Таким чином, для підприємств професійне шахрайство завдає значні збитки. Тому необхідно або залучати консультантів з боку, або збільшувати підрозділ, який займається забезпеченням економічної безпеки всієї організації в цілому. На підприємстві користуються певним набором математичних методів аналізу підприємства. У той же час, необхідно використовувати неструктуровані методи аналізу, що ускладнює отримати кількісні оцінки рівня забезпечення економічної безпеки. Сюди можна віднести: випуск продукції, рівень заробітної плати працівників, витрати на маркетингові заходи, щодо реалізації продукції на ринку товарів і послуг тощо.

Використані джерела:

1. Артем Ковбель. Шахрайство в компанії: що потрібно знати бізнесу. [Електронний ресурс]. – Режим доступу: https://uteka.ua/ua/publication/commerce-12-pravovie-soveti-67-moshennichestvo-v-kompanii-chto-nuzhno-znat-biznesu
2. Report To The Nations. 2018 Global Study On Occupational Fraud And Abuse. [Електронний ресурс]. – Режим доступу: https://www.acfe.com/report-to-the-nations/2018/#download

Свиридова М.С. - курсант 4 курсу факультету підготовки фахівців для підрозділів кримінальної поліції;
Прокопов С.О. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

АКТУАЛЬНІ ПИТАННЯ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

Актуальним питанням на сьогоднішній день постала гібридна агресія до нашої країни з боку Росії. Постійно, зарубіжні країні планують ввести новітні зміні в інформаційний простір та намагаються вдосконалити технології його захисту.

Увага до цього питання дуже довго не була загострена з боку влади нашої держави, аж поки в червні 2017 року не сталась кібератака. Ця кібератака, повністю на певний період часу заблокувала діяльність не тільки тисячі компаній, але й нормальну діяльність державних органів[2]. Вірус, яким були заражені персональній комп'ютери, вимагав викуп у розмірі певної суми (валюта-доллар). Саме цією подією, весь світ зрозумів наскільки важлива кібербезпека та наскільки вона в нас не розвинена. Тому, з боку законодавства було прийнято новий закон, яким має напрям діяльності – сформувати загальнодержавну кібезбезпеку. На основі цього було створено відповідні підрозді-

ли в різних відомствах, які виконують покладені на них функції. Новим для України є факультет кіберзлочинності в Харкові. Вищий навчальний заклад зі специфічними умовами навчання подібний нашому ДДУВС, проте в ньому функціонує новий для інших ВНЗ факультет – боротьби з кіберзлочинністю. В такий спосіб, держава вирішила не тільки запровадити новітні зміни щодо захисту інформації та протидії кіберзлочинам, а повністю розробити систему, яка буде функціонувати та забезпечить безпеку інтересів громадян, та і України в цілому [1].

Також, ще одним прикладом забезпечення кібербезпеки є СБУ. На Службу безпеки України покладається розслідування кіберінцидентів та кібератак, здійснених проти державних інфосистем. Паралельно цьому Міністерство оборони має бути підготовленим так би мовити «до відбиття військової агресії в кіберпросторі». Ще одним прикладом є Національний банк України – в його повноваженнях, забезпечення кібербезпеки у сфері банківської діяльності.

За захищений доступ держорганів, антивірусний захист і аудит інформаційної безпеки відповідатиме Державний центр кіберзахисту.

Розвиток сучасних країн, дозволяє виділяти не просто злочини як убивство, крадіжка, незаконне поводження з вогнепальною зброєю тощо, а виділяє нові злочини – вчинені в кіберпросторі. В свою чергу це дасть можливість призначати покарання та засуджувати винних за вчинення таких діянь в Україні. Тобто, навряд чи будуть рецедиви в даній сфері, а отже запобігти майбутнім кіберзлочинам можливо.

