2. Вівчар О. І. Сучасна прагматика та вектори розвитку в контексті зміцнення фінансової складової економічної безпеки суб'єктів господарювання / О. І. Вівчар // Збірник матеріалів Міжнародної науково-практичної конференції [«Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід»] – Тернопіль, ЮФ ТНЕУ 8-9 квітня 2016. – С. 318–321.

3. Шлемко В.Т. Економічна безпека України: сутність і напрямки забезпечення / В.Т. Шлемко, І.Ф. Бінoко. – К.: НІСД, 2009. – 435 с.

4. Кваснюк Б.Є. Конкурентоспроможність національної економіки / за ред. д-ра екон. наук Б.Є. Кваснюка. – К.: Фенікс, 2010. – 582 с.

Ковальчук О.

студент магістратури юридичного факультету
Тернопільського національного економічного університету
Науковий керівник: к.е.н., доц., доцент кафедри
економічної безпеки та фінансових розслідувань ТНЕУ
Муравська Ю.Є.

НЕЙТРАЛІЗАЦІЯ ЗАГРОЗ, ЩО ВИНИКАЮТЬ В РЕЗУЛЬТАТІ ВИКОРИСТАННЯ ШКІДЛИВОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ НА МОБІЛЬНИХ ПРИСТРОЯХ

XXI ст. – це століття інформаційних технологій та інновацій. За останні десятиліття змінилось життя як окремих людей, так і всього суспільства в цілому. Значно зросла роль інформації та чисельність людей, задіяних у сфері інформаційних технологій.

Переважаюча більшість людей використовує інформаційні технології як для роботи, так і в особистому житті. Адже ці технології здатні обробляти, передавати та зберігати інформацію з вражаючою швидкістю та об'ємом. Майже у кожного вдома є персональний комп'ютер або мобільний пристрій (смартфон, планшет, тощо) за допомогою яких здійснюється доступ в інтернет, проводяться грошові операції з банками, зберігається конфіденційна інформація.

Разом з цими принадами технологічний прогрес надає можливість здійснювати злочини у новий спосіб, з використанням інформаційних технологій.

Особливо вразливими є смартфони, які по суті є кишеньковими комп'ютерами.

В першу чергу, метою шахраїв є інформація, яка надає доступ до особистого та професійного життя користувача. У другу — вимагання грошей або просто бажання нашкодити. Шахраям не обов'язково викрадати смартфон для того, щоб отримати дані, що на ньому зберігаються. Достатньо просто завантажити шкідливе програмне забезпечення, яке і призведе до втрати даних.

Проаналізувавши українське суспільство можна відмітити вкрай низький рівень обізнаності громадян щодо шкідливого програмного забезпечення в цілому та захисту мобільних пристроїв від атак злочинців. Навіть підключення

через вільно доступну мережу Wi-Fi може становити загрозу викрадення особистих даних.

Важливо розуміти, всі операційні системи вразливі до атак. Найпоширенішими видами кібер-злочинів є:

— кардинг – використання в операціях реквізитів платіжних карт, отриманих з платіжних та розрахункових систем, а також із персональних комп'ютерів та мобільних пристроїв (або безпосередньо, або через програми віддаленого доступу, «трояни», «боти»).

— фішинг – злочин, відповідно до якого користувачам платіжних систем надсилають повідомлення електронною поштою під видом адміністрації системи з проханням вказати свої рахунки та паролі.

— вішинг – вид шахрайства, суть якого полягає в проханні зателефонувати на певний номер, при розмові дізнаються конфіденційні дані жертви.

— соціальна інженерія – технологія управління людьми за допомогою спілкування в Інтернет-просторі.

— мальвар – написання та розповсюдження шкідливого програмного забезпечення.

— рефайлінг – незаконна підміна трафіку мобільного пристрою.

За прогнозами експертів, до 2020 року населення планети становитиме 7,8 мільярдів людей, а кількість мобільних пристроїв - 11,6 мільярдів, тобто більше ніж 1 пристрій на людину. В свою чергу результати дослідження в 2016 році показали, що рівень вразливості мобільних пристроїв в Україні становить 34%.

Якщо порівнювати статистичні дані за 2015 та 2016 роки, то можна прослідкувати, що загроза враження мобільного пристрою зростає в геометричній прогресії. Адже, порівняно з 2015 у 2016 році викрадено в 4 рази більше коштів з платіжних карток. Ця сума становить 339 мільйонів гривень. У свою чергу відповідальність за скоєні злочини понесло лише 10 злочинців. Правопорушення у сфері інформаційних технологій, без перебільшення, стали однією з найбільших загроз перед суспільством. Тому 15 жовтня 2015 року здійснюється ряд заходів щодо формування підрозділу Департаменту кіберполіції, основним завданням якого є протидія поширенню кіберзлочинності в Україні.

Сучасні тенденції державотворення України характеризуються поступовим формування системних підходів до національної безпеки, в контексті яких забезпечення інформаційної безпеки, у тому числі і кібербезпеки, займає одне з головних місць [1].

Жертвами кіберзлочинців щодня стають близько 1 мільйона людей по всьому світі. За рік злочинці завдають збитків на суму більше 290 мільярдів доларів. Більшість з них залишається непокараними. Саме через це протидію інтернет злочинцям потрібно вести на міжнародному рівні, адже шахрай може знаходитись за тисячі кілометрів від своєї цілі і державні кордони не є перешкодою. Для цього у 2013 році було створено Європейський центр боротьби з кіберзлочинністю, який є частиною поліцейської служби Євросоюзу. Фінансування центру йде також з бюджету Європолу.

