УДК 004;621.391

Хлапонін Юрій Іванович
Доктор технічних наук, старший науковий співробітник кафедри кібернетичної безпеки та комп'ютерної інженерії, *orcid.org/0000-0002-9287-0817*
Київський національний університет будівництва і архітектури, Київ
Шабала Євгенія Євгенівна
Кандидат технічних наук, доцент кафедри кібернетичної безпеки та комп'ютерної інженерії, *orcid.org/0000-0002-0428-9273*
Київський національний університет будівництва і архітектури, Київ
Бойко Олексій Віталійович
Студент магістратури кафедри кібернетичної безпеки та комп'ютерної інженерії за спеціальністю «125-Кібербезпека», *orcid.org/0000-0003-4552-5348*
Київський національний університет будівництва і архітектури, Київ
Бондаренко Богдан Олегович
Студент магістратури кафедри кібернетичної безпеки та комп'ютерної інженерії за спеціальністю «125-Кібербезпека», *orcid.org/0000-0001-6340-1897*
Київський національний університет будівництва і архітектури, Київ

ПОБУДОВА КОМПЛЕКСНИХ СИСТЕМ ЗАХИСТУ ДЛЯ ГРОМАДСЬКИХ ІНФОРМАЦІЙНИХ СИСТЕМ УПРАВЛІННЯ

Анотація. *Запропоновано єдиний стандартизований підхід до побудови комплексних систем захисту інформації для громадських інформаційних систем управління, на базі обґрунтованого визначення цінності інформації в системі, а також структуризації як самих інформаційних систем, так і можливих загроз та шляхів їх реалізації. Найефективнішим інструментом вирішення поставленої задачі є розвиток нормативної бази для структуризації громадських інформаційних систем за цінністю даних та обумовленим до них доступом. Така нормативна база значно спростить оцінку ризиків для кожної такої системи з метою вибору найефективніших з точки зору «ціна-якість» програмно-технічних засобів захисту інформації.*

Ключові слова: інформаційна система; захист інформації; комплексна система; модель порушника; загроза; ризик; мережеві канали зв'язку

Актуальність та аналіз проблеми

У XXI столітті світова спільнота перейшла на новий рівень розвитку – суспільство інформаційне. Будь-яка інформаційна система в умовах сучасного ступеня інформатизації суспільства України перетворюється на громадську інформаційну систему управління, тобто організовану мережу соціальних структур, оснащену засобами для виробництва, комплектування, обробки та зберігання значущої для даної системи інформації. Для ефективного використання наявних у суспільства інформаційних ресурсів необхідною умовою є забезпечення належної безпеки даних, які зберігаються, опрацьовуються та надаються системою, на рівні, необхідному для оновлення та розвитку системи [1].

У цьому сенсі збереження, розвиток та раціональне використання інформаційних ресурсів набуває величезної ваги.

Мету, задачі, основні напрями, етапи, базові принципи та цілі інформатизації в Україні визначає «Стратегія розвитку інформаційного суспільства в Україні» [2]. 14 січня 2016 р. на прес-конференції президент України П. Порошенко зазначив, що найбільш важливими вважає податкову реформу та реформу системи охорони здоров'я. Важливою умовою таких реформ визнано створення єдиного інформаційного простору.

Роль громадських інформаційних систем управління невпинно зростає в усіх сферах життєдіяльності України. Впроваджуються системи автоматизації державних організацій, комунальних підприємств, закладів освіти та медицини. Підвищення рівня інформатизації усіх сфер діяльності потребує вдосконалення процесів збереження якості, забезпечення безпеки інформації, розроблення дієвих методик управління інформаційними ресурсами. На сьогодні спостерігається певна невизначеність саме в області

комплексного захисту інформації в громадських інформаційних ресурсах:

– нормативно-правова база, що регулює сферу захисту даних та інформаційної власності, не містить чітких положень щодо регулювання захисту та моніторингу громадських інформаційних систем управління;

– відсутні сучасні стандарти ідентифікації, аутентифікації та цифрового підпису користувачів інформаційної системи;

– недостатньо розвинено інфраструктуру та апаратно-програмне забезпечення на різних рівнях суспільства та державних структур в цілому;

– низький рівень готовності суб'єктів інформаційного простору до запровадження громадських інформаційних систем управління [3].

Мета статті

Метою науково-дослідницької роботи, коротка характеристика якої представлена в даній статті, є дослідження сучасних алгоритмів і методів побудови комплексних систем захисту інформації у великих системах та аналіз можливостей їх застосування в громадських інформаційних системах управління. Першочерговим завданням визначено розв'язання проблеми забезпечення та оптимізації компромісу між двома пріоритетними вимогами – потребою прозорості та доступності для всіх користувачів єдиної інформаційної моделі, з одного боку, і гарантією цілісності та захищеності даних. Забезпечення відповідного рівня інформаційної та кібернетичної безпеки, з іншого боку. При цьому мають бути гарантовані: повна свобода доступу широкого кола користувачів системи та незалежність їх роботи в межах наданих прав і повноважень.

У процесі аналізу було визначено основні принципи та вимоги до побудови комплексної системи захисту інформації в громадських інформаційних системах управління, проведено порівняльний аналіз найбільш поширених програмно-технічних методів захисту даних; проведено аналіз існуючих систем оцінки ризиків, які б дозволили забезпечити постійний моніторинг інформаційних систем, їх ресурсів, загроз та своєчасно визначати вразливі місця, досліджена законодавча база захисту даних в Україні.

Виклад основного матеріалу

Загальні принципи функціонування громадських інформаційних систем управління визначено Законами України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Національну систему конфіденційного зв'язку», «Про захист інформації в інформаційно-телекомунікаційних системах», постановою Кабінету Міністрів України від 29 березня 2006 року № 373 «Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [4].

Комплексна система захисту інформації складається з організаційних та інженерно-технічних заходів. Щодо інженерно-технічних заходів, то це сукупність спеціальних програмно-технічних засобів захисту інформації. Вибір інженерно-технічних засобів залежить від класу ресурсу та визначеного необхідного рівня захищеності інформації [5].

Оскільки фізично неможливо і недоцільно захищати усі наявні дані в різноманітних інформаційних системах, на першому етапі дослідження було виконано розподілення громадських інформаційних систем за рівнем «цінності» даних, що потребують захисту [6]. Закон України «Про інформацію» класифікує всю інформацію за режимом доступу [7]:

– відкрита;

– з обмеженим доступом (персональні дані, таємниця слідства та судочинства, службова таємниця, професійні види таємниць, комерційна таємниця, авторська таємниця);

– секретна (державна таємниця).

Зрозуміло, що інформація, яка зберігається та оброблюється в громадських інформаційних системах управління може належати за своєю цінністю, як до відкритої, так і до конфіденційної, тобто набувати якостей інформації з обмеженим доступом [8].

Система комплексної безпеки інформаційної системи управління призначена для вирішення таких завдань:

– визначення цілей захисту, інакше кажучи, «кого або що захищати»;

– визначення і оцінка загроз, інакше кажучи, «від чого захищати»;

– визначення і реалізація адекватних заходів захисту, інакше кажучи, «чим і як захищати».

Загрози для ресурсів збереження, передачі та обробки інформації, їх вразливість і ймовірність виникнення загроз, а також можливий збиток, визначаються шляхом оцінки ризиків. Єдиного підходу не існує. Оцінюючи ризик здійснення загроз, ми враховували специфіку конкретних інформаційних систем. Для проведення аналізу вразливостей було створено моделі каналів витоку інформації і несанкціонованого доступу (так звана «модель порушника») та визначено ймовірності інформаційного контакту. У даному дослідженні було виконано комплексну оцінку за допомогою використання графічних і математичних методів [10].

Комбінуючи зазначені методи оцінки ризику, можна представити «модель порушника» для кожної

з наявних громадських інформаційних систем управління. «Модель порушника» зазвичай відображає теоретичні та практичні знання, навички і ресурси, необхідні для здійснення загрози. Щодо технічного забезпечення і використовуваних методів порушники поділяються на «пасивних» (використовують засоби перехоплення даних без модифікації компонентів системи), «внутрішніх» (використовують тільки штатні засоби та недоліки системи захисту, виконують несанкціоновані дії з використанням дозволених засобів) та «активних» (застосовують методи і засоби активного впливу: підключення додаткових технічних засобів, підключення до каналів передачі даних, впровадження програмних і спеціальних інструментальних програм) [10; 11]. В загальному вигляді модель порушника зображено на рисунку.

Проаналізувавши «модель порушника», можна визначити вимоги до системи захисту від кожного виду загрози [10].

Відповідно на кожному з рівнів загрози виділяються об'єкти захисту. Для цього інформаційну систему необхідно розділити на чотири рівні:

– зовнішній рівень характеризується інформаційними, переважно мережевими, сервісами. На цьому рівні повинні відсікатися спроби зовнішнього несанкціонованого доступу до даних та різноманітних атак з метою виведення з ладу мережевих сервісів;

– мережевий рівень повинен забезпечувати перевірку автентичності користувачів і розмежування доступу до ресурсів мережі (ідентифікація, аутентифікація і авторизація);

– системний рівень пов'язаний з управлінням доступом до ресурсів операційної системи серверу збереження та обробки інформації;

– рівень додатків пов'язаний з використанням прикладних ресурсів.

Для певних інформаційних систем управління, наприклад, систем з відкритою інформацією, найбільший ризик становлять зовнішні навмисні атаки з метою виведення з ладу мережевої доступності інформації. Для систем управління, що включають збирання та обробку персональних даних, наприклад, системи інформатизації медичної сфери, до високих ризиків загроз зовнішнім та мережевим сервісам додаються не менш високі ризики загроз цілісності та адекватності даних. Це викликає необхідність розробки алгоритмів контролю доступу. Наприклад, впроваджувана в Україні модель громадської медичної інформаційної системи викликає здивування в частині контролю доступу, а саме ідентифікації, аутентифікації та авторизації, оскільки ідентифікація виконується за номером мобільного телефону, а авторизація шляхом введення чотирьох цифр, отриманих в СМС-повідомленні на відповідний номер. На наш погляд для системи такого рівня це дуже вразливий алгоритм.

Для забезпечення комплексного захисту в громадських інформаційних системах управління, що збирають та обробляють персональні дані, необхідно забезпечувати повний комплекс програмно-технічних методів захисту [10 – 12]:

– засоби захисту кабельної системи. Найкращим способом попередити збої в кабельних мережах є побудова структурованої кабельної системи. Це означає, що кабельна система мережі серверів накопичення та обробки даних повинна бути розподілена на кілька рівнів з різним призначенням;

– на серверах накопичення та обробки даних мають бути наявні засоби архівації та дублювання інформації. Доцільно організувати виділений спеціалізований сервер для архівації даних. Архівну інформацію слід зберігати у спеціальному приміщенні, що охороняється;

– із розповсюдженням мобільних пристроїв та доступу мобільними каналами зв'язку, наприклад, WI-FI, доцільно використовувати шифрування каналу доступу шляхом обміну сеансовими ключами;

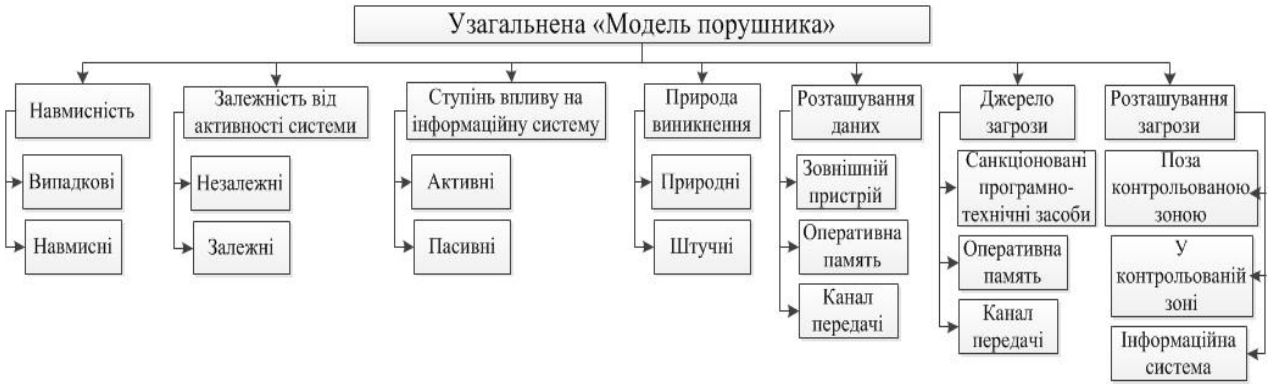

Рисунок – Узагальнена «Модель порушника»

– програмні засоби захисту, що забезпечують ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів згідно з повноваженнями користувачів, реєстрацію подій в інформаційних системах, криптографічний захист інформації, захист систем управління базами даних, захист від комп'ютерних вірусів мають бути наявні в усіх громадських інформаційних системах управління, що виконують обробку персональних даних.

Програмні засоби захисту даних пропонується розподілити таким чином [12; 13]:

– підсистема антивірусного захисту розміщується для контролю шлюзів входу/виходу в мережу Інтернет, шлюзів входу/виходу між доменами, окремо має бути підсистема, що частково або повністю буде забезпечувати логування дій користувачів;

– підсистема управління контролем доступу та ідентифікацією в інформаційній системі. Найбільш оптимальною для громадських інформаційних систем управління є двофакторна аутентифікація. У громадських системах управління в Україні, в кращому випадку, використовуються сьогодні ім'я користувача і пароль. Але в сучасному світі така аутентифікація не забезпечує достатнього захисту [11; 16]. Актуальним методом аутентифікації для таких систем є система додаткового PIN-коду з функцією маршруту, щоб змушувати людей переміщувати дані тільки по певних маршрутах, так зване створення логічних зон;

– підсистема криптографічного захисту завдяки шифруванню даних на сьогодні використовується лише в системах громадського управління таких як, інформаційна система ДФС, системи електронних платежів. Однак, в інформаційній системі управління в медицині на певних рівнях було б також доцільно використовувати хоча б не складний криптографічний захист;

– на рівні серверів, що накопичують та обробляють персональні дані, необхідна підсистема забезпечення цілісності даних, що буде забезпечувати управління зберіганням та резервним копіюванням даних;

– підсистема виявлення вторгнень і спроб несанкціонованого доступу, що забезпечує реалізацію захисних заходів з протидії атакам, має бути на дуже високому рівні, оскільки атака може бути здійснена в тому числі одним із зареєстрованих користувачів системи, який мав час на віддалене вивчення всіх недоліків системи [11].

Для захисту інформації, що передається різноманітними каналами зв'язку можуть використовуватися скремблери і шифратори, які захищають канали шляхом частотно-тимчасових перестановок зі змінним вікном. Ряд відомих у світі фірм випускає криптографічні пристрої орієнтовані на роботу в мережах, наприклад, шифратор ScaNet фірми Dowty Network Systems (Великобританія), шифратор Datacryptor-64 фірми Racal Datacom (США) для користувачів мережі з пакетною комутацією по протоколу X.25 МККТТ. Фірма Xerox (США) створила блок високоякісного шифрування даних Xerox Encription Unit, що забезпечує захист особливо секретної інформації, в локальній мережі. Фірма Calmes Semiconductor Inc. (США) виробляє криптопроцесори CL34C168 для блокового шифрування на швидкості до 300 Кбіт/с. За останній час запропоновані нові алгоритми шифрування, наприклад NEWDES і FEAL, розраховані на шифрування потоків зі швидкостями до 1 Гбіт/с. Все більшого поширення на ринку програмно-апаратних засобів захисту інформації набувають системи запобігання несанкціонованому копіюванню типу «HASP – ключів».

Висновок

Не дивлячись на те, що останнім часом в Україні велика увага приділяється розвитку нормативно-правової бази для захисту інформації, все ж залишається проблема дисбалансу між стрімким розвитком інформатизації громадських сфер діяльності та відсутністю єдиного системного підходу з точки зору нормативних документів, які б регламентували застосування методів технічного та криптографічного захисту інформації в таких системах. Систематизувати громадські інформаційні системи управління для регламентації необхідних рівнів захисту ми пропонуємо таким чином:

1. Громадські інформаційні системи з відкритою інформацією. Прикладом такої системи можуть бути системи законодавчої та нормативної документації. Найвищий рівень захисту має бути забезпечено на рівні серверів зберігання. На рівні доступу має бути забезпечено відкритий доступ з високим контролем і відсіканням спроб модифікації чи знищення. Для досягнення зазначеного рівня безпеки в даному випадку доцільно використовувати доменне розмежування із застосуванням засобів міжмережевих екранів.

2. Громадські інформаційні системи збирання та обробки персональних даних. Прикладом такої системи може бути громадська інформаційна система в медицині. Для уніфікації та захисту користувацького доступу в таких системах необхідно

реалізувати двофакторну аутентифікацію користувачів. Для успішної реалізації відповідного рівня захисту також необхідно забезпечити матеріально-технічну базу з реалізацією політик безпеки. Для захищеного обміну інформацією в таких системах доцільно використовувати стандарти DICOM. Сервери збереження даних мають бути захищені за найвищим рівнем безпеки, що має вміщувати повний комплекс технічних та програмних засобів захисту, а також розміщуватись у спеціальних режимних приміщеннях.

3. Громадські інформаційні системи наукової та інтелектуальної власності. Прикладом такої системи може бути база досліджень та наукова бібліотека вищого навчального закладу. Для інформаційних систем даного класу додатково потрібно мати систему розбиття даних на різні рівні доступу. Додатково до заходів зазначених в попередніх пунктах має бути розроблено програмно-технічні засоби ідентифікації користувача при отриманні доступу до інформації певного рівня.

4. Громадські інформаційні системи державної та фінансової звітності. Прикладом такої системи може бути інформаційно-довідкова система ДФС України. На сьогодні системи цієї групи є найбільш захищеними відповідно до визначених вимог. Однак, як будь-яка інформаційна система з клієнт-серверною архітектурою, системи цього класу найбільше потребують розробки стандартів та процесів тестування використовуваного програмного забезпечення на стійкість до атак за допомогою програмних експлонтів та захисту від внутрішніх загроз.

Впровадження комплексних систем захисту в громадських інформаційних системах управління заслуговує на велику увагу, оскільки є однією з магістральних передумов успішної реалізації пріоритетних напрямів розвитку українського суспільства в інформаційному світі.

Список літератури

1. Горовий В. Формування інформаційної системи як принцип організації інформаційної діяльності в умовах глобалізації / В. Горовий. – Режим доступу: http://nbuviap.gov.ua

2. Стратегія розвитку інформаційного суспільства в Україні, схвалена розпорядженням Кабінету Міністрів України від 15 травня 2013 р. за № 386-р. – Режим доступу: http://zakon.rada.gov.ua/laws/show/386-2013-р.

3. Інформатизація в Україні: основні тенденції та проблеми / Наукові записки КНТУ, вип.11, ч.1, 2011.

4. Березовська І.Р. Адміністративно-правові засоби забезпечення інформаційної безпеки. Юридичний вісник України: 1 (34) 2015, автореф. дис.канд. юрид. наук: 12.00.07 / І. Р. Березовська; Нац. акад. внутрішніх справ. – К., 2012. – 18 с.

5. Литвинюк А.А. Основи інформаційної безпеки. Комплексна система захисту інформації: структура, встановлення та підтримка функціонування / А.А. Литвинюк. – [Електронний ресурс]. – Режим доступу: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

6. Інформаційна безпека: навчальний посібник / С. В. Кавун, В. В. Носов, О. В. Манжай. – Харків: Вид. ХНЕУ. 352 с.

7. Закон України «Про інформацію» – Режим доступу: http://zakon2.rada.gov.ua/laws/show/2657-12

8. Закон України «Про доступ до публічної інформації» – Режим доступу: http://search.ligazakon.ua/l_doc2.nsf/link1/T112939.html

9. BS ISO/IEC 27001:2005BS 7799-2:2005 Режим доступу: http://iso-management.com/wp-content/uploads/2013/12/ISO-27001.pdf

10. Курило А. П. Аудит информационной безопасности / А. П. Курило, С. Л. Зефиров, В. Б. Голованов и др. – М. : Издательская группа «БДЦ-пресс», 2006. – 304 с.

11. Бирюков А.А. Информационная безопасность: защита и нападение. – 2-е изд. – М: ДМК Пресс, 2017. – 434 с.

12. Петренко С. А. Политика безопасности компании при работе в Интернет / С.А. Петренко, В.А. Курбатов. – 2011. – М.: ДМК Пресс. – 400 с.

13. Петренко С.А., Петренко А.А. Аудит безопасности интернет. – М.: ДМК Пресс, 2002-416 с.

14. Електронний ресурс – ITDom. Режим доступу: http://www.itdom.info/Bezpeka.

15. Електронний ресурс – Режим доступу: http://pidruchniki.com/zahist_informatsiyi_informatsiynih_sistemah.

16. Alan Calder & Steve Watkins. Information Security Risk Management for ISO 27001/ISO 17799. – IT Governance Publishing, 2007.

Стаття надійшла до редколегії 23.04.2018

Рецензент: д-р техн. наук, проф. В.М. Міхайленко, Київський національний університет будівництва і архітектури, Київ.

Хлапонин Юрий Иванович
Доктор технических наук, старший научный сотрудник кафедры кибернетической безопасности и компьютерной инженерии, *orcid.org/0000-0002-9287-0817*
Киевский национальный университет строительства и архитектуры, Киев
Шабала Евгения Евгеньевна
Кандидат технических наук, доцент кафедры кибернетической безопасности и компьютерной инженерии, *orcid.org/0000-0002-0428-9273*
Киевский национальный университет строительства и архитектуры, Киев
Бойко Алексей Витальевич
Студент магистратуры кафедры кибернетической безопасности и компьютерной инженерии «125-Кібербезпека», *orcid.org/0000-0003-4552-5348*
Киевский национальный университет строительства и архитектуры, Киев
Бондаренко Богдан Олегович
Студент магистратуры кафедры кибернетической безопасности и компьютерной инженерии «125-Кібербезпека», *orcid.org/0000-0001-6340-1897*
Киевский национальный университет строительства и архитектуры, Киев

ПОСТРОЕНИЕ КОМПЛЕКСНЫХ СИСТЕМ ЗАЩИТЫ ДЛЯ ПУБЛИЧНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ УПРАВЛЕНИЯ

Аннотация. *Разработан единый стандартизированный подход к построению комплексных систем защиты информации для публичных информационных систем управления на базе обоснованного определения ценности информации в системе, а также структуризации как самих информационных систем, так и возможных угроз и путей их реализации.В качестве примера современных публичных систем управления взята современная украинская система МОЗ. В ходе анализа установлено, что современные информационные системы предназаченные для публичных целей, находятся на низком уровне защищенности от угроз информационного общества и нуждаются в улучшении своих систем защиты. Это диктует необходимость внедрения качественных комплексных систем защиты для публичных информационных систем управления с целью сохранности и конфиденциальности электронных данных. Наиболее эффективным инструментом решения поставленной задачи является развитие нормативной базы для структуризации общественных информационных систем по ценности данных и обусловленным к ним доступом. Такая нормативная база значительно упростит оценку рисков для каждой такой системы с целью выбора наиболее эффективных с точки зрения «цена-качество» программно-технических средств защиты информации. Это позволит определить необходимые системы защиты, при успешном внедрении которых защищенные системы будут выведены на новый уровень защищенности от угроз современного информационного общества.*

Ключевые слова: информационная система; ***защита информации***; ***комплексная система***; ***модель нарушителя***; ***угроза***; ***риск***; ***сетевые каналы связи***

Khlaponin Yurii
Ph.D., major professor, Department of cyber security and Computer Engineering, *orcid.org/0000-0002-9287-0817*
Kyiv National University of Construction and Architecture, Kyiv
Shabala Yevheniia
Ph.D., associate professor, Department of cyber security and Computer Engineering, *orcid.org/0000-0002-0428-9273*
Kyiv National University of Construction and Architecture, Kyiv
Boiko Oleksii
Master level student at the department of cyber security and Computer Engineering of the majority "125-Cybersecurity", *orcid.org/0000-0003-4552-5348*
Kyiv National University of Construction and Architecture, Kyiv
Bohdan Bondarenko
Master level student at the department of cyber security and Computer Engineering of the majority "125-Cybersecurity", *orcid.org/*0000-0001-6340-1897
Kyiv National University of Construction and Architecture, Kyiv

ENGINEERING OF COMPLEX SECURITY SYSTEM FOR PUBLIC INFORMATION MANAGEMENT SYSTEMS

Abstract. *The aim of the research is development of the solely standardized approach to solving the problem of building complex information security systems for public information management systems on the basis of a justified definition of the value of information in the system, the structuring of both the information systems themselves, and the possible threats and ways to implement them. As an example of modern public management systems, a modern Ukrainian MHI system was adopted. The most effective tool for solving the task is the need to develop a regulatory framework for the structuring of public information systems on the value of data and the intended of access. In turn, such a regulatory framework will greatly simplify the risk assessment for*

each such system with the purpose of selecting the most effective software and hardware means of information protection from the point of view of "price-quality".This will allow us to determine the necessary protection systems for each type of such systems, which, with the successful introduction of protection systems, will bring these systems to a new level of protection from the threats of the modern information society.

Keywords: information system; information security; complex system; violator model; threat; risk; network communication channels

References

1. Horovyi, V. Formation of the information system as a principle of organization of information activities in the conditions of globalization. – Access mode: http://nbuviap.gov.ua.

2. «Strategy of the Information Society Development in Ukraine», approved by The order of the Cabinet of Ministers of Ukraine from 15 May 2013 № 386-p. – Access mode: http://zakon.rada.gov.ua/laws/show/386-2013-p.

3. Informatization in Ukraine: main trends and problems. (2011). Scientific notes KNTU, 11, p.1.

4. Berezivska, I.R. (2012). Administrative and legal means of ensuring information security. Legal Bulletin of Ukraine: 1 (34) 2015, dissertation abstr.: 12.00.07 / I.R. Berezivska; National Academy of Internal Affairs. – K., 2012. – 18.

5. Litvinyuk, A.A. (2008). Fundamentals of Information Security. Complex information security system: structure, installation and support of the functionality. // A.A. Litvinyuk. – Access mode: http://www.cvk.gov.ua/visnyk/pdf/2008_4/visnik_st_08.pdf

6. Kavun, S.V., NOSOV, V.V., Manjie, O.V. Information security. Tutorial manual. Kharkiv: PH. KNEU. 352.

7. Law of Ukraine «About information» – Access mode: http://zakon2.rada.gov.ua/laws/show/2657-12;

8. Law of Ukraine «About access to public information» – Access mode: http://search.ligazakon.ua/l_doc2.nsf/link1/T112939.html;

9. BS ISO/IEC 27001:2005BS 7799-2:2005 Access mode: http://iso-management.com/wp-content/uploads/2013/12/ISO-27001.pdf;

10. Kurilo, A P. (2006). Information Security Audit / A. P. Kurilo, S.L. Zefirov, V.B. Golovanov &others // Moscow, Russia: Publishing group "BDC-press", 304.

11. Biryukov, A.A. (2017). Information security: protection and attack. – 2-d ed. Moscow, Russia: DMK Press, 434.

12. Petrenko, S.A., Kurbatov, V.A. (2011). The company's security policy when working on the Internet. Moscow, Russia: DMK Press, 400.

13. Petrenko, S.A., Petrenko, A.A. (2002). Internet Security Audit. Moscow, Russia: DMK Press, 416.

14. Electronic resource – ITDom. Access mode: http://www.itdom.info/Bezpeka;

15. Electronic resource – Access mode: http://pidruchniki.com/zahist_informatsiyi_informatsiynih_sistemah;

16. Calder, Alan & Watkins, Steve. (2007). Information Security Risk Management for ISO 27001/ISO 17799. IT Governance Publishing.

Посилання на статтю

APA *Khlaponin, Yu., Shabala, Ye. &Boiko, O. (2018). Engineering of complex security system for public information management systems. Management of Development of Complex Systems, 34, 104 – 110.*

ДСТУ *Хлапонін Ю.І. Побудова комплексних систем захисту для громадських інформаційних систем управління [Текст] / Ю.І. Хлапонін, Є.Є. Шабала, О.В. Бойко, Б.О. Бондаренко // Управління розвитком складних систем. – 2018. – № 34. – С. 104 – 110.*