово-економічною безпекою підприємства [Текст]: навч. посібник / І. П. Мойсеєнко, О. М. Марченко. – Львів, 2011. – 380 с.

4. Клименко Т. В. Основні елементи механізму забезпечення фінансової безпеки суб'єктів господарювання [Текст] / Т. В. Клименко // Вісник ЖДТУ. Серія: Економічні науки. – 2011. – № 4(58). – С. 340-343.

Тіньова економіка та її вплив на економічну безпеку держави

Федоренко Є.В.
студент 1 курсу спеціальність «Менеджмент», ДДУВС
Соломіна Г.В.
науковий керівник, к.е.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

В умовах сучасної кризи гостро постає питання боротьби з тіньовою економікою, яка виступає одним з негативних факторів, що впливає на рівень економічної безпеки країни. За аналітичними джерелами відсоток тіньової економіки відповідно до розвитку країни

знаходиться у межах від 17% (у високорозвинених країнах) до 40% ВВП (в країнах, що розвиваються).

У теоретичному аспекті сутність тіньової економіки розглядається, як незафіксовані державою економічні дії, а також як реакцію в поведінці економічних агентів на встановлені збоку держави обмеження. Вона складається з нелегальної, прихованої та неофіційної економіки. Основними видами тіньової економіки є: а) контрабанда, нелегальні азартні ігри, нелегальна торгівля наркотиками, проституція, шахрайство, крадіжки, привласнення виданих під розписку грошей; б) приховані рентні доходи, прихована зайнятість, робота без ліцензій, нелегальне проживання іноземців, зайнятість пенсіонерів та осіб, що отримують соціальні допомоги з безробіття; в) приховування угод, «чайові», самозайнятість; г) бартер товарів та послуг. При цьому результати такої діяльності не зараховуються до ВВП через відсутність методологічної бази обліку нелегального виробництва товарів і послуг [1,с. 16].

Виділяють три блоки тіньової економіки: неформальна економічна діяльність – легальне (нерегламентоване державою); підпільна економіка – порушення в межах дозволеної економічної діяльності; незаконна економіка – здійснення заборонених видів діяльності [2, с. 442].

Серед основних ознак тіньової економіки Україні можна визначити: ухилення від сплати податків; приховане безробіття; подвійна бухгалтерія на підприємствах; корупція та хабарництво; відтік капіталу; «чорна» торгівля.

До основних чинників тінізації вітчизняної економіки відносять: недосконалу законодавчу базу; складний механізм адміністрування податків та суттєво завищенні їх ставки; відсутність механізма антикорупційного законодавства, судової та правоохоронної системи; високий рівень загальної злочинності [2, с. 445].

Так, після прийняття Податкового кодексу України, в результаті посилення податкового тиску на підприємців, що раніше працювали на єдиному податку, майже третина їх пішла в «тінь». За даними Міністерства економіки та з питань європейської інтеграції України, уряду вдалося знизити процес тінізації економіки на 5-8%. Проте питома вага тіньового сектору економіки в Україні й далі залишається досить високою: за оцінками Національного банку України поза контролем банків знаходиться в обігу 4,8 млрд. гривень, що складає майже половину грошової маси [3].

Важливе значення у посиленні боротьби з економічною злочинністю в Україні був призваний зіграти Кримінальний кодекс України, що встановив кримінальну відповідальність за легалізацію (відмивання) коштів або іншого майна, отриманих злочинним шляхом. Крім цього, в Україні діє постанова Кабінету Міністрів України і Національного банку України «Про сорок рекомендацій групи по розробці фінансових заходів боротьби з відмиванням грошей (РАТР)», що зобов'язує органи виконавчої влади, банківські й інші фінансові установи керуватися у своїй діяльності запропонованими рекомендаціями [4]. Проте слід визнати, що такі заходи дещо позитивно вплинули на розвиток легальної економіки, гальмуючи тіньовий сегмент підприємницької діяльності, але бажаних результатів не принесли [5, с. 19]. Тому необхідно негайне впровадження дієвих заходів щодо детінізації вітчизняної економіки.

1. Васенко В.К. Тіньова економіка країни та шляхи її детінізації / В.К. Васенко // Вісник Черкаського університету. – 2016. – №1. – С. 15-23.

2. Економічна безпека: навч. посіб. / за ред. З.С. Варналій. – К.: Знання, 2009. – 647 с.

3. Тенденції тіньової економіки в Україні І квартал 2016 р. [Електронний ресурс]. – Режим доступу: file:///D:/Users/user/Downloads/%D0%A2%D1%96%D0%BD%D1%8C%D0%BE%D0%B2%D0%B0%20%D0%B5%D0%BA%D0%BE%D0% BE%D (1).pdf.

4. Савич О.В. Основні чинники та шляхи протидії тінізації економіки України / О.В. Савич, І.В. Савич // Ефективна економіка. – 2015 [Електронний ресурс]. – Режим доступу: www.economy.nayka.com.ua/?op=1&z=3827.

5. Безпалько І. Тіньова економіка як загроза економічній безпеці країни / І. Безпалько // Економічна безпека держави та суб'єктів підприємницької діяльності в Україні: проблеми та шляхи їх вирішення: Матеріали ІІ Всеукр. наук.-практ. Інтернет-конференції. – 2015. – С. 18-20.

