– раскрытие персональных данных;

– социально-опасный контент: кибербулинг, призывы к суициду и др;

– вмешательство в выборы, атаки на электронные системы голосования и обработки информации;

– атаки на электронные системы, которые обслуживают физическую инфраструктуру поставок различных товаров.

Авторы изучили состав основных продуктов и услуг криминальной направленности, относящихся к ТЦЭ. Но их спектр постоянно изменяется, появляются новые сегменты, требующие исследования и описания. В докладе будут рассмотрены следующие основные сегменты: кибероружие, как сосредоточение всех достижений информационных и коммуникационных технологий на уровне противодействия между государствами; целенаправленные атаки и АТР-группы или киберкриминал; кража личных данных. В качестве нового сегмента выделена деятельность криминальных групп по отношению к криптовалютам и нападение на криптобиржи. Следует отметить, что технология блокчейн внушает доверие клиентам и доказывает безопасность криптовалютных транзакций. Но развитие криптовалютного бизнеса не обошло пристальным вниманием компьютерных мошенников. Они обратили внимание и усилия на деятельность бирж, которые специализировались на покупке, продаже и хранении виртуальных валют.

Библиографические ссылки

1. Borta, G. (2015). The Dark Side of Information Economics. Economica (An. XXIII, nr2. (92)).
2. Охрименко, С., & Бортэ, Г. (2018). Тень цифровой экономики. ГОДИШНИК ТОМ CXXI, АКАДЕМИЧНО ИЗДАТЕЛСТВО „ЦЕНОВ",СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ". № 121.
3. Охрименко, С., & Бортэ, Г. (2019). Новое наполнение науки секьюритологии. В Nauka i praktyka bezpieczeństwa (стр. 112-147). Krakow: WYDAWNICTWO EAS.
4. Ohrimenco, S. & Borta, G., (2021). The nature of shadow digital economics. MEST Journal, 15 January, 9(1), pp. 146-156.

Панченко Л. В., викладач кафедри загальноправових дисциплін Дніпропетровського державного університету внутрішніх справ

МУЛЬТИСТЕЙКХОЛДЕРСЬКА МОДЕЛЬ УПРАВЛІННЯ ІНТЕРНЕТОМ

В наш час розвитку інформаційних технологій відбувається зростання кіберзагроз та їх вплив на функціонування національних та транснаціональних структур, що сприяє формуванню нової глобальної

ситуації в безпеці.

Між світовими центрами відбувається поділ сфер впливу у кіберпросторі, внаслідок цього посилюється їх прагнення до забезпечення власних геополітичних інтересів, що впливає на рівень розвитку інформаційного суспільства держав. Посилюється маніпулювання громадською думкою та використання кібератак як інструменту спеціальних інформаційних операцій.

Необхідним фундаментом інформаційного суспільства є проголошене у *ст. 19 Загальної декларації прав людини* право кожного на свободу переконань, що серед іншого включає свободу переконань та свободу шукати, отримувати та поширювати інформацію та ідеї будь-якими засобами та незалежно від державних кордонів.

За результатами всесвітньої зустрічі з питань інформаційного суспільства *в Женеві 2003 р.* була розроблена *Декларація принципів інформаційного суспільства (Туніс),* що визначила основні завдання побудови інформаційного суспільства у світі та *План дій.* Також було затверджено щорічне проведення форуму з питань управління Інтернетом та визначено, що політичні повноваження питань регулювання Інтернету є суверенним правом кожної держави [1].

Основними підходами до управління Інтернетом є такі:

- технологічна координація елементів (розподіл IP-адрес);
- створення протоколів і стандартів;
- управління системою доменних імен тощо;
- розробка урядами принципів, норм, правил, програм та процедур ухвалення рішень.

У сферу забезпечення інтересів кожної держави входить: забезпечення кібербезпеки та встановлення режиму регулювання Інтернету. Крім того, виявленню кіберзагроз сприяє Інтерпол.

Платформа Інтерполу використовується як централізований портал для забезпечення координації силових структур у боротьбі з кіберзлочинцями, у своєму складі має 194 країни, що створюють своєрідну глобальну систему поліції, яка співпрацює з Генеральним секретаріатом для обміну даними під час поліцейських розслідувань. Для цього в кожній країні створено національне центральне бюро Інтерполу (NCB), яке пов’язує національну поліцію з глобальною мережею [5].

Законодавством України, яке регулює Інтернет, є Конституція України, закони України «Про національну безпеку України», «Про основні засади забезпечення кібербезпеки України», Конвенція про захист прав людини і основоположних свобод, Конвенція про кіберзлочинність, Стратегія національної безпеки України, Концепція боротьби з тероризмом в Україні, тощо. В глобальному контексті пр*отидії кіберзагрозам була прийнята Стратегія кібербезпеки України.*

З огляду на протидію злочинам в інформаційному полі національного

законодавства 15 жовтня 2021 року РНБО затвердила Стратегію інформаційної безпеки України на період до 2025 року.

Основними завданнями стратегії визначено: захист інформаційного простору України, протидію поліцією поширенню незаконного контенту; інформаційну реінтеграцію громадян, підвищення рівня медіакультури та медіаграмотності; забезпечення захисту прав працівників інформаційної сфери тощо [1].

Стратегія визначає підтримку *мультистейкхолдерської моделі* управління Інтернетом. Мультистейкхолдерська модель управління містить у собі багатостороннє управління Інтернетом.

Стейкхолдери – це фізичні та юридичні особи, зацікавлені у фінансових та інших результатах діяльності певної організації та здатні здійснювати на неї вплив, що пояснює та формує стратегію розвитку з врахування інтересів зацікавлених сторін [3].

Відповідно до *мультистейкхолдерської моделі* для досягнення цілей управління Інтернетом потрібно брати до уваги різні інтереси *стейкхолдерів* (представників держав, урядових та міжурядових організацій), які будуть представляти певний тип неформальної коаліції.

Ще в березні 2021 року для протидії дезінформації, пропаганді, реагування на кіберінциденти та кібератаки в Україні створено спеціальні органи: *Міжнародний центр протидії дезінформації* та *Центр стратегічних комунікацій та інформаційної безпеки*. Відповідно до Стратегії 15 жовтня 2021 року утворюється *Національний центр резервування державних інформаційних ресурсів, урядова команда – CERT-UA, Національний координаційний центр кібербезпеки.*

Загалом Консорціум Всесвітньої мережі «Інтернет» містить у собі 350 організацій, що займаються розробкою та поширенням стандартів Інтернет.

На виконання цілей Україною планується: формування системи дієвої кібероборони, забезпечення у протидії розвідувально-підривній діяльності у кіберпросторі, завершення імплементації міжнародного законодавства; удосконалення системи розвідувального забезпечення та низка інших заходів. [1].

Отже, *мультистейкхолдерської моделі* управління Інтернетом – це *моделі* управління для досягнення цілей з урахуванням інтересів зацікавлених сторін.

Бібліографічні посилання

1. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України» : Указ Президента України від 26.08.2021р. № 447/2021.
2. Всемирная встреча на высшем уровне по вопросам информационного общества. Документ WSIS-05/TUNIS/DOC/7-R. Тунисское обязательство. Тунис, 2005. URL: www.itu.int/wsis/docs2/tunis/off/7-ru.doc
3. Гурова А. Р., Морозова В. К. Стейкхолдерский подход к управлению предприятием-

субъектом ВЭД. URL: /donampa.ru/images/document/repablic_o/1/9.pdf
4. Декларація принципів побудови інформаційного суспільства. URL: /www.itu.int/dms_pub/itu-s/md/03/wsis/doc/S03-WSIS-DOC-0004!!PDF-R.pdf.
5. Innovation to beat cybercrime acceleration the theme of 2021 Europol-INTERPOL Cybercrime Conference. 11 November 2021. Cybersecurity innovation the backbone of digital transformation. URL: https://www.interpol.int/News-and-Events/News/2021/Innovation-to-beat-cybercrime-acceleration-the-theme-of-2021-Europol-INTERPOL-Cybercrime-Conference

Паршин Ю. І.,
професор кафедри фінансових
та стратегічних розслідувань
Дніпропетровського державного
університету внутрішніх справ,
доктор економічних наук, професор

ВПЛИВ ПОДАТКОВИХ СХОВИЩ НА ЕКОНОМІКУ ДЕРЖАВИ

Глобалізація світової економіки сприяє зростанню міжнародного співробітництва, торгівлі, а економіки країн стають більш взаємозалежними одна від одної, що змушує країни поступово уніфіковувати податкові системи з метою формування сприятливого середовища для розвитку бізнесу.

Зазначимо, що в кожній країні своя система валютного регулювання, а також своя система оподаткування. Такі обставини можуть бути використаними нерезидентами країн для отримання додаткового прибутку, часткової нейтралізації вимог валютного законодавства країни, де базується організація в умовах «переміщення» її в іншу юрисдикцію. Це стосується також і конкуренції між валютними ринками держав за схемою торгів, де наявні кращі умови для ведення бізнесу, а зважаючи на динамічний інформаційно-технологічний розвиток світової економіки, такі питання і процеси не є проблемними. Ці та інші фактори і призвели до активного розвитку офшорного бізнесу в кінці минулого століття.

Податкове сховище, або інша його назва офшор – це фінансовий центр, основу якого становить спеціалізація на залученні іноземного капіталу [1]. Основою діяльності таких податкових зон є надання податкових пільг для іноземних компаній, які зареєстровані в країні, де вони розташовані, але з управлінням ними з-за кордону. У різних країнах є різне податкове навантаження на компанії, від помірного до такого, що компанії повністю звільняються від оподаткування, під час здійснення їх діяльності за межами місця реєстрації.

Необхідно також зазначити, що одним з найбільш привабливих критеріїв є анонімність фактичних власників компаній. Реєстрація компаній в податкових сховищах дозволяє компаніям більш ефективно планувати свою