УДК 004.056:004.7 **В.Г.Кононович, І.В.Кононович, С.В.Стайкуца, О.О. Цвілій**

ВИЗНАЧЕННЯ ІДЕНТИЧНОСТІ ОБ'ЄКТІВ У СИСТЕМІ СОЦІАЛЬНОЇ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті аналізується взаємозв'язок інформаційної безпеки з інформаційно-психологічною безпекою людини, соціальною безпекою суспільства та кібербезпекою інформаційно-комунікаційних мереж, як складових частин національної безпеки. Враховуючи роль соціально-психологічного (людського) фактору в інцидентах інформаційної безпеки сформульовано цілі та обґрунтовані задачі, функції та процеси визначення ідентичності об'єктів соціальної взаємодії та менеджменту ідентичності в інформаційно - комунікаційних мережах.Впровадження системи визначення ідентичності об'єктів взаємодії може привести до покращення ситуації з кіберзлочинністю та укріпити безпеку людини та безпеку суспільства.

Ключові слова: інформаційна безпека, соціальна безпека, кібербезпека, захист інформації, визначення ідентичності, менеджмент ідентичності, загрози, інформаційне суспільство, соціальна організація, соціальні комунікації.

Вступ

Актуальність інформаційної безпеки зростає завдяки новим особливостям життя, діяльності та управління у суспільстві, в якому інформація та інтелект стають найважливішими ресурсами. Національні інформаційні ресурси є основою інформаційного суверенітету. На порозі інформаційної епохи стають важливими відповідні концепції та моделі безпеки соціальної організації та безпеки управління, у яких «… нові технології генерування обробки та передачі інформації стали фундаментальним джерелом продуктивності та влади [1]».

Аналіз досягнень та публікацій

Задачі безпеки стали міждисциплінарною областю знань. Для їх вирішення залучаються методи філософії, економіки, соціології, психології, інформатики, технічної кібернетикита телекомунікацій. Взаємозв'язок інформації та безпеки як стійкості та соціальної упорядкованості, безпека суб'єкта в умовах зростання інтенсивності інформаційних потоків та особливостей соціальних практик у забезпеченні інформаційної безпеки філософськи концептуалізовані у монографії [2]. «Усяка соціальна практика, особливо пов'язана з виробництвом та управлінням, у широкому сенсі цього слова, актуалізує певний спектр інформації та обумовлена проблемою інформаційної безпеки [2, с. 5]». Соціальна природа інформаційної безпеки та основи методології, теорії, інституціоналізації проблем безпеки розглянуті у [3]. Там же представлено соціологічний аналіз процесів, технологій та механізмів безпеки людини, суспільства, держави. Наростання складності, багатоаспектності соціальних практик, зростання швидкості їх протікання пов'язані з ростом інтенсивності соціальних процесів у суспільстві, процесів обміну інформацією та із зростаючими ризиками та загрозами. Внаслідок росту інтенсивності комунікацій у суспільстві, розрегульованість соціальних комунікацій, затримки в отриманні інформації негативно впливають на безпеку суб'єктів і безпеку суспільства в цілому.

Основні принципи розробки та реалізації кібербезпеки інформаційно-комунікаційних мереж (ІКМ) формуються з урахуванням міжнародних стандартів та рекомендацій, зокрема Рекомендації X.1205 [4], рекомендацій серії Y та інших. Безпека ІКМ забезпечується за розподілом ролей та відповідальності постійно взаємодіючих між собою служб кібербезпеки доменів телекомунікацій, взаємоузгодженим моніторингом та адмініструванням систем кібербезпеки телекомунікаційних мереж, а також систем виявлення та протидії кібератакам. Функціонування системи інформаційної безпеки телекомунікацій в Україні регламентуються Законами [5, 6], та низкою нормативних документів сфери технічного захисту інформації (ТЗІ). Проте, проблеми безпеки, яка є складним багаторівневим явищем, досліджені ще недостатньо. Актуальними є необхідність вироблення загальних інтегрованих уявлень щодо інтегрованої (консолідованої) безпеки тавпровадження нових технологій і технік

інформаційної та соціальної безпеки в частині визначення ідентичності об'єктів та його менеджменту.

Метою даної роботи єрозробка основних концептуальних положень, моделі загроз інформаційної безпеки людини та безпеки суспільства, окреслення та обґрунтування цілей та задач менеджменту визначення ідентичності об'єктів як складової системи соціальної та інформаційної безпеки.

Основна частина дослідження

В основу побудови моделі об'єктів захисту – суб'єктів, суспільства та держави, та їх середовища – покладемо ідеї Нікласа Лумана, який запропонував цілісну, універсальну теорію суспільства. «Його погляди, що спираються на революційні досягнення кібернетики та теорії інформації, отримують нове звучання у контексті сучасного інформаційного суспільства [2, с. 10]. Основні положення у дослідженні соціальної природи інформаційної безпеки вироблені завдяки теорії соціальної еволюції [7] і теорії комунікації [8] Н. Лумана». Інформаційна безпека суб'єкта розглядається як для психічної системи, а безпека суспільства – як для соціальної системи. Далі, спираючись на концепції [2] та теорії інформаційної і соціальної безпеки [3], розглянемо основні принципи системи інформаційної безпеки та соціального захисту інформації.

Основні принципи системи інформаційної безпеки людини та суспільства. Інформаційна безпека є вагомою складовою національної безпеки. При цьому інформаційна безпека у певній мірі присутня при забезпеченні всіх видів безпеки: екологічної, економічної, тощо. З іншого боку, соціально-психологічний (людський) фактор породжує значну частину інцидентів з інформаційною безпекою. Цей фактор враховується у системах інформаційної безпеки у вигляді організаційних заходів захисту та заходів з управління інформаційною безпекою. Конвергенція соціального захисту інформації із захистом інформації може бути корисною подібно конвергенції захисту від несанкціонованого доступу до інформації із технічним захистом інформації.

У вітчизняній практиці сформувалось таке розуміння інформаційної безпеки: «Це такий стан інформаційного середовища (інформації, інформаційної системи, інформаційного ресурсу), при якомугарантується розвиток цього середовища і її використання в інтересах особистості, суспільства і держави, а також захищеність від будь-яких загроз [9, с. 121]».

Можливийнормативно-правовий підхід до поняття інформаційної безпеки поділяє її на два напрями: «безпека інформації (захист інформації) та безпека від інформації (захист від «небезпечної», неадекватної картині світу інформації) [10, с. 18]». Обидва напрями взаємно-пов'язано реалізуються як у гуманітарній, так і у технічній сферах. Успішна реалізація такого підходу можлива при його збалансованому використанні разом з демократичними принципами свободи та вільного розповсюдження інформації. Вільне обертання інформації є однією з умов процесів формування та розвиту і особистості (соціальної людини), і сучасного суспільства, і демократичної держави. Невиконання таких умов створює нові загрози у соціальному аспекті інформаційної безпеки.

«Головна соціальна функція інформаційної безпеки полягає у забезпеченні стабільності та стійкості соціально-економічного та соціально-політичного розвитку суспільства у відповідності до об'єктивно діючих закономірностей та тенденцій за наявності внутрішніх та зовнішніх загроз. … Під інформаційно-психологічною безпекою розуміється така ситуація у системі «людина – інформаційне середовище», яка не викликає зниження індивідуального або популяційного потенціалу за допустимі межі. Психологічний потенціал – це сукупність властивостей індивідууму (соціуму), яка лежить у основі його можливостей здійснювати продуктивну діяльність [2, с. 28]». «Основними інформаційно-психологічними загрозами є обсяг, повнота, кількість, точність, доступність, своєчасність, приймання інформації, адекватність її ергономічних характеристик перцептивним параметрам органів почуття,

властивостям уваги, пам'яті, мислення, диспозиціям особистості, поведінковим стереотипам та соціально-психологічні установки суспільства. Особливо небезпечні в інформаційних потоках спеціальні елементи, які цілеспрямовано змінюють психологічний стан людей, а також модифіковані фізичні носії інформації, що впливають безпосередньо на фізіологічні системи [2, с. 29]». Звідси витікає увага до ролі ІКМ як засобу телекомунікацій у забезпеченні усіх видів безпеки.

Міжнародний підхід співзвучний національному підходу та передбачає наступне. Кібербезпека ІКМ є складовою частиною національної безпеки України. ІКМ реалізують потреби суспільства у якісних комунікаціях, надаючи широку номенклатуру інфокомунікаційних послуг та забезпечуючи гнучкість, інтеграцію, конвергенцію та уніфікацію мереж. Маючи широкі функціональні можливості, ІКМ потребують посиленої уваги до проблем кібербезпеки інфраструктури, середовища послуг, комунікаційних процесів та управління телекомунікаціями.

Соціальна безпека може бути розглянута через співставлення понять соціального порядку та девіантної поведінки. Соціальний порядок у всі часи являється цінністю як для окремої людини, так і для системи суспільства. Соціальний порядок і стабільність – це умови благополучного існування суспільства та необхідною основою будь-якої соціальної діяльності, творчої реалізації особистості. Соціальний порядок гарантується виконанням індивідуумами соціальних норм. Соціальна норма, зокрема, закріплена у законі держави – це правило поведінки, стандарт, який регулює взаємовідносини між людьми.

«Усяке суспільство представляє собою стійку впорядковану соціальну систему. Елементами цієї системи являються комунікації, які у своїй сукупності складають систему зв'язків та відношень між соціальними суб'єктами. Система відслідковує та контролює свою стійкість та відтворювання. Основою стійкості та гарантією відтворення суспільства являється ціннісна та нормативно-правова система соціальних відносин. Відтворення цінностей та нормативно-правової системи являється життєво важливою умовою існування суспільства [2, с. 32]». Одним із механізмів забезпечення стійкості суспільства є контроль інформаційних потоків і, зокрема, визначення ідентичності та менеджмент визначенням ідентичності об'єктів комунікацій.

Навчальна й наукова література, наприклад [11, с. 525] серед сучасних методів і засобів захисту інформаційних ресурсів виокремлює концепцію трьох «А» – аутентифікація, авторизація, аудит. Вирішивши послідовно проблеми технології інформаційної безпеки за допомогою міжмережного екрану, системи виявлення атак, аудиту тощо, спеціалісти з безпеки виявляють нові проблеми.

У 2007 році Міжнародний союз електрозв'язку виступив з глобальною ініціативою із стандартизації менеджменту ідентичності [12, с. 2]. Мова йде не про цензуру і не про тотальні перевірки, а про управління інформаціями, що підтверджують ідентичність об'єкта, наприклад, ідентифікаторами, реєстраційними даними й атрибутами. У групі Рекомендацій МСЕ-Т X.1250 – X.1279 [13] 17-ю дослідною комісією представлено стандарти менеджменту ідентичності об'єктів у телекомунікаціях, а в групі Рекомендацій МСЕ-Т Y.2720 – Y.2739 – стандарти менеджменту визначення ідентичності об'єктів у ІКМ [14].

Актуальність проблеми визначення ідентичності обгрунтовується двома факторами: заходи боротьби з кіберзлочинністю поки що не досягають бажаних результатів і необхідно удосконалювати систему кібербезпеки телекомунікацій, як критичної ланки інформаційно-комунікаційних систем; інтенсивність інформаційних потоків посилюється, інформація відіграє все більш значущу роль у життєдіяльності людини і підвищення захищеності інформації стає однією з найважливіших задач. Точно також, як при нестачі кисню через 5 хвилин припиняється життя, так і без руху інформації зупиняється діяльність, виробництво, розпадаються суспільство і спільноти. Крім того, багато сучасних інформаційних послуг, таких як електронна торгівля, електронній уряд, вимагають від телекомунікаційного середовища посиленої спостережності.

Обґрунтування ефективності визначення ідентичності.

У рамках сучасного підходу до кібербезпеки телекомунікацій і, зокрема ІКМ, автори висувають *твердження*– забезпечення визначення ідентичності всіх об'єктів та їх інформаційних потоків, на всіх рівнях та на всіх компонентах телекомунікаційної мережі при максимальному сприянні вільному, але контрольованому обертанні інформації. Тут доречно провести аналогію між інфокомунікаційною системою та транспортною системою. Коли транспортні системи досягли значних інтенсивностей, управління ними поступово удосконалювалось: побудовані спеціальні дороги, введені єдині правила регулювання дорожнього руху транспорту та пішоходів, вироблені правила перевозки пасажирів та вантажу, кожен транспортній засіб отримав індивідуальний номер, винайдені світлофори, дорожні знаки та розмітка полотна дороги, нарешті сьогодні ми на порозі повсюдного встановлення камер спостереження і автоматичного аналізу ситуацій та дій окремих людей. В результаті ми маємо ситуацію, коли ми вільно пересуваємось там і туди, куди нам потрібно, але при цьому суворо дотримуємось правил дорожнього руху і правил поведінки на дорогах.

Аналогічно, подібний контроль необхідно встановити у кіберпросторі та в телекомунікаційних мережах. Кожна людина може вільно отримати будь-яку відкриту інформацію, дотримуючись правил обміну інформацією та правил поводження з нею. Цілі впровадження системи визначення ідентичності об'єктів можна обґрунтувати наступним чином. Спілкування людей для досягнення цілей діяльності можуть бути або через безпосередні контакти між собою, або контакти за допомогою телекомунікаційних каналів. При безпосередньому контакті повністю проявляються перцептивна функція спілкування. Люди безпосередньо сприймають (за допомогою усіх своїх органів почуттів) один одного і мають можливість пізнавати фізичні, психологічні та індивідуальні особливості, притаманні кожній стороні. Співрозмовники у процесі контактів мають змогу скласти більш-менш об'єктивне враження про те, що становить собою партнер по спілкуванню, проникнути в його внутрішній світ, зрозуміти мотиви поведінки, звички, оцінити ставлення до фактів дійсності.

При контакті через телекомунікаційні засоби перцептивна функція спілкування обмежується. Проте бажано, щоб телекомунікації надавали хоча б частину можливостей, які доступні при безпосередньому контакті. У майбутньому розвиток телебіометрики, сенсорних мереж з сенсорами навколо людини, на людині та в середині людини, які будуть обслуговувати її, засоби віртуальної реальності дозволять наблизити можливості телекомунікаційніх контактів до можливостей безпосереднього спілкування людей. Визначення ідентичності об'єктів є першочерговим і необхідним кроком на цьому шляху.

Повинна бути забезпечена ідентичність кожної трансакції у мережі і, за необхідності, трансакція має бути проконтрольована законними засобами. Крім правил та засобів маршрутизації, засобів законного моніторингу в інформаційних транспортних системах доцільно впровадити менеджмент визначення ідентичності об'єктів інформаційного обміну. Технологія ІКМ завдяки широкій функціональності та гнучкості послуг має можливості, за порівняно невеликих витрат, розробки й впровадження необхідних механізмів та процедур.

Ефект від системи визначення ідентифікації об'єктів телекомунікаційного обміну інформацією полягає у суттєвому зменшенні числа потенційних порушників за рахунок організаційно-технічних методів контролю. З психології відомо, що людей (персонал, користувачів та споживачів) можна поділити на три психологічних групи (рис. 1).

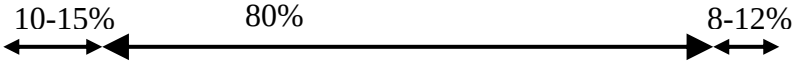

Рис. 1. Поділ людей на психологічні групи за відношенням до законів.

За даними Леоніда Чупрія – директора центру соціально-політичних досліджень «Генезис» – приблизно 10-15% людей ні за яких обставин не будуть порушувати морально-етичні норми і закон. Кількість законослухняних людей на протязі останніх 15 років практично не змінюється. Навпаки, 8-12% осіб будуть порушувати норми і закони, навіть якщо будуть точно знати, що покарання буде неминучим. Останні 80% нормальних людей не будуть порушниками, якщо мають перед собою приклади покарання і, в той же час, будуть порушниками, якщо знають, що покарання не наступить. Таким чином, при відсутності контролю у спільноті приблизно 85% потенційних порушників. За наявності контролю та системи покарання/заохочення потенційних порушників може бути не більше 12%.
Зауважимо, що наявність злочинців не є «абсолютним злом». Без розумної міри девіантної поведінки неможливий прогрес. Так Еміль Дюркгейм стверджує, що злочинність є результатом природних відхилень поведінки від «середнього типу» поведінки і залежать від відмінностей людської індивідуальності. Він робить парадоксальний висновок: «Щоб був можливим прогрес, індивідуальність повинна мати можливість виразити себе. Щоб отримали можливість вираження індивідуальності ідеаліста, чиї мрії випереджають час, необхідно, щоб існувала можливість вираження індивідуальності і злочинця, що стоїть нижче рівня сучасного йому суспільства [15, с. 43]». Таким чином, ми бачимо, що за рахунок лише організаційно-технічних заходів досягається значне підвищення захищеності інформації.

Цілі, термінологія та можливості менеджменту визначення ідентичності.

У середовищі ІКМ інфокомунікаційні послуги базуються на контекстах та ролях [див. 14, с. 4] і можуть бути доступними у будь-якому місці, у будь-який час, гарантування безпеки інформації, підтвердження ідентичності стають все актуальнішими. Відносно людей ***ідентичність*** (англ. *Identity*) – є властивість психіки людини у концентрованому вигляді виражати для нього те, як він уявляє собі свою належність до різних соціальних, національних, професійних, мовних, політичних, релігійних, расових та інших груп або інших спільнот, або ототожнює себе з тією чи іншою людиною як втілення притаманним цим групам або спільнотам властивостей. Але відносно об'єктів телекомунікаційної мережі ідентичність означає зовсім інше (у об'єктів нема психіки). Зокрема, ідентичність об'єктів телекомунікаційної мережі не передбачає яку-небудь певну характеристику тієї чи іншої людини. Мова йде про ідентичність (належність) інформації.

Визначення ідентичності об'єктів значно простіше і є розширенням поняття ідентифікація. «*Ідентичність* – це інформація щодо об'єкта, якої досить для ідентифікації цього об'єкта у тому чи іншому контексті. Менеджмент визначенням ідентичності – MBI (identifymanagement) – це набір функцій та можливостей (наприклад, адміністрування, управління та технічне обслуговування, виявлення, обмін повідомленнями, співставлення та ув'язування, забезпечення реалізації політики, автентифікація та затвердження), які використовуються для: гарантування інформації, що підтверджує ідентичність (наприклад, ідентифікаторів, реєстраційних даних, атрибутів); гарантування ідентичності об'єкта; забезпечення комерційних застосувань та застосувань безпеки (рис. 2) [див. 14, с. 3]».

Для пояснення визначення та конспекту необхідно додати супутні визначення, слідуючи Рекомендації МСЕ-Т Y.2720. *Анонімність* (*anonymity*) – це здатність забезпечувати анонімний доступ до послуг, за якого не допускається відслідковування персональної інформації щодо користувача та його поведінки, наприклад, місцеположення користувача, частота користування послугою тощо. *Автентифікація* (*authentification*) – це забезпечення гарантії заявленої ідентичності об'єкта. *Авторизація* (*autohorization*) – це надавання прав, які включають доступ на основі прав доступу. *Заявник* (*claimant*) – це об'єкт, який є адміністратором доступу або представляє його з метою автентифікації. Заявник має функції, що необхідні для участі в автентифікаційних обмінах від імені адміністратора обміну. *Ідентифікатор* (*Identifier*) – це серія цифр, букв і символів або даних у будь-якій формі, що використовується для визначення абонентів, користувачів, елементів мережі, функцій,

об'єктів мережі, що надають послуги/застосування або інших об'єктів, фізичних або логічних. *Атрибут* (*attribute*) – цеінформація описового типу, що призначена для об'єкта, в якій вказується такі характеристики об'єкта, як стан, якість, або інша інформація, що стосується цього об'єкта. *Реєстраційні дані* (*credential*) – це об'єкт, який можна ідентифікувати і який можна використати для автентифікації того, що заявник є саме тим, за кого він себе видає, і для того, що дати заявнику дозвіл на право доступу. *Об'єкт* (*entity*) – це все, що існує самостійно і є розрізнюваним, що може бути ідентифіковано унікальним чином. Прикладом об'єктів є абоненти, користувачі, групи, мережні елементи, мережі, програмні застосування, послуги та пристрої користувачів, організацій, постачальників доступу до мережі та постачальників послуг, а також віртуальні об'єкти. *Модель поведінки* (*pattern*) – це структурований вираз, отриманий на основі поведінки, який пов'язаний з об'єктом та описує об'єкт, даючи можливість його розрізнити чи виокремити; це може включати минулий досвід об'єкта. *Інформація, що дозволяє встановити особистість* (*personallyidentifiableinformation*) – це інформація, що відноситься до будь-якої живої особи, яка дає можливість ідентифікувати таку особу. *Приватність* (*Privacy*) – це захист інформації, що дозволяє встановити особистість. *Довіра* (*trust*) – це міра того, наскільки покладаються на характер, можливості, сильні сторони або істинність кого-небудь або чого-небудь.

Функції та можливості МВІ використовуються для гарантування та підтвердження інформації, що підтверджує ідентичність, гарантування ідентичності об'єкта а також для підтримки послуг на основі ідентичності, виявлення та підтвердження інформації, що підтверджує ідентичність. МВІ дає можливість розробки різноманітних застосувань, наприклад, комерційні пропозиції (одноразовий вхід до системи та вихід із системи; групові послуги), послуги на основі ідентичності (послуги в області ідентифікаторів, реєстраційних даних та атрибутів; послуги сполучення; послуги з надання інформації з моделі поведінки), застосування безпеки (управління доступом до мережних та прикладних послуг та ресурсів; управління доступом до інформації, ресурсів та засобів за рольовими прикметами; управління авторизацією та привілеями; послуги із забезпечення захисту ресурсів чи інформації; захист інформації, що дозволяє встановити особистість.

Поряд з іншими механізмами захисту, міжмережними екранами, системами виявлення вторгнень, захистом від вірусів, МВІ відіграє важливу роль у захисті інфраструктури, послуг та застосування ІКМ від кіберзлочинності, таких як шахрайство та крадіжка даних ідентичності. Трансакції у ІКМ будуть захищеними та надійними. Різні ідентичності використовуються в усіх операціях ІКМ. МВІ забезпечує послуги, можливості та функції підтримання цілісності ідентичності та використання ідентичностей ІКМ.

У мережному середовищі МВІ має забезпечувати можливості, які забезпечують гарантування безпечного обміну інформацією між об'єктами. Обмін інформацією засновується на розробленій політиці та довіри, що встановлюється між цими об'єктами у середовищі з участю багатьох постачальників послуг. Така довіра заснована на затвердженні (*assertion*) та перевірці достовірності (*validation*) ідентичностей об'єктів в усіх системах розподілених ІКМ: у страті транспорту (мережах доступу, функціях управління приєднанням мереж, функціях транспорту, функціях управління ресурсом і допуском, функції профілю користувача транспорту); у страті обслуговування (компонентах мультимедійних послуг, компонентах телекомунікаційних послуг, функціях управління послугами, застосуваннях, функціях підтримки застосувань та підтримки послуг, функції профілю користувача послуг); системах конечного користувача (традиційних терміналах, абонентських мережах, терміналах передачі даних); інших мереж. МВІ надає можливості захисту конфіденційності інформації об'єктів та *забезпечує, щоб у ІКМ розповсюджувалась лише авторизована інформація*.

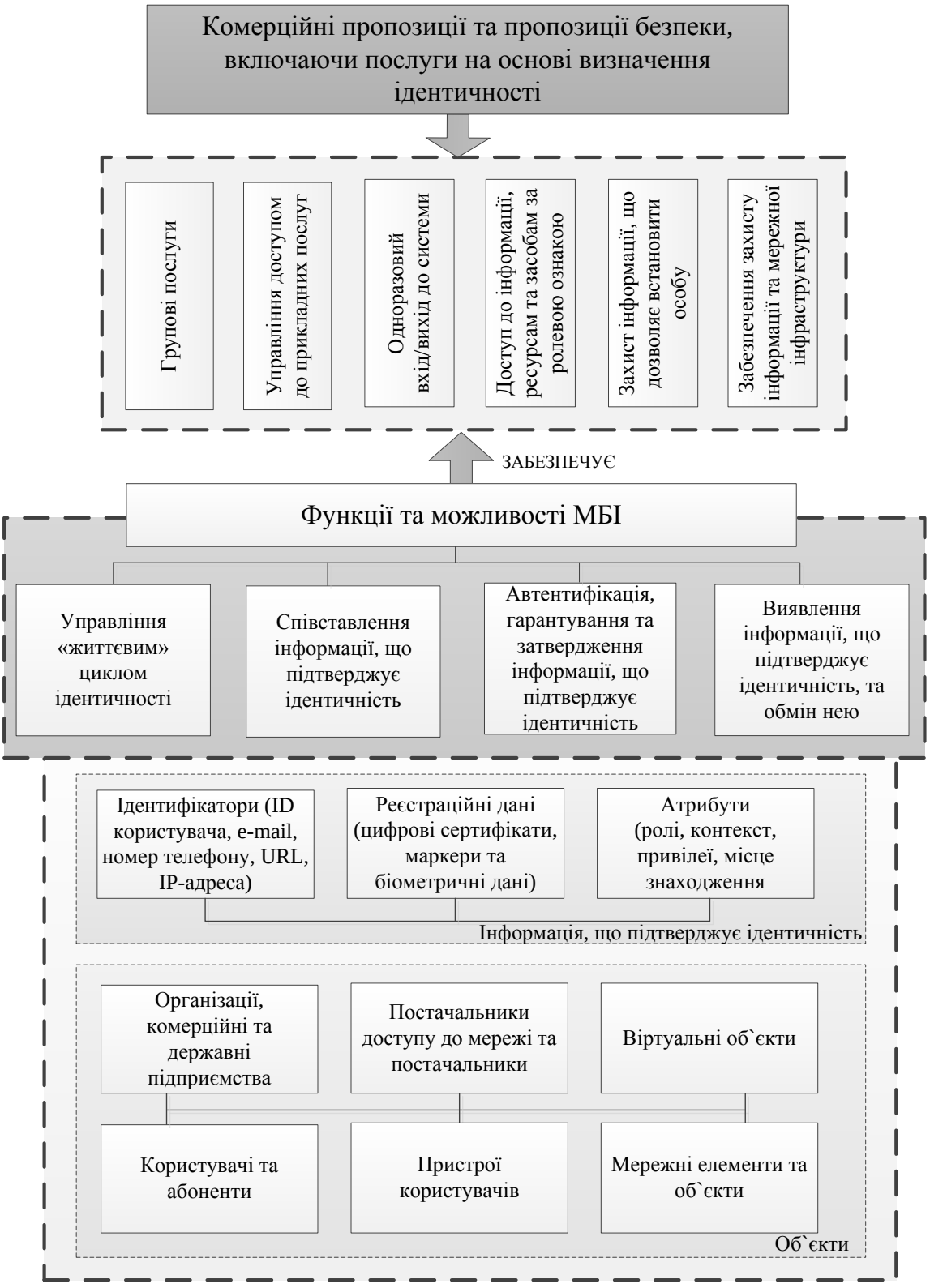

Рис. 2. Функції, об’єкти та можливості менеджменту визначенням ідентичності

Структура менеджменту визначенням ідентичності.

Рекомендація МСЕ-Т Y.2720 визначає сім функцій МВІ у ІКМ.

1. Управління життєвим циклом ідентичності, що включає процеси управління життєвим циклом та функцій для даних ідентичності та інформації, що підтверджує ідентичність (ідентифікатори, реєстраційні дані й атрибути тощо). Це управління охоплює

процеси і процедури, що пов'язані з реєстрацією та видачею даних ідентичності об'єкта.

2. Функції експлуатації, адміністрування, технічного обслуговування та забезпечення (OAM&P) при MBI, які включають функції та можливості, що відносяться до підтримки MBI. OAM&P раніше була окремою службою – це група функцій з управління, які забезпечували пошук несправностей у системі або мережі, моніторинг якості роботи, управління безпекою, функції діагностики, конфігурацію та забезпечення користувачів.

3. Функції сигналізації та контролю при MBI, які включають функції та можливості підтримки послуг MBI і забезпечують сигналізацію та контроль при зв'язку у реальному часі та близькому до реального часу.

4. Функції групової ідентичності при MBI для підтримання функцій та можливостей групових послуг.

5. Функції користувачів та абонентів при MBI, які включають функції та процеси, що пов'язані із контролем із боку кінцевих користувачів та абонентів за інформацією, стосовну їх ідентичності. Сюди ж відносяться функції контролю, делегування та дозволу використання та розповсюдження інформації, пов'язаної з ідентичністю.

6. Функції та процедури відносно якості роботи, надійності та масштабованості.

7. Безпека при MBI, що включає функції та процедури, що стосуються забезпечення захисту систем, послуг та можливостей MBI.

У структурі MBI використовуються ресурси ІКМ, такі як: інформація у серверах абонентських профілів, місцеположення, політики, присутності, серверах абонентських даних, інформація функції управління сеансами зв'язку, сервера прикордонного контролера сеансів зв'язку тощо. Останнє свідчить, що у ІКМ, за порівняно не великих витратах може бути реалізована структура та підтримка послуг MBI.

Впровадження MBI на ІКМ надають нові можливості користувачам, абонентам, підприємствам. Зокрема державним підприємствам MBI надає можливості впровадження послуг та застосувань із гарантування ідентичності та підвищує рівень довіри до підтримуваним даним ідентичності й рівень їх безпеки: у послугах електронного уряду; у суспільній службі невідкладної допомоги 911; у службі охорони правопорядку; у службі телекомунікацій у надзвичайних ситуаціях; у службі національної безпеки. Як результат, забезпечується захист інфраструктури телекомунікацій проти загроз кібербезпеки.

Висновки

Аналізуючи взаємозв'язок інформаційної безпеки з інформаційно-психологічною безпекою людини, соціальною безпекою суспільства та кібербезпекою інформаційно-комунікаційних мереж, як складових частин національної безпеки, та зважаючи на роль соціально-психологічного (людського) фактору в інцидентах інформаційної безпеки знайдено цілі та обґрунтовані задачі визначення ідентичності об'єктів соціальної взаємодії та менеджменту ідентичності. Впровадження системи визначення ідентичності об'єктів взаємодії може привести до покращення ситуації з кіберзлочинністю та укріпити безпеку людини та безпеку суспільства.

Розробка механізмів, функцій та процесів визначення ідентичності об'єктів телекомунікаційних мереж може бути темою подальшої роботи.

Література

1. Кастельс М. Информационная эпоха: экономика, общество и культура / М. Кастельс ; пер. с англ. под научн. ред. О.И. Шкаратана. – М.: Гос. ун-т = Высш. шк. экономики, 2000. – 606 с.

2. Владимирова Т.В. Социальная природа информационной безопасности : монография / Т.В. Владимирова ; АНО содействия развитию соврем. отечеств. науки. Изд. дом «Научное обозрение». – М.: АНО Изд. дом «Научное обозрение», 2014. – 239 с.

3. Кузнецов В.Н. Социология безопасности: Учебное пособие / В.Н. Кузнецов. – М.: Изд. МГУ, 2007. – 423 с.

4. Рекомендация МСЭ-Т X.1205. Безопасность электросвязи. Обзор кибербезопасности. – Женева: 2008. – 56 с.

5. Про телекомунікації / Закон України № 1280 від 18.11.03. – 33 с.

6. Про захист інформації в інформаційно-телекомунікаційних системах/ Закон України № 2994-15 від 31.05, із змінами вкл. Закону від 15.01.2009 № 879-VI. – 13 с.

7. Луман Н. Эволюция / Н. Луман. Пер. с нем. А. Антоновский. – М.: Издательство «Логос», 2005. – 256 с.

8. Назарчук А.В. Учение Никласа Лумана о коммуникации / А.В. Назарчук. – М.: Издательство «Весь мир», 2012. – 248 с. (Введение доступно на сайте: http://www.vesmirbooks.ru/fragments/2368/).

9. Кавун С. В. Економічна та інформаційна безпека підприємств у системі консолідованої інформації : навчальний посібник / С. В. Кавун, А. А. Пилипенко, Д. О. Ріпка. – Х. : Вид. ХНЕУ, 2013. – 364 с.

10. Расторгуев С.П. Основы информационной безопасности : учеб. пособие для студ. высших учеб. заведений / С.П. Расторгуев. – М.: Изд. центр «Академия», 2009. – 192 с.

11. Юдін О.К. Захист інформації в мережах передачі даних / О.К. Юдін, О.Г. Корченко, Г.Ф. Конахович // Підручник. – К. : Вид-во ТОВ «НВП» ІНТЕРСЕРВІС, 2009. – 716 с.

12. Глобальная инициатива по стандартизации управления идентичностью (ГИС-УИд) / Циркуляр 184 БСЭ. Приложение 1. – Женева, 2007. – 5 с.

13. Рекомендация МСЭ-Т X.1250. Базовые возможности для улучшения доверия и функциональной совместимости пи глобальном управлении определением идентичности. – Женева, 2009. – 26 с.

14. Рекомендация МСЭ-Т Y.2720. Структура управления определением идентичности в сетях последующих поколений. – Женева, 2010. – 26 с.

15. Дюркгейм Э. Норма и патология / Эмиль Дюркгейм. [Электронный ресурс] // Сборник статей: Социология преступности (Современные буржуазные теории). – М.: Издательство «Прогресс», 1966. – С. 39-44. – Режим доступа: http://www.gumer.info/bibliotek_Buks/Sociolog/Durkgeim/Norm_Pat.php.

Надійшла 20.02.2015 р. Рецензент: д.т.н., с.н.с. Бурячок В.Л.