Інновації у використанні інформаційно-комунікаційних технологій в освітньому процесі

Фрунзе К.С.
курсант 402 взводу факультету №1 Одеського державного університету внутрішніх справ
Шелехов А.О.
науковий керівник, завідувач кафедри адміністративної діяльності ОВС та економічної безпеки Одеського державного університету внутрішніх справ, к.ю.н. , доцент

Сучасна соціально-економічна ситуація, що склалася в нашій державі, потребує сутнісних змін у всіх сферах суспільного життя і, зокрема - в сфері освіти. Адже, саме освіта являється основою розвитку особистості, визначальним показником життєдіяльності суспільства, відтворює його потенціал.

З приводу цього, нагальною вимогою для поліпшення освітнього процесу в усьому світі та безпосередньо в державі, стало впровадження інновації в різних напрямках та аспектах. Це, в першу чергу, стосується застосуванню інноваційних інформаційно-комунікаційних технологій (далі – ІКТ) в освітньому процесі, починаючи з початкових шкіл, і, закінчуючи у вищих навчальних закладах [1, с. 12].

Варто зауважити, що саме використання ІКТ посідає особливе місце в освітньому процесі, адже, саме такі технології відкривають учням, студентам та курсантам доступ до нетрадиційних джерел інформації, підвищують ефективність самостійної роботи, дають нові можливості для творчості, знаходження і закріплення будь-яких професійних навичок, дозволяють реалізовувати принципово нові форми і методи навчання. І тому, застосування та використання таких технологій являється також і актуальним питанням в освітньому процесі [2].

Проблемі розвитку інноваційних процесів в освіті нині присвячено вже досить велику кількість досліджень ряду вчених-науковців, одними з яких є: В.Г. Кремень, С.Д. Поляков, С.А. Бараннікова, В.І. Загвязинский, М.В. Кларін, А.І. Пригожін, В.Я. Ляудіс, В.І. Рибакова, В.О. С.О. Сисоєва, П.І. Щедровицкий, та ін [3, 4].

Загалом, говорячи про актуальність і, як результат, корисність використання таких технологій, слід в першу чергу зазначити, що вони в

себе включають. Таким чином, до ІКТ можна віднести різного роду телекомунікації, комп'ютери, накопичувальні та аудіовізуальні системи, які дозволяють користувачам створювати, одержувати доступ, зберігати, передавати та змінювати інформацію. Іншими словами, ІКТ складається з інформаційних технологій, а також телекомунікацій, мультимедіа, усіх видів аудіо і відеообробки, передачі, мережевих функцій управління та моніторингу [5].

Відповідно до зазначеного переліку, варто виділити такий вид інформаційно-комунікаційних технологій, як мультимедіа. Адже саме даний вид ІКТ набув свого поширення не лише серед школярів, слухачів та курсантів, а й серед вчителів в шкільних загальноосвітніх закладах і викладачів у вищих навчальних закладах. Даний факт можна підтвердити, мабуть, тим, що використання саме мультимедіа у навчанні не тільки збільшує швидкість передачі інформації користувачам та підвищує рівень її засвоєння, а й сприяє розвитку таких процесів, як увага, пам'ять, мислення, уява та мовлення [6].

Проте, слід також зазначити і про корисність використання різного виду телекомунікацій, які мають безпосередній доступ до мережі Інтернет. Адже, вивчаючи, наприклад, нормативну базу на юридичній дисципліні, слухачам та курсантам буде зручніше знаходити потрібний їм той чи інший нормативно-правовий акт вже з останніми змінами та оновленнями. Окрім цього, зручність та корисність використання даного виду ІКТ стосується також і інших дисциплін, адже певний зміст навчальної інформації додатково можна знайти на певному інформаційному ресурсі локальної та глобальної мереж.

Досліджуючи інновації у використанні ІКТ в освітньому процесі, варто також зазначити, що їхнє значення має, як позитивні, так і негативні сторони. Адже, сьогодення показує, що застосування таких технологій в навчальному процесі сягає і певних проблем. Одними із таких проблем, зокрема, виділяють:

1) недостатнє матеріально-технічне та науково-методичне забезпечення навчальних закладів;

2) недостатньо розроблені методики використання сучасних інформаційних технологій навчання у навчальному процесі під час вивчення усіх навчальних предметів;

3) недостатня підготовка педагогічних кадрів до використання в навчальному процесі засобів сучасних інформаційно-комунікаційних технологій;

4) відсутність у вчителів та викладачів мотивації, щодо використання сучасних інформаційних технологій навчання тощо [2].

У зв'язку з цим, варто зауважити, що використання ІКТ в освітньому процесі посідає особливе значення, адже, такі технології, незважаючи на певні проблеми в їхньому застосуванні, виступають дійсно корисними засобами отримання навчальної інформації учнями, слухачами та курсантами.

Дані технології починають застосовуватись в освітньому процесі не лише для зручності використання навчального матеріалу, а й для отримання задоволення від перегляду нового потоку інформації, яку можна отримати під час навчального процесу з різного виду ІКТ по-різному.

1. Дубасенюк О.А. Інновації в сучасній освіті // Інновації в освіті: інтеграція науки і практики: збірник науково-методичних праць / за заг. ред. О.А. Дубасенюк. – Житомир : Вид-во ЖДУ ім. І. Франка, 2014. – С. 12-28;

2. Когут С. А. Впровадження ІКТ в навчально-виховний процес як шлях до розвитку освіти. [Електронний ресурс]. – Режим доступу: http://chito.in.ua/vprovadjennya-ikt-v-navchaleno-vihovnij-proces-yak-shlyah-do-r.html?page=2;

3. Кремень В.Г. Філософсько-освітня діяльність: інноваційні аспекти // Становлення і розвиток науково-педагогічних шкіл: проблеми, досвід, перспективи: зб. наук. праць. / за ред. Василя Кременя та Тадеуша Левовицького. – Житомир, Вид-во ЖДУ ім. І. Франка, 2012. – С.10-26.

