

## **ІДЕНТИЧНІСТЬ ОБ'ЄКТІВ ІНФОРМАЦІЙНОЇ МЕРЕЖІ ЯК ЕЛЕМЕНТ МОДЕЛІ КІБЕРБЕЗПЕКИ**

*Анотація. Наведені потенційні загрози безпеки телекомунікаційної мережі. 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. Розроблені моделі загроз інформації та дій порушника як складові моделі кібербезпеки. Впровадження системи визначення ідентичності об'єктів взаємодії може привести до покращення ситуації з кіберзлочинністю та укріпити безпеку людини та безпеку суспільства.*

*Ключові слова: кібербезпека, ідентичність, мережа, менеджмент ідентичності.*

S.V. STAYKUTSA, V.Y. KILDISHEV

Odessa National Academy of Telecommunications named after O.S. Popov

## **OBJECTS OF IDENTITY INFORMATION NETWORK AS AN ELEMENT MODEL CYBERSECURITY**

*Abstract. These potential threats to the security of telecommunication networks. Given the role of social and psychological (human) factor in incidents of information security formulated objectives and reasonable tasks, functions and processes determine the identity of social interaction and identity management in the information and communication networks. The models of information threats and actions as offending component model cybersecurity. Implementation of determining the identity object interaction may lead to improvement in cybercrime and strengthen human security and safety of society.*

*Keywords: cyber, identity, network, identity management.*

### **Вступ**

Елементами взаємодії у кіберпросторі є криптографічні, технічні та соціальні методи та засоби захисту інформації. З міркувань потреб практичної діяльності має бути реалізований такий клас систем захисту інформації, в якому головну роль, поряд з технічним та криптографічним забезпеченням системи захисту, відігравали б соціально-психологічні організаційні засоби – робота з персоналом, користувачами, кадровим забезпеченням, тобто в якому головна увага приділялась би людському факторові [1].

В даному разі є вагомі обґрунтування введення поняття ще одного виду захисту – соціального захисту інформації (СЗІ). З численних статистичних даних випливає що до 60% інцидентів з інформаційною безпекою пов'язані з людським фактором: помилки чи некомпетентність персоналу та користувачів, зловмисні та незловмисні дії, підкуп персоналу, порушення корпоративної солідарності тощо [2]. У 2007 році Міжнародний союз електрозв'язку виступив з глобальною ініціативою із стандартизації менеджменту ідентичності [3]. 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 [4] 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 інформаційно-комунікаційних мереж (ІКМ) [5].

Актуальність проблеми визначення ідентичності обґрунтовується 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. Крім того, багато сучасних інформаційних послуг, таких як електронна торгівля, електронний уряд, вимагають від телекомунікаційного середовища посиленої спостережності.

Метою даної роботи є огляд цілей задач, функцій та процесів визначення ідентичності об'єктів соціальної взаємодії та менеджменту ідентичності в інформаційно - комунікаційних мережах, як засобів підвищення ефективності забезпечення кібербезпеки.

### **Модель дій порушника**

Порушник розглядається, як особа, що може отримати доступ до роботи з включеними до складу ІКМ засобами. Порушники класифікуються за рівнем можливостей, що надаються їм штатними засобами ІКМ [6]. Виходячи з класифікації типів порушника складемо модель дій порушника (рис. 1).

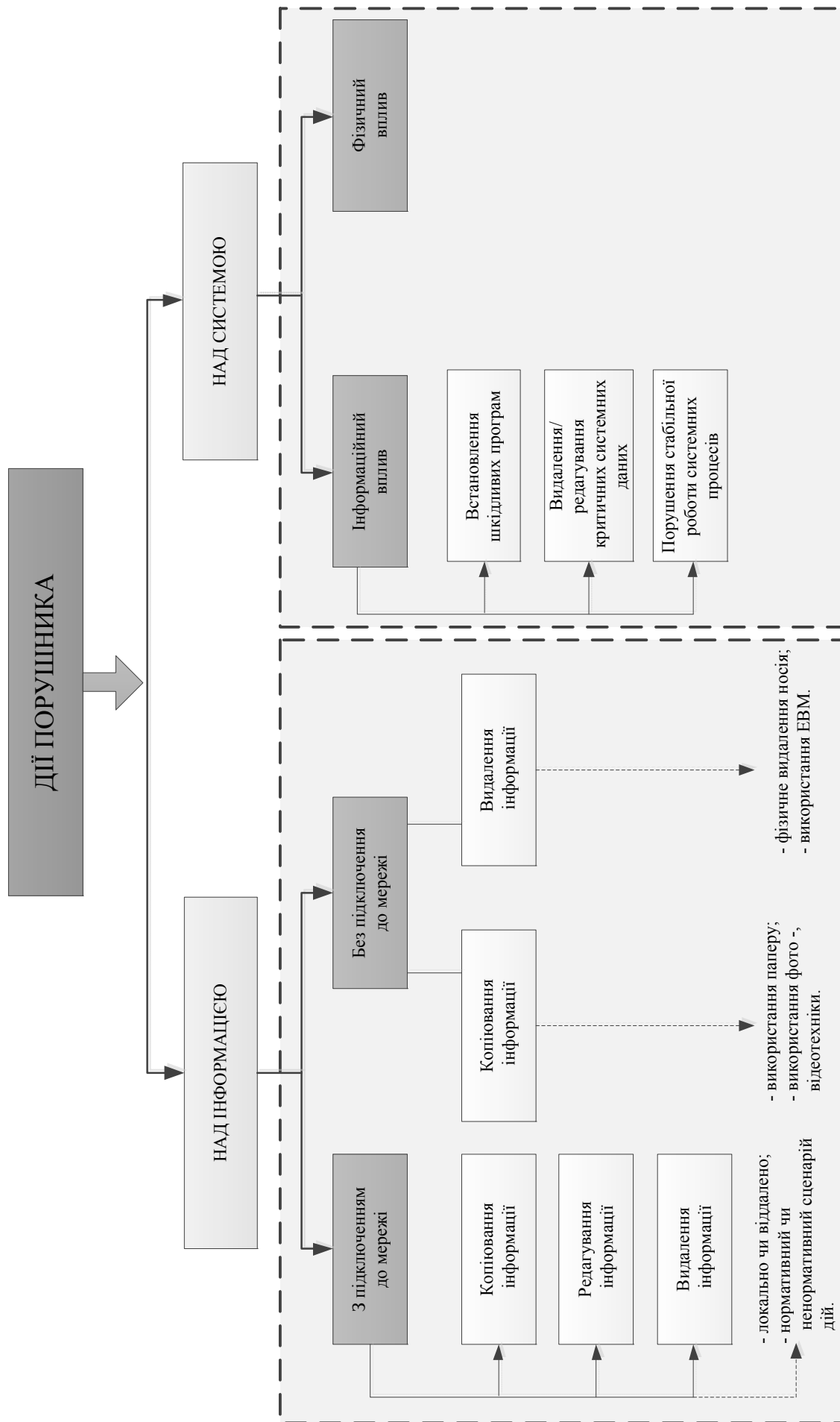


Рис. 1. Модель дій порушника

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 телекомунікаційних контактів до можливостей безпосереднього спілкування людей. Визначення ідентичності об'єктів є першочерговим і необхідним кроком на цьому шляху.

Повинна бути забезпечена ідентичність кожної транзакції у мережі і, за необхідності, транзакція 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. Таким чином, при відсутності контролю у спільноті приблизно 85% потенційних порушників. За наявності контролю та системи покарання/заохочення потенційних порушників може бути зменшено до 12%.

Потенційні канали проникнення в ІКМ – це сама автоматизована система комутації та її канали. Інформаційні загрози безпеки ІКМ показані на рис. 2.

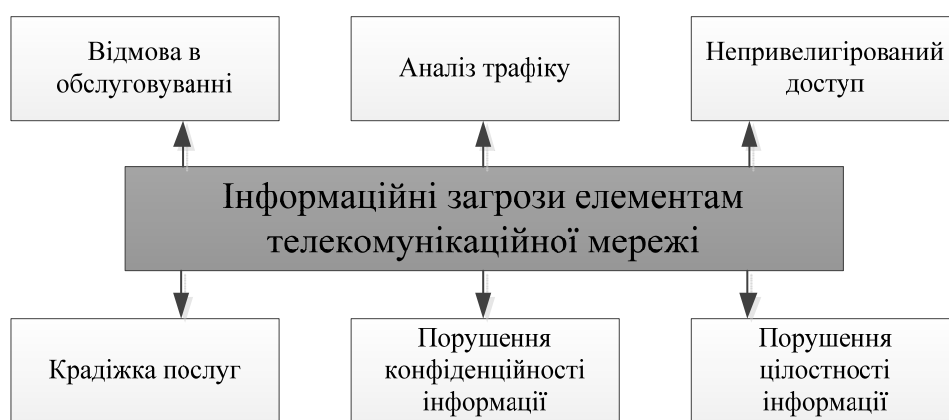


Рис. 2. Інформаційні загрози безпеки ІКМ

Крадіжка послуг – веденням зловмисником переговорів за чужий рахунок. Порушення конфіденційності інформації, включаючи зміст телефонних розмов і баз даних телекомунікаційного обладнання. Порушення цілісності інформації – неавторизована зміна конфігураційних баз цих, білінгових записів та іншої інформації. Непривілейований доступ – доступ неавторизованих користувачів з метою отримання контролю над системними ресурсами. Відмова в обслуговуванні – дії, націлений на порушення роботи системи зв'язку. Аналіз трафіку – пасивна дія з метою отримання інформації про трафік.

#### Менеджмент визначенням ідентичності

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 (identify management) – 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. 3) [5].

Виходячи з розглянутих вище загроз витоку інформації в ІКМ, представимо структуру менеджменту визначенням ідентичності як елементу моделі кібербезпеки.

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.

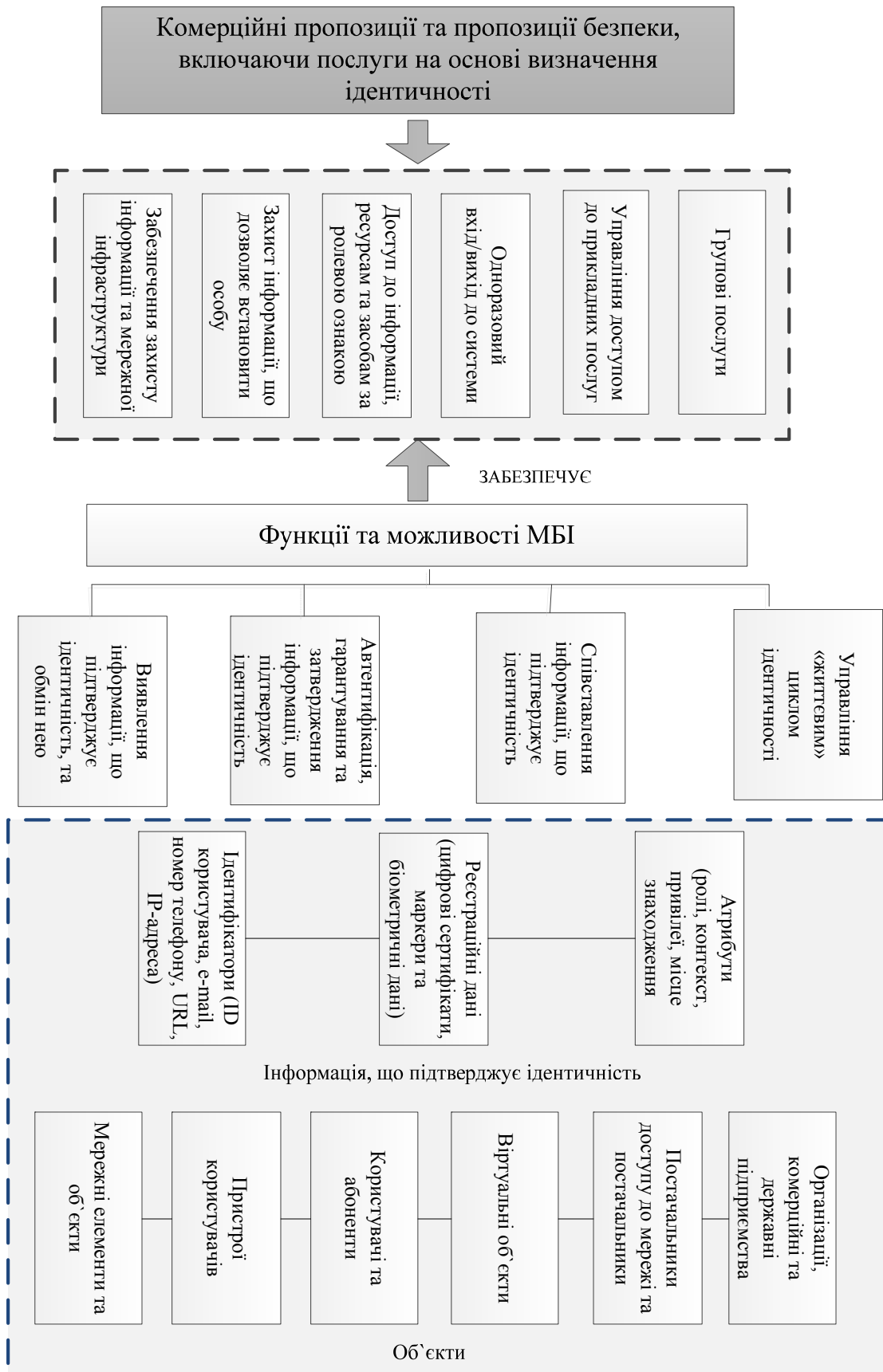


Рис. 3. Функції, об'єкти та можливості менеджменту визначенням ідентичності

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

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

5. Функції користувачів та абонентів при МБІ, 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 МБІ, що включає функції та процедури, що стосуються забезпечення захисту систем, послуг та можливостей МБІ. У структурі МБІ використовуються ресурси ІКМ, такі як: інформація у серверах абонентських профілів, місцезнаходження, політики, присутності, серверах абонентських даних, інформація функцій 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 МБІ.

### Висновки

Впровадження МБІ на ІКМ надають нові можливості користувачам, абонентам, підприємствам. Зокрема державним підприємствам МБІ 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.

### Література

1. Кононович В.Г. Еволюція парадигми інформаційної, соціально-психологічної та кібербезпеки / В.Г. Кононович // X Міжнародна науково-технічна конференція «ABIA-2011». – 2011. – №2. – С. 38-41.
2. Кононович В.Г. Соціальний захист інформації в класах систем захисту інформації / В.Г. Кононович // Науково-технічний журнал «Захист інформації». – 2008. – №4. – С. 4-16.
3. Глобальная инициатива по стандартизации управления идентичностью (ГИС-УИд) / Циркуляр 184 БСЭ. Приложение 1. – Женева, 2007. – 5 с.
4. Рекомендация МСЭ-Т X.1250. Базовые возможности для улучшения доверия и функциональной совместимости при глобальном управлении определением идентичности. – Женева, 2009. – 26 с.
5. Рекомендация МСЭ-Т Y.2720. Структура управления определением идентичности в сетях последующих поколений. – Женева, 2010. – 26 с.
6. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено наказом № 22 ДСТСЗІ СБ України від 28.05.99.

### References

1. Kononovich V.G. Evolyutsiya paradigmi informatsiynoyi, sotsialno-psihologichnoyi ta kiberbezpeki / V.G. Kononovich // X Mizhnarodna naukovu-tehnichna konferentsiya «AVIA-2011». – 2011. – №2. – S. 38-41.
2. Kononovich V.G. Sotsialniy zahist informatsiyi v klasah sistem zahistu informatsiyi / V.G. Kononovich // Naukovu-tehnichniy zhurnal «Zahist informatsiyi». – 2008. – №4. – S. 4-16.
3. Globalnaya initsiativa po standartizatsii upravleniya identichnostyu (GIS-UIId) / Tsirkulyar 184 BSE. Prilozhenie 1. – Zheneva, 2007. – 5 s.
4. Rekomendatsiya MSE-T H.1250. Bazovye vozmozhnosti dlya uluchsheniya doveriya i funktsionalnoy sovmestimosti pri globalnom upravlenii opredeleniem identichnosti. – Zheneva, 2009. – 26 s.
5. Rekomendatsiya MSE-T Y.2720. Struktura upravleniya opredeleniem identichnosti v setyah posleduyuschih pokoleniy. – Zheneva, 2010. – 26 s.
6. ND TZI 1.1-002-99. Zagalni polozhennya schodo zahistu informatsiyi v komp'yuternih sistemah vid nesanktsionovanogo dostupu. Zatverdzheno nakazom № 22 DSTSZI SB Ukrayini vid 28.05.99.

Рецензія/Peer review : 21.6.2016 р.

Надрукована/Printed : 28.6.2016 р.

Стаття рецензована редакційною колегією