МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

МІЖНАРОДНИЙ ТЕХНОЛОГІЧНИЙ УНІВЕРСИТЕТ «МИКОЛАЇВСЬКА ПОЛІТЕХНІКА»

МИКОЛАЇВСЬКИЙ ІНСТИТУТ ПРОФЕСІЙНОГО РОЗВИТКУ І ОСВІТИ

ЗБІРНИК ТЕЗ ДОПОВІДЕЙ НАУКОВО-ПРАКТИЧНОЇ КОНФЕРЕНЦІЇ

СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО –ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (SITS'2016)

09 – 12 червня 2016 року

МИКОЛАЇВ – КОБЛЕВО

Стан та удосконалення безпеки інформаційно-телекомунікаційних систем (SITS'2016). – Миколаїв: ДП НВКГ «Зоря-Машпроект», 2016. - 76 с.

У збірник ввійшли матеріали, представлені і обговорені під час проведення 8-ої Всеукраїнської науково-практичної конференції «**СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО – ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (SITS'2016)**» 09-12 червня 2016 року в с. Коблево Миколаївської області.

Матеріали збірника можуть бути корисними для науковців і фахівців сфери інформаційних технологій та кібербезпеки, персоналу з безпеки установ і підприємств різних форм власності, керівників вищих навчальних закладів, професорсько-викладацького складу, аспірантів і студентів.

Редакційна колегія випуску:
Вільський Г.Б., PhD, професор; Корченко О.Г., д.т.н., професор;
Мельник С.В., к.е.н., доцент; Корнейко О.В., к.т.н., професор;
Михалишин Б.Є., к.т.н.; Гнатюк С.О., к.т.н., доцент

Матеріали публікуються за оригіналами, наданими авторами.
Претензії до організаторів не приймаються.

МИКОЛАЇВ – КОБЛЕВО
2016

ЗМІСТ

1. Ахмєтов Б.С., Лахно В.А., Корченко О.Г., Бекетова Г.С. **ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ** **5**

2. Балтовський О.А., Сифоров О.І. **АЛГОРИТМ ВИЗНАЧЕННЯ СТРУКТУРИ МАТЕМАТИЧНОЇ МОДЕЛІ ОПТИМАЛЬНОЇ СКЛАДНОСТІ** **7**

3. Васєв О.В., Майданюк П.В. **ТИПОВА МОДЕЛЬ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОГО ОРГАНУ** **11**

4. Васєв О.В., Майданюк П.В. **СУЧАСНІ МЕТОДИ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ** **15**

5. Вільський Г.Б., Михалишин Б.Є. **СТАНОВЛЕННЯ І РОЗВИТОК НЕФОРМАЛЬНОЇ ОСВІТИ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ** **18**

6. Воронов В.В. **НОРМАТИВНІ ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ** **20**

7. Гавриленко О.В. **ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ДЕРЖАВНИХ ОРГАНАХ НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТІВ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ** **22**

8. Герганов Л.Д., Герганов М.Л. **ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НАВЧАННЯ В ПРОЦЕСІ ПІДГОТОВКИ ПЛАВСКЛАДУ НА ВИРОБНИЦТВІ** **24**

9. Гнатюк В.О., Іванченко І.С., Наджі Абду Ахмед Алі. **МЕРЕЖЕВО-ЦЕНТРИЧНИЙ ПІДХІД ДО МОНІТОРИНГУ КІБЕРІНЦИДЕНТІВ В ІНФОР-МАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ** **26**

10. Гнатюк С.О., Поліщук Ю.Я., Одарченко Р.С., Сейлова Н.А. **ДОСЛІДЖЕННЯ МЕТОДУ СТВОРЕННЯ ІНФОРМАЦІЙНОЇ РЕАЛЬНОСТІ НА БАЗІ СТРУКТУРНО-АНАЛІТИЧНИХ МОДЕЛЕЙ ДЕЗІНФОРМУВАННЯ** **28**

11. Гнатюк С.О., Шаховал О.А., Бекетова Г.С., Жумангалієва Н.К. **ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ АСПЕКТ КІБЕРПЕЗПЕКИ УКРАЇНИ** **32**

12. Голубєв В.О. **КІБЕРЗЛОЧИННІСТЬ: ПРИХОВАНА ТА ЯВНА ЗАГРОЗИ** **34**

13. Дудатьєв А.В., Дудатьєв В.М., Літушко О.А. **КОМПЛЕКСНИЙ МЕТОД ПРОТИДІЇ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ** **35**

14. Ісмайлов К.Ю., Косаревська О.В. **АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ПРАВООХОРОННОЇ СФЕРИ У ВНЗ З ОСОБЛИВИМИ УМОВАМИ НАВЧАННЯ** **37**

15. Карпінський Н.П., Корченко А.О., Казмирчук С.В. **ФАЗИФІКАЦІЯ ПАРАМЕТРІВ В КОРТЕЖНІЙ МОДЕЛІ ДЛЯ ВИЯВЛЕННЯ КІБЕРАТАК** **39**

16. Кінзерявий В.М., Кінзерявий О.М., Гізун А.І., Рябий М.О. **АЛГОРИТМ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ВЕКТОРНІ ЗОБРАЖЕННЯ** **42**
17. Корнейко О.В. **ТЕОРІЯ РОЗРЯДНИХ ПЕРЕТВОРЕНЬ В СУЧАСНІЙ КРИПТОГРАФІЇ** **45**
18. Кузнєцова А.В., Василіу Є.В. **ПЕРСПЕКТИВИ РОЗВИТКУ КВАНТОВИХ ПРОТОКОЛІВ З НЕПЕРЕРВНИМИ ЗМІННИМИ** **47**
19. Лахно В.А., Корченко О.Г., Бекетова Г.С. **ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІНТЕЛЕКТУАЛЬНОГО РОЗПІЗНАВАННЯ КІБЕР-ЗАГРОЗ** **49**
20. Мельник С.В. **НОВІ ПІДХОДИ ЩОДО ЗАКОНОДАВЧО-НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ РЕФОРМИ ОСВІТИ** **51**
21. Нємкова О.А, Шандра З.А., Костирко Т.М. **ТОПОЛОГІЯ МУЛЬТИФРАКТАЛІВ ШУМІВ ПРИСТРОЮ В ЗАДАЧАХ ДИНАМІЧНОЇ ІДЕНТИФІКАЦІЇ** **53**
22. Огбу Д.О., Шестак Я.В. **МОНІТОРИНГ ОБРОБКИ ДАНИХ ЦЕНТРУ (DPC) В ІНФОРМАЦІЙНОМУ ЗАХИСТІ ДАНИХ ВІД КІБЕРАТАК** **55**
23. Павленко В.М., Зряхов М.С., Пономаренко М.М. **МЕТОДИКА ОБЧИСЛЕННЯ РЕЙТИНГОВИХ ПОКАЗНИКІВ В ІНФОРМАЦІЙНІЙ СИСТЕМІ ХАІ** **57**
24. Пядишев В.Г. **КІБЕРТЕРОРИЗМ: ЙОГО МІСЦЕ У СТРУКТУРІ КІБЕРЗЛОЧИННОСТІ ТА КОМПЛЕКСНИЙ ПІДХІД ДО БОРОТЬБИ З НИМ У США** **59**
25. Сахно О.П., Жепало А.С. **ОСОБЛИВОСТІ ПРОВЕДЕННЯ РОБІТ З ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ** **61**
26. Стайкуца С.В., Семенов О.С. **АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ КОМПАНІЙ З РОЗРОБКОЮ МЕТОДОЛОГІЇ ЗАХИСТУ** **63**
27. Ткач Ю.М., Казмирчук С.В. **ЗАСТОСУВАННЯ СТАТИСТИЧНОГО ІНСТРУМЕНТАРІЮ У ПРОЦЕСІ ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ** **67**
28. Толюпа С.В., Розумяк С.В. **ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В МЕРЕЖЕВУ ІНФРАСТРУКТУРУ** **70**
29. Хохлачова Ю.Є., Скворцов С.О. **ОСОБЛИВОСТІ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ** **72**

Ахмєтов Б.С., д.т.н., професор,
директор Інституту інформаційних та телекомунікаційних технологій Казахського національного дослідницького технічного університету імені К.І. Сатпаєва, Алмати,
Лахно В.А., д.т.н., доцент,
Європейський університет, Київ,
Корченко О.Г., д.т.н., професор,
Національний авіаційний університет, Київ,
Бекетова Г.С.,
Інститут інформаційних і телекомунікаційних технологій, Казахський національний дослідницький технічний університет імені К.І. Сатпаєва, Алмати

ЗАБЕЗПЕЧЕННЯ КІБЕРЗАХИСТУ В СУЧАСНИХ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Ефективність функціонування сучасних КС та технологій виявлення кібератак істотно залежить від оперативності та достовірності моніторингової інформації активності кіберзлочинців на попередніх стадіях реалізації кібернападів на інформаційні ресурси державних установ та приватних компаній. Як показав світовий досвід, на сьогодні найбільш ефективним методологічним підходом до побудови інноваційних інтелектуальних моніторингових систем кібернападів є шлях створення ієрархічних багаторівневих структур розпізнавання кібератак на початкових стадіях їхньої реалізації. При цьому ієрархічний підхід дає змогу розв'язувати складні задачі управління процесом захисту інформації від кібератак в розподілених інформаційних системах критичної інфраструктури держави як послідовність локальних задач, скоординованих між собою.

Розробка і використовування інтелектуальних систем моніторингу, розпізнавання кібератак та управління подіями інформаційної безпеки (ІБ) в даний час є одним з найбільш перспективних напрямків в області забезпечення кіберзахисту в КС і мережах. Подібні системи дозволяють на основі збору і оперативного аналізу даних про події ІБ, зокрема кібератаки, виявляти і попереджувати мережеві вторгнення, оцінювати і прогнозувати рівень захищеності об'єктів інформатизації, наприклад, інформаційно-комунікаційних систем (ІКС) критичної інфраструктури держави. Тому вирішення задач, пов'язаних із здійсненням інтелектуального моніторингу інцидентів ІБ і формуванням оперативних рішень по кіберзахисту в інтегрованих територіально-розподілених інформаційних системах, є актуальним.

В США, державах ЄС, Китаї, Південній Кореї та Японії дослідженням проблематики створення інтелектуальних систем виявлення кібератак приділяється багато уваги, про що свідчить велика кількість публікації з цієї тематики [1-5]. На пострадянському просторі питанням розробки розподілених систем виявлення кібератак (РСВК) в різний час теж займалися різні вчені [6-11]. Однак в галузі кіберзахисту побудову моделей РСВК засновано на різнорідних підходах, вони носять точковий характер, відповідно до об'єктів кібернападу. Моделі та алгоритми розпізнавання кібернападів часто не взаємопов'язані, що наразі ускладнює їх використання при створенні ефективних РСВК. Таким чином, розробка та застосування інноваційних РСВК стримується недостатньою ефективністю функціонування моделей та алгоритмів розпізнавання загроз у межах відомих та нових класів кібератак, що викликано низькою точністю моделей об'єктів моніторингу кіберзахисту. На наш погляд, основними причинами є:

1. Низька ефективність управління системами виявлення кібератак, яка пов'язана із недостатньою кількістю інформації про стан об'єктів кіберзахисту, особливо, для критичної інфраструктури держави.

2. Значна кількість непов’язаних між собою об’єктів моніторингу, що у свою чергу ускладнює формалізацію задач виявлення складних кібератак та традиційних математичних методів опису шаблонів кібернападів.

Для синтезу адекватних моделей РСВК необхідне підсилення можливостей традиційних статистичних підходів [4, 5, 7] методами, які є менш чутливими до вимоги незалежності параметрів. Аналіз методів визначення причиново-наслідкових зв’язків між вхідними параметрами та вихідною величиною при розробці РСВК дозволяє дійти висновку, що жоден з них з притаманними їм перевагами і недоліками не може окремо повною мірою відповідати моделі "багатовимірний вхід – вихід". Отже, існує велика кількість неформалізованих задач кібербезпеки, які не можуть бути розв’язані за допомогою лише одного методу, а необхідний консорціум методологій, які забезпечили б основи конструювання та розвитку інтелектуальних РСВК або ІРСВК. Першим шляхом комплексного використання таких напрямків, як нечітка логіка, нейро- і генетичні обчислення та інших інтелектуальних технологій ідентифікації стали м’які обчислення (Soft Computing), які більшою мірою пристосовані до роботи з неточними та невизначеними даними, що дозволяє розв’язати проблему лінгвістичної невизначеності. Однак, наряду з подоланням труднощів використання нечітко заданої вхідної інформації необхідно також забезпечити можливість урахування відмінностей між різними класами кібератак за важливістю контрольованих параметрів і врахувати їх взаємодії необхідного порядку. Ця проблема може бути вирішена методами нечіткої логіки та регресійного аналізу.

Метою даної роботи є апробація методу інтелектуального розпізнавання кібератак на основі дискретних процедур для побудови адаптивних систем кіберзахисту інформаційно-комунікаційних систем, в умовах збільшення кількості дестабілізуючих впливів на збереженість, доступність і цілісність інформаційних ресурсів.

Неповнота інформації про загрози для ІБ у ІКС є двоякою. По-перше, це часткова відсутність апріорної інформації, навіть на рівні уявлення про структуру всього об'єкта нападу на інформацію, що має, як правило, стохастичну природу. По-друге, обмежена можливість спостереження об'єкта нападу й розпізнавання загроз, що належать певному класу. У граничному випадку заздалегідь відома лише загальна множина загроз ІБ і способів їх реалізації.

Однак, як показує практика, одна з основних характеристик сучасних загроз полягає у тому, що вони довгий час не активуються, іноді до двох-трьох років [7, 8]. Цільові атаки, зокрема спрямовані на ІС підприємств, об'єкти інфраструктури, енергетики, транспорту тощо, зазвичай розробляються з урахуванням того середовища, на яке вони будуть націлені. Сучасні загрози створюються таким чином, щоб обійти захист, і, як правило, вже не виявляються за допомогою сигнатур. Розробка сценаріїв кібератак виконується з дотриманням всіх стандартів і технологій, з технічним завданням, робочим проектом, тестуванням, підтримкою і оновленням.

Оцінка можливості реалізації загрози залежить від багатьох факторів. У багатьох джерелах можливість реалізації загрози визначається як певна ймовірність [1, 4, 11]. Однак, загроза, яка є джерелом потенційного збитку, а тому представляє деяку небезпеку, будь-яким чином повинна бути виміряна. Фактично, мова йде про формування моделі загроз для ІКС. Безумовно, вимірювання загрози слід почати з оцінки можливості її виникнення. Така оцінка може бути зроблена на основі даних по відомим фактам появи загрози, вираженим через статистичну частотність. Дану оцінку можна розглядати як оцінку, засновану на наявному досвіді експлуатації СЗІ ІКСТГ.

Другим фактором оцінки можливості реалізації загрози є оцінка витрат, що неминуче виникають при введенні тих чи інших засобів захисту.

Таким чином, нові моделі розпізнавання кіберзагроз для ІКС не тільки становлять самостійний практичний інтерес, але і є прикладом можливої формалізації опису нових, ще невідомих класів кібератак.

Перспективи подальших досліджень полягають у тому, щоб визначити найбільш критичні об'єкти ІКС, що підлягають захисту, а також дослідити запропонований метод інтелектуального розпізнавання загроз на більш широкому класі задач кількісного і якісного розпізнавання кібернападів.

Література

1. U.S. Department of Transportation, Research and Innovative Technology Administration, "Intelligent Transportation Systems (ITS) Strategic Plan: Background and Processes," January 8, 2010, http://www.its.dot.gov/strat_plan/pdf/ IntelliDriveBook_Jan2010.pdf.
2. Maras Marie-Helen. Cybercrime Laws: Which Statute for Which Crimes. (2012). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning. – P. 104-06.
3. Adel W. Sadeka, Byungkyu "Brian" Parkb & Mecit Cetinc (2014). Special Issue on Cyber Transportation Systems and Connected Vehicle Research. Journal of Intelligent Transportation Systems: Technology, Planning, and Operations. Volume 20, Issue 1, 2016. DOI:10.1080/15472450.2014.889914
4. Teodor Sommestad, Henrik Karlzén, Jonas Hallberg (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy* (IJISP). Volume 9. - P. 26-46.
5. Sumeet Dua. Data Mining and Machine Learning in Cybersecurity / Sumeet Dua, Xian Du. — Taylor & Francis Group, 2011. — 223 p.
6. Дудикевич В. Б. Проблеми оцінки ефективності систем захисту / В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник Національного університету "Львівська політехніка". – Сер.: Автоматика, вимірювання та керування. – Львів : НУ "Львівська політехніка". – 2012. – № 741. – С. 118–122.
7. Корченко А. А. Система формирования нечетких эталонов сетевых параметров / А. А. Корченко // Захист інформації, 2013. – Т. 15, №3. – С. 240 –246.
8. Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук // Сучасна спеціальна техніка, 2011. – №1(24). – С.61-66.
9. Харченко В. П. Кибертерроризм на авиационном транспорте / В. П. Харченко, Ю. Б. Чеботаренко, О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр. : Вип. 4 (28). – К. : НАУ, 2009. – С. 131-140.
10. Корченко О. Г. Ознаковий принцип формування класифікацій кібератак / О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк, В. М. Кінзерявий, С.В. Казмірчук // Вісник Східноукраїнського національного університету імені Володимира Даля, 2010. –№1. – С. 32–38.
11. Lahno V. Ensuring of information processes' reliability and security in critical application data processing systems. / V. Lahno // MEST Journal. – Belgrade, 2014. –Vol. 2. No 1. – P. 71–79.

Балтовский А.А., д.т.н., доцент,
Сифоров А. И., к.т.н., доцент,
Одесский государственный университет внутренних дел

АЛГОРИТМ ОПРЕДЕЛЕНИЯ СТРУКТУРЫ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ОПТИМАЛЬНОЙ СЛОЖНОСТИ

Одним из путей повышения эффективности систем управления и обработки информации является использование более точных и достоверных математических моделей

объектов или процессов на основе применения современных методов идентификации, что становится возможным с применением достижений цифровой вычислительной техники.

Основные задачи разработки математических моделей объектов и процессов отвечают государственным научно-техническим программам, которые сформулированы в законах Украины «О научной и научно-технической деятельности» и «О национальной программе информатизации» [7,19]. В этой связи актуальность статьи очевидна.

Известные из литературных источников [1,2] подходы к построению математических моделей основаны на использовании регрессионного анализа.

При этом используется корреляционный, дисперсионный и факторный анализы, а также анализ показателей существенности переменных. Основная цель перечисленных методов заключается в выявлении и исключении из аргументов исследуемой модели факторов, незначительно влияющих на выходную переменную модели.

Помимо регрессионного анализа, одним из рекомендуемых методов построения математических моделей объектов является метод группового учета аргументов (МГУА) [3], обеспечивающий по сравнению с регрессивным анализом объективный характер моделирования и структурной идентификации объекта [4-8]. Объективность достигается тем, что при построении моделей руководствуются не заранее заданным числовым значением отдельных ограничений (порогового коэффициента парной корреляции, критерия существенности Стьюдента), а критериями весьма общего вида: критерия регулярности, минимума смещения и др. В качестве критерия селекции (выбора структуры модели оптимальной сложности) рекомендуется использовать критерий минимума смещения $(\eta_{см})$, позволяющий решать задачу восстановления закона, скрытого в зашумленных экспериментальных данных и применяемого вследствие этого для задачи идентификации

$$\eta^2_{см} = \frac{\sum_{i=1}^{N} \left(q_{A_i} - q_{B_i}\right)^2}{\sum_{i=1}^{N} q_{T_i}} \to \min ,$$

где N - все точки таблицы исходных данных;

q - выходная величина;

q_A - значения q, рассчитанные по модели , оценки параметров которой получены по точкам с большим значением дисперсии выходной величины;

q_B - то же, по точкам с меньшим значением дисперсии выходной величины;

q_T - табличное значение переменой.

В МГУА применяются две основные структуры генерации множества моделей, оцениваемых по критерию селекции:

1. Комбинаторные (непороговые) алгоритмы МГУА.
2. Многорядные (пороговые) алгоритмы МГУА.

В первом случае требуется задание некоторой заведомо усложненной математической зависимости выходной величины от вектора входных переменных, например, в виде полинома высокой степени, из которой путем обнуления (приравнивания нулю) тех или иных коэффициентов получаются математические модели различной структуры. Лучшая структура определяется по тому или иному критерию селекции.

В многорядном алгоритме первоначально на первом ряду селекции образуются математические зависимости (частные описания), каждая из которых связывает выходную величину с двумя переменными. Полученные частные описания сравниваются по критерию селекции, и из них выбирается F_1 лучших.

На втором ряду селекции образуются частные описания, каждое из которых связывает выходную величину с двумя переменными, в качестве которых выступают частные

описания, полученные на предыдущем ряду селекции. Из новых частных описаний выбирается F_2 наилучших для использования в следующем, третьем ряду селекции. Для каждого ряда находится наилучшая (по критерию селекции) модель. Ряды селекции наращиваются, пока оценка критерия уменьшается (правило останова).

Целью является разработка модифицированного алгоритма МГУА.

Объектом исследований - алгоритмы для определения структуры математической модели. *Предметом исследований* - комбинаторные и многорядные алгоритмы МГУА.

Научная задача обусловлена необходимостью разработки более совершенного алгоритма для определения структуры математической модели или процесса.

Поставленная цель определила необходимость решение следующих задач:

- разработка комбинированного алгоритма;
- практическая реализация комбинированного алгоритма в виде блок - схемы.

Для решения сформулированных задач использовались методы математического моделирования и программирования.

Предлагаемый нами модифицированный многорядный алгоритм МГУА для построения математических моделей обеспечивает определение на каждом ряду селекции структуру четкого описания с использованием для его построения комбинаторного алгоритма. При этом используются таблицы постепенного усложнения полинома для двух переменных. Алгоритм приведен на рис. 1, где приняты следующие обозначения:

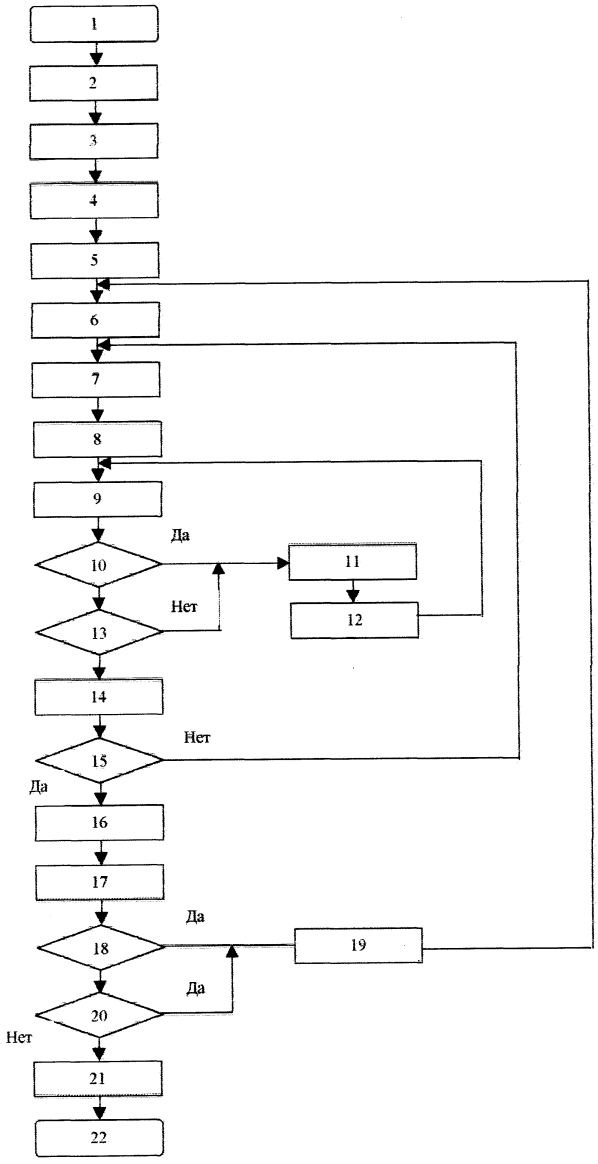

Рис. 1. Алгоритм определения структуры математической модели оптимальной сложности

1 - Начало.

2 - Ввод экспериментальных данных, расчет значений функции отклика по экспериментальным данным Y_i и значений аргументов модели X_{ij} (i = 1,..., N; j = 1,...,M; N - число измерений; M - число выходных переменных модели).

3 - Ранжирование точек $\{Y\}$ по дисперсии, выделение обучающей $\{YB_i\}$ и проверочной $\{YA_i\}$ последовательностей $\{YB_i\}$ - точки с меньшим значением дисперсии выходной величины; $\{YA_i\}$ - точка с большим ее значением.

4 - Определение числа частных описаний K:

$$K = C_m^2 = \frac{M!}{2!(M-2)}.$$

5 - Начало цикла по рядам селекции: S = 1.

6 - Начало цикла по частным описаниям.

7 - Выбор наиболее простой структуры для 2-х переменных G-го описания.

8 - Начало цикла по структурам: L = 1.

9 - Расчет параметров модели МНК G-го описания по $\{YA_i\}(A_a)$ и $\{YB_i\}(A_b)$ расчет $\eta_{см}$ для G-го описания.

10 - (L = 1)?.

11 - Определение критерия, для G-го описания: $KR_G = \eta_{см}$; $L = L + 1$.

12 - Усложнение структуры.

13 - $(KR_G \le \eta_{см})$?.

14 - В качестве G-го описания принимается структура, соответствующая (L-1)-му циклу, расчет переменной по G-му описанию Z_{qi} (i= 1,...,N); в следующем ряду селекции $\{Z_{qi}\}$ являются аргументами частных описаний.

15 – ($G = K$)?.

16 - $G = G + 1$.

17 - Выбор M наилучших частных описаний по $min\ KR_G$; $KR1_S = min\ KR_G(1...K)$.

18 – (S = 1)?.

19 - $S = S + 1$.

20 - $(KR1_S < KR1_{S-1})$?.

21 - Определение оптимальной структуры модели: в качестве структуры оптимальной сложности принимается структура модели с наименьшим значением критерия на предыдущем (S - 1) - m ряду селекции.

22 - Конец.

ВЫВОДЫ

1. Использование модифицированного алгоритма обеспечивает получение более точных и достоверных математических моделей объектов и процессов.

2. Затраты времени для получения структуры математической модели находятся в функциональной зависимости от сложности объекта или процесса.

ЛИТЕРАТУРА

1. Иванов В.В. Обзор достижений в области кибернетики и вычислительной техники: Вопр. точности и эффективности вычисл. Алгоритмов. - Киев: ИК АН УССР, 1989.-135с.

2. Монтгомери Д.К. Планирование эксперимента и анализ данных: Пер. с англ.-Л. : Судостроение, 1990. - 384с.

3. Справочник по типовым программам моделирования / А.Г. Ивахненко, Ю.В. Коппа, В.С. Степашко и др.; под ред. А.Г. Ивахненко. - К.: Техніка, 1990.- 184с.

4. Месарович М., Такахара М. Общая теория систем: математические основы . - М.: Мир, 1987. - 311с.

5. Александров В.В., Горский Н.Д. Алгоритмы и программы структурного метода обработки данных. Л.: Наука, 1983. - 288с.

6. Грекул В.И. Проектирование информационных систем / В.И. Грекул. . - М.: ООО «БИНОМ. Лаборатория знаний»; ООО «ИНТУИТ.ру», 2005. – 296 с.

7. Turban, McLean, Wetherbe. Information technology for management. John Wiley & Sons. Inc. New York, 1999.

8. Nickerson R.C. Information & business systems.// Addison-Wesley, 1998.

Васєв О.В.,
Майданюк П.В.,
Управління Державної служби спеціального зв'язку та захисту інформації України в Миколаївській області

ТИПОВА МОДЕЛЬ ЗАХИЩЕНОЇ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНОЇ СИСТЕМИ ДЕРЖАВНОГО ОРГАНУ

Протягом останніх років в Україні спостерігається процес інформатизації суспільства та органів публічного управління на всіх її рівнях, що обумовлено впровадженням в повсякденне життя країни новітніх інформаційно-телекомунікаційних технологій. Завдяки процесу інформатизації та глобалізації інформаційно-телекомунікаційних систем (ІТС) з'являються нові можливості несанкціонованого втручання в процеси обробки та передачі даних, які можуть нанести особі, суспільству чи державі політичні, економічні, фінансові та інші збитки. Тобто, процес удосконалення та спрощення процедури передачі даних збільшує уразливість системи в цілому та потребує приділяти все більше уваги захисту електронних інформаційних ресурсів (ІР). Тобто на сьогоднішній день все більш актуальною стає проблема забезпечення захисту інформації від загроз витоку, знищення, блокування, порушення цілісності та режиму до її доступу.

Для забезпечення захисту інформації в ІТС під час її обробки зберігання та передачі каналами зв'язку законодавством України передбачено створення комплексної системи захисту інформації, що спрямована на запобігання або максимальне ускладнення порушень конфіденційності, цілісності та доступності інформації, що оброблюється в ІТС та прикладних програмних засобах (ППЗ), що функціонують у її складі.

Над загальними та конкретними питаннями у сфері інформаційної безпеки працюють В. Ліпкан, Г. Почепцов, В. Кормич [3, 4, 6]. Дослідженням з проблем правового забезпечення інформаційної безпеки присвячені роботи з теорії держави та права П. Рабиновича, А. Колодій, В. Копейчикова, С. Лисенков [7,9]. Серед вітчизняних дослідників з питань організації діяльності у сфері криптографічного та технічного захисту інформації доцільно виділити В. Домарева та В. Хорошка [1]. Проте, сучасний стан захищеності інформації з обмеженим доступом та відкритої інформації, що належить до державних інформаційних ресурсів, під час її передачі каналами зв'язку, вказує на гостру необхідність вдосконалення систем інформаційної безпеки.

*Метою роботи є р*озробка моделі захищеної інформаційно-телекомунікаційної системи, яка забезпечує запобігання або максимальне ускладнення порушень

конфіденційності, цілісності та доступності інформації, що передається каналами зв'язку у складі телекомунікаційної мережі.

У якості прикладу пропонується модель захищеної ІТС, що являє собою розподілену обчислювальну мережу, до складу якої входять наступні складові:

– локальні обчислювальні мережі (ЛОМ), відкрита та захищена серверні зони вузла першого (центрального) рівня;

– ЛОМ вузлів другого (регіонального та районних) рівня;

– транспортна мережа спеціального призначення.

Режим функціонування компонентів системи:

– всі сервери відкритої та захищеної серверної зони – цілодобово;

– РС адміністраторів безпеки та користувачів – протягом робочого дня.

Особливості функціонування ІТС:

– безперервний цілодобовий режим функціонування серверних компонентів та необхідність забезпечення дотримання заявленого часового регламенту оброблення запитів користувачів;

– оброблення як відкритої інформації, так і інформації з обмеженим доступом (ІзОД, конфіденційної інформації);

– використання для оброблення інформації прикладного програмного забезпечення, яке створене та підтримується різними (у тому числі сторонніми) виробниками.

При побудові захищених ІТС державних органів пропонується інтеграція її компонентів в Національну систему конфіденційного зв'язку (НСКЗ) [8]. НСКЗ базується на власних спеціальних телекомунікаційних системах (мережах) і комплексах технічних засобів, використовує ресурси телекомунікаційноної мережі спеціального призначення та у разі потреби ресурси телекомунікаційних мереж загального користування. Схема взаємодії між компонентами ІТС наведена на рис.1.

НСКЗ складається з таких відокремлених інформаційно-телекомунікаційних систем (мереж) спеціального зв'язку:

– спеціальна транспортна мережа НСКЗ – телекомунікаційна мережа, призначена для транзиту трафіку між системами (мережами) НСКЗ;

– спеціальні інформаційно-телекомунікаційні системи (мережі) субєктів НСКЗ, призначені для обміну відкритою, службовою та конфіденційною інформацією;

– система захищеного електронного документообігу НСКЗ, призначена для забезпечення оперативного обміну електронними документами У складі системи захищеного електронного документообігу функціонує акредитований центр сертифікації ключів, призначений для надання органам державної влади та органам місцевого самоврядування послуг електронного цифрового підпису.

З урахуванням особливостей архітектури, інформації, що оброблюється, та технології її оброблення, згідно з НД ТЗІ 2.5-005-99 такі ІТС слід відносити до автоматизованих систем класу "3" – розподілений багатомашинний багатокористувачевий комплекс, який обробляє інформацію різних категорій конфіденційності, з підвищеними вимогами до забезпечення конфіденційності, цілісності та доступності оброблюваної інформації [2]. З урахуванням вимог діючих нормативних документів України з питань технічного захисту інформації, створення комплексної системи захисту інформації (КСЗІ) в ІТС має здійснюватися у такій послідовності [5]:

1 етап – Розроблення плану захисту інформації та технічного завдання (ТЗ) на створення КСЗІ в ІТС.

На цьому етапі мають бути виконані наступні роботи:

– вивчення інформаційної технології, що використовується або планується для використання в ІТС, та розроблення інформаційної моделі ІТС;

– визначення, з урахуванням розробленої моделі загроз інформації та вимог діючих НД ТЗІ, переліку функціональних послуг безпеки (ФПБ) (функціонального профілю захищеності), що має бути реалізований у КЗЗ КСЗІ, та необхідного рівня гарантій

коректності їх реалізації;

– визначення вимог до структури та складу КСЗІ в ІТС;

– розроблення плану захисту інформації в ІТС;

– розроблення та подання на узгодження до ДССЗЗІ технічного завдання (ТЗ) на створення КСЗІ в ІТС.

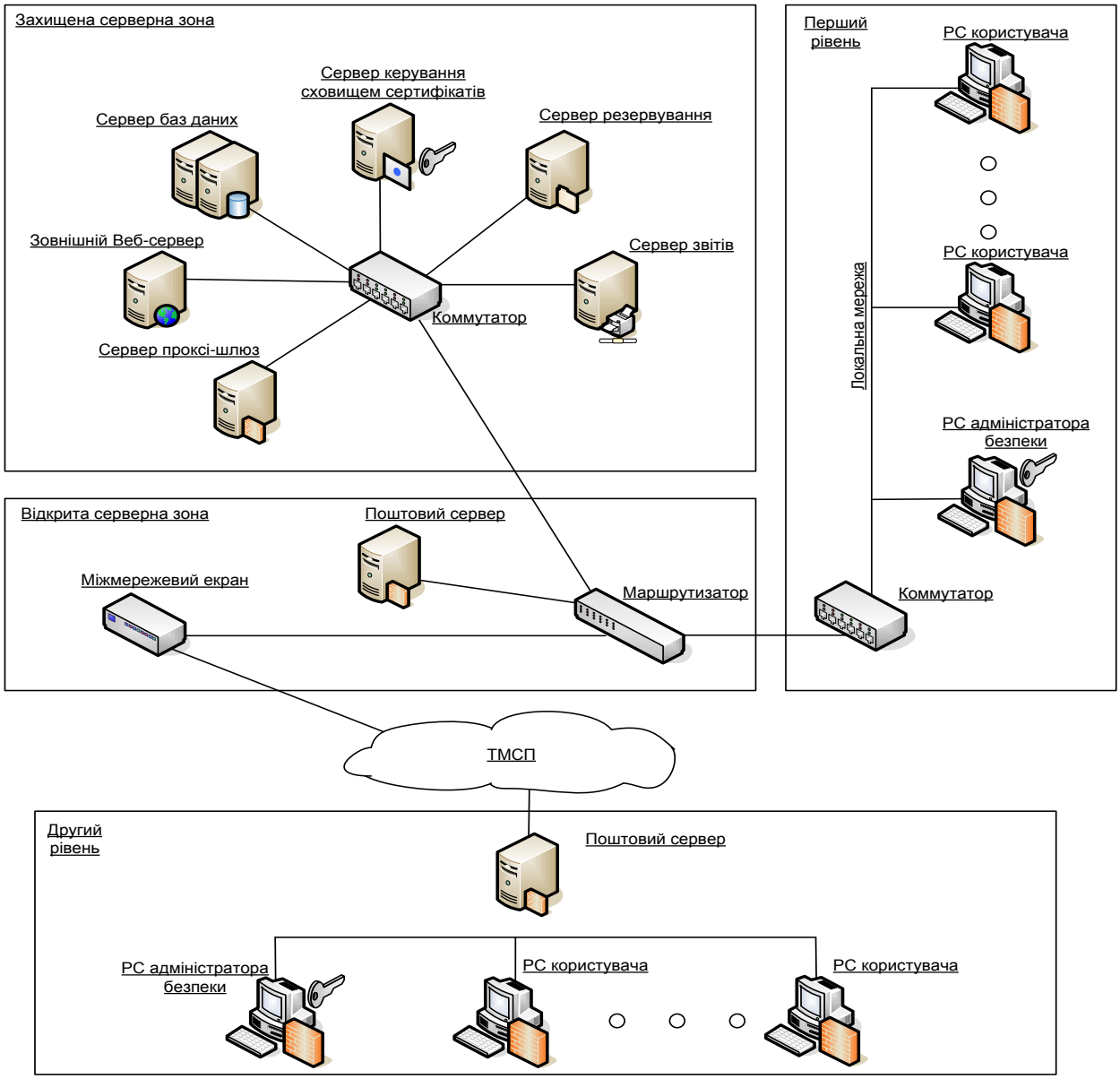

Рис.1. Схема взаємодії між компонентами ІТС.

2 етап – Розроблення технічного проекту (ТП) КСЗІ в ІТС.

На цьому етапі мають бути виконані наступні роботи:

– уточнення структури та складу КСЗІ в ІТС;

– визначення порядку функціонування та взаємодії підсистем та засобів КСЗІ в ІТС;

– визначення механізмів захисту, за допомогою яких будуть реалізовані визначені в ТЗ на створення КСЗІ ФПБ, та порядку їх функціонування;

– визначення послідовності розробки та впровадження засобів КСЗІ в ІТС;

– розроблення Положення про СЗІ в ІТС;

– розроблення пояснювальної записки до ТП КСЗІ в ІТС.