4. Кларин М.В. Инновации в мировой педагогике: обучение на основе исследования / Кларин М.В. – Рига: Эксперимент, 1995. – 176 с.

5. Електронний ресурс. – Режим доступу: https://uk.wikipedia.org/wiki/

6. Електронний ресурс. – Режим доступу: https://dnz38.edu.vn.ua/viko ristannya-ikt-3/.

Кіберзлочинність як одна із проблем інформаційного суспільства

Циб І.С.
курсант VI курсу факультету підготовки фахівців органів досудового розслідування Дніпропетровського державного університету внутрішніх справ
Краснобрижий І.В.
науковий керівник, к.ю.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

На сьогоднішній день у світовому просторі дуже бурхливо обговорюється питання інформаційного забезпечення суспільства. Сучасне суспільство досягло дуже високого рівня розвинутості з точки зору поінформованості/інформативності.

У світі налічується дуже багато засобів, способів, а також прийомів отриманої інформації. Вбачається широкий спектр впроваджень інформаційних технологій у всебічних проявах, таких як: державні органи, виробництво, банківська сфера, освіта та наука, а також повсякденне життя людей. Саме дане явище започаткувало так званий феномен інформаційно залежного суспільства, основним джерелом якого є загальновідома мережа «інтернет». Практично всі важливі для громадян служби, пошта та комунальні підприємства на пряму мають певну залежність від надійної роботи комп'ютерних систем, за допомогою яких здійснюється керування цими процесами, а також належне інформаційне забезпечення в цілому.

Тобто, можна вести мову про те, що виникає певна залежність від засобів інформації та зв'язку у світі. Загальновідомим є факт того, що рівень злочинності не тільки на території нашої держави, а й за кордоном зростає з кожним роком, статистика зафіксованих правопорушень збільшується все більше і більше, особливо у галузі «інформаційного забезпечення». Злочинні угрупування також стають більш модернізованими та використовуючи новітні засоби та знаряддя для скоєння злочинів.

Даному питанню присвятили свої наукові праці такі вчені, а саме: О. Бандурка, А. Губанова, О. Долженкова, Є. Желєзов, В. Заросил, В. Золотарева, І. Козаченка, В. Некрасов, В. Ортинський, В. Сапальов, М. Смирнова, М. Стащака, та ін.

Деякі з вище зазначених науковців ще кілька років тому вважали акти негативного впливу через інформаційні технології малоймовірними, особливо в Україні, після подій у грудні 2015 року, коли внаслідок кібератаки на Прикарпаття обленерго без світла залишилися близько 230 000 користувачів, сумніви розвіялися [1]. Указом Президента України від 15 березня 2016 року № 96/2016 з метою створення умов для безпечного функціонування кіберпростору була затверджена «Стратегія кібербезпеки України», у якій прямо зазначено, що сучасні інформаційно-комунікаційні технології можуть використовуватися для здійснення терористичних актів, зокрема шляхом порушення штатних режимів роботи автоматизованих систем керування технологічними процесами на об'єктах критичної інфраструктури [2].

Якщо брати до уваги закордонний досвід, то за кордоном вивчення даної проблеми активно розпочалося після подій 11 вересня 2001 року, коли з'ясувалося, що для організації терористичного акту злочинці користувалися Інтернетом, хоча самої кібератаки не було.

На сьогоднішній день за статистичними даними відомо, що терористи активно використовують інформаційно-комунікаційні технології та Інтернет не тільки для вчинення своїх злочинних намірів, а й для підшукування однодумців, використовуючи переконливі доводи та активно маніпулюючи. Для планування терористичних актів терористи можуть використовувати інформацію як з відкритих джерел, так і конфіденційну інформацію, яка не захищена відповідним чином. При цьому вони висловлюють загрози та обіцяють винагороди з метою залучення фахівців із хакерської спільноти для ефективного виконання ними різноманітних завдань. Для зв'язку між собою терористи можуть використовувати шифрування даних, що значно ускладнює роботу правоохоронців. Ще однією можливістю Інтернету терористи користуються для фінансування своїх операцій. Для цього вони можуть розміщувати різноманітні оголошення в мережі для своїх спонсорів, використовують віртуальні азартні ігри, а під час перерахунку коштів, здобутих злочинним шляхом, широко експлуатують фальшиві інтернет-магазини, які імітують операційну діяльність, проте жодних товарів фактично не продають. Для ефективного захисту від терористичних актів у інформаційному просторі необхідними є прийняття відповідного законодавства, підготовка спеціальних підрозділів по боротьбі з кіберзлочинністю, проведення технічних заходів щодо забезпечення відповідного рівня безпеки інформаційних ресурсів, особливо для об'єктів

критичної інфраструктури. Значним кроком у виконанні цих завдань стала затверджена Указом Президента України від 15 березня 2016 року № 96/2016 «Стратегія кібербезпеки України». Розпорядженням Кабінету Міністрів України від 24 червня 2016 року № 440-р. затверджено План заходів на 2016 рік із реалізації Стратегії кібербезпеки України [3]. Важливим документом для створення відповідної нормативно-правової бази стала постанова Кабінету Міністрів України від 23 серпня 2016 року № 563 «Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави».