Велику підтримку в забезпеченні кібербезпеки отримала Україна з боку зарубіжних країн. Не виключенням стали і США. Ще в в лютому 2018 конгресмени схвалили проект Закону про співпрацю з Україною з питань кібербезпеки, спрямований на просування активної взаємодії між Україною та США в сфері кібербезпеки [1]. Законопроект розроблено на Капітолійському пагорбі під керівництвом члена комітету з міжнародних справ палати представників Брендана Бойла – безпосередньо для української держави. В ході обговорення документа Бойл заявив: «Впродовж останніх років Росія використовувала Україну як полігон для кібератак, які ставлять під загрозу національну безпеку нашого великого союзника, України, а також її сусідів по регіону» [2]. Експерти зазначають, що це буде перший закон США в сфері кібербезпеки, де слово Україна винесено в заголовок.

Отже, підсумовуючи вищезазначене, слід вказати, що забезпечення кібербезпеки це одна з найважливіших складових в системі забезпечення нормальної діяльності країни. Забезпечення кібербезпеки завдання не окремої країни, це завдання всіх країн світу. Тому, для розроблення єдиного плану дій, необхідна підтримка один одного на законодавчому рівні та максимальне об’єднання сил. Забезпечення кібербезпеки в контексті глобальних загроз, поряд з спільними зусиллями міжнародного співтовариства, диктує важливість розробки і здійснення превентивних дієвих заходів проти кібератак і кіберзлочинів в світовому кіберпросторі

Бібліографічні посилання:

1. Від кібератаки вірусом Petya.A постраждали до 10 % комп'ютерів в Україні – Шимків [Електронний ресурс] / Новое Время. – Режим доступу : http://nv.ua/ukr/ukraine/events/vid-kiberatakivirusom-petya-a-postrazhdali-do-10- komp-juteriv-v-ukrajini-shimkiv-1442363.html
2. Спільно з Україною в ролі лідерів з кібербезпеки: Законопроект Конгресу США [Електронний ресурс] – Режим доступу : https://www.ukrinform.ua/rubric-polytics/2399870-spilno-z-ukrainou-v-rolilideriv-z-kiberbezpeki-zakonoproekt-kongresu-ssa.html

Сокол Р. - студентка 3 курсу факультету соціально-психологічної освіти та управління;
Гавриш О.С. – науковий керівник, старший викладач кафедри економічної та інформаційної безпеки (Дніпропетровський державний університет внутрішніх справ)

АГРЕСІЯ В СОЦІАЛЬНІЙ МЕРЕЖІ: РОЗПОВСЮДЖЕННЯ КІБЕРБУЛІНГУ В УКРАЇНІ

Фахівці зі сфери соціальних комунікацій та психологи зазначають, що чим більше ми занурюємось у соціальні мережі та стаємо співучасниками різноманітних дискусій — тим далі ми від справжнього життя. Всі ми пов'язані з мережами, існуємо в уявному світі, віримо в його символи, ніби вони реальні та по-справжньому емоційно реагуємо на віртуальну взаємодію з іншими людьми. Науковці вже не говорять про інтернет-залежність. Вони говорять про травму від інтернет-насилля та використовують для її ідентифікації спеціальний термін – кібербулінг.

Щодо світової практики, яка визначає булінг - як прояв дискримінації дитини, що виражається у фізичних і психічних формах насильства [1]. Форми прояву булінгу досить різноманітні: фізична (завдання ударів, штовхання, пошкодження або крадіжка власності), словесна (обзивання, глузування або висловлювання, якими ображається стать, раса або сексуальна орієнтація), соціальна (виключення інших із групи чи розповсюдження пліток або чуток), письмова форма (написання записок або знаків, що є болючими чи образливими) та безпосередньо електронна форма або кібербулінг (розповсюдження чуток та образливих коментарів з використанням електронної пошти, мобільних телефонів, сайтів соціальних мереж) [2].

Психолог із Києва, Світлана Паніна підкреслює, що: «Насильство у мережі має низку особливостей, через які ми стаємо більш вразливими до нього. І головна — це те, що конфлікт відбувається в уявному світі людини, а реакція на нього — на фізичному рівні людини. Якщо кількість переслідувачів, які цькують людину офлайн, зазвичай обмежена, у мережі масштаб кібербулінга може бути практично безмежним. Кібербулінг зазвичай розвиває-