Національний університет «Острозька академія»

Науково-дослідний інститут інформатики і права Національної академії правових наук України

Секція права національної безпеки та військового права Національної академії правових наук України

Національна академія Служби безпеки України

Інститут Управління державної охорони Київського національного університету імені Тараса Шевченка

Національна академія Державної прикордонної служби України імені Богдана Хмельницького

(За підтримки Міністерства закордонних справ Республіки Болгарія та Посольства Республіки Болгарія в Україні проекту з метою розвитку: «Підтримка демократичного контролю над сектором безпеки в контексті євроатлантичної інтеграції України»)

ОСВІТА І НАУКА У СФЕРІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ПРОБЛЕМИ ТА ПРІОРИТЕТИ РОЗВИТКУ

Матеріали ІІІ міжнародної науково-практичної конференції,
присвяченої 25-річчю відродження та 450-річчю утворення Національного університету «Острозька академія»

14 червня 2019 р.
м. Острог

УДК 355/359

Рекомендовано до друку
Вченою радою Науково-дослідного інституту інформатики і права
Національної академії правових наук України
Протокол № 5 від 8 липня 2019 р.
Секцією права національної безпеки та військового права
Національної академії правових наук України,
протокол № 4-Б від 10 липня 2019 р.

Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку : збірник матеріалів ІІІ міжнародної науково-практичної конференції / 14 червня 2019 р., м. Острог / Упорядн.: Дорогих С.О., Доронін І.М., Довгань О.Д., Лебединська О.В., Пилипчук В.Г., Радзієвська О.Г., Романов М.С. – НУОА, НДІІП НАПрН України. – К.: ТОВ «Видавничий дім «АртЕк», 2019. – 308 с..

ISBN 978-617-7814-10-7

Збірник матеріалів конференції присвячений розгляду проблем імплементації Закону «Про національну безпеку України», розвитку системи цивільного демократичного контролю над сектором безпеки та суб'єктів сектору безпеки і оборони в контексті євроатлантичної інтеграції України, актуальним питанням гібридної війни, освіти і науки у сфері національної безпеки.

Видання розраховане на широке коло фахівців, експертів і вчених у сфері національної та міжнародної безпеки.

Збірник опубліковано за підтримки Міністерства закордонних справ Республіки Болгарія та Посольства Республіки Болгарія в Україні в рамках проекту з метою розвитку.

Автори тез доповідей несуть повну відповідальність за підбір, точність наведених фактів, цитат, статистичних даних, власних імен та інших відомостей.

УДК 355/359

ISBN 978-617-7814-10-7

5. Концепция формирования информационного пространства Содружества Независимых Государств (18 октября 1996 г.) [Електронний ресурс] // Единый реестр правовых актов и других документов Содружества Независимых Государств. – Режим доступу: http://cis.minsk.by/reestr/ru/index.html#reestr/view/text?doc=643 (дата звернення: 31.10.2018)

6. Сурма И. В. Единое информационное пространство СНГ: 20 лет спустя [Електронний ресурс] / И. В. Сурма // Вопросы безопасности. – 2015. – № 5. – Режим доступу: http://e-notabene.ru/nb/article_17473.html (дата звернення: 31.10.2018)

----------***----------

Євгенія Тихомирова
доктор політичних наук, професор,
Східноєвропейський національний
університет ім. Лесі Українки

ЄВРОПЕЙЦІ ПРО БЕЗПЕКУ В ІНТЕРНЕТІ: ДОСЛІДЖЕННЯ ЄВРОБАРОМЕТРУ

Сьогодні країни Європи опинилися перед глобальними викликами кіберагресій, а кіберзагрози стали цілком реальними. У суспільстві формується свідоме ставлення до кіберзахисту, їх наслідки вже відчули на собі і пересічні громадяни. Підвищення обізнаності у кібербезпеці, поширення загальних правил кіберзахисту й умов повсякденної кібергігієни, залежить від людей, їх поняття вирішальної ролі у забезпеченні безпеки мереж та інформаційних систем.

ISACA[9] дає наступне визначення *кібербезпеки*: захист інформаційних активів шляхом боротьби із загрозами безпеці інформації, яка обробляється, зберігається та передається за допомогою інформаційних систем, що взаємодіють за допомогою мереж [1].

Багато людей вважають кібербезпеку технічною або технологічною проблемою, проте широка громадськість відіграє важливу роль у кібербезпеці. Громадська підтримка зусиль, спрямованих на зменшення кіберзлочинності та дотримання кібербезпеки, є критично важливою для зусиль суспільства щодо збереження переваг цифрових технологій.

[9] Раніше відома як Асоціація аудиту та контролю за інформаційними системами, ISACA тепер за своєю абревіатурою незалежна, неприбуткова, глобальна асоціація, що бере участь у розробці, впровадженні та використанні глобально прийнятих галузевих знань та практик для інформаційних систем.

Ось чому дослідників і політиків цікавить, що громадськість думає про кіберзлочинність і кібербезпеку, а знання того, що думає громадськість про них, має важливе значення для успішної політики в сфері кіберзлочинності і має вирішальне значення для успіху в кібербезпеці суспільства.

Європейський Союз обстежує своїх громадян про злочини всіх видів і, зокрема настрої про кібербезпеку. Дослідження проблем кібербезпеки Євробарометр здійснював неодноразово: у 2012р. [2]; 2013р. [4], 2014р. [3]; 2015р. [7]; 2017р. [5]; 2018р. [6].

Як бачимо з назв доповідей, три останніх дослідження були присвячені безпосередньо ставленню європейців до кібербезпеки.

В останньому дослідженні зазначається, що *кіберзлочинність* – це проблема без кордонів, що складається зі злочинних дій, вчинених в Інтернеті та електронних комунікаційних мережах та інформаційних системах. Основними видами злочинів вважаються атаки на інформаційні системи, які можуть перешкоджати або відключати їх функціонування, форми шахрайства та фальсифікації в Інтернеті, такі як крадіжка особистих даних та поширення шкідливого коду, поширення нелегального онлайнового контенту, наприклад дитячої порнографії. Згідно з оцінками аналітиків, кіберзлочинність призводить до втрати мільярдів євро на рік і збільшує навантаження на правоохоронні органи. Зі зростанням використання Інтернету, розповсюдження різного роду пристрої з підтримкою Інтернету, і все більшої передачі персональних даних в Інтернеті, питання про кіберзлочинність, швидше за все, збільшиться, якщо органи влади не будуть вживати узгоджених заходів для її викорінення [6].

Метою спеціального опитування Євробарометра 2018 р. стало розуміння обізнаності громадян ЄС, їх досвіду і сприйняття питань кібербезпеки. У цьому звіті представлені такі результати дослідження.

По-перше, він визначає *закономірності та тенденції частоти використання Інтернету*, засоби, за допомогою яких респонденти мають доступ до Інтернету, а також види діяльності, за допомогою яких зазвичай використовується Інтернет. Близько трьох чвертей респондентів (73%) щодня користуються Інтернетом, ще 9% роблять це часто або іноді. Проте існують значні відмінності щодо країн. Респонденти в країнах Західної та Північної Європи в цілому частіше користуються Інтернетом щодня. Існують також значні та стійкі соціально-демографічні відмінності в доступі до Інтернету: молодь (97%), добре освічені (88%), економічно забезпечені (76%) та міські мешканці (77%) частіше користуються Інтернетом щоденно,

ніж люди похилого віку (46%), респонденти з низьким рівнем освіти (33%), економічно незабезпечні (58%) і жителі сільської місцевості (69%) [6].

По-друге, на прохання вибрати *серед переліку загальних ризиків при використанні Інтернету два загальні занепокоєння* були названі зловживання персональними даними та безпека онлайн-платежів (як 43%). Значну меншість користувачів Інтернету не турбують ці ризики, а майже п'ята частина (19%) не висловила жодних побоювань. Занепокоєння щодо конфіденційності та безпеки в Інтернеті вплинули на поведінку більшості Інтернет-користувачів:

– Майже половина встановила або змінила антивірусне програмне забезпечення (47%) або не відкривали електронні листи від людей, яких вони не знають (45%), а майже чотири з десяти (37%) скоротили особисту інформацію, яку вони надають на веб-сайтах. Проте мало хто зробив крок до скорочення товарів та послуг, які вони купують в Інтернеті (11%), скасовують онлайн-покупки (10%) або відмовляються від онлайн-банкінгу (9%).

– Близько шести з десяти (58%) користувачів Інтернету змінили свій пароль доступу принаймні до одної Інтернет-служби протягом останніх 12 місяців, причому у найбільшій пропорції змінюють пароль електронної пошті (34%), пароль онлайн-банкінгу (26%) або пароль онлайн-соціальної мережі (24%).

– Молодші респонденти (63%), вищі рівні освіти (65%) та менеджери (71%) частіше, ніж старші респонденти (48%), менш освічені (41%) і ручні працівники (55%) змінили хоча б один пароль [6].

– По-третє, тут аналізується *обізнаність респондентів щодо кіберзлочинності*, дивлячись на те, наскільки люди вважають себе добре поінформованими ризики кіберзлочинності, *їхнє ставлення до кібербезпеки*, їх занепокоєння щодо ризику потрапляння жертви до кіберзлочинності та їх сприйняття конкретних видів кіберзлочинності. Половина респондентів вважають себе добре поінформованими про кіберзлочинність:

– 51% респондентів вважають себе добре інформованими про кіберзлочинність, але лише один з десяти (10%) вважають, що вони дуже добре поінформовані;

– між країнами існують значні відмінності: у Данії та Швеції більше трьох четвертих (76%) вважають себе добре інформованими, але в Болгарії та Румунії таких лише третина (30%).

– Більшість людей в ЄС бояться проблем кібербезпеки, але багато хто з них впевнені, що можуть захистити себе від цього:

– близько восьми з десяти респондентів вважають, що існує підвищений ризик бути жертвою кіберзлочинності (79%), тоді як трохи більше шести з десяти (61%) вважають, що вони здатні захистити себе проти нього;

– поінформованість про ризик кіберзлочинності залежить від країни, але в більшості країн переважають ті, хто заявляє, що вони можуть захистити себе від цього ризику;

– молодші респонденти та особи з вищими рівнями освіти впевнені, що вони можуть захистити себе від кіберзлочинності;

– більше третини (36%) європейців вживають заходів для захисту дітей, які стають жертвами домагань в Інтернеті, найпоширеніші дії – моніторинг використання Інтернету (22%), обговорення онлайн-ризиків (20%) та обмеження часу, проведеного в Інтернеті (19%).

– однак менш чверті (21%) європейців знають про існування державних веб-сайт або адрес електронної пошти для повідомлення про кіберзлочинність, і лише 5% використовували такі ресурси [6].

– По-четверте, *аналіз досліджень фактичних контактів респондентів і відповідей на них у зв'язку з цими злочинами* особи та їхні знайомі пережили кіберзлочинність, вжиті заходи та кроки захист своїх дітей від жертви кіберзлочинності:

– більшість респондентів стурбовані тим, що вони є жертвами різних форм кіберзлочинності, причому найбільша частка респондентів висловлює занепокоєння щодо виявлення шкідливого програмного забезпечення на своєму пристрої (71%), крадіжки особистих даних (70%) та банківської картки та онлайн банківського шахрайства (70%);

– більш половини респондентів (54%) знають того, хто був жертвою кіберзлочинності, частіше вказують на шахрайські електронні листи або телефонні дзвінки або зловмисне програмне забезпечення (обидва 26%);

– менш половини респондентів фактично стали жертвами різних форм кіберзлочинності – дві найпоширеніші ситуації, з якими стикаються респонденти, – це отримання шахрайських електронних листів або телефонних дзвінків (34%) і виявлення шкідливого програмного забезпечення (33%);

– більшість європейців у всіх країнах вживають заходів, якщо вони стають жертвою кіберзлочинності, особливо у випадку банківських карт або шахрайства з онлайн-банкінгами (88%) та крадіжками особистих даних (87%) [6].

Отже, європейці є дуже уважними до загроз безпеці і впевнені, що можуть захистити себе від них. Коли мова йде про вжиття заходів у відповідь на кіберзлочинність, результати є досить обнадійливими:

більшість респондентів заявляють, що будуть вживати заходів, якщо вони стануть жертвами кіберзлочинності. Проте ці добрі наміри не завжди можуть бути вжиті на практиці, оскільки лише меншість європейців знають про наявність офіційних ресурсів, до яких слід повідомляти про кіберзлочинність і дуже мало хто з них фактично використовував їх. Дослідження показало, що поінформованість про проблему кіберзлочинності, як правило, є високою в Європі загалом, незважаючи на відмінності в обізнаності та уявленні про те, чи адекватно європейці поінформовані про цю проблему на рівні країн і окремих демографічних груп.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Впровадження європейської кібербезпеки:загальний огляд [Електронний ресурс] – Режим доступу : https://www.isaca.org/Knowledge-Center/Research/Documents/European-Cybersecurity-Implementation-Overview_res_Ukr_1215.pdf

2. Cyber security Special Eurobarometer 390. Report [Electronic resource]. – Mode of access : http://ec.europa.eu/public_opinion/archives/ebs/ebs_390_en.pdf

3. Cyber security. Special Eurobarometer 423. Report [Electronic resource]. – Mode of access : http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_423_en.pdf

4. Cyber security. Special Eurobarometer 404. Report [Electronic resource]. – Mode of access : http://ec.europa.eu/public_opinion/archives/ebs/ebs_404_en.pdf

5. Europeans' attitudes towards cyber security Special Eurobarometer 464a Report [Electronic resource]. – Mode of access : http://ec.europa.eu/commfrontoffice/publicopinion

6. Europeans' attitudes towards Internet security. October-November 2018. Special Eurobarometer 480. Report [Electronic resource]. – Mode of access : http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm

7. Europeans' attitudes towards security. Special Eurobarometer 432. Report [Electronic resource]. – Mode of access : http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_432_en.pdf

----------***----------