ISSN 2411-3816 (Print)
СУЧАСНА СПЕЦІАЛЬНА ТЕХНІКА
MODERN SPECIAL TECHNICS
DOI (Issue): https: //doi.org/
Issue 4(59) 2019

УДК 004.056

Дудикевич Валерій Богданович,
доктор технічних наук, професор, завідувач кафедри
НУ "Львівська політехніка", м. Львів, Україна
ORCID ID 0000-0001-8827-9920,
Микитин Галина Василівна,
доктор технічних наук, професор, професор
НУ "Львівська політехніка", м. Львів, Україна
ORCID ID 0000-0003-4275-8285

БАГАТОРІВНЕВА БЕЗПЕКА ІНФОРМАЦІЙНИХ СИСТЕМ

У статті розроблено багаторівневу модель інформаційної безпеки (ІБ) інформаційних систем (ІС) на основі концепції "об'єкт – загроза – захист". Зовнішній рівень моделі представлено комплексом систем безпеки: керування доступом, радіочастотної ідентифікації, відеоспостереження, біометрії. На внутрішньому рівні моделі розглянуто технології апаратного та програмного забезпечення ІБ. Мандатна політика безпеки спрямована на запобігання витоку інформації від об'єктів, що мають високий рівень доступу, до об'єктів із низьким рівнем доступу.

Ключові слова: *інформаційна система, інформаційна безпека, багаторівнева модель, концепція "об'єкт – загроза – захист", технології.*

Разработана многоуровневая модель информационной безопасности (ИБ) информационных систем (ИС) на основе концепции "объект – угроза – защита". Внешний уровень модели представлен комплексом систем безопасности: управления доступом, радиочастотной идентификации, видеонаблюдения, биометрии. На внутреннем уровне рассмотрены технологии аппаратного и программного обеспечения ИБ. Мандатная политика безопасности направлена на предотвращение утечки информации от объектов, имеющих более высокий уровень доступа, к объектам с низким уровнем доступа.

Ключевые слова: *информационная система, информационная безопасность, многоуровневая модель, концепция "объект – угроза – защита", технологии.*

Вступ. В Україні тривають процеси інформатизації об'єктів критичної інфраструктри суспільства. Серед комплексу завдань Національної програми інформатизації – створення методологічних засад та розроблення інструментарію забезпечення ІБ засобів інформатизації – інформаційних систем, призначених для контролю/діагностування технічного стану об'єктів і на цій основі прийняття рішення на управління проблемною ситуацією [1]. Розгортаються процеси інтелектуалізації об'єктів предметних сфер промислової інфраструктури України, в яких інформаційні системи функціонують у режимі "контроль – обробка – управління", що спрямований на відбір інформації з системи давачів, передавання

її на вбудований в об'єкті контролю комп'ютер для обробки та прийняття управлінського рішення [2]. Актуальною проблемою є розвиток методології забезпечення інформаційної безпеки ІС, яка є ядром функціональної безпеки у структурі гарантоздатності [3].

Постановка проблеми і мета статті. Розроблена методологія побудови комплексної системи безпеки ІТ на основі системної, нормативної, комплексної моделей безпеки [4; 5], де структура ІТ представлена багаторівневою платформою "інформаційні ресурси – інформаційні системи – інформаційні процеси – інформаційні мережі (канали) – управління", що є підґрунтям для вирішення задач безпеки у сфері управління проблемними ситуаціями. Триває розвиток підходів до побудови комплескних систем безпеки ІТ на основі: моделей порушника, моделей загроз, моделей захисту, методів і технологій захисту [6].

Метою статті є розроблення багаторівневої моделі безпеки ІС на основі концепції "об'єкт – загроза – захист".

Основна частина. З метою об'єднання завдань інформатизації та інтелектуалізації в частині інформаційної безпеки ІС розглянемо багаторівневу модель забезпечення безпеки ІС на основі концепції "об'єкт – загроза – захист", як основного інструментарію безпечного функціонування об'єктів інфраструктури суспільства (рис. 1). Інформаційна система – організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів. Модель безпеки ІС представлена згідно з концепцією "об'єкт – загроза – захист": ІС – об'єкт; загрози інформаційній безпеці ІС – об'єктивні – А, суб'єктивні – В, випадкові – С, цілеспрямовані – D; захист ІС на зовнішньому рівні – І, захист ІС на внутрішньому рівні – ІІ; мандатна політика безпеки – ІІІ. Модель передбачає систему "виявлення – блокування – нейтралізації" загроз, яка на рис. 1 показана двосторонньою лінією на кожному з рівнів безпеки.

Зовнішній рівень безпеки ІС. У табл. 1 розглянуто технології забезпечення ІБ інформаційних систем згідно з концепцією "об'єкт – загроза – захист". Основним інструментарієм протидії загрозам на зовнішньому рівні є: 1) системи керування доступом – персональні ідентифікатори, які використовують безконтактну проксіміті-технологію дистанційного радіочастотного передавання/приймання інформації в систему контролю доступу для ідентифікації персоналу; зчитувачі персональних ідентифікаторів; автоматизовані робочі місця, які здійснюють збір та обробку інформації з метою ідентифікації персоналу та прийняття рішення; 2) системи радіочастотної ідентифікації – RFID-технологія: комп'ютерна система збору інформації і зчитувач, транспондер, канал взаємодії зчитувача і транспондера; 3) системи відеоспостереження – передають інформацію з відеокамер (корпусних, безкорпусних, купольних, міні, зокрема тепловізійних), встановлених по зовнішньому периметру об'єкта, на пристрої обробки відеоінформації для аналізу та прийняття рішення на управління інформаційною безпекою; 4) біометричні системи розпізнавання за відбитками пальців, геометрією обличчя, райдужною оболонкою ока, геометрією руки, малюнком вен, голосом, почерком/ підписом тощо (рис. 1) [7].

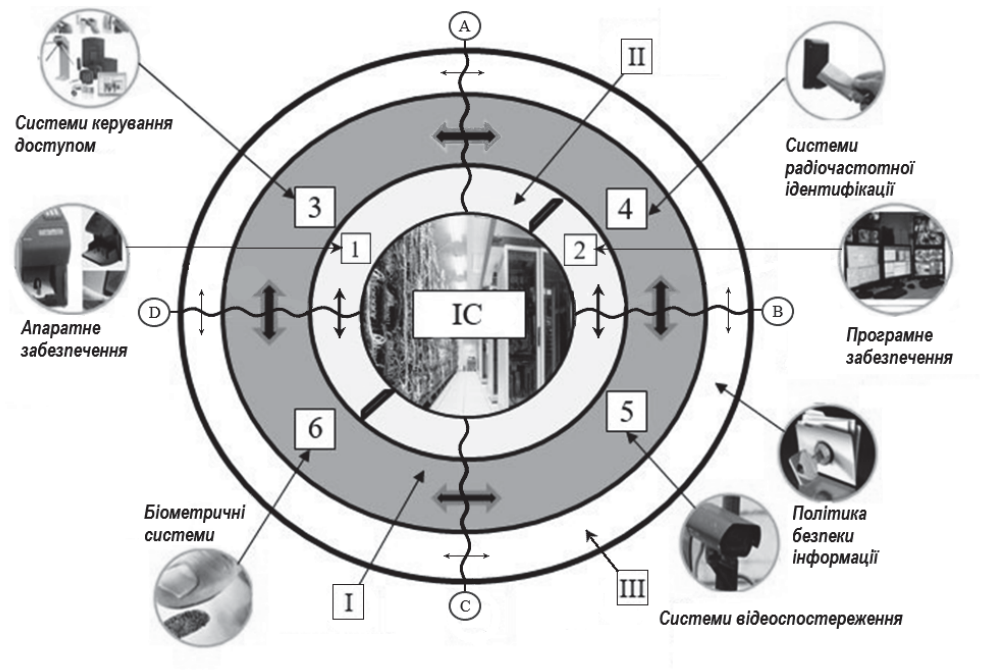

Рис. 1. Багаторівнева модель забезпечення інформаційної безпеки ІС

Таблиця 1

Концепція "об'єкт – загроза – захист": зовнішній рівень моделі безпеки ІС

Загроза	Захист
• Несанкціонований в'їзд /виїзд транспортних засобів на територію, яка знаходиться під охороною; • Відсутність процедури проходження пропускного контролю транспортних засобів; • Відсутність зон санкціонованого доступу; • Несанкціонований доступ (НСД) персоналу і транспорту на об'єкт; • Відсутність засобів обробки подій відповідно до процедури доступу на об'єкт; • НСД до інформації в умовах ремонту апаратури та зі сторони терміналів; • НСД до внутрішніх мереж/ каналів зв'язку; • НСД до технічного обладнання та органів управління; • Збої основної апаратури систем передавання даних; • Відмови систем живлення, систем забезпечення нормальних умов функціонування апаратури та персоналу; • Обхід механізмів захисту об'єкта: псевдосанкціонований доступ порушника.	• Контроль та обмеження доступу; • Захист від несанкціонованого доступу; • Використання власних аварійних електрогенераторів /резервних ліній електроживлення; • Розмежування доступу; • Моніторинг стану приміщень за допомогою автоматизованих робочих місць; • відображенням сигналів тривоги / несправності згідно з планом охорони об'єкта; • Ведення електронного журналу, в якому реєструються дії операторів у стандартних/ нештатних ситуаціях; • Ручне /автоматизоване управління постановкою/ зняттям з охорони за допомогою електронних карт-пропусків; • Використання паролей та ієрархічний розподіл доступу співробітників до функціонування системи; • Створення можливості незалежної роботи в разі порушення зв'язку з сервером або виходу з ладу інформаційних систем.

Внутрішня безпека ІС. У табл. 2 розглянуто технології забезпечення ІБ інформаційних систем на апаратному і програмному рівні згідно з концепцією "об'єкт – загроза – захист".

Таблиця 2

Концепція "об'єкт – загроза – захист": внутрішній рівень моделі безпеки ІС

Об'єкт: Інформаційні системи – рівень апаратно-програмного забезпечення безпеки	
Загроза	1. *Об'єктивні* – залежать від особливостей побудови і технічних характеристик обладнання, застосовуваного в ІС. 1.1. Перехоплення випромінювання технічних засобів: • перехоплення побічного випромінювання елементів технічних засобів, кабельних ліній технічних засобів, випромінювань на частотах функціонування генераторів і підсилювачів; • перехоплення наведень електромагнітних випромінювань; • перехоплення звукових коливань (акустичних, віброакустичних); 1.2. Закладки: • апаратні закладки (встановлені в: технічні засоби, телефонні лінії мережі електроживлення); • програмні закладки (шкідливі програми, технологічні виходи з програм, нелегальні копії програмного забезпечення (ПЗ). 1.3. Перехоплення сигналів електроакустичного перетворення; 1.4. Перехоплення інформації з каналів обміну інформацією (радіоканалів, глобальних інформаційних мереж); 1.5. Незаконне підключення до ліній зв'язку та модифікація потоку даних від давача до комп'ютерної системи. 2. *Суб'єктивні* – залежать від дій співробітників (операторів, адміністраторів). 2.1. Помилки: • при підготовці та використанні ПЗ розробка алгоритмів і ПЗ, інсталяція та завантаження ПЗ, експлуатація ПЗ, введення даних); • при управлінні складними системами (використання можливостей самонавчання систем, організація управління потоками обміну інформації); • при експлуатації технічних засобів (включення / виключеннія технічних засобів, використання засобів обміну інформацією); • при виконанні поставлених задач, які призводять до надсилання з давачів хибних даних. 2.2. Порушення: • режиму експлуатації технічних засобів (енергозабезпечення/ життєзабезпечення); • режиму використання інформації (обробка та обмін інформацією, зберігання/ знищення носіїв інформації); • розкриття шифрів криптозахисту інформації; • режиму конфіденційності ; • режиму опитування давачів; • режиму відбору та модифікація алгоритму обробки даних з давачів; 3. *Випадкові* – залежать від особливостей навколишнього середовища ІС і непередбачених обставин. 3.1. Збої і відмови:

Об'єкт: Інформаційні системи – рівень апаратно-програмного забезпечення безпеки	
	• відмови і несправності технічних засобів (які обробляють інформацію, забезпечують роботоздатність засобів обробки інформації; • старіння і розмагнічування носіїв інформації; • збої ПЗ (операційних систем, прикладних, сервісних програм та антивірусних програм); • збої електропостачання (обладнання обробки інформації; допоміжного обладнання); • помилкові спрацювання давачів; • надходження хибних даних з давачів; • стихійні лиха та аварії; 3.2. Пошкодження: • життєзабезпечуючих комунікацій; • огороджувальних конструкцій. 4. *Цілеспрямовані* – пов'язані з навмисними діями порушника (співробітника, відвідувача, конкурента тощо): ознайомлення з конфіденційною інформацією; • ознайомлення співробітників з інформацією, до якої відсутній доступ; • несанкціоноване копіювання програм і даних; • викрадення носіїв інформації, що містять конфіденційну інформацію; • викрадення роздрукованих документів; • навмисне знищення інформації; • несанкціонована модифікація співробітниками фінансових документів/ звітності/ баз даних; • фальсифікація повідомлень, що передаються каналами зв'язку; • відмова від авторства повідомлення, переданого каналом зв'язку; • відмова від факту отримання інформації; • пошкодження інформації, викликане впливом вірусів; • пошкодження архівної інформації, розміщеної на змінних носіях; • викрадення обладнання ***Технології забезпечення ІБ – апаратне забезпечення*** • контроль доступу до підсистеми керування станцією з боку віддалених терміналів обслуговування; • очищення робочих областей пам'яті ЕОМ після завершення роботи з даними, що захищаються; • облік вихідних друкарських та графічних форм і твердих копій; • контроль цілісності програмної та інформаційної частин системи
Захист	розмежування доступу; • виявлення позаштатних впливів на елементи устаткування, програми, дані і процеси; • реєстрація позаштатних впливів; • ідентифікація і розпізнавання процесів; • введення в дію засобів протидії непередбаченим змінам параметрів середовища експлуатації ІС; • керування засобами нейтралізації позаштатних впливів на параметри середовища експлуатації ІС; • виявлення закладних пристроїв; • реєстрація впливів закладних пристроїв; • нейтралізація/ знешкодження закладних пристроїв;

Об'єкт: Інформаційні системи – рівень апаратно-програмного забезпечення безпеки	
Захист	• виявлення побічного електромагнітного випромінювання і наведення (ПЕМВН) від елементів ІС; • виявлення електромагнітного наведення в елементах ІС; • придушення (ослаблення, екранування) ПЕМВН від елементів ІС; • нейтралізація інформативних складових ПЕМВН від елементів ІС; • нейтралізація електромагнітних наведень в елементах ІС від джерел інформативних випромінювань у зонах розміщення елементів ІС; • моніторинг з метою виявлення перевищень припустимих значень ПЕМВН; • тестування засобів підсистеми захисту від витоку через канали ПЕМВН; • виявлення спроб несанкціонованого впливу на інформацію; ***Технології забезпечення ІБ – програмне забезпечення*** • ізоляція програм, що виконуються в інтересах суб'єкта, від інших суб'єктів; • керування потоками даних і команд з метою запобігання помилкових з'єднань, помилкового надання послуг і відмов в обслуговуванні; • ідентифікація/ аутентифікація суб'єктів; • реєстрація дій суб'єкта та його процесу; • надання можливостей вилучення/ включення нових суб'єктів та об'єктів доступу, а також зміни повноважень суб'єктів; • шифрування інформаційних ресурсів; • контроль цілісності програмної та інформаційної частин засобів захисту від позаштатних впливів; • тестування засобів захисту від позаштатних впливів; • виявлення програмних закладок; • реєстрація впливів програмних закладок; • нейтралізація/ знешкодження програмних закладок; • ідентифікація і виявлення моментів активізації інформаційно уразливих режимів, функцій і послуг; • сигналізація про активний стан інформаційно уразливих режимів, функцій і послуг; • придушення каналів витоку інформації в інформаційно уразливих режимах, функціях і послугах; • аварійне завершення активних процесів; • керування надлишковими ресурсами з метою протидії збоям і відмовам у функціонуванні ІС; • тестування засобів підсистеми захисту від збоїв і відмов; • виявлення спроб несанкціонованого впливу на інформацію; • реєстрація спроб впливу на інформацію; • реакція на спроби несанкціонованих впливів (сигналізація, відмова в доступі, знищення інформації, відновлення після впливів);
Захист	• ідентифікація та аутентифікація суб'єктів доступу; • виявлення фактів реалізації загроз; • реєстрація фактів реалізації загроз; • тестування засобів системи ліквідації наслідків реалізованих загроз.

Серед інструментарію протидії загрозам ІС актуальними є – комплекси та апаратні засоби криптографічного захисту інформації, розроблені Інститутом інформаційних технологій (м. Харків) [8]. Комплекси криптографічного захисту інформації спрямовані на сертифікацію ключів, забезпечення захищеності електронної пошти, захист зберігання даних тощо. Відомі апаратні засаби крипто-

графіного захисту: електронні ключі "Кристал 1", "Алмаз 1К"; криптографічні модулі "Гряда 61", "Гряда 301"; IP-шифратори "Канал-401", шлюзи захисту "Бар'єр – 301" тощо. Державним підприємством "Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості" розроблено алгоритм симетричного блокового шифрування "Калина" за ДСТУ 7624: 2014, який у відповідних режимах забезпечує два профілі безпеки ІС – конфіденційність та цілісність як окремо, так і разом та призначений для поступової заміни криптографічного перетворення за ДСТУ ГОСТ 28147:2009.

Політика безпеки інформації. Керівництво щодо використання багаторівневої моделі інформаційної безпеки ІС, яка забезпечує – конфіденційність, цілісність, доступність інформації на зовнішньому і внутрішньому рівнях, здійснює політика безпеки інформації. Політика безпеки інформації в інформаційній системі – це набір законів, правил, обмежень, рекомендацій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз [9]. Основною перевагою мандатної (багаторівневої) політики безпеки інформації у порівнянні з дискреційною та рольовою політиками безпеки є високий ступінь надійності захисту, оскільки вона передбачає: 1) визначення ступеня конфіденційності інформації; 2) надання кожному об'єктові системи відповідного рівня конфіденційності, що зумовлює ступінь секретності інформації; 3) забезпечення вимог щодо ідентифікації об'єктів і суб'єктів системи та комплексно спрямована на реалізацію алгоритму запобігання витоку інформації від об'єктів, що мають високий рівень доступу, до об'єктів із низьким рівнем доступу (рис. 2) [10].

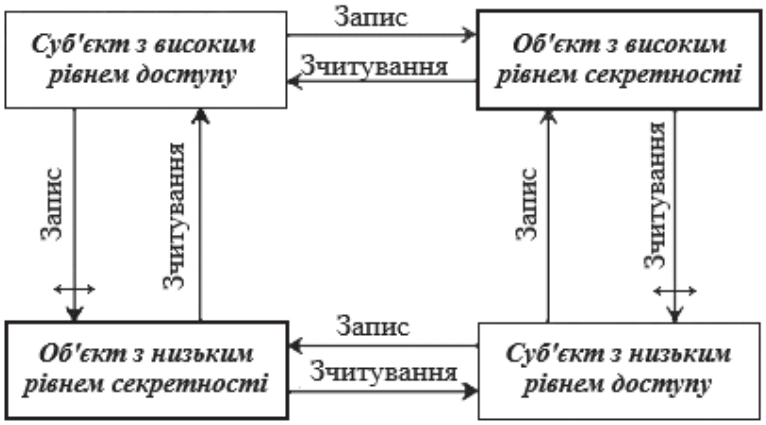

Рис. 2. Модель мандатної політики безпеки

Для реалізації процедур – відбору/збору і обробки даних, управління, підтримки прийняття рішення, забезпечення експертних знань у прикладних задачах контролю технічного стану об'єктів та в прикладних задачах інтелектуалізації промислових об'єктів використовують ІТ на основі функціонування: автоматизованих систем управління, інформаційно-аналітичних систем, систем підтримки прийняття рішення, експертних систем, вимірювальних інформаційних систем. Відповідно, для кожної ІС мандатна політика безпеки інформації є спеціалізованою,

оскільки залежить від: 1) категорії інформаційних ресурсів за ступенем секретності; 2) від комплеску апаратно-програмних засобів реалізації життєвого циклу інформації; 3) профілів безпеки – конфіденційності, цілісності, доступності інформації.

Висновок

У роботі представлено багаторівневу модель ІБ інформаційних систем, яка розгорнута: 1) комплексом засобів безпеки на зовнішньому рівні і технологіями апаратного та програмного забезпечення ІБ на внутрішньому згідно з концепцією "об'єкт – загроза – захист"; 2) мандатною політикою безпеки – розмежування доступу суб'єктів до об'єктів, що дозволяє цілісно забезпечити профілі безпеки ІС у сферах інформатизації та інтелектуалізації об'єктів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про Національну програму інформатизації: Закон України від 4 лютого 1998 року № 74/98-ВР. Остання редакція від 02.12.2012. URL: http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (дата звернення: 01.09.2019).

2. Industry 4.0. Вікіпедія. URL: http://en.wikipedia.org/wiki/Industry_4.0 (дата звернення: 02.09.2019).

3. Проект Концепції інформаційної безпеки України. URL: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf (дата звернення: 01.09.2019).

4. *Дудикевич В.Б., Микитин Г.В., Рудник О.Я.* Функціональна безпека інформаційних технологій: засади, методологія, реалізація. Сучасна спеціальна техніка. 2013. № 1(32). С. 115–125.

5. *Микитин Г.В.* Комплексна система безпеки інформаційних технологій для задач управління проблемними ситуаціями. Сучасна спеціальна техніка. 2014. № 4(39). С. 65–74.

6. *Домарев В.В.* Безопасность информационных технологий. Системный подход. К.: ООО ТИД "Диасофт", 2004. 992 с.

7. *Гарасимчук О.І., Дудикевич В.Б., Ромака В.А.* Комплексні системи санкціонованого доступу: навч. посібник. Львів: Видавництво Львівської політехніки, 2010. 212 с.

8. Комплекси та засоби захисту інформації. URL: https://iit.com.ua/products (дата звернення: 02.09.2019).

9. НД ТЗІ 1.1-002-99. Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу – ДСТСЗІ СБ України. Київ, 1999. 14 с.

10. Політика інформаційної безпеки / Голубенко О.Л. та ін. Луганськ: Вид. СНУ ім. В. Даля, 2009. 300 с.

REFERENCES

1. Zakon Ukrainy "Pro Natsionalnu Prohramu Informatyzatsii" № 74/98-VR. Law of Ukraine "On National Program of Informatization" № 74/98-VR". URL: http://zakon4.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80 (date of application: 01.09.2019) [in Ukrainian].

2. Industry 4.0. Wikipedia, URL: http://en.wikipedia.org/wiki/Industry_4.0 (date of application: 02.09.2019) [in English].

3. Proekt Kontseptsii Informatsiinoi Bezpeky Ukrainy. "Draft Concept of Ukraine Information Security". URL: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf (date of application: 01.09.2019) [in Ukrainian].

4. *Dudykevych V.B., Mykytyn H.V., Rudnyk O.Ya.* (2013). "Funktsionalna Bezpeka Informatsiinykh Tekhnolohii: zasady, metodolohiia, realizatsiia. [Functional Security of Information Technologies: principles, methodology, implementation], Modern Special Technics, No. 1(32), P. 115–125 [in Ukrainian].

5. *Mykytyn H.V* (2014). Kompleksna systema bezpeky informatsiinykh tekhnolohii dlia zadach upravlinnia problemnymy sytuatsiiamy. "Integrated Information Security System for Problem Situation Management", Modern Special Technics, No. 4(39), P. 65–74 [in Ukrainian].

6. *Domarev V.V* (2004). Bezopasnost informatsionnykh tekhnologiy. Sistemnyy podkhod. "Security of Informaton Technologies: System Concept". K.: OOO "Diasoft", 992 p. [in Russian].

7. *Harasymchuk O.I., Dudykevych V.B., Romaka V.A.* (2010), Kompleksni systemy sanktsionovanoho dostupu: navch. Posibnyk. "Integrated systems of Authorized Access", training manual. Vydavnytstvo Lvivskoi Politekhniky, Lviv, 212 p. [in Ukrainian].

8. Kompleksy ta zasoby zakhystu informatsii. "Information security systems and complexes", URL: https://iit.com.ua/products. (date of application: 02.09.2019) [in Ukrainian].

9. ND TZI 1.1-002-99. Zahalni Polozhennia Shchodo Zakhystu Informatsii V Kompiuternykh Systemakh Vid Nesanktsionovanoho Dostupuiu, DSTZI. RD ITS 1.1-002-99. "General provisions for information security in computer systems from unauthorized access", DSTSIP of SSU" 1999. Kyiv, 14 p. [in Ukrainian].

10. *Holubenko O.L. Khoroshko V.O. Petrov O.S. Holovan S.M. Yaremchuk Yu.Ye.* (2009). Polityka Informatsiinoi Bezpeky. "Information Security Policy", Vyd. SNU V. Dalia, 300 p. [in Ukrainian].

UDC 004.056

Dudykevych Valerii,
Doctor of Technical Sciences, Professor,
Head of the Department
of Lviv Polytechnic National University,
Lviv, Ukraine,
ORCID ID 0000-0001-8827-9920,
Mykytyn Halyna,
Doctor of Technical Sciences, Full Professor,
Professor at the Department
of Lviv Polytechnic National University,
Lviv, Ukraine,
ORCID ID 0000-0003-4275-8285

MULTI-LEVEL SECURITY OF INFORMATION SYSTEMS

Multi-level Information Security (infosec) model of Information Systems (IS) is made of three levels: external, internal and mandatory security policy. External and internal security levels are based on conception "object – threat – protection". Among the IS external security threats: the absence of zones of authorized access, unauthorized access (UAA) in the equipment repair mode, hardware and power supply failures. To protect information on IS external level are used: access control systems, radio frequency identification systems, closed circuit television, biometric systems that provides: access control and restriction, monitoring of buildings and rooms by using workstations, usage of passwords and employees' access sharing , biometric protection against UAA. The threats of internal IS was considered: objective, subjective, casual, purposeful. Among the casual threats to IS security: failures and malfunctions of hardware, power supply failures, sensor glitches etc. Purposeful threats are based on offender's behavior model and lead to leakage of confidential data, its unauthorized modification and its purposeful destruction. Technologies of providing infosec on hardware and software IS

levels were presented. The infosec hardware levels provides: detection of tap devices, suppression of side electromagnetic radiation and interference etc. The infosec software level provides: subject identification/authentication, encryption of information resources, detecting software taps etc. Mandatory security policy provides a high level of information protection security due to the algorithm of countering information leakage from high-access objects to low-access objects. Multi-level IS security model is universal-designed and can be modified for informatization tasks and intellectualization of public infra-structure objects in the area of providing security infosec.

Keywords: information system, information security, multi-level model, conception "object – threat – protection", technologies.

Отримано 17.10.2019