Питання інформаційного забезпечення поліції є актуальним у світовому просторі. Поліцейські структури різних країн дедалі частіше взаємодіють між собою у службово-бойовій протидії міжнародній злочинності, тероризму тощо. Також поліцейські структури співпрацюють із миротворчими місіями ООН, двосторонні угоди між країнами та багатосторонні договори, укладені міжнародними організаціями, дозволяють поліцейським із різних країн обмінюватися інформацією та накопиченим досвідом, завдяки чому збільшується ефективність службової діяльності. Саме для протидії даному явищу працівникам поліції особливо органам досудового розслідування, суду, прокуратурі необхідно весь час поширювати свій рівень знань та підвищувати кваліфікаційний рівень під час виконання службових обов'язків, здебільшого при роботі з доказовою базою яка зберігається на електронних носіях, або яка передається іншим підрозділам через мережу «Інтернет».

Спираючись на все вище викладене, варто зазначити, що наше суспільство дійсно дуже розвинуте саме з точки зору інформаційності. Інформація є основним джерелом для спілкування, передачі даних та виконання певними службами своїх обов'язків. З урахуванням цього факту, з'явилася нова, модернізована форма злочинності, а саме кіберзлочинність. З даною проблемою зіштовхнулася не тільки наша держава, а й цілий світ. Злочинні угрупування стали більш винахідливими, про що свідчить статистика скоєння злочинів через мережу «Інтернет». З огляду на це, працівникам правоохоронної сфери необхідно розвивати свої навички, постійно підвищувати свій кваліфікаційний рівень, та вміння прораховувати на перед злочинні наміри. За допомогою даних вмінь можна буде з використанням комп'ютерних технологій та інформації створювати обмежувальні пастки для злочинців та передувати злочинам.

Важливою також безумовно залишається домовленість та співпраця між усіма державами-членами шляхом створення групи співпраці з метою надання підтримки і сприяння стратегічній співпраці та обміну інформацією між державами-членами; – високий рівень безпеки в усіх секторах, які мають життєво важливе значення для економіки і суспільства та, до того ж, значною мірою залежать від інформаційно-комунікаційних технологій.

1. Розслідування Wired: як відбувалася атака на Прикарпаттяобленерго [Електронний ресурс]. – Режим доступу: http://firtka.if.ua/?action=show&id=101335

2. Стратегія кібербезпеки України, затверджена Указом Президента України від 15 берез- ня 2016 року № 96/2016 [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/ documents/962016-198363

3. Розпорядженням Кабінету Міністрів України від 24 червня 2016 року № 440-р. [Електронний ресурс]. – Режим доступу: http://zakon.rada.gov.ua/laws/show/440-2016-%D1%80

Інформаційне забезпечення спеціальної поліцейської діяльності

Чанцева Т.П.
слухачка магістратури юридичного факультету ДДУВС
Косиченко О.О.
науковий керівник, к.т.н., доцент кафедри економічної та інформаційної безпеки ДДУВС

Інформаційне забезпечення сил охорони правопорядку є актуальним питанням не тільки для України, але й для багатьох зарубіжних країн, в яких значна увага приділяється створенню і використанню інформаційних систем спеціальної поліцейської діяльності. Поліцейські структури різних країн дедалі частіше взаємодіють між собою у протидії міжнародній злочинності, тероризму тощо. Також поліцейські структури співпрацюють із миротворчими місіями ООН, двосторонні угоди між країнами та багатосторонні договори, укладені міжнародними організаціями, дозволяють

поліцейським із різних країн обмінюватися інформацією та накопиченим досвідом, завдяки чому збільшується ефективність службової діяльності. В умовах модернізації всієї системи державної служби в Україні закономірно зростає потреба в удосконаленні діяльності ОВС, зокрема оптимізації професійної підготовки особового складу, здійсненні системних перетворень у правовому регулюванні, а також використанні досвіду інформаційного забезпечення спеціальної поліцейської діяльності. Вивчаючи іноземний досвід спеціальної поліцейської діяльності щодо інформаційного забезпечення, потрібно виділяти найбільш ефективні й сучасні способи забезпечення інформацією, які у свою чергу можуть бути використані підрозділами ОВС у практичній діяльності під час виконання завдань. Питанням інформаційного забезпечення та в цілому спеціальної поліцейської діяльності у вітчизняній правовій науці не було приділено достатньо уваги. Категорія «інформаційне забезпечення» отримала достатній розвиток у межах інформаційного права. Питання інформаційного забезпечення також розглядалося в окремих працях з кримінального процесу, оперативно-розшукової діяльності під час висвітлення пропозицій, спрямованих на підвищення ефективності боротьби зі злочинністю.

Зарубіжний і частково вітчизняний досвід діяльності ОВС в особливих умовах і досвід збройних конфліктів та антитерористичних операцій засвідчив, що одним із найважливіших і специфічних видів оперативного (бойового забезпечення) на сьогодні стає інформаційне забезпечення. За розповсюдженою у вітчизняній літературі позицією, інформаційне забезпечення здійснюється у великомасштабних операціях за допомогою: «налагодженого механізму державного контролю над процесом інформаційної політики… Впливу через засоби масової інформації на суспільну свідомість як у середині країни, так і за її межами». Нашій державі слід урахувати позитивний досвід розвинутих світових країн. Особливу увагу заслуговує досвід Великобританії в розробці та запровадженні корпоративної об'єднаної інформаційної моделі даних для потреб поліції. Цей проект містить кілька ключових елементів. Відповідно основною корпоративної інформаційної моделі стає каталог інформаційних об'єктів. Особливої уваги заслуговує той факт, що як звичайний словник він визначає кожен елемент інформації, використовуваний різними поліцейськими підрозділами, – від ордерів на арешт до листків тимчасової непрацездатності. Але на відміну від звичайного словника він створений таким чином, що встановлює і

наочно показує ієрархічні взаємовідносини між інформаційними об'єктами. Реалізація цих відносин під час попередження правопорушень та їх швидкого розкриття у забезпечується введенням новітніх комп'ютерних відеоспостережень, створених завдяки фінансуванню міських адміністрацій та приватних підприємств . Таким чином забезпечується значне скорочення кількісного складу поліцейських, які задіяні для спеціальної поліцейської діяльності.

