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.