КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

УДК 004.62

Бржевська Зореслава Михайлівна
Аспірант, асистент кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0002-7029-9525
zoreska.puzniak@gmail.com
Гайдур Галина Іванівна
Д.т.н., доцент, завідуюча кафедри Інформаційної та кібернетичної безпеки
Державний університет телекомунікацій, Київ, Україна
OrcID 0000-0003-0591-3290
gaydurg@gmail.com
Аносов Андрій Олександрович
К.в.н., доцент, доцент кафедри Інформаційної та кібернетичної безпеки
Київський університет імені Бориса Грінченка, Київ, Україна
OrcID 0000-0002-2973-6033
a.anosov@kubg.edu.ua

ВПЛИВ НА ДОСТОВІРНІСТЬ ІНФОРМАЦІЇ ЯК ЗАГРОЗА ДЛЯ ІНФОРМАЦІЙНОГО ПРОСТОРУ

Анотація. У статті розглянуто та проаналізовано визначення достовірності інформації, об’єктів та суб’єктів інформації, які стануть першим кроком для розроблення такої методики, яка буде виявляти вплив на достовірність інформаційних ресурсів. Під терміном достовірність інформації слід розуміти наближеність інформації до першоджерела та адекватне сприйняття об'єкта розгляду суб’єктами системи інформаційного простору. В якості об’єктів інформаційної безпеки виступають особа, суспільство та держава. Всі види інформації, які відповідають потребам суб’єкта, відповідають таким властивостям як конфіденційність, цілісність та доступність інформації. Щодо впливу на інформацію та систему її обробки найбільший інтерес становлять загрози. Загроза в загальному вигляді буде представляти собою будь-який потенційно можливий несприятливий вплив на об’єкти, який (яка) завдає збиток суб’єкту інформаційної діяльності. Останнім часом значно поширився вплив на достовірність інформації, а отже з’явилося таке явище, як фальшива інформація. Для простого прикладу, це – новини, сторінки в соціальних мережах, підроблені під рейтингові сайти, за допомогою яких певні групи людей або окремі особи привертають увагу суспільства до недостовірних подій некоректним шляхом. Подібна інформація, зокрема, недостовірна, розповсюджуються з великою швидкістю, поступово поповнюючись новими подробицями, які є реакцією індивідуумів. Розглянуто шляхи появи недостовірної інформації. також надано рекомендації щодо виявлення недостовірної інформації. Зважаючи на те, що достовірність інформації залежить від самих видань, аналітикам слід звертати увагу на першоджерело, уважно вивчати факти, які лежать в основі інформації, ретельно перевіряти сумнівні відомості. Недостовірною дослідник має вважати інформацію, що надходить до інформаційного простору з «конфіденційних» джерел, навіть якщо матеріал містить посилання на організацію, яку представляє «джерело».

Ключові слова: інформація; достовірність; загроза; інформаційний простір; Інтернет.

1. ВСТУП

На жаль, сьогодні як ніколи є актуальним поняття «інформаційна війна». Всі ми мимоволі стаємо свідками та учасниками різних інформаційних протиборств - чи то передвиборних перегонів, чи то спроб рейдерських атак, чи то просто просування деяких товарів і послуг у конкурентному середовищі. У класичному розумінні інформаційна війна - це одна з форм інформаційного протиборства, комплекс заходів щодо інформаційного впливу на масову свідомість для зміни поведінки людей і нав'язування їм цілей, які не відповідають їхнім інтересам, а також, природно, захист від подібних впливів.

Постановка проблеми. Сучасний інформаційний простір [3] є унікальною можливістю одержувати будь-яку інформацію з визначеного питання за умови наявності відповідного інструментарію, застосування якого дає змогу аналізувати взаємозв'язок можливих подій, які вже відбуваються, з інформаційною активністю певного кола джерел інформації. Виходячи із реалій сьогодення ефективна інформаційна політика держави залежить не тільки від надійності функціонування інформаційно-телекомунікаційних систем, а й у значній мірі від захищеності її інформаційних ресурсів. Тому аналіз визначення достовірності інформації, об'єктів та суб'єктів інформації стануть першим кроком для розроблення такої методики, яка буде виявляти вплив на достовірність інформаційних ресурсів.

Аналіз останніх досліджень та публікацій. За основу дослідження в даній статті проаналізовано роботи: [1], [2], [3].

Метою статті є аналіз термінів і понять достовірності, об'єту та суб'єту інформації, а також розглянуто шляхи шляхи появи в ресурсах Інтернету недостовірних матеріалів.

2. ТЕОРЕТИЧНІ ОСНОВИ ДОСЛІДЖЕННЯ

Системи інформаційної безпеки вирішують питання широкого спектру проблем, в тому числі пов'язані з безпекою комп'ютерних систем. Цей зв'язок розглядає ті чи інші принципи і підходи системи безпеки, які відносяться до предметної області інформаційних систем.

Всі види інформації, які відповідають потребам суб'єкта, відповідають таким властивостям як конфіденційність, цілісність та доступність інформації.

В деяких випадках виділяють інші властивості, такі як достовірність інформації. Під цим терміном розуміється її адекватне сприйняття об'єкта, що її розглядає в межах системи інформаційного сховища. Розглядаючи визначення достовірності можна сміливо сказати, що достовірність розглядається не зовсім в рамках підсистеми інформаційної безпеки, а у визначенні цінності інформації, що зберігається.

У реальному житті навряд чи можлива ситуація, коли можна розраховувати на повну достовірність інформації. Завжди наявний деякий ступінь невизначеності. Від ступеня достовірності інформації до реального стану інформаційного об'єкта чи процесу залежить правильність прийняття рішень людиною чи системою. Одні з базових властивостей інформації наступні: якість інформації, достатність (повнота) інформації, актуальність інформації, адекватність інформації, стійкість інформації, своєчасність та точність інформації.

Достовірність інформації (probability of information) визначається її властивістю відображати реально існуючі об'єкти з потрібною точністю. Вимірюється достовірність інформації довірчою ймовірністю потрібної точності, тобто ймовірністю того, що

відображуване інформацією значення параметра відрізняється від істинного значення цього параметра в межах потрібної точності. (3)

Дії щодо поширення в інформаційному просторі викривленої, недостовірної та упередженої чи фальшивої інформації або негативні інформаційні впливи на суспільну свідомість в ІП прийнято відносити до порушення цілісності інформації. Однак, слід сказати, що фактично цілісність інформації не змінюється. Завдяки діям щодо викривлення інформації змінюється відношення до достовірності інформації, що циркулює у державних інформаційних ресурсах. Тобто відбувається вплив на достовірність інформації.

Під терміном достовірність інформації слід розуміти наближеність інформації до першоджерела та адекватне сприйняття об'єкта розгляду суб'єктами системи інформаційного простору. Розглядаючи визначення достовірності можна сміливо заявити, що достовірність потрібно розглядати у рамках підсистеми інформаційної безпеки.

Щодо впливу на інформацію та систему її обробки найбільший інтерес становлять загрози. Під загрозою безпеки інформаційних ресурсів будемо розуміти дії, які можуть призвести до спотворення, несанкціонованого використання або, навіть, до руйнування інформаційних ресурсів. Таким чином, загроза в загальному вигляді буде представляти собою будь-який потенційно можливий несприятливий вплив (дію або бездіяльність) на об’єкти, який (яка) завдає збиток суб’єкту інформаційної діяльності.

У кожній державі об’єктами інформаційної безпеки виступають передусім люди (усі громадяни) і держава, як цілісність, а основним каналом інформаційного впливу завжди є свідомість, психіка людини, свідомість (переконання, утвердження і т. ін.) великого етносу. Коли ведуть мову про захист національного інформаційного простору, як такого, то мають на увазі насамперед державний інформаційний суверенітет, тобто належне володіння й розповсюдження всією спільнотою у державі відповідних національних інформаційних ресурсів. Інформаційний суверенітет – це виняткове право держави на формування й використання усіх інформаційних засобів, створених на засадах і за державний кошт [10].

Таким чином, в якості об’єктів інформаційної безпеки виступають:

• особа – її права та свободи в інформаційній сфері, техніка та свідомість;

• суспільство – його духовні цінності, засади солідарної діяльності;

• держава – її конституційний лад, ефективне функціонування, суверенітет [11].

Інформаційна безпека особистості – це стан захищеності психіки та здоров’я людини від деструктивного інформаційного впливу, який призводить до неадекватного сприйняття нею дійсності та (або) погіршення її фізичного стану. Інформаційна безпека суспільства – можливість безперешкодної реалізації суспільством та окремими його членами своїх конституційних прав, пов’язаних з можливістю вільного одержання, створення й поширення інформації, а також ступінь їхнього захисту від деструктивного інформаційного впливу. Інформаційна безпека держави – це стан її захищеності, при якій спеціальні інформаційні операції, акти зовнішньої інформаційної агресії, інформаційний тероризм, незаконне зняття інформації за допомогою спеціальних технічних засобів, комп’ютерні злочини та інший деструктивний інформаційний вплив не завдає суттєвої шкоди національним інтересам [12].

Тому слід ввести термін для класифікації атак на державні інформаційні ресурси держави – вплив на достовірність державних інформаційних ресурсів. Дії щодо поширення у інформаційному просторі викривленої, недостовірної та упередженої інформації або негативні інформаційні впливи на суспільну свідомість через засоби

масової інформації, а також мережу Інтернет відносяться до порушення цілісності інформації [6], однак, фактично цілісність інформації не змінюється, змінюється відношення до інформації. Тобто відбувається вплив на достовірність офіційної інформації.

Останнім часом значно поширився цей вплив, а отже з'явилося таке явище, як фальшива інформація. Для простого прикладу, це – новини, сторінки в соціальних мережах, підроблені під рейтингові сайти, за допомогою яких певні групи людей або окремі особи привертають увагу суспільства до недостовірних подій некоректним шляхом [13]. Подібна інформація, зокрема, недостовірна, розповсюджуються з великою швидкістю, поступово поповнюючись новими подробицями, які є реакцією індивідуумів (резонансна інформація може довго висвітлюватись і навіть сприяти створенню нових груп).

Можливості інформаційного простору дають змогу створювати псевдореальних особ, наділяючи їх вигаданою історією, яких індивідууми вважатимуть цілком реальними.

Вкидаючи фальшиву інформацію в інформаційний простір, її автори враховують таку особливість мережі Інтернет, як анонімність, можливість множинної дії. Фальшиві матеріали можуть одночасно просуватися через велику кількість сайтів, форумів, блогів, гостьових книг. При цьому у користувачів, які зустрічають одну й ту саму інформацію в різних місцях, складається враження, що вона є достовірною.

Розглянемо інші шляхи появи в ресурсах Інтернету недостовірних матеріалів. Одними з перших на сьогодні, як правило, нову інформацію подають інформаційні агенції. Вона є короткою за змістом, без оцінок і прогнозів. Але ЗМІ, готуючи на її базі свої матеріали, змінюють акценти, подають новини в різному контексті. Тому одне й те саме повідомлення з різних джерел інформації сприйматиметься по-різному. Це можна пояснити тим, що:

– ЗМІ працюють з різною аудиторією, тому форма подання матеріалів відрізняється (теоретична версія);

– напрями інтерпретації матеріалу визначають власники та спонсори видань (прагматична версія).

Зважаючи на те, що достовірність інформації залежить від самих видань, аналітикам слід звертати увагу на першоджерело, уважно вивчати факти, які лежать в основі інформації, ретельно перевіряти сумнівні відомості.

Недостовірною (через неможливість її перевірити) дослідник має вважати інформацію, що надходить до інформаційного простору з «конфіденційних» джерел, навіть якщо матеріал містить посилання на організацію, яку представляє «джерело».

Якщо прізвище автора публікації є невідомим, необхідно ознайомитися з іншими його роботами, спробувати проаналізувати їх на предмет використання скандальних фактів, лобіювання інтересів конкретних організацій або осіб. Аналіз значної кількості статей за тривалий час, блогу автора, сторінок у соціальних мережах, відгуків читачів на його роботи нададуть можливість зробити висновок стосовно статусу автора в електронному інформаційному середовищі, його компетентності. Значно підвищує ступінь достовірності матеріалів той факт, що автор є представником певної офіційної установи.

3. РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Дослідникам слід звернути увагу на те, що матеріал може мати недостовірний характер, якщо автор:

1) посилається у публікації на нерейтингові джерела за наявності рейтингових з порушеної теми;

2) використав сумнівні факти або документи, отримані неофіційним шляхом;

3) зосередив увагу лише на тих повідомленнях, які підтверджують його припущення;

4) приховує від користувачів частину інформації;

5) перебільшує або зменшує значення частини інформації.

Наявність однієї з вказаних тенденцій може бути результатом того, що автор або сам не володіє всією інформацією, або виконує певне замовлення.

Якість інформації сьогодні страждає і через те, що у процес її виробництва та представлення в інформаційному просторі включилася значна частина суспільства. З одного боку, це сприяє розширенню можливостей для вивільнення їхнього творчого потенціалу, з іншого – до процесу інфотворення приєднується дедалі більше некваліфікованих учасників, а також людей, що часто переслідують шкідливі для суспільства цілі [14].

Обов’язково слід враховувати, що упередженість підходу автора до проблеми може маскуватись під нібито об’єктивний розгляд різних точок зору. При цьому на захист однієї він наводитиме виключно слабкі аргументи, іншої – тільки вагомі.

Відомі дослідники Інтернету К. Шерман та Г. Прайс радять користувачам під час оцінки достовірності інформації використовувати такі ж самі фільтри, як і під час використання друкованої продукції: той факт, що інформація є надрукованою, не є доказом її достовірності і навпаки.

4. ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

З позицій впливу на інформацію та систему її обробки найбільший інтерес представляють загрози за метою реалізації. На їх підґрунті формується, як правило, формалізована модель оцінювання ступеня порушення системи захисту інформації у досліджуваній системі. Згідно з нормативними документами ТЗІ України (НД ТЗІ 1.1-002-99 та НД ТЗІ 2.5-004-99) такі загрози полягають у порушенні конфіденційності, цілісності та доступності.

Такий параметр як достовірність інформації цілком визначається на методичному рівні розроблення інформаційних систем. Параметри достовірності обумовлюються більшою мірою також на методологічному рівні, проте на їх величину суттєво впливає і характер функціонування системи, передусім її надійність. При цьому параметри достовірності та своєчасності жорстко пов’язані з параметрами точності та актуальності.

Сучасний інформаційний простір, зокрема Інтернет, крім виконання функцій обміну думками та отримання інформації його користувачами в період інформаційного протистояння, стає об’єктом і засобом інформаційного керування. Серед користувачів мережі з’являються групи людей або окремі особи, які навмисно поширюють помилкову або спотворену інформацію.

Тому розробка методики виявлення впливу на достовірність інформації буде напрямком подальших розвідок та досліджень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

[1] В. Богуш і О. Юдін, Інформаційна безпека держави. 1-е изд, Київ: МК-Прес, 2005.
[2] О. Юдін і С. Бучик, «Державні інформаційні ресурси. Нормативно-правовий аналіз, зміст та визначення», *Безпека інформації*, №1 (20), сс. 72–75, 2014.
[3] Р. Грищук, *Основи кібернетичної безпеки*. Житомир: ЖНАЕУ, 2016.
[4] О. Юдін і С. Бучик, «Аналіз загроз державним інформаційним ресурсам», *Проблеми інформатизації та управління*, №4 (44), сс. 93–99, 2013.
[5] В. Бурячок, В. Толубко, В. Хорошко і С. Толюпа, *Інформаційна та кібербезпека: соціотехнічний аспект*. Київ : ДУТ, 2015.
[6] О. Юдін і С. Бучик, «Загрози державним інформаційним ресурсам: терміни та визначення», *Захист інформації*, №2 (16), сс. 121–125, 2014.
[7] Д. Дубов, *Кібербезпека: світові тенденції та виклики для України*. Київ: НІСД, 30 с., 2011.
[8] Є. Кирильчук, «Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції», *Наукові праці МАУП*, №1, сс. 89–95, 2013.
[9] О. Сагайдак, «Інформаційна безпека України в умовах глобалізаційних викликів», *Вісник Луганського національного університету ім. Т. Шевченка. Соціологічні науки*, Т. 2 (2), №12, сс. 110–125, 2010.
[10] В. Петрик, «Сутність інформаційної безпеки держави, суспільства та особи», *Юридичний журнал*, №5, сс. 122–134, 2009.
[11] С. Горова, *Інтернет-ЗМІ як об'єкт бібліотечної інформаційної діяльності*. Київ: НАН України, 2013.