Апаратура відеоспостереження здатна здійснювати нагляд під час стеження за громадянами, особливістю якого є моментальне сканування обличь цих осіб та їх перевірка у файлах поліції. Електроніка впізнає людину з кримінальним минулим, отримані відомості передаються до найближчого підрозділу поліції, поряд із цим у Великобританії є багато спецслужб оперативно-розвідувального спрямування, зокрема оперативно-розвідувальний підрозділ (OIU – operational intelligence unit) 22-го полку SAS, що забезпечує широке інформаційне забезпечення діяльності сил спецпризначення. Серед функцій OIU відзначається збір даних про можливі райони майбутніх бойових дій (фізико-географічні умови, історія, культура, релігія тощо), збройні сили імовірного противника, зокрема про наявність протидиверсійних підрозділів; адміністрування баз даних про організації, віднесені до терористичних, та осіб терористів, про вчинення терористичних актів. OIU збирає дані та узагальнює досвід бойового застосування спеціальних антитерористичних підрозділів усіх країн. Він активно взаємодіє з комітетом з оборони і зовнішньої політики, британською військовою розвідкою і контррозвідкою, іншими розвідувальними службами національних збройних сил, а також зі спеціальними підрозділами країн НАТО. У Сполученому Королівстві поліцейська розвідка, яка має назву національної розвідувально-інформаційної служби, має завдання які полягають у тому, щоб якісно зібрати, оцінити, проаналізувати й обробити інформацію про серйозних злочинців; вчасно надавати інформацію певним поліцейським органам з метою більш швидкого притягнення до кримінальної відповідальності кримінальних елементів; координувати діяльність поліцейських служб, пов'язану з отриманням відомостей. Заходи, що приймаються у цьому напрямку, дозволяють досягти високої ефективності діяльності поліції щодо попередження злочинів або їх припинення та розкриття.

Керівництво правоохоронних органів України повинно прийняти ці ідеї до свого відома та застосувати їх відповідно до можливостей нашої держави. Що стосується спеціальної поліції, то в США існує багато різних

підрозділів (SWAT – підрозділи в американських правоохоронних органах), які використовують легке озброєння армійського типу та спеціальну тактику в операціях з високим ризиком, в яких потрібні здібності та навички, що виходять за рамки можливостей звичайних поліцейських. На відміну від більшості країн у США немає єдиного поліцейського управління; а отже, немає й офіційного терміну поліція США. Замість цього кожний штат, а також кожне велике місто, а іноді і більш дрібний населений пункт, мають своє поліцейське відомство, не залежне від інших. Власні поліцейські відомства можуть бути також при великих транспортних підприємствах. Існує в США спеціальна поліція ФБР, завданням якої є захист об'єктів, майна, персоналу, користувачів, відвідувачів ФБР від шкоди і реалізація певних законів й адміністративних правил. Поліцією США і ЄС було спеціально створено підрозділи поліцейської розвідки, основною функцією яких є отримання оперативно-розшукової інформації про злочинців, їх дії, наміри та предмети, що добуті незаконним шляхом.

Щодо цього заслуговує на увагу досвід поліцейських Ізраїлю, які неодноразово доводили свою здатність захопити й обеззброїти «терористів-смертників» із вибуховими пристроями, що підтверджує спроможність забезпечити швидке реагування на будь-які злочинні діяння. У Ізраїлі також особлива увага приділяється інформаційному забезпеченню охорони громадського порядку, а кожен патрульний автомобіль оснащено комп'ютером, який дозволяє в лічені секунди отримати необхідну інформацію, що міститься в базі даних інформаційних систем поліції.

У складі департаменту Ізраїлю діє особливий відділ спеціальних розслідувань і завдань метою якого є збір і аналіз інформації щодо кримінального світу, організованої злочинності, контрабанди, незаконного обігу наркотичних засобів. Окремим напрямком діяльності цього департаменту є збір інформації, що стосується палестинських громадських організацій та окремих осіб. У штабі ізраїльської поліції працює відділ оперативної інформації, у розпорядженні якого є центральний комп'ютер, тобто централізована база даних, зокрема з проблем боротьби з кримінальною злочинністю, розвідки, операціями поліції.

Робота поліції Швеції є проблемне орієнтованою: її метою є налагодження добрих відносин із місцевим населенням та реагування на його потребу в забезпеченні безпеки . Мова йде про застосування в повсякденній роботі та під час масових громадських заходів «тактики

національної поліції», що заснована на принципах «діалогу» та «безконфліктності». У разі, коли доводиться мати справу з натовпом людей, поліцією Швеції застосовується «спеціальна поліцейська тактика» із залученням спеціально навчених діалогових поліцейських .

Оперативні підрозділи поліції Канади отримують оперативно-розшукову інформацію від служби зі збору відомостей про організовану злочинність. До її складу входять центральні і місцеві бюро, які займаються збиранням, аналізуванням і поширенням інформації. Центральні бюро діють у національному масштабі, а місцеві – в межах провінцій і між провінціями. У кожній країні спецслужби і підрозділи спеціального призначення мають свою назву і свої функції, однак серед іншого їх об'єднує залежність отримання найкращих результатів під час виконання своїх службових обов'язків від інформаційного забезпечення. Аналізуючи діяльність спеціальної поліції, можна чітко сказати, що вона не є безпосереднім суб'єктом інформаційної діяльності – уся інформаційна діяльність пов'язана з виконанням конкретних завдань. Поліція зарубіжних країн багато уваги приділяє комунікативному впливу на правопорушників у певний спосіб на основі вербальної, візуальної інформації, що є добрим прикладом для нашої держави.

