Кібернетична безпека

УДК 004.056

Л.М. Дегтярьова, В.Г. Ляшевський

Полтавський національний технічний університет імені Юрія Кондратюка, Полтава

ПРАКТИЧНІ ПРИЙОМИ ТА КЕРІВНІ ПРИНЦИПИ РОЗРОБКИ КОМПЛЕКСІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті розглянуті результати порівняльного аналізу розвитку концепції інформаційної безпеки автоматизованих систем, використання сучасних інтелектуальних технологій в сфері інформаційної безпеки. Показано, що втілення принципів науковості і професіоналізму та використання сучасних тенденцій у практичній складовій забезпечення інформаційної безпеки сприяє зміцненню принципів інформаційної безпеки.

***Ключові слова**: інформаційна безпека, автоматизована інформаційна система, несанкціонований доступ, конфіденційність інформації, інформаційні загроз, інтелектуальні мультиагентні технології.*

Вступ

Наявність великої кількості критично важливої для підприємств та організацій інформації, що зберігається і обробляється в комп'ютерних системах, призвела до створення єдиної інфраструктури. Її використання дозволяє отримати доступ до інформації найбільших бібліотек і світових баз даних, оперативно виконувати складні розрахунки, швидко обмінюватися інформацією з іншими респондентами мережі незалежно від їх віддаленості один від одного – в межах міста, країни або світу. Така кількість точок доступу у значній мірі підвищує загрозу інформаційній безпеці обробки і передачі даних. Особливо вразливими виявляються дані, що передаються в глобальних телекомунікаційних мережах.

В даний час вже неможливо уявити сучасну організацію без застосування новітніх інформаційних технологій. Їх застосування – від автоматизації окремих робочих місць і до побудови корпоративних розподілених інформаційних систем. Але в той же час, розвиток мереж, їх ускладнення, взаємна інтеграція призводять до появи якісно нових загроз, збільшення кількості кіберзлочинців, які мають потенційну можливість порушувати стабільність роботи системи.

В результаті дослідження історії питання були проаналізовані погляди вчених з вітчизняної [1 – 7] та зарубіжної літератури [13 – 17] на систему інформаційної безпеки. Даний аналіз проблеми інформаційної безпеки українських і зарубіжних дослідників дозволив з'ясувати загальні тенденції розвитку системи інформаційної безпеки та виявити сучасні тенденції у створенні дієвих комплексів інформаційної безпеки.

Виклад основного матеріалу

Успіх діяльності сучасного підприємства/організації та її розвиток за умов гострої конкуренції значною мірою залежить від застосування інформаційних технологій, і, відповідно, від рівня інформаційної безпеки, яка запобігає як незаконному втручанню в інформаційні ресурси інформаційної системи, так і перешкоджає витоку конфіденційних персональних даних (особисті справи працівників, трудові договори, зміст регістрів бухгалтерського обліку, і внутрішньої бухгалтерської звітності), наявних в інформаційних системах.

Серед пріоритетів, які визначені для систем управління інформаційною безпекою сучасного бізнес-процесу це:

стабільність бізнесу;

захист інтересів власників;

підвищення рівня довіри клієнтів (партнерів).

Головною ціллю будь-якої системи інформаційної безпеки є забезпечення коректної та безперебійної роботи об’єкта, що охороняється, запобігання можливих фінансових втрат через загрози безпеки, розголошення таємниць бизнес-процесів, спотворення і руйнування службової інформації. Іншою ціллю можна вважати забезпечення якості послуг і гарантій безпеки інтересів як власників інформаційних ресурсів так і їх клієнтів, гарантування обопільної конфіденційності даних. Встановлена ступінь конфіденційності інформації, як правило, зберігається при її обробці в інформаційних системах і при передачі по телекомунікаційних мережах.

Для того, щоб вищезгадані цілі були досягнуті, необхідно вирішити деякі завдання:

обмежити доступ до інформації, визначеної як службова таємниця;

визначити та здійснити адміністративні заходи для виявлення загроз безпеці інформаційних ресурсів;

з’ясувати можливі мотиви, що мають на меті нанесення фінансових і моральних збитків;

використання правових, організаційних і тех.-нічних засобів забезпечення безпеки;

створення умов для максимальної локалізації можливих збитків: фінансових, матеріальних і моральних, що призводять до порушення нормального функціонування і розвитку організації.

Режим інформаційної безпеки в подібних системах забезпечується:

на адміністративному рівні — політикою безпеки організації, в якій сформульовані цілі в області інформаційної безпеки і способи їх досягнення;

на процедурному рівні — шляхом розробки і виконання розділів інструкцій для персоналу, присвячених інформаційній безпеці, а також заходами фізичного захисту;

на програмно-технічному рівні — вживанням апробованих і сертифікованих рішень, стандартного набору контрзаходів: резервного копіювання, антивірусного і парольного захисту, міжмережевих екранів, шифрування даних і т.д.

При створенні системи інформаційної безпеки важливо не виключити жодного істотного аспекту — в цьому випадку інформаційній технології, яка вживається, буде гарантований відповідний рівень інформаційної безпеки.

Щоб система інформаційної безпеки була збалансованою, на початку процесу її формування проводиться аналіз можливих ризиків, які потенційно можуть загрожувати інформаційній системі підприємства. Спираючись на аналіз загроз, ризиків, вразливостей, потенційних місць проникнення в систему, оцінюючи збитки, формується обґрунтування вибору заходів протидії загрозам, що спричиняють збиток підприємству чи організації у вигляді моральної чи матеріальної шкоди (рис. 1).

Загальний підхід щодо забезпечення інформаційної безпеки передбачає наступні кроки [8]:

визначити цілі забезпечення інформаційної безпеки АІС (наприклад, забезпечення технологічної незалежності та високої конкурентоспроможності технічного потенціалу підприємства/організації, захист інформаційного поля комерційної таємниці та досягнення необхідного рівня інформаційного забезпечення роботи усіх підрозділів тощо);

створити ефективну систему управління інформаційною безпекою (чинником ефективності системи управління інформаційною безпекою є її побудова на базі міжнародних стандартів ISO / IEC 17799: 2005 [9] та ISO/IEC 27001:2011 [10];

оцінити відповідність запропонованих заходів із забезпечення інформаційної безпеки заявленим цілям (оцінка поточного рівня ефективності системи; локалізація "вузьких" місць у системі; оцінка відповідності системи підприємства існуючим стандартам в галузі інформаційної безпеки; вироблення рекомендацій і регламентів по забезпеченню безпеки об'єктів захисту).

Прийняті вимоги до системи інформаційної безпеки, що розробляється, повинні враховувати відповідні заходи на всіх етапах життєвого циклу інформаційної системи, тобто за весь період існування системи від початку розроблення до закінчення її використання та утилізації комплексу засобів автоматизації інформаційної системи. Таким чином, розробка відповідних заходів інформаційної безпеки відбувається після закінчення аналізу ризиків і вибору заходів, які повинні запобігати цим ризикам. Слід зазначити, що в якості обов'язкової складової цих заходів виступає рекурентна перевірка: наскільки наявний режим інформаційної безпеки відповідає політиці безпеки, яка була розроблена для певних умов роботи певного підприємства.

У зв‘язку з відсутністю надійного і разом з цим простого і доступного методичного інструментарію створення адекватної системи захисту інформації, набуває необхідності пошук та визначення шляхів, які сприятимуть розробці саме комплексу інформаційної безпеки в умовах гетерогенної інформаційної системи підприємства [11]. Формування та втілення рекомендацій/вказівок політики інформаційної безпеки повинно стосуватись всіх стадій життєвого циклу інформаційної системи, носити комплексний характер і спиратися на апробовані прийоми та методи, що зарекомендували себе як дієві та надійні з одного боку, а з іншого використовувати перспективний підхід до побудови комплексних систем захисту інформації в комп'ютерних мережах, що дозволяє подолати деякі з недоліків традиційних методів захисту, а саме - технологію інтелектуальних багатоагентних систем [12].

Серед таких методів можна назвати обов'язкове використання певних засобів ідентифікації й аутентифікації об’єктів та суб’єктів, засобів резервного копіювання, антивірусного контролю: для виявлення та протистояння комп'ютерним вірусам, внесення до опису об'єкта автоматизації структури цінності і проведення аналізу ризиків, визначення правил

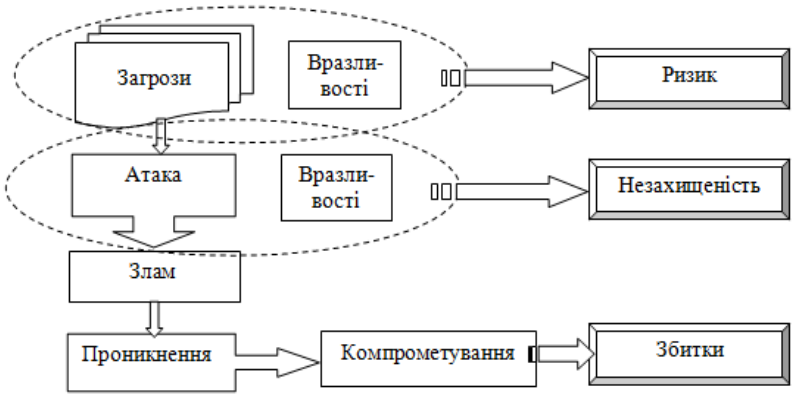

Рис. 1. Модель реалізації загроз інформаційної безпеки

будь-якого процесу користування цим видом доступу до ресурсів об'єкта автоматизації, що мають цей ступінь цінності і т.д.

Прийоми та методи розподіляються по групах заходів, спрямованих на забезпечення інформаційної безпеки організації [4], серед яких виділяють:

управління персоналом;

фізичний захист;

підтримка працездатності;

реагування на порушення режиму безпеки;

планування відновних робіт.

Слід зазначити, що при розробці концепції інформаційної безпеки підприємства слід не тільки спиратись на вищезазначені групи заходів, але й зважати на сферу діяльності компанії/організації, що дозволить сформувати конкретні вимоги до інформаційної безпеки, кількість коштів, які планується витратити та рівень і кількість спеціалістів, що будуть залучені до розробки та втілення політики збереження конфіденційних даних, можливі втрати від можливого зниження репутації організації, дезорганізації її діяльності.

Система управління інформаційною безпекою повинна виконувати управління ризиками, слідкувати за ефективністю роботи системи в цілому, корегувати управління персоналом, впорядковувати документацією та записи безпосередньо системи управління ІБ, з можливістю її перегляду та модернізації, відповідати за безперервність бізнесу і швидкість його відновлення після критичних (з точки зору інформаційної безпеки) переривань (рис. 2).

Вимоги, що диктує система управління інформаційною безпекою, виконують або спеціальні співробітники відповідної служби, або відповідальні співробітники з досвідом роботи та авторитетом, призначені адміністрацією, та спроможні довести до відома рядових співробітників правила роботи з системою, навчаючи їх та своєчасно інформуючи.

У даному випадку використання технології інтелектуальних багатоагентних систем дозволяє істотно в порівнянні з традиційними методами підвищити ефективність захисту інформації, в тому числі її адекватність, відмовостійкість, стійкість до деструктивних дій, універсальність, гнучкість і т. д. Багато- або мультиагентною системою можна вважати мережеву сукупність автономних об'єктів/агентів), здатних отримувати, зберігати, обробляти і передавати інформацію як в інтересах вирішення власних, так і корпоративних задач аналізу і синтезу інформації. В подібних системах кожен агент розглядається як система, заснована на знаннях з додаванням компонентів, що забезпечують безпеку, якість обслуговування, взаємодію з мережевими ресурсами та користувачами. Поняття агент відповідає апаратно або програмно реалізованої сутності, яка здатна діяти в інтересах досягнення цілей, бо однією з ознак мультиагентних систем є можливість вирішення складних погано формалізованих завдань, які вимагають побудови оригінального алгоритму рішення в залежності від конкретної ситуації, яка характеризується невизначеністю і динамічністю вихідних даних і знань.

Забезпечення інформаційної безпеки є постійно присутнім фактором, обов'язковим та необхідним елементом цілеспрямованої діяльності мультиагентних систем підтримки функціонування інформаційно-безпечних систем, заснованих на політиках безпеки.

Висновки

Невід'ємною частиною робіт по захисту є оцінка ефективності засобів захисту, що здійснюється за методикою, що враховує всю сукупність технічних характеристик оцінюваного об'єкта, включаючи технічні та програмні рішення, а також практичну реалізацію засобів захисту.

Аналіз безпеки комп'ютерних систем та інформаційних систем на різних стадіях їх життєвого циклу спирається на використання різних методів аналізу вразливостей, загроз та ризиків, виявленні відмінностей між політикою безпеки і конфігурацією системи та її поточним станом, завдання політик

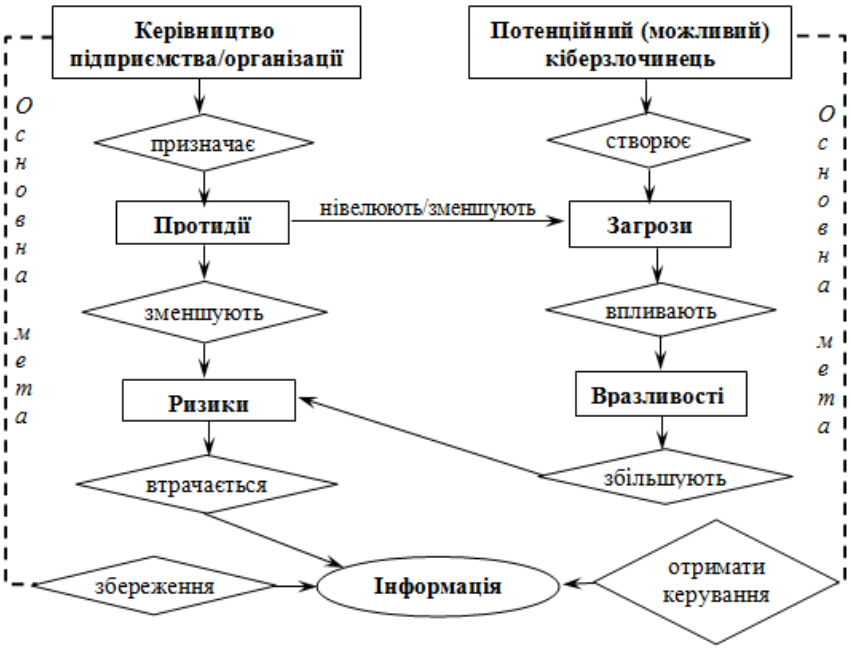

Рис. 2. Модель системи безпеки підприємства в інформаційній сфері

безпеки як сукупності правил забезпечення безпеки з наступною розробкою програмно-апаратних засобів підтримки інтелектуальних багатоагентних систем, здатних виявляти нові типи атак (несанкціонованих вторгнень), при необхідності уникнути наслідків атаки виконати зміну конфігурації комп'ютерних мереж і змінити профілі користувачів, сервісів і додатків.

Список літератури

1. Соціально-правові основи інформаційної безпеки: Навчальний посібник / [Петрик В.М., Кузьменко А.М., Остроухов В.В. та ін.]; з а ред. В. В. Остроухова. – К.: Росава, 2007. – 496 с.

2. Петрик В.М. Щодо визначення інформаційної безпеки та її різновидів / В.М. Петрик // Форми та методи забезпечення інформаційної безпеки держави: Збірник матеріалів міжнародної науково-практичної конференції (м. Київ, 13 березня 2008 р.). – К.: Видавець Захаренко В.О., 2008. – С. 160–164.

3. Тихомиров О.О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: мета, засоби і методи, принципи, результати// Information Security of the Person, Society and State – 2012 – № 3(10) – С. 11-17.

4. Галатенко В.А. Основы информационной безопасности. - М.: Изд-во "Интернет-университет информационных технологий - ИНТУИТ.ру", 2003. - 280 с..

5. . Ожеван М. А. Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії / М. А. Ожеван // Стратегічні пріоритети. – 2011. – № 3. – С. 118–126.

6. Сороківська О.А. Інформаційна безпека підприємства: нові загрози та перспективи / О.А. Сороківська, В.Л. Гевко // Економічні науки: Вісник Хмельницького національного університету 2010. – № 2. – Т. 2. – С.32-35.

7. Щербина В.М. Інформаційне забезпечення економічної безпеки підприємств та установ / В.М. Щербина // Актуальні проблеми економіки. – 2006. – № 10. – С. 220-225.

8. Велігура А.В. Дослідження шляхів розробки комплексів інформаційної безпеки / А.В. Велігура, Л.М. Дегтярьова, О.М. Степанова // Вісник Східноукраїнського національного університету імені В. Даля. - № 6(136), 2009, Ч. 1 – С 154–161

9. ISO/IEC 17799:2005 - Информационные технологии. Методы и средства обеспечения безопасности. Свод правил по менеджменту информационной безопасности

10. Information technology. Security techniques. Information security management systems. Requirements"; Методология. «Создание комплексной системы управления информационной безопасностью» // http://itzashita.ru; URL:http://itzashita.ru/theory/sozdanie-kompleksnoj-sistemy-upravleniya-informacionnoj-bezopasnostyu.html; (дата звертання 18.03.2017).

11. Степанова О.М. Інформаційна безпека в умовах розвитку інформаційної системи підприємства. / Степанова О.М., Дегтярьова Л.М. // Інформаційна безпека, № 1. – Вид-во: Східноукраїнського нац. ун-ту ім. В. Даля, 2009. – С. 59-63

12. И.В. Котенко, Р.М. Юсупов. Перспективные направления исследований в области компьютерной безопасности//Защита информации. INSIDE. – 2006. – № 2. – С. 46-57

13. John R. Vacca. Public Key Infrastructure: Building Trusted Applications and Web Services. /John R. Vacca. – Public Key Infrastructure: Building Trusted Applications and Web Services. Front Cover. John R. Vacca. CRC Press, May 11, 2004 - Computers - 448 pages.

14. John R. Vacca. Computer Forensics: Computer Crime Scene Investigation, Том 1. – Charles River Media, 2005 – 832 pages

15. Jason Andress. The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. – Imprint: Syngress, 2011. – 240 pages.

16. V.S.Bagad. Networks And Information Security. Front Cover. / I.A.Dhotre, V.S.Bagad. – Technical Publications, 2009. – 292 pages.

17. Richard E. Smith. Elementary Information Security. /Jones & Bartlett Publishers, Nov 18, 2011. - Computers - 890 p.

Надійшла до редколегії 15.02.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

ПРАКТИЧЕСКИЕ ПРИЕМЫ И УПРАВЛЯЮЩИЕ ПРИНЦИПЫ РАЗРАБОТКИ КОМПЛЕКСОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Л.Н. Дегтярева, В.Г. Ляшевский

В статье рассмотрены результаты сравнительного анализа развития концепции информационной безопасности автоматизированных систем, использования современных интеллектуальных технологий в сфере информационной безопасности. Показано, что воплощение принципов научности и профессионализма и использования современных тенденций в практической составляющей обеспечения информационной безопасности способствует укреплению принципов информационной безопасности.

***Ключевые слова**: информационная безопасность, автоматизированная информационная система, несанкционированный доступ, конфиденциальность информации, информационных угроз, интеллектуальные мультиагентные технологии.*

PRACTICAL TECHNIQUES AND MANAGEMENT PRINCIPLES DEVELOPMENT OF SYSTEMS OF INFORMATION SECURITY

L.N. Degtyarev, V.H. Lyashevsky

In the article the results of comparative analysis of the development of the concept of information security of automated systems, the use of modern intelligent technologies in the field of information security. It is shown that the embodiment of the principles of scientific character and professionalism and use of modern trends in the practical component of information security contributes to strengthening the principles of information security.

***Keywords**: information security, automated information system, unauthorized access, confidentiality of information, information threats, intelligent multi-agent technology.*