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (2), 2018
ISSN 2663 - 4023

Zoreslava M. Brzhevska
Postgraduate student, assistant professor of information and cybersecurity department
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0002-7029-9525
zoreska.puzniak@gmail.com
Galyna I. Gaidur
Ph.D., Associate Professor, Head of the Department of Information information and cybersecurity
State University of Telecommunications, Kyiv, Ukraine
OrcID 0000-0003-0591-3290
gaydurg@gmail.com
Andriy O. Anosov
Candidate of sciences, associate professor, assistant professor of information and cybernetic security department
Kyiv Boris Grinchenko University, Kyiv, Ukraine
OrcID 0000-0002-2973-6033
a.anosov@kubg.edu.ua

INFLUENCE ON INFORMATION RELIABILITY AS A THREAT FOR THE INFORMATION SPACE

Abstract. The article considers and analyzes the determination of the reliability of information, objects and subjects of information, which will become the first step for the development of such a method that will affect the reliability of information resources. The term reliability of information should be understood as the proximity of information to the original source and adequate perception of the object of consideration by the subjects of the information space. As objects of information security act a person, society and the state. All types of information that meets the needs of the subject meet such properties as the confidentiality, integrity and availability of information. As to the impact on information and its processing, the greatest interest is threats. The threat in its general form will be any potentially possible adverse effect on objects that (which) causes damage to the subject of information activity. Recently, the influence on the reliability of information has become much widespread, and therefore there has been a phenomenon like false information. For a simple example, this is news, social networking sites, fake rating sites, by which certain groups of people or individuals draw the attention of society to incorrect events in the wrong way. Such information, in particular, is unreliable, is spreading at a high rate, gradually being replenished with new details that are the reaction of individuals. The ways of appearance of inadequate information are considered. Also, recommendations are provided to identify false information. Given the fact that the reliability of the information depends on the publications itself, analysts should pay attention to the source, carefully study the facts underlying the information, carefully check the questionable information. An unreliable researcher should consider information coming to the information space from "confidential" sources, even if the material contains a link to the organization represented by the "source".

Keywords: information; certainty; threat; information space; Internet.

REFERENCES

[1] V. Bogush and O. Yudin, *Informatsiyna bezpeka derzhavy [Information security of the state]*. 1st ed. Kyiv: MK-Press.
[2] O. Yudin and S. Buchik, “Derzhavni informatsiyni resursy. Normatyvno-pravovyy analiz, zmist ta vyznachennya [State information resources: Regulatory analysis, content and definition],” *Information security*, no. 1 (20), pp. 72–75, 2014.

[3] R. Grishchuk, *The basics of cybernetic security [Fundamentals of cybernetic security]*. Zhytomyr: ZNAEU, 2016.
[4] O. Yudin and S. Buchik, "Analiz zahroz derzhavnym informatsiynym resursam [Analysis of threats to state information resources]," *Problems of informatization and management*, no. 4 (44), pp. 93–99, 2013.
[5] V. Buryachok, V. Tolybko, V. Khoroshko, and S. Tolyuta, *"Informatsiyna ta kiberbezpeka: sotsiotekhnichnyy aspekt [Information and cybersecurity: sociotechnical aspect]*. Kyiv: SUT, 2015.
[6] O. Yudin and S. Buchik, "Zahrozy derzhavnym informatsiynym resursam: terminy ta vyznachennya [Threats to state information resources: terms and definitions]," *Information protection*, no. 2 (16), pp. 121–125, 2014.
[7] D. Dubov, *Kiberbezpeka: svitovi tendentsiyi ta vyklyky dlya Ukrayiny [Cybersecurity: world trends and challenges for Ukraine]*. Kyiv: NISD, 30 p., 2011.
[8] E. Kyrylchuk, "Problemy natsional'noyi informatsiynoyi bezpeky Ukrayiny v konteksti suchasnykh natsional'nykh derzhavotvorchykh protsesiv ta svitovoyi intehratsiyi [Problems of national information security of Ukraine in the context of modern national state-building processes and world integration]," *Scientific works of MAUP*, vol. 1, pp. 89–95, 2013.
[9] O. Sagaydak, "Informatsiyna bezpeka Ukrayiny v umovakh hlobalizatsiynykh vyklykiv [Information security of Ukraine in the context of globalization challenges]," *Visnyk of Lugansk National University named after. T. Shevchenko. Sociological sciences*, vol. 2 (2), no. 12, pp. 110–125, 2010.
[10] V. Petryk, "Sutnist' informatsiynoyi bezpeky derzhavy, suspil'stva ta osoby [Essence of information security of the state, society and person]," *Law journal*, no. 5, pp. 122–134, 2009.
[11] S. Gorova, *Internet-ZMI yak ob"yekt bibliotechnoyi informatsiynoyi diyal'nosti [Internet media as an object of library information activity]*. Kyiv: NAS of Ukraine, 2013.