Отже, вирішення завдань сучасного інформаційного забезпечення має бути досягнуто за рахунок впровадження єдиної політики інформаційного забезпечення; створення багатоцільових інформаційних підсистем діяльності ОВС; удосконалення організаційно-кадрового забезпечення інформаційних підрозділів; розбудови інформаційної мережі; створення умов для ефективного функціонування інформаційних обліків, забезпечення їх повноти, вірогідності, актуальності та безпеки; переоснащення інформаційних підрозділів сучасною потужною комп'ютерною технікою; поширення мережі комп'ютерних робочих місць користувачів інформаційних підсистем; подальшої комп'ютеризації інформаційних обліків; установлення взаємодії поліції з населенням у розробці ефективних способів такого забезпечення; упровадження нових форм і методів інформаційного забезпечення ОВС, правове виховання через засоби масової інформації та удосконалення законодавства.

Нормативно-правове регулювання забезпечення кібербезпеки в Україні

Чепеляк К.В.
курсант 2-ого курсу факультету ПФОДР, ДДУВС
Поливанюк В.Д.
старший викладач кафедри тактико-спеціальної підготовки ФПФППД Дніпропетровського державного університету внутрішніх справ, кандидат юридичних наук, доцент

Актуальність даної теми визначена тим, що на сьогодні, відносини у сфері кібербезпеки в Україні не врегульовані на законодавчому рівні, хоча при цьому проблеми протидії кіберзлочинцям носять транснаціональний характер.

Питання, що стосуються нормативно-правової регламентації у забезпеченні кібербезпеки були предметом багатьох наукових публікацій, як іноземних так і вітчизняних дослідників. Ця тема не є виключенням, а отже знаходить широке відображення у наукових працях таких вчених: О.А. Баранова, В.М. Бутузова, В.М.Петрик, Д.В. Дубова, В.П. Шеломенцева.

Постановкою проблеми виступає дослідження правового забезпечення кібербезпеки в нашій державі, а також окреслення шляхів нормативно-правового регулювання останньої.

На сучасному етапі розвитку, нагальним є вирішення такої проблеми, як формування спільної політики кібербезпеки у провідних державах світу. При цьому варто звернути увагу на відсутність міжнародно-правових документів, а також термінологічну невизначеність у цій сфері. Тому ця проблема все частіше стає предметом дискусій не тільки на національному, а й на міжнародному рівні.

Сьогодні досить важко уявити наше життя без інформаційних та комунікаційних технологій. Адже майже кожен є активним користувачем соціальних мереж, а також велика кількість людей керує банківськими рахунками за допомогою інтернету. Щодня вноситься велика кількість не тільки особистої, а й державної інформації. Саме тому, необхідно звернути увагу не тільки на те, як захистити себе від негативного впливу таких інформаційних технологій, а й на те , щоб таке питання знайшло своє закріплення на законодавчому рівні. У нашій державі документом,

що регулює відносини у сфері забезпечення кібербезпеки, є Стратегія кібербезпеки України, що була прийнята 15 березня 2016 р. [1].

При цьому, необхідно зазначити, що Стратегія не відображає всіх способів інформаційного та психологічного впливу на суспільство, державу, а також особу. Все це викликає досить вагому необхідність врегулювати такі питання на законодавчому рівні, шляхом прийняття окремого закону, що регулював би саме діяльність у сфері інформаційної безпеки, особливо на сьогодні, в умовах конфлікту на сході України, а також поступового зниження міжнародного іміджу.

Аналіз правових засад правового регулювання забезпечення кібербезпеки в Україні вказує на недоліки, що існують в зазначеній сфері. До таких недоліків можна віднести:

- значну кількість правових норм у сфері забезпечення кібербезпеки, що містяться у різних нормативно-правових актах, що досить ускладнюють пошук, а також аналіз їх практичного застосування;
- неузгодженість таких нормативно-правових актів з чинною Конституцією України;
- декларативність норм, що призводить до низького рівня правореалізації останніх;
- штучне розширення предмету інформаційної безпеки на максимальну кількість сфер, що, на думку деяких авторів, розмиває сам предмет інформаційної безпеки, а також обумовлює відсутність частини «кібер» у вітчизняних нормативно-правових документах [2].

Таким чином, підсумовуючи вище наведене можна дійти висновку, що наразі в Україні існує потреба удосконалення національного законодавства у сфері правового регулювання забезпечення кібербезпеки та визначити правовий статус суб'єктів відносин у цій сфері.

---

1. Стратегія кібербезпеки України [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/962016-19836;

2. Черноног О.О. Напрями підвищення ефективності забезпечення кібербезпеки інформаційних технологій в системі публічного управління [текст]://О.О. Черноног/ [Електронний ресурс]: http://mino.esrae.ru/178-1484.

Огляд ефективних заходів протидії кіберзагрозам

Шкарупа І.В.
студентка Запорізького національного технічного університету
Нікуліщев Г.І.
старший викладач Запорізького національного технічного університету

Сучасний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює глобальний ринок ідей, досліджень та інновацій.

Стрімкий розвиток інформаційних технологій обумовлює появу нових загроз національній та міжнародній безпеці. Зростає кількість та потужність кібератак, мотивованих інтересами окремих держав, груп та осіб.[1] З цього випливає актуальність розробки, вибору і правильного використання методів, засобів і заходів ефективної протидії ним.

Мета роботи полягає у аналізі поняття кіберзагроз, огляді методів їхньої реалізації на сучасному етапі розвитку інформаційних систем та ефективних заходів протидії.

Існують 3 основні підходи до пояснення терміну «кібербезпека».

Кібербезпека – безпека кібернетичних систем. Кібернетика охоплює багато дисциплін, деякі з яких можуть стати цілями для кібератак: штучний інтелект, робототехніка, системи керування, соціальні системи тощо.

Згідно з аналітичним терміном, кібербезпека охоплює широке коло дій, засобів і концепцій, що пов’язані з забезпеченням інформаційної безпеки.

За стандартом ISO/IEC 27032 кібербезпека - стан захищеності інформації від кіберзагроз, тобто загроз доступності, повноті, цілісності, достовірності інформації, яка циркулює в об’єктах національної інформаційної інфраструктури. [2]

Ще в 2010 році було виявлено шкідливе програмне забезпечення Stuxnet, яке продемонструвало реальність загроз, які раніше вважалися лише уявними. Ця програма мала наступні важливі особливості:

- здатна атакувати локальні мережі, не підключені до Інтернету;

- призначена для атаки на промислове обладнання ядерного об’єкта.

Пізніше спеціалістами були виявилені зразки програмного забезпечення, яке мало розвідувальні функції. Найбільш відомими прикладами є DuQu, Flamer, Red October. Як з’ясувалось, деякі з масштабних розвідувальних операцій у кіберпросторі проводились протягом майже десяти років. Цілями були США, Західна Європа, Росія, Казахстан, Білорусь, Україна.[3]

Останнім часом вищенаведений список програм, які можуть становити загрозу кібербезпеці, в тому числі і національній, стрімко поповнюється. Також зростає кількість і частота кібератак, що проводяться організованими групами кіберзловмисників.

Для протистояння кіберзагрозам використовуються наступні засоби: антивірусний захист, комплексні системи захисту інформації, системи управління інформаційною безпекою, навчання користувачів і підготовка фахівців тощо.

Антивірусний захист полягає в виявленні та знешкодженні програм, які створені для того, щоб порушити безпеку інформації в системі. Антивірусний захист є одним із базових компонентів захисту сучасних інформаційно-телекомунікаційних систем.

Наступним засобом забезпечення кібербезпеки є комплексні системи захисту інформації (КСЗІ), які є необхідним компонентом будь-якої інформаційної системи, в яких обробляється інформація, що належить державі. Розробка і впровадження КСЗІ передбачає декілька етапів: обстеження об'єкта, розробка моделі загроз, оцінка ризиків, розробка політики безпеки, державна експертиза з метою підтвердження відповідності КСЗІ.

Будь-які зміни у системі вимагають повторного обстеження і внесення змін у модель загроз, переоцінки ризиків, коригування політики безпеки тощо.

Одним із ефективних засобів забезпечення безпеки інформаційних об’єктів є використання системи управління інформаційною безпекою (СУІБ), в основу якої покладено модель PDCA: планування (Plan) — етап розроблення СУІБ, оцінювання ризиків і підбір заходів; дія (Do) — етап реалізації і впровадження обраних заходів; перевірка (Check) — етап оцінювання ефективності та продуктивності СУІБ, що переважно виконують внутрішні аудитори; удосконалення (Act) — виконання коригуючих дій.

Таким чином, кіберпростір є територією активного протистояння, в якому спеціалісти з кібербезпеки поки що програють. Атаки здійснюються за допомогою спеціально розробленого програмного забезпечення, що використовує вразливості комп'ютерних систем. Виявлення таких атак ускладнюється тим, що вони здійснюються на обмежену кількість спеціально визначених цілей, не викликають збоїв і відмов комп'ютерів і тому тривалий час не потрапляють у поле зору дослідників з антивірусних лабораторій.

Для розробки дієвого механізму протидії кіберзагрозам Україні варто взяти за приклад існуючу практику зарубіжних країн та міжнародної спільноти та привести її у відповідність до українських реалій.

1. Стратегія кібербезпеки України: Указ Президента України № 96/2016 від 15.03.2016 р. [Електронний ресурс]. - Режим доступу: http://zakon3.rada.gov.ua/laws/show/96/2016.

2. Міжнародні стандарти, що захищають кіберпростір [Електронний ресурс]. - Режим доступу: http://csm.kiev.ua/

3. Поняття та зміст кіберзагроз на сучасному етапі [Електронний ресурс]. - Режим доступу: http://goal-int.org/ponyattya-ta-zmist-kiberzagroz-na-suchasnomu-etapi/

Методологія проведення рейдерських захоплень в Україні

Шукюров К.Ю.
студент 1 курсу спеціальність «Менеджмент», ДДУВС
Соломіна Г.В.
науковий керівник, к.е.н., доцент кафедри економічної та інформаційної безпеки, ДДУВС

Загальносвітова статистика свідчить про те, що близько 90% рейдерських атак закінчуються успіхом. Успішність рейдерів - результат наявності стратегії, тактичних прийомів і ресурсів, а також повна або часткова відсутність такої стратегії у компанії, що підлягає поглинанню. Загальної методики, за якою здійснюється захоплення, не існує, оскільки це - унікальний, високопрофесійний захід, схожий на гру, яку планують фахівці дуже високого рівня.

Аналізуючи рейдерські підходи захоплень, що відбуваються в Україні, нами здійснено їх узагальнення та розроблена загальна концепція, що є найбільш вживаною.

Методологія проведення рейдерських операцій має наступний вигляд:

Збір інформації → Атака → Піар рейдера → Протистояння підприємства і рейдера → Легалізація рейдера → Завершення перехоплення управління → Результати захоплення → Підсумки рейдерської роботи.

Збір інформації (підготовчий етап). Рейдер збирає інформацію про підприємство, оцінює її привабливість і рентабельність операції, окреслює напрями атаки й запускає «пробну версію» (перевіряє здатність підприємства оборонятися). Тривалість етапу залежить від розмірів підприємства і намірів рейдера (від одного до шести-семи місяців).

Атака (розробляється індивідуально для підприємства з передбаченням необхідної корекції). На думку експертів, на кожному підприємстві є кілька слабких місць для рейдерських атак: по-перше, за умов, якщо контрольний пакет акцій (30 відсотків) не консолідовано, у рейдера є три варіанти: він може скупити акції у працівників, «вплинути» на менеджмент та через номінального акціонера отримати контроль над підприємством; по-друге, борги підприємства; по-третє, невдоволені дрібні акціонери та звільнені працівники або навіть і керівники.

Рейдер, шляхом судових рішень захоплює контроль над підприємством або відчужує активи («засипає» власників позовами від імені акціонерів з приводу різних порушень, пред'являє до арбітражу попередньо куплені борги підприємства, ініціює різні перевірки за «сигналами» акціонерів та на надуманих підставах порушує кримінальні справи щодо керівництва). Тривалість етапу – від одного дня до кількох років, залежно від зусиль протидії.

Піар рейдера. Для досягнення своєї мети рейдери вдаються до тактики інтриг, змов, маніпулювання громадською думкою. Часто вони намагаються «вплинути» на керівний орган і зіграти на внутрішніх суперечностях, за використання шантажу, проведенні чорного піару в засобах масової інформації, створення конфліктної ситуації з органами виконавчої влади. Тобто використовуються всі засоби та можливості, щоб зібрати навколо себе невдоволених дрібних акціонерів, створити умови для приходу до влади штучно створеної опозиції.

Протистояння між підприємством та рейдером. Ґрунтуючись на впровадженні попередніх етапів, відчувши загрозу, власники та

керівники намагаються захиститися. На цьому етапі кожна сторона (керівництво та рейдери) намагається продемонструвати підконтрольну їм кредиторську заборгованість і отримати в будь-якому підконтрольному суді рішення, що блокує виконання здійснення угод з активами. На цьому етапі програє підприємство, бо в рейдера більше часу на підготовку та створення перешкод.

Легалізація рейдера. Для створення формальних передумов захоплення підприємства, рейдер організовує паралельний орган управління, який максимально дотримується всіх формальних процедур і вимог чинного законодавства, шляхом організації позачергових зборів акціонерів, переобрання на ньому ради директорів та генерального директора. На цьому етапі, власники перешкоджають таким зборам, але якщо вони відбулися, то оскаржують їх легітимність. Контролюючи достатній пакет акцій, рейдер створює видимість того, що він надіслав до діючого органу управління вимогу про проведення позачергових акціонерних зборів (надсилає чистий аркуш у конвертах з повідомленням). У результаті створюється ситуація, коли орган управління ігнорує вимоги акціонерів, а рейдер отримує право провести збори і не допустити на них своїх суперників (з обмеженим доступом акціонерів). Цей процес триває доти, доки на зборах з аналогічним порядком денним не набереться кворум і більшістю голосів переобирається нова рада директорів. Наступний крок – один з акціонерів подає позов до суду з вимогою визнати рішення зборів недійсним. Суд, розглянувши справу, виносить відмову. Отже, рейдер отримує цінний документ про визнання судом зборів законними і правомочними.

Завершення перехоплення управління. Створений рейдером паралельний орган управління фактично бере контроль над підприємством. На цьому етапі, як правило, розпочинається жорстока інформаційна та адміністративна війна.

Результати захоплення. Якщо атака пройшла успішно, подальші дії рейдера залежать від мети та завдань операції. В разі досягнення мети (захоплення активів підприємства для отримання значного доходу) реалізуються угоди із продажу нерухомості, устаткування, транспорту та іншого майна підприємства. Якщо рейдерська операція проводилася для захоплення бізнесу загалом, то захоплювачі реалізують низку заходів з його утримання. Придбане підприємство приєднується до холдингу, в результаті чого створюється нова вертикаль управління та відповідна структура безпеки.

Підсумки рейдерської роботи. Самі рейдери стверджують, що основною статтею витрат у бюджеті є стаття роботи з законодавчою владою, а загальна собівартість рейдерської операції із захоплення становить від 100 тисяч до 1 мільйона доларів США.

1. Рейдерство: українські реалії. – Електронний ресурс.- Режим доступу: http://biz.nv.ua/ukr/experts/tsykhonya/rejderstvo-ukrajinski-realiji-175061.html

2. Рейдерство в Украине.- Електронний ресурс. – Режим доступу: https://censor.net.ua/tag/2480/reyiderstvo.

НАУКОВЕ ВИДАННЯ

ВИКОРИСТАННЯ СУЧАСНИХ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В ДІЯЛЬНОСТІ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Збірник матеріалів
Всеукраїнського науково-практичного семінару
24 листопада 2017, ДДУВС

Відповідальний за випуск Е.В. Рижков
Упорядник О.С. Гавриш
Комп'ютерна верстка О.С. Гавриш

Опубліковано в авторській редакції

Дніпропетровський державний університет
внутрішніх справ 49005, м. Дніпро, проспект Гагаріна, 26