Важливим документом, у рамках країн-учасниць ООН є «Резолюція з боротьби із злочинним використанням інформаційних технологій» [2],

прийнята у 2001 р., у якій вказано на необхідність співробітництва між державами та приватним сектором у боротьбі із злочинним використанням інформаційних технологій. Співробітництво у боротьбі із злочинами у сфері інформаційних технологій повинно досягатися шляхом уведення до законодавства відповідальності за інформаційні злочини, транснаціонального співробітництва правоохоронних органів, міжнародного обміну інформацією про проблеми зло

чинного використання інформаційних технологій, навчання співробітників правоохоронних органів за умови інформаційного суспільства, захисту комп'ютерних систем від несанкціонованого втручання, забезпечення зберігання інформаційних даних та своєчасний збір доказів при розслідуванні злочинів. У п. 1 Резолюції вказано, що інформаційні технології мають розроблятися таким чином, щоб сприяти попередженню та виявленню випадків злочинного використання, відстежуванню злочинців та збиранню доказів[2].

Вкрай важливою є співпраця на міжнародному рівні. За останній період в Україні почали працювати кілька програм для зміцнення кібербезпеки. На приклад, програма Safe Card [3], ініційована Українською міжбанківською Асоціацією членів платіжних систем ЄМА за підтримки Державного департаменту США. Проект стартував в Україні 1 жовтня 2016 року і продовжуватиметься до 30 вересня 2017 року. Програма передбачає комплекс заходів та активностей Асоціації ЄМА, медіа, учасників платіжного ринку та державних органів за п'ятьма напрямками протидії:

— підвищення обізнаності громадян України про ефективні способи захисту власної інформації та правила безпечного використання платіжних карток, електронних платежів та банкоматів;

— удосконалення кримінального законодавства України у сфері неправомірного обігу засобів платежу та приведення його у відповідність світовим стандартам з урахуванням актуальних видів карткових та платіжних злочинів;

— удосконалення системи оперативного отримання й перевірки правоохоронними органами інформації про злочини із платіжними картками, електронними платежами та в банкоматах;

— удосконалення взаємодії між банками, патрульною поліцією, кіберполіцією і слідством при розслідуванні та протидії злочинам із платіжними картками, електронними платежами та в банкоматах;

— підвищення проінформованості суддів і прокурорів про схеми здійснення злочинів із платіжними картками, інтернет-платежами та в банкоматах, аналіз судової практики і формування рекомендацій із кваліфікації карткових та платіжних злочинів.

У рамках Програми проводяться соціологічні дослідження, розробляються інформаційні матеріали, створюються міжвідомчі робочі групи тощо.

Отже, для ефективної боротьби з злочинами такого типу необхідна співпраця на національному і міжнародному рівнях. Темпи розвитку кіберзлочинності вимагають адекватної реакції правоохоронних органів і законодавства в цілому.

Список використаних джерел

1. Якубівська Ю.Є. Світові тенденції розвитку кіберзлочинності [Електронний ресурс] / Ю.Є. Якубівська // Зовнішня торгівля: економіка, фінанси, право : Науковий журнал. Серія: Економічні науки. – К.: УДУФМТ. – 2014. – Режим доступу до ресурсу: http://dspace.tneu.edu.ua/handle/316497/1538.
2. Резолюція, прийнята Генеральною Асамблеєю 55/63 Боротьба із злочинним використанням інформаційних технологій. [Електронний ресурс]. – 2001. – Режим доступу: http://www.pravoznavec.com.ua/period/article/9044/%C1.
3. Програма Safe Card [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://ema.com.ua/

Мацех А.

студент магістратури юридичного факультету
Тернопільського національного економічного університету
Науковий керівник: к.е.н., доцент кафедри
економічної безпеки та фінансових розслідувань ТНЕУ
Вівчар О.І.

НАУКОВІ ПІДХОДИ ДО ДЕТЕРМІНАЦІЇ ФЕНОМЕНА ЛОГІСТИЧНОЇ СТРАТЕГІЇ ЕКОНОМІЧНОЇ БЕЗПЕКИ ПІДПРИЄМСТВ

В сучасних умовах макроекономічної нестабільності, функціонування будь-якого підприємств залежить від вірно обраної логістичної стратегії в системі економічної безпеки підприємств, яка становить комплексний, впорядкований та інтеґрований процес, спрямований на отримання сукупних результатів системи в контексті ефективного використання фінансових та матеріально-технічних ресурсів. Основними логістичними стратегічними цілями підприємницьких структур є проведення оптимізаційного процесу витрат матеріальних та інформаційних потоків.

Слід зазначити, що на сучасному етапі розвитку економіки України велика кількість вітчизняних підприємств знаходиться в кризовому становищі. Тому перед підприємствами постає актуальна задача формування ефективної стратегії забезпечення економічної безпеки підприємств з метою протидії загрозам зовнішнього та внутрішнього походження [1]. Неможливо залишити поза увагою те, що серед підприємств лише одиниці мають добре опрацьовану логістичну стратегію діяльності, яка передбачає комплексне управління матеріальними та інформаційними потоками з урахуванням сучасних концепцій управління економічною безпекою. Можна дати наступне визначення логістичної стратегії у системі забезпечення економічної безпеки підприємств – це довгостроковий, якісно визначений напрямок розвитку логістики, що стосується форм і засобів її реалізації у фірмі, міжфункціональній і міжорганізаційній координації й інтеґрації, сформульоване вищим менеджментом компанії відповідно до корпоративних цілей та з метою підвищення рівня економічної безпеки підприємств.

В таких умовах функціонування основними характеристиками сучасної логістичної стратегії досліджуваних підприємств можна вважати наступні: