DOI: https://doi.org/10.32836/2521-6643-2020.2-60.6
УДК 621.396.96

Ю. С. Тарасенко, кандидат фізико-математичних наук наук, доцент, доцент кафедри кібербезпеки та інформаційних технологій Університету митної справи та фінансів
В. Г. Соляннiков, студент магістратури Університету митної справи та фінансів
О. Е. Калюжний студент магістратури Університету телекомунікацій

КОНЦЕПТУАЛЬНО-ГНОСЕОЛОГІЧНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ (ЗАХИЩЕНОСТІ) З ПОЗИЦІЙ СОЦІАЛЬНОЇ ІНЖЕНЕРІЇ

Розглянуто можливе підвищення надійності інформаційної захищеності в конкретній галузі людської діяльності з позицій обов'язкового виконання штатних регламентних робіт при жорсткому контролі дотримання кодексу ділового поведінки в сукупності з впровадженням і реалізацією систем забезпечення анонімності задіяного персоналу, наприклад, співробітників критично важливих об'єктів або ключових систем інформаційної інфраструктури. Проведено аналіз публікацій по системам інформаційної інфраструктури.

Ключові слова: *соціальна інженерія, інформаційна безпека, кібератака, кібербезпека, інформаційна захищеність, ключові системи інформаційної інфраструктури, критично важливі об'єкти.*

Рассмотрено возможное повышение надежности информационной защищенности в конкретной области человеческой деятельности с позиций обязательного выполнения штатных регламентных работ при жестком контроле соблюдения кодекса делового поведения в совокупности с внедрением и реализацией систем обеспечения анонимности задействованного персонала, например, сотрудников критически важных объектов или ключевых систем информационной инфраструктуры. Проведен анализ публикаций по системам информационной инфраструктуры.

Ключевые слова: *социальная инженерия, информационная безопасность, кибератака, кибербезопасность, информационная защищенность, ключевые системы информационная инфраструктура, критически важные объекты.*

A possible increase in the reliability of information security in a specific area of human activity is considered from the standpoint of the mandatory performance of regular routine maintenance with strict control of compliance with the code of business conduct in conjunction with the implementation and implementation of systems to ensure the anonymity of the personnel involved, for example, employees of critical facilities or key information infrastructure systems.

Analysis of publications on conceptual, organizational, legal, engineering, software and mathematical and their complex aspects of information security of key information infrastructure systems shows that there is still a weak point - the so-called "human factor". This determines the urgency of the problem of generalization of the basic principles of information security by implementing an additional system of information security (security) from the standpoint of the use of social engineering.

The very concept of "social engineering", symbolically formed in the form of a generalized form of implementation of the engineering approach in the social sphere, should correspond to the specifics of engineering. Therefore, in scientific publications, directly, social engineering, as a special kind of activity, is focused on purposeful change and regulation of various organizational structures (social institutions, formal organizations, etc.).

This determines the urgency of the problem of generalization of the basic principles of information security, clarification of the possibility of implementing a system of anonymity of personnel in protection against cyber-attacks through social engineering and, from the standpoint of modern cyber safety, development of recommendations for improving the reliability of information protection. Discerned and revealed in reality the advancement of the hopes of information abduction in a specific hallucination of human activity.

Keywords: *social engineering, information security, cyber-attack, cyber safety, information security, key information infrastructure systems, critical objects.*

Вступ. В класичних загальноприйнятих напрямках будь-якій області пізнання зі сфер людського буття, як правило, використовують поняття, формування яких обґрунтовано закінчується за допомогою їх відображення у вигляді вітчизняної (гостованої) термінології, що корелюється з міжнародними стандартами, які розробляються відповідно до правил, встановлених в Директивах ISO / IEC [1,2]. Цілком очевидно, що сучасні наукові та супутні їм освітні напрямки оперують новою термінологією, успішним опануванням яких (крім гносеологічних і концептуальних основ сприйняття), є реалізація чіткості і однозначності понятійного трактування нової використовуваної термінології. В даному випадку озвучене в назві – це авторське пізнавальне трактування можливої реалізації інформаційної безпеки (ІБ) або захищеності з позицій соціальної інженерії в конкретній галузі людської діяльності. При цьому тут, за аналогією з [1,2], запропоновано "концептуально-гносеологічні аспекти", які потрібно сприймати у вигляді реалізації простежування діалектичного розвитку моделі раціональної діяльності (парадигми) з точки зору вироблення оцінки відповідності достовірності досліджуваних явищ підтверджуючи прямими або непрямими звіреннями даних питань (процесів) в конкретній сфері людського буття за допомогою реалізації існуючих (або нових) методів і засобів соціальної інженерії.

Постановка задачі. Саме поняття "соціальна інженерія", символічно сформоване у вигляді узагальненої форми реалізації інженерного підходу в соціальній сфері, має відповідати специфіці інженерної діяльності. Тому, в наукових публікаціях, безпосередньо, соціальна інженерія (СІ), як особливий рід діяльності, орієнтована на цілеспрямовану зміну і регулювання різних організаційних структур (соціальних інститутів, формальних організацій та ін.). Однак, історично склалось так, що "соціальною інженерією" стали називати і хакерство з використанням людського фактору [3]. З метою уточнення і конкретизації використання соціальної інженерії, нижче запропоновано розглянути можливість вирішення одного з головних завдань управління в соціальній інженерії з позицій оптимальності видачі прийнятих рішень і вибору альтернатив в безпосередній політиці розвитку інформаційної безпеки (захищеності) підвідомчої організації.

Мета. Метою публікації є узагальнення основних принципів інформаційної захищеності, вияснення можливості реалізації системи забезпечення анонімності роботи персоналу при захисті від кібератак за допомогою вико-

ристання соціальної інженерії та, з позиції сучасної кібербезпеки, розробка рекомендації удосконалення підвищення надійності інформаційного захисту задіяного персоналу.

Виклад основного матеріалу. Зауважимо, що використання поняття "інформаційна безпека", а нижче і застосування, згідно ISO / IEK 27032 2012 [4], терміну "кібербезпека - (КБ)", об'єднаних спільним однокореневим базисом "безпека", вимагає введення досить коректного терміну типу "інформаційна захищеність" (ІЗ), більш асоційованого з практичною реальністю.

Дійсно, згідно з [5, стаття 1, п.5], "кібербезпека – захищеність життєво-важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі». Саме ж поняття кіберпростору, насамперед, асоціюється зі сферою діяльності в інформаційному просторі людського буття, спрямовану на реалізацію захищеності кібероб'єктів від всіх відомих і вивчених кібернебезпечних джерел. При цьому тут (див. [5, стаття 1 п.11]), кіберпростір – це «середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних». У такому випадку прийнято розрізняти об'єкти (див. [5, стаття 4 та 6]) на об'єкти кібербезпеки (стаття 4, п.1), у тому числі об'єднані з об'єктами критичної інфраструктури (стаття 6), та на об'єкти кіберзахисту (стаття 4, п.2). Таким чином, термін "кібербезпека об'єкта", що відповідає рекомендаціям [6], відображає внутрішні властивості об'єкта не бути небезпечним для навколишнього середовища при його функціонуванні у всіх штатних режимах роботи. Причому, можливий збиток кібероб'єкту розцінюється як спеціально реалізована кібератака у вигляді навмисно організованої сукупності дій за допомогою засобів електронних комунікацій (включаючи інформаційно-комунікаційні технології, програмні, програмно-апаратні засоби, інші технічні та технологічні засоби і обладнання) [5, стаття 1 п.4]), що спрямовані на нанесення економічної, технічної або інформа-

ційної шкоди. Самі ж кібератаки по відношенню до кібероб'єкту можуть бути внутрішніми і зовнішніми, а по відношенню до інформації, як відомо, можливі лише зовнішні впливи. Звідки виходить, що захищеність об'єкта - це його захист від зовнішніх джерел небезпеки, в той час, як безпека об'єкта – це внутрішня властивість об'єкта не бути джерелом небезпеки для навколишнього середовища. Оскільки ж саме визначення інформації до теперішнього часу досить нечітке, через це і однозначно сформувати поняття безпеки інформації на підставі її тлумачення як внутрішньої структури, так і внутрішніх властивостей, не представляється можливим. Тому, замість терміну "безпека інформації", пов'язаного тільки з намірами її володаря, доцільно використовувати поняття "інформаційна захищеність (ІЗ)", що відображає захист конфіденційності, цілісності та доступності інформації в конкретній галузі людської діяльності,. що використовуємо нижче і відповідає викладеному в [6,7].

Очевидно, що, безпосередній стан об'єкта інформаційної захищеності залежить від багатьох чинників і, насамперед, від сфери його застосування, оскільки в сучасному світі не слабшає тенденція деструктивних впливів на потенційно значущі інформаційні ресурси будь-яких організацій, як на державному, з точки зору, так званого, "промислового шпигунства", так і на рівні терористичних і кримінальних структур. Перш за все, це пов'язано з особливою вразливістю інфраструктури і високою професійною відповідальністю, наприклад, співробітників критично важливих об'єктів (КВО), від роботи яких залежить не тільки штатне функціонування цих об'єктів, а й ступінь захисту від будь-яких загроз і їх передумов, здатних викликати техногенну, екологічну або фінансову катастрофу [8-12]. При цьому, згідно [5, стаття 1, п.16], критично важливі об'єкти інфраструктури (далі - об'єкти критичної інфраструктури) – це "підприємства, установи та організації незалежно від форми власності, діяльність яких безпосередньо пов'язана з технологічними процесами та/або наданням послуг, що мають велике значення для економіки та промисловості, функціонування суспільства та безпеки населення, виведення з ладу або порушення функціонування яких може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей».

Обсяг кількості публікацій з концептуальним, організаційним, юриди-

чно-правових, інженерно-технічним, програмно-математичним і їх комплексних аспектів забезпечення інформаційної захищеності як КВО, так і ключових систем інформаційної інфраструктури (КСІІ) не тільки підтверджує актуальність порушеної теми, а й приховано припускає наявність апріорного професіоналізму персоналу і серйозного рівня їх безпосередньої захищеності. Зараз, фактично, за рахунок синтезу різних верств захисту як по інформаційним ресурсам, так і по задіяному персоналу, незважаючи на реалізацію різних захисних технологій, наприклад [13], від базового рівня захисту типу: оператор-користувач → VPN / TOR / SSH- тунель → ціль і до рівня (назвемо його гіпотетично квазі-ідеальним рівнем захисту), типу: оператор-користувач → Double VPN (в різних дата центрах, але поруч один з одним) → Віддалене робоче місце + Віртуальна машина → VPN, все одно, як і раніше, залишається слабке місце, - так званий "людський фактор". Саме від якості (морально-професійного рівня) задіяного кадрового складу відповідно до штатного кодексу ділової поведінки, що забезпечує специфічні заходи, в тому числі, по прогнозуванню, виявлення, стримування, запобіганню, відбиття інформаційних загроз і ліквідації наслідків їх прояву, а, частіше і від анонімності їх роботи, залежить безпечне функціонування КВО і КСІІ.

Як відомо [14-17], в даний час розробляються системи комп'ютерного зору, що, безперечно, мають широкий позитивний спектр застосування (у тому числі в галузі забезпечення безпеки), які досягли рівня вирішення завдань не тільки виявлення, а й розпізнавання фігур людей (і навіть їх відстеження) в пішохідних потоках. Пам'ятаючи, що "кожна медаль має і зворотний бік", завдання забезпечення анонімності при відбитті атак несанкціонованого стеження за об'єктом спостереження (а їм, в тому числі, може бути і вище згаданий професіонал з КСІІ) також має право на існування і обговорення можливих контрзаходів (тобто можливих захисних способів вирішення), в тому числі що і реалізують їхню особисту безпеку шляхом створення режиму анонімності власної роботи. Для нашого випадку, пропонується використовувати активні і пасивні радіолокаційні методи захисту [18], спрямовані на нівелювання, частіше і на повну нейтралізацію так званих в радіолокації "блискучих точок" об'єктів спостереження. Дана пропозиція ґрунтується на тому факті, що існуючі методи розпізнавання образів, викладених, наприклад, в [15], базуються на алгоритмі формування HOG дескрипторів, завдяки чому "об'єкт на області зображення може бути описаний напрямком

країв або розподілом градієнтів яскравості. Реалізація таких дескрипторів проводиться поділом зображення на зв'язкові області (осередку), і підрахунком напрямків градієнтів для кожного осередку або напрямків країв пікселів всередині. Комбінація гістограм називається дескриптором. Щоб збільшити точність проводять "нормалізацію за контрастом для локальних гістограм". Фактично алгоритм отримання кінцевого результату "нормалізації по контрасту локальних гістограм" аналогічний радіолокаційному розпізнаванню об'єктів, сформованому, при високій роздільній здатності, у вигляді якогось образу з конфігурацій блискучих точок, в даному випадку аналогом градієнтів яскравості (країв пікселів).

Висновки та перспективи подальших досліджень у даному напрямі. Виявлено, що можливе реальне підвищення надійності інформаційної захищеності в конкретній галузі людської діяльності з позицій обов'язкового виконання штатних регламентних робіт при жорсткому контролі щодо дотримання кодексу ділової поведінки та в усій сукупності з впроваджування і реалізації систем забезпечення анонімності задіяного персоналу.

В подальшому пропонується докладніше розглянути напрямки з реалізації системи захисту від соціотехнічних атак з використовуванням активних і пасивних методів нелінійної радіолокації для виявлення та розпізнання технічних засобів виведення з ладу штатного функціонування об'єктів критичної інфраструктури та систем протидії знімання і передачі службової інформації хакерам з метою покращення безпеки об'єктів інфраструктури, у тому числі КВО та КСП.

Список використаних джерел:

1. ИСО/МЭК 17007:2009 «Оценка соответствия. Методические указания по разработке нормативных документов, предназначенных для применения при оценке соответствия» (ISO/IEC 17007:2009 «Conformity assessment — Guidance for drafting normative documents suitable for conformity assessment»).

2. ИСО/МЭК 17000:2004 Оценка соответствия. Словарь и общие принципы (ISO/IEC 17000:2004, Conformity assessment — Vocabulary and general principles).

3. Социальная инженерия и социальные хакеры / М. В. Кузнецов, И. В. Симдянов. СПб.: БХВ-Петербург, 2007. 368 с.

4. ISO/IEK 27032 2012. Information technology — Security techniques

— Guidelines for cybersecurity. Код КС (ОКС, МКС) 35.040. «Информационные технологии. Методы обеспечения безопасности. Руководящие указания по обеспечению кибербезопасности». 58с.

5. Закон України Про основні засади забезпечення кібербезпеки України від 05.10.2017 N 2163-VIII. (Відомості Верховної Ради (ВВР), 2017, № 45, ст.403). {Із змінами, внесеними згідно із Законами № 2469-VIII від 21.06.2018, ВВР, 2018, № 31, ст.241, № 720-IX від 17.06.2020, ВВР, 2020, № 47, ст.408, № 912-IX від 17.09.2020}.

6. Ежемесячное приложение к журналу «Стандарты и качество». Экологические аспекты проблем надежности и безопасность технических систем. «Основные понятия безопасности». Алпеев А.С. М., 1994, вып. 7.

7. История и основы информационной триады безопасности: целостность, доступность, конфиденциальность. 1 Марта, 2018. URL: https://falcongaze.ru/pressroom/publications/articles/security-triad.html.

8. Иванченко О.В. Концепция управления готовностью критических инфраструктур на основе применения информационных технологий / О.В.Иванченко, К.В.Смоктий, О.Д.Смоктий, В.С.Харченко// Системи та технології. 2016. Вып.1 (55). С.5-23.

9. Породин Д. Защита ключевых систем информационной инфраструктуры Журнал "Information Security / Информационная безопасность" №3, 2012. АМТ-ГРУП, ЗАО. Москва, E-mail: info@amt.ru www.amt.ru.

10. Безопасность ключевых систем информационной инфраструктуры: точка доверия. Лаборатория Касперского - Октябрь 16, 2012.

11. Кубанков А.Н., Кубанков Ю.А. Свойства процесса защиты информации, определяющие его качество // Стандарты и качество. 2016, №9. С. 104-107.

12. Кубанков А.Н., Кубанков Ю.А., Симонов П.И. Подходы к комплексному измерению качества защиты информации. // Технологии информационного общества. Сб. трудов XI Международной отраслевой научно-технической конференции «Технологии информационного общества». М.: ООО «ИД Медиа Паблишер», 2017. С.280-282.

13. Мысли об идеальной анонимности / Блог компании Whoer.net, URL: https://habr.com/company/whoer/blog/2016.

14. Поташников А.М. Методы обнаружения и отслеживания объектов в системах видеонаблюдения на основе систем компьютерного зрения // Технологии информационного общества. Сб. трудов XI Международной отраслевой научно-технической конференции «Технологии информационного общества». М.: ООО «ИД Медиа Паблишер», 2017 с.149-151.

15. Яшина М.В., Толмачев А.А. Методы распознавания образов для оценки характеристик пешеходных потоков // Технологии информационного общества. Сборник трудов XI Международной отраслевой научно-технической конференции «Технологии информационного общества». М.: ООО «ИД Медиа Паблишер», 2017 с.466-468.

16. Попова Л. П., Датьев И.О. Обзор существующих методов распознавания образов. М.: Сборник научных трудов, 2007. 11 с.

17. Зенин А. В. Анализ методов распознавания образов // Молодой ученый. 2017. №16. С. 125-130. URL: https://moluch.ru/archive/150/42393/.

18. Тарасенко Ю.С. Фізичні основи радіолокації. Дніпро: Пороги, 2011. 487 с.

References:

1. ISO / IEC 17007: 2009 «Conformity assessment - Guidance for drafting normative documents suitable for conformity assessment».

2. ISO / IEC 17000: 2004, Conformity assessment - Vocabulary and general principles.

3. Sotsial′na inzheneriya ta sotsial′ni khakery / M. V. Kuznyetsov, I. V. Simdyanov. - SPb .: BKHV-Peterburh, 2007. 368 p.

4. ISO/IEC 27032:2012. Information technology — Security techniques — Guidelines for cybersecurity.

5. Zakon Ukrayiny Pro osnovni zasady zabezpechennya kiberbezpeki Ukrayiny ot 05.10.2017 N 2163-VIII. (Vidomosti Verkhovnoyi Rady (VVR) 2017, № 45, st.403). {Iz zminami, vnesenymy sohlasno iz Zakonamy № 2469-VIII vid 21.06.2018, VVR, 2018, № 31, st.241, № 720-IX vid 17.06.2020, VVR, 2020 roku, № 47, st.408, № 912 -IX vid 17.09.2020}.

6. Shchomisyachne dodatok do zhurnalu «Standarty ta yakist′». Ekolohichni aspekty problem nadiynosti i bezpeku tekhnichnykh system. «Osnovni ponyattya bezpeky». Alpyeyev A.S. M., 1994, vyp. 7.

7. Istoriya ta osnovy informatsiynoyi triady bezpeky: tsilisnist′, dostupnist′, konfidentsiynist′. 1 Bereznya, 2018. URL: https://falcongaze.ru/pressroom/publications/articles/security-triad.html.

8. Ivanchenko O.V. Kontseptsiya upravlinnya hotovnistyu krytychnykh infrastruktur na osnovi zastosuvannya informatsiynykh tekhnolohiy / O.V.Ivanchenko, K.V.Smoktiy, O.D.Smoktiy, V.S.Kharchenko // Systemy ta tekhnolohiyi. 2016. Vyp.1 (55). S.5-23.

9. Porodin D. Zakhyst klyuchovykh system informatsiynoyi infrastruktury Zhurnal "Information Security / Informatsiyna bezpeka" №3, 2012.

10. Bezpeka klyuchovykh system informatsiynoyi infrastruktury: tochka doviry. Laboratoriya Kaspers′koho 10.16, 2012.

11. Kubantsi A.N., Kubantsi Yu.A. Vlastyvosti protsesu zakhystu informatsiyi, shcho vyznachayut′ yoho yakist′ // Standarty i yakist′. 2016, №9. P. 104-107.

12. Kubantsi A.N., Kubantsi Yu.A., Symonov P.I. Pidkhody do kompleksnoho vymiryuvannya yakosti zakhystu informatsiyi. // Tekhnolohiyi informatsiynoho suspil′stva. Zb. prats′ XI Mizhnarodnoyi haluzevoyi naukovo-tekhnichnoyi konferentsiyi «Tekhnolohiyi informatsiynoho suspil′stva». M .: TOV «VD Media Pablysher», 2017. pp.280-282.

13. Dumky pro ideal′nu anonimnosti / Pres-tsentr kompaniyi Whoer.net, URL: https://habr.com/company/whoer/blog/2016.

14. Potashnyk A.M. Metody vyyavlennya ta vidstezhennya ob'yektiv v systemakh videosposterezhennya na osnovi system komp'yuternoho zoru // Tekhnolohiyi informatsiynoho suspil′stva. Zb. prats′ XI Mizhnarodnoyi haluzevoyi naukovo-tekhnichnoyi konferentsiyi «Tekhnolohiyi informatsiynoho suspil′stva». M.: TOV «VD Media Pablysher» 2017 pp.149-151.

15. Yashyna M.V., Tolmachov A.A. Metody rozpiznavannya obraziv dlya otsinky kharakterystyk pishokhidnykh potokiv // Tekhnolohiyi informatsiynoho suspil′stva. Zbirnyk prats′ XI Mizhnarodnoyi haluzevoyi naukovo-tekhnichnoyi konferentsiyi «Tekhnolohiyi informatsiynoho suspil′stva». M .: TOV «VD Media Pablysher» 2017. pp.466-468.

16. Popova L. P., Dat′ev I.O. Ohlyad isnuyuchykh metodiv rozpiznavannya obraziv. M .: Zbirnyk naukovykh prats′, 2007. 11 p.

17. Zenin A. V. Analiz metodiv rozpiznavannya obraziv // Molodyy vchenyy. 2017. №16. P. 125-130. URL: https://moluch.ru/archive/150/42393/.

18. Tarasenko Yu.S. Fizychni osnovy radiolokatsiyi. Dnipro: Porohy, 2011. 487 p.