БУБНОВ ДЕНИС ВАЛЕРІЙОВИЧ

Національний університет «Одеська юридична академія», викладач кафедри іноземних мов, доктор філософії

ГУСЕЙНОВА КАМІЛА САРХАНІВНА

Національний університет «Одеська юридична академія», викладач кафедри іноземних мов

АКТУАЛЬНІ ПРОБЛЕМИ КІБЕРБЕЗПЕКИ У СУЧАСНОМУ СВІТІ

Актуальність проблеми. В умовах глобальних загроз забезпечення безпеки у світі потребує координації та врегулювання багатьох політичних та економічних питань. Зокрема, це осередки громадянських, міжетнічних конфліктів та воєн, продовольчі загрози, негативні наслідки зміни клімату, забруднення навколишнього середовища, виснаження природних ресурсів та уповільнення їх повторного відновлення, необхідність забезпечення економного режиму енергоносіями, розвитку зеленої економіки, раціонального використання природних ресурсів та людського потенціалу, та інше. Однак серед усіх компонентів забезпечення безпеки з'явився новий і водночас складний елемент безпеки – кібербезпека.

Зазначимо, що поняття кібербезпеки включає безліч проблем різного типу, а також ще більше рішень. Кібербезпека, безумовно, найбільше пов'язана з Інтернет-безпекою, включаючи технічні проблеми та вразливість, соціальні та поведінкові проблеми, кримінальну діяльність у кіберпросторі, і ця сфера вважається найскладнішою щодо забезпечення кібербезпеки у світі. Кібербезпека – це розділ безпеки, що вивчає процеси формування, функціонування та еволюції кібероб'єктів, з метою виявлення джерел кібернебезпеки, які можуть завдати їм збитків, АНІ: економіка та управління. Під кібероб'єктом тут розуміється будь-який об'єкт, функціонування якого здійснюється за участю програмованих засобів.

Метою цієї статті є аналіз кібербезпеки та її проблем, які розглядаються серед стратегічних проблем у багатьох країнах світу. Буде розглянуто більш оптимальну модель державної політики кібербезпеки, яка повинна ґрунтуватися на посиленні безпеки та надійності інформаційних систем, мережі Інтернет та всього кіберпростору країни.

Щороку зростає збиток великих організацій, компаній, окремих громадян та ділових людей від кіберних атак та нападів зловмисників. Згідно з прогнозами компанії Gartner щорічні витрати корпорацій та компаній світу щодо підвищення безпеки системи інформаційних технологій становлять 76-77 млрд. дол. США. А загалом зростання кіберрисків за 2015 рік коштувало світовій економіці 445 млрд. дол., із цієї суми 108 млрд. припали на частку США. Ризики, пов'язані з кібершпигунством та злочинами у сфері Інтернет-діяльності, продовжують

нести все більші загрози для бізнесу. Половина витрат на запобігання кіберрискам несли на собі економіки США, Китаю, Німеччини та Японії, що становить понад 200 млрд. дол. США.

Найбільш помітними кіберзлочинами є викрадення даних та порушення недоторканності приватного життя. Найближчими роками набере сили крадіжка інтелектуальної власності, кібер-вимоги та диверсії високих технологій. Серед головних причин злому та зовнішнього втручання в систему ІКТ, Інтернет-мережі та інші мережі є слабка система захисного механізму, відсутність обміну даними кібератак на державні організації та суб'єкти приватного бізнесу, підприємців, фізичних осіб, відсутність детального дослідження та розробки адекватних інструментаріїв протидії, організованого обміну інформацією та системи консультацій, і т.д.

Крім того, багато державних організацій та суб'єктів ринкових відносин, комерсанти та ділові люди надають маленького значення проблемам та серйозній організації заходів щодо підвищення надійної системи кібербезпеки, і у багатьох випадках для цього навіть не роблять елементарні кроки, і не проводять необхідних робіт з тих чи інших елементам кібербезпеки, підвищення ефективності та раціональності захисних механізмів кіберпростору, стійкості та надійності Інтернет-мережі.

Більше того, назріла необхідність удосконалення механізмів та правил багатостороннього міжнародного документа, що відіграє істотну роль у координації зусиль світової спільноти з питань кібербезпеки – Європейської Конвенції з кіберзлочинів, прийнята Радою Європи 23 листопада 2001 року в Будапешті, що містить класифікацію комп'ютерних преступлений виконавчої влади держав боротьби з кіберзлочинами.

Зазначимо, що ця конвенція була підписана 39 країнами Євросоюзу, а також США, Канадою, Японією та ПАР. Конвенція набула чинності з 1 липня 2004 року і наразі є єдиним міжнародним механізмом у сфері кібербезпеки, що має обов'язкову силу, і являє собою набір основних принципів для будь-якої країни щодо організації та зміцнення захисту кіберпростору, формування та розвитку національного законодавства та державної політики щодо припинення кіберзлочинності та забезпечення кібербезпеки в країні.

Не лише проблеми, пов'язані з кіберпростором, одночасно є проблеми технічні, правові, державні та культурно-економічні .Практично «кібербезпека» виступає як чистильник елементів розриву, підриву, викрадень, шкідництва, тероризму та інших злочинних діянь у сфері кіберпростору. Враховуючи масштаби завданих збитків та збитків у світовому масштабі, кібербезпека в кіберпростір є найважливішою проблемою у всьому світі.

Проблеми кібербезпеки є проблемами у світовому масштабі і одночасно новим напрямом для дослідників, тому невивчені елементи сфери кібербезпеки потребують більш детального розгляду для вдосконалення протидії діяльності хакерів і зловмисників.

Вважається, що кібератаки є засобом боротьби проти держави, які можуть застати і не застати своїх супротивників зненацька, тому що кібератаки не супроводжуються надмірними людськими витратами, але водночас руйнують комунікацію та економіку. Справді, характер кібератак і кібервійни, що відбуваються у світі, практично для держави і для окремих суб'єктів не сильно відрізняються і в діях хакери суворо дотримуються раптовості атаки, руйнування, заподіяння шкоди і збитків потенційній жертві. Розглядається збереження важливої інформації бізнес-процесів, їхньої передачі; Справа в тому, що хакери та інші зацікавлені особи в цю інформацію можуть без особливих труднощів проникнути і отримати доступ до бізнес-систем конкурента, заволодіти важливою інформацією про обсяг та інші цінні компоненти ведення бізнесу, використовувати їх для руйнування бізнесу конкурента, заподіяння його діяльності, здійснювати інші шкідливі дії, кодувати вимкнення записів натисканням клавіші активізації будь-яких системних вірусів, що заражають, вкрасти фінансові засоби, поширити компромати, і т.д.

Проблема глибокого вивчення характеру і сутності елементів і концептуальних основ кібербезпеки, його ефективності обумовлює необхідність вироблення єдиного, комплексного підходу до формування дієвих систем і механізмів кібербезпеки, розробки та здійснення раціональних заходів з функціонування кіберпростору, забезпечення його захисту від можливих сервісів для протидії кібератакам, забезпечення застосування інтелектуальних методів з удосконалення системи кібербезпеки, запобігання потраплянню вірусних елементів, своєчасного виявлення та нейтралізації атак і проникнень, і т.д.

Зазначимо, що узагальнення і розкриття причин, що породжують, і коріння кіберзлочинів, дій хакерів і зловмисників залишається одним із складних завдань у сфері забезпечення кібербезпеки у світі. Необхідно точно і широко скласти класифікацію та елементи небезпеки в кіберпросторі, вивчити їх характеристику та сутність з виділенням основних особливостей тактики та дії хакерів та зловмисників, та розробити адекватні механізми щодо припинення подібних злочинних діянь у кіберпросторі.

Таким чином, результати дослідження зумовлюють важливість усвідомлення та осмислення серйозних проблем, а питання забезпечення кібербезпеки світу вимагає розробку та здійснення більш ефективних механізмів функціонування та забезпечення роботи кіберпростору, підвищення надійності основних механізмів та компонентів глобальної Інтернет-мережі та інших пристроїв, комплексного та системного підходу до визначенні методичних принципів та інструментів формування державної політики щодо кібербезпеки в нинішніх умовах, і т.д.

Список використаних джерел:

1. Views on cybersecurity. Internet Security. Geneva, Switzerland. http://www.internetsociety.org

2. Кибербезопасность: на что глобальные компании потратят $76,9 млрд. IT GROUP DF, 2014. http://www. delo.ua
3. Word Politics, Security and International Law in Cyber Space. Australian Centre for Cyber Security. UNSW, Canberra. http://www.unsw.adfa.edu.au
4. Convention on Cybercrime. Budapest, 23/11/2001. https://www.coe.int

Ключові слова: кібербезпека, глобальні загрози у світі, захист системи кібербезпеки, надійність системи кіберпростору.
Key words: cybersecurity, global threats in the world, protection of cybersecurity system, reliability of cyberspace system.

УФІМЦЕВА ОЛЕНА СЕРГІЇВНА

Національна академія Служби безпеки України,
провідний науковий співробітник, кандидат юридичних наук

ВИКОРИСТАННЯ OSINT В УМОВАХ ЗБРОЙНОЇ АГРЕСІЇ РФ ПРОТИ УКРАЇНИ

Однією зі складових збройної агресії РФ проти України є інформаційна війна, метою якої є послабити моральний дух українців і їхню віру в перемогу, для чого використовуються різноманітні фейки та пропагандистські матеріали. З початком російської агресії щодо України питання отримання інформації з відкритих джерел і розвінчання фейків отримало нове звучання [1].

Протидія інформаційним впливам включає з-поміж іншого формування умінь та навичок працювати з інформацією он-лайн, перевіряти її, а також використання методів критичного аналізу для спростування викладеної інформації.

В умовах глобалізації, цифровізації, стрімкого розвитку інформаційних технологій існує безліч джерел і масивів інформації, достовірність якої потребує обов'язкової перевірки. За кількістю інформації саме мережа Інтернет знаходиться на першому місці у світі, випереджаючи ЗМІ, галузеві видання і одержувані від колег новини, спеціальні огляди, закриті бази даних [1]. Проте найбільшою проблемою є знаходження загальнодоступних змістовних і надійних джерел. У таких умовах надзвичайно важливим інструментом стає OSINT, який передбачає пошук інформації з відкритих, тобто загальнодоступних, джерел, її збір, співставлення та аналіз.

OSINT – термін який розшифровується як open-source intelligence, – це методи пошуку, збору, вибору та аналізу інформації, яка являє оперативний інтерес, з відкритих джерел. Отримані таким чином дані використовують маркетологи, журналісти, фахівці з комп'ютерної та інтернет-безпеки та ін. [1]. Вперше термін OSINT був використаний військовими і розвідувальними службами для позначення збору стратегічно важли-