3 етап – Реалізація КСЗІ в ІТС.

На цьому етапі мають бути виконані такі роботи:

– розроблення експлуатаційної документації на засоби захисту, використовувані в КЗЗ КСЗІ;

– розроблення пакету нормативно-розпорядчих документів (положень, інструкції і т.ін.), які регламентують порядок встановлення та експлуатації КСЗІ в ІТС та дії всього персоналу;

– пусконалагоджувальні роботи засобів підсистем КСЗІ в ІТС.

4 етап – попередні випробування та дослідна експлуатація ІТС з КСЗІ.

На цьому етапі мають бути виконані такі роботи:

– розроблення та узгодження з програми та методики попередніх випробувань;

– проведення попередніх випробувань КСЗІ в ІТС;

– проведення навчання персоналу порядку роботи з засобами КСЗІ;

– передача ІТС з КСЗІ в дослідну експлуатацію;

– супроводження процесу дослідної експлуатації ІТС з КСЗІ (консультації персоналу щодо експлуатації засобів КСЗІ, усунення недоліків, виявлених в процесі дослідної експлуатації і т.п.);

– розроблення та узгодження програми та методики приймальних випробувань;

– проведення приймальних випробувань КСЗІ в ІТС;

– розроблення комплекту документів (формуляр ІТС, заявка на проведення експертизи), необхідних для подання КСЗІ в ІТС на державну експертизу.

5 етап – експертиза КСЗІ та атестація ІТС.

На цьому етапі мають бути виконані такі роботи:

– розроблення програми експертних випробувань КСЗІ в ІТС, погодження її з власником ІТС та ДССЗЗІ;

– розроблення методики експертних випробувань КСЗІ в ІТС, погодження її з ДССЗЗІ;

– проведення експертних випробувань КСЗІ в ІТС згідно з затвердженими програмою та методикою;

– підготовка протоколу експертних випробувань та експертного висновку;

– затвердження в ДССЗЗІ протоколу експертних випробувань та експертного висновку.

6 етап – Впровадження ІТС з КСЗІ в промислову експлуатацію.

На цьому етапі має бути виконано затвердження відповідних директивних документів та впровадження ІТС з КСЗІ в промислову експлуатацію. Результатом робіт по шостому етапу має бути акт про введення ІТС з КСЗІ в промислову експлуатацію.

Висновки

Як свідчить досвід, ефективно вирішувати завдання щодо захисту інформації, що циркулює в інформаційних та телекомунікаційних системах, можна лише шляхом створення в їх складі комплексних систем захисту інформації, що поєднують правові, організаційні, інженерні заходи, а також технічні і програмні засоби захисту. Метою створення КСЗІ є забезпечення захисту інформації, що обробляється, передається та зберігається ІТС державних органів від несанкціонованого доступу, порушення цілісності баз даних, порушення конфіденційності, несанкціонованої модифікації та знищення, а також забезпечення доступності інформації для авторизованих користувачів. Реалізація функцій захисту досягається шляхом використання об`єднаних в єдину систему вбудованих послуг безпеки операційних систем робочих станцій, сертифікованих криптографічних засобів захисту, можливостей спеціалізованого і антивірусного програмного забезпечення, а також шляхом виконання спеціальних організаційних, інженерних та технологічних заходів із захисту інформації. Компоненти комплексу програмно-апаратних засобів ІТС, що беруть участь в реалізації політики безпеки інформації, є складовими КСЗІ ІТС. Захист інформації в розподілених інформаційно-телекомунікаційних системах є складною системною задачею,

яка вимагає застосування комплексу інженерно-технічних, криптографічних, апаратно-програмних та організаційних заходів захисту.

Література

1. Домарев В.В. Безопасность информационных технологий. Системный подход. - К.: ООО «ТИД «ДС», 2004. - 992 с.

2. Класифікація автоматизованих систем і стандартних функціональних профілів захищеності оброблюваної інформації від несанкціонованого доступу НД ТЗІ 2.5-005-99 [Електронний ресурс]. – Режим доступу : http://www.dstszi.gov.ua/dstszi/control/uk/ publish/ article?art_id=101870&cat_id=89734&ctime=1344501089407&showHidden=1.

3. Кормич В.А. Інформаційна безпека України: організаційно-правові основи: Навч. посібник. - К.: Кондор, 2004. - 384 с.

4. Ліпкан В.А. Інформаційна безпека як складова національної безпеки України / В. А. Ліпкан // Інформаційні технології в економіці, менеджменті і бізнесі : Проблеми науки, практики і освіти : Зб. наук. праць VIII Міжнар. наук.-практ. конф. — Ч. 2. — К. : Вид-во Європ. ун-ту, 2003. — С. 443— 453.

5. Порядок проведення робіт зі створення комплексної системи захисту інформації в інформаційно-телекомунікаційній системі НД ТЗІ 3.7-003-05[Електронний ресурс]. – Режим доступу http://www.dstszi.gov.ua/dstszi/control/ uk/publish/article?art_id=46074&cat_id=38835

6. Почепцов Г. Г. Коммуникативные технологии двадцатого века. - М.: Рефл-бук; К.: Ваклер, 2000. - 352 с.

7. Рабинович П.М. Основи загальної теорії права і держави : [посіб. для студ. спец-ті «Правознавство»] / П. М. Рабинович. — К., 1994. — 236 с.

8. Сайт ДССЗЗІ. [Електронний ресурс]. – Режим доступу : http://dstszi.kmu.gov.ua/dstszi/control/uk/publish/category?cat_id=112509.

9. Теорія держави та права: [навч. посіб.] / А.М.Колодій, В.В.Копейчиков, С.Л.Лисенков та ін.; За заг. ред. С.Л. Лисенкова, В.В. Копейчикова. – К. : Юрінком Інтер, 2003. — 368 с.

Васєв В.О,
Майданюк П.В.,
Управління Державної служби спеціального зв'язку та захисту інформації України в Миколаївській області

СУЧАСНІ МЕТОДИ ОЦІНЮВАННЯ ЗАХИЩЕНОСТІ ІНФОРМАЦІЇ

Для оцінки ефективності заходів із технічного захисту інформації (ТЗІ) та аналізу можливості використання систем захисту на об'єктах інформаційної діяльності (ОІД) використовуються наступні методи:
- атестація комплексів технічного захисту інформації;
- експертиза в сфері технічного захисту інформації (підтвердження відповідності);
- оцінка стану захищеності державних інформаційних ресурсів;
- сертифікація системи управління інформаційною безпекою;
- державний контроль.

1. Атестація комплексу технічного захисту інформації

Атестація комплексу ТЗІ - оцінка відповідності комплексу ТЗІ та показників захищеності інформації (у тому числі їх визначення) від витоку технічними каналами на об'єктах інформаційної діяльності (об'єктах електронно-обчислювальної техніки) вимогам

нормативно-правових актів і нормативних документів з питань ТЗІ. Комплекси технічного захисту інформації створюються на об'єктах інформаційної діяльності, де передбачається:
- озвучення інформації з обмеженим доступом;
- здійснення обробки інформації з обмеженим доступом технічними засобами, автоматизованими системами;
- обіг іншої інформації з обмеженим доступом при проектуванні, будівництві, експлуатації об'єктів, виробництві технічних засобів тощо.

Суб'єктами атестації є:
- замовник створення комплексу ТЗІ;
- виконавець робіт зі створення комплексу ТЗІ;
- виконавець робіт з пошуку закладних пристроїв;
- виконавець проведення атестації комплексу ТЗІ;
- Адміністрація Держспецзв'язку.

Атестація комплексу ТЗІ передбачає розробку програми та методики атестації, проведення інструментального контролю ефективності захисту, перевірку на наявність закладних пристроїв, аналіз впроваджених заходів захисту, складання акту атестації, реєстрація акту атестації в Адміністрації Держспецзв'язку.

2. Експертиза в сфері технічного захисту інформації

Експертиза в сфері технічного захисту інформації (експертиза) проводиться з метою дослідження, перевірки, аналізу та оцінки об'єктів експертизи щодо їх відповідності вимогам нормативних документів з технічного захисту інформації та можливості їх використання для забезпечення технічного захисту інформації.

Об'єкти експертизи:
- комплексні системи захисту інформації в ІТС;
- технічні та програмні засоби захисту інформації.

Суб'єкти експертизи:
- юридичні та фізичні особи (замовники експертизи);
- Адміністрація Держспецзв'язку;
- підприємства, установи та організації, які проводять експертизу (організатори експертизи);
- державні органи, які проводять експертизу в сфері свого управління;
- фізичні особи (експерти).

Способи проведення експертизи КСЗІ в ІТС:
- шляхом експертних випробувань;
- шляхом аналізу декларації про відповідність КСЗІ вимогам нормативних документів.

За результатами проведених робіт організатор експертизи складає Експертний висновок відповідного змісту щодо відповідності об'єкта експертизи вимогам нормативних документів з ТЗІ. Експертний висновок разом з протоколом експертизи подається на розгляд Експертної ради Держспецзв'язку. Після реєстрації експертного висновку замовнику експертизи надається Атестат відповідності КСЗІ в ІТС. Розгляд декларації і поданих разом із нею документів, та прийняття рішення про її реєстрацію здійснюється Експертною радою Держспецзв'язку в місячний строк.

3. Оцінка стану захищеності інформації

Оцінка стану захищеності інформації в інформаційно-телекомунікаційній системі - це заходи щодо виявлення в інформаційно-телекомунікаційній системі технічних рішень, що створюють можливість здійснення дій з порушення цілісності, конфіденційності та доступності інформації, яка в ній циркулює.

Оцінка стану захищеності здійснюється з метою виявлення існуючих загроз державним інформаційним ресурсам в ІТС і є складовою частиною заходів із захисту інформації.

Об'єктом оцінки є стан захищеності державних інформаційних ресурсів, які обробляються в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, незалежно від наявності комплексної системи захисту інформації.

Суб'єкти оцінки стану захищеності:

- органи державної влади місцевого самоврядування;
- військові формування, утворені відповідно до законів України;
- підприємстві, установі, організації незалежно від форми власності;
- Державний центр кіберзахисту та протидії кіберзагрозам Держспецзв'язку.

Форми проведення оцінки стану захищеності:

- комплексний аудит інформаційної безпеки;
- сканування державних інформаційних ресурсів, розміщених в мережі Інтернет.

Комплексний аудит інформаційної безпеки включає:

- аналіз документації, інженерних систем, систем життєзабезпечення;
- вивчення ІТС, побудова карт комутації, схем адресації та маршрутизації;
- аналіз політики безпеки в АРМ, мережному та серверному обладнанні, стан засобів захисту;
- опитування персоналу (керівників, адміністраторів, користувачів);
- сканування складових ІТС за допомогою спеціалізованого програмного забезпечення з метою виявлення вразливостей;
- тест на проникнення (за згодою);
- складання висновку, розробка рекомендацій, підготовка звіту.

4. Сертифікація системи управління інформаційною безпекою

Сертифікація системи менеджменту інформаційної безпеки підприємства на відповідність стандарту ISO 27001 проводиться установами, акредитованими міжнародними органами сертифікації.

Основні переваги сертифікації:

- надається міжнародний сертифікат відповідності;
- аудит інформаційної безпеки проводиться незалежними експертами;
- надається об'єктивна оцінка ефективності СМІБ;
- покращується керованість ризиками інформаційної безпеки;
- підвищується рівень довіри та конкурентоспроможність, переваги на міжнародних ринках;
- збільшується капіталізація та вартість акцій.

5. Державний контроль

Державний контроль за станом технічного захисту інформації полягає в перевірці виконання вимог нормативно-правових актів і нормативних документів з ТЗІ та здійснюється з метою визначення стану технічного захисту інформації в органах, щодо яких здійснюється ТЗІ, виявлення порушень з ТЗІ та запобігання їм.

Державний контроль за станом технічного захисту інформації здійснюється Держспецзв'язку шляхом організації та проведення контрольно-інспекторської роботи з питань ТЗІ стосовно органів, щодо яких здійснюється ТЗІ.

Контрольно-інспекторська робота з питань технічного захисту інформації включає планування, проведення інспекційних перевірок стану ТЗІ в органах, щодо яких здійснюється ТЗІ аналіз їх результатів та надання рекомендацій щодо вдосконалення стану ТЗІ в зазначених органах.

За результатами перевірки здійснюється оцінка адміністративно-правового стану ТЗІ, повноти та достатності заходів щодо впровадження комплексу технічного захисту інформації та їх відповідності вимогам нормативно-правових актів з ТЗІ.

Вільський Г.Б., PhD, доцент,
Михалишин Б.Є., к.т.н.,
МТУ «Миколаївська політехніка»

СТАНОВЛЕННЯ І РОЗВИТОК НЕФОРМАЛЬНОЇ ОСВІТИ З ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

В Україні сформовