Матковська Інга Олексіївна
Національний університет «Одеська юридична академія»,
студентка 4-го курсу факультету кібербезпеки
та інформаційних технологій

ВИЗНАЧЕННЯ ІНТЕРНЕТ РЕСУРСІВ З ЗАБОРОНЕННИМ КОНТЕНТОМ

Відимо, що процеси глобалізації, в тому числі глобалізації інформаційних технологій, надають необмежені можливості для здійснення впливу на особистість і суспільство. Одним з негативних наслідків розвитку інформаційних технологій є поява і розвиток нової форми злочинності – злочинності в сфері високих технологій, коли комп'ютери або комп'ютерні мережі виступають в якості об'єкта злочинних посягань, а також кошти або способи вчинення злочинів. Проблема кіберзлочинності актуалізувалася в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охопили всі сфери життєдіяльності людини і держави, а глобальна мережа Інтернет стала однією з найбільш швидких складових розвитку телекомунікаційних технологій.

На сьогоднішній день більшість розвинених країн світу вдаються до фільтрації інтернет-контенту і ніякому іншому обмеженню свободи в мережі. Однак цілі, завдання та конкретні механізми реалізації подібних обмежень істотно варіюються. Виділяють саме категорії контенту, які піддаються фільтрації в різних країнах світу. До них відносять: політичний контент; соціально-небезпечну інформацію; контент, пов'язаний з національною безпекою; сайти і сервіси, які порушують економічні інтереси.

Методи цензури контенту в Інтернеті можна розбити на дві категорії: нетехнічні і технічні. До категорії нетехнічних методів відносяться закони, що забороняють публікацію того чи іншого контенту, тиск на інтернет-провайдерів, власників сайтів і користувачів з метою змусити їх прибрати небажані матеріали. До категорії технічних методів відноситься блокування

інтернет-ресурсів за IP-адресою, спотворення DNS-записів, блокування сайтів за URL, пакетна фільтрація, фільтрація через HTTP проксі-сервер, порушення роботи мережі і фільтрація результатів пошуку. Для підвищення ефективності механізмів цензури також активно використовуються різні методи збору інформації в Інтернеті. Через складність і недосконалість технічних інструментів обходу фільтрів до технічних методів вдаються не більше двох відсотків користувачів навіть в тих державах, де фільтрації піддається велика кількість інтернет-ресурсів [2].

Закони, що регулюють Інтернет, визначають методи фільтрації, коли блокується контент, що є спецефічним для кожної держави. Проте, існують групи країн, які переслідують схожі цілі в питаннях інтернет-цензури. Варто привести в приклад континентальну модель, де застосовуються методи фільтрації для блокування контенту. Для континентальної моделі характерна фільтрація соціально-небезпечних ресурсів по чітко позначеним категоріям, а також боротьба з порушеннями авторських прав. Цим методом користуються більшість європейських держав.

Тим самим кіберзлочинність, а саме інтернет ресурси с забороненним контентом визнані глобальною міжнародною проблемою. Найбільші труднощі, що стоять перед правоохоронними органами, полягає в неможливості ефективно координувати свої дії через державні кордони, рамки різних юрисдикцій і законодавчих систем. Протидія кіберзлочинності на увазі цілої системи заходів, що включає в себе аналіз об'єктивних умов, що породжують злочин, механізмів їх здійснення, способів виявлення, припинення, розслідування, досвід судового розгляду. Необхідно також створити ефективні механізми впровадження результатів кримінально-правових і кримінологічних досліджень в законодавчу і нормотворчу практику, а також навчання співробітників правоохоронних органів. В рамках комплексного підходу до боротьби з кіберзлочинністю має бути вирішено ряд загальних і приватних науково-практичних завдань [3].

Незалежно від інтелектуальної бази мислення конкретної людини, специфіки техногенної або соціальної ситуації, в якій він змушений діяти, особливості морально-етичних, моральних установок, ступеня інтенсивності їх відстоювання індивідом всі варіанти прийняття ризикованого рішення об'єднує загальна властивість – вони є реалізацією суб'єктом інтелектуально-особистісних зусиль, спрямованих на зниження рівня невизначеності ситуації. При цьому людина сприймає своє рішення як довільний вибір, здійснений ним відносно вільно (аспект вимушеність присутній завжди, але не завжди пригнічує волю) в рамках певної альтернативи можливих варіантів поведінки. Інформаційна складова цього ризику найбільш вагома у випадках використання прогнозної інформації, дефіциту часу на обробку інформації і ухвалення рішення, в умовах активної інформаційної протидії конкурентів або супротивника. На відміну від інших складових ризику інформаційна складова обов'язково є присутньою в кожній ризиковій події. Змінюється лише її відносна величина.

Достатньо швидко технічні системи захисту все більше й більше удосконалюються за рахунок постійного розвитку сучасних технологій, обліку безлічі потреб, які створюють додаткові ризики. До грамотно відбудованих технічних систем захисту можна тривалий час не підходити і останні будуть справно виконувати свої основні функції та завдання, а люди як і раніше будуть залишатися найбільш вразливою ланкою, коли вони мають доступ до інформації.

Кіберзлочинці користуються тим, що психологічні маніпуляції не вимагають великих витрат і специфічних знань (крім кількох психологічних прийомів), їх можна застосовувати протягом тривалого часу, а ще їх складно виявити. Люди, які володіють цінною інформацією або мають до неї доступ, можна порівняти з доступним плодом: вони на увазі і до них дуже легко дотягнутися [1].

Блокувати інтернет ресурси с забороненним контентом складно, так як цьому сприяє низька інституційна цінність

соціальних медіа в країнах, які продовжують знаходиться в ситуації політичної нестабільності. Дискурс, який показав себе в організації протестного руху, виявився куди менш ефективним після кризових піків. Крім того, відкритий і розширюється громадський дискурс, представлений в соціальних мережах, дозволяє представникам влади відстежувати і аналізувати потенційно кризові явища та запобігання їм.

Значимість оперативного реагування державної влади на порядок соціальних медіа зростає з кожним роком. Поступово це явище втрачає суть феномену і перестає бути надзвичайно популярним об'єктом для вивчення. Соціальні мережі з плином часу стають таким же звичним інструментом мобілізації і значущим фактором при організації масових протестних рухів, як канали традиційних ЗМІ, мобільні засоби зв'язку і безпосереднє «живе» спілкування.

Особливу роль відіграє правильно обрана цільова аудиторія для відповідної інформаційної політики. Наприклад, масове залучення неполітизованих користувачів далеко не завжди приносить бажаний результат. Регулярний моніторинг і аналіз трендів дискусій, виявлення потенційних конфліктів, також важко переоцінити в контексті запобігання кризовим ситуаціям.

Зворотною стороною даної ситуації є силовий сценарій, при якому правоохоронні органи держави отримують полегшений доступ до особистих даних мережевих активістів, підозрюваних в порушенні закону і закликах до масових заворушень.

Тему ризиків в контексті блокувння інтернет ресурсов з забороненим контентом можна продовжуваті і далі, але це все одно не захистить інформаційні технології і апаратуру від зловмісників і шахраїв усіх мастей, так як тотальна мережева цензура (блокування головних ресурсів), яка може бути введена наприклад під час загострення політичної обстановки, не буде гарантувати зниження рівня мобілізації, а навпаки може призвести до ескалації конфлікту поза мережею. Ослаблення соціальних зв'язків у віртуальному просторі дійсно

можуть надати владі тимчасові переваги, але ними треба вміти грамотно скористатися.

Список використаних джерел:

1. Осипенко А. Л. Боротьба зі злочинністю в глобальних комп'ютерних мережах: Міжнародний досвід: монографія. М., 2004. С.185.
2. Ефективне попередження злочинності: в ногу з новітніми досягненнями / Матеріали Десятого Конгресу Організації Об'єднаних Націй з профілактики злочинності і поводження з правопорушниками: A / CONF.187 / 10. Відень, 10–17 квітня 2000 року, п. 5.
3. Будапештська Конвенція про комп'ютерні злочини: [Електронний ресурс]. – Режим доступу: https://rm.coe.int/1680081580

Ключові слова: інтернет ресурси, заборонений контент, кіберзлочин, інформаційні технології.

Ключевые слова: интернет ресурсы, запрещенный контент, киберпреступление, информационные технологии.

Keywords: internet resources, prohibited content, cybercrime, information technology.

***Науковий керівник**: д. фіз. - мат. н., професор Василенко М. Д.*

Пальчук Андрій Вікторович
Національний університет «Одеська юридична академія»,
студент 4 курсу факультету кібербезпеки
та інформаційних технологій

РОЗРОБКА КОМПЛЕКСУ ЗАХИСНИХ ЗАХОДІВ ЩОДО ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Конфіденційна інформація входить в сферу підвищеного інтересу конкуруючих компаній. Для недобросовісних конкурентів, корупціонерів та інших зловмисників особливий інтерес представляє інформація про склад менеджменту підприємств, їх статус та діяльності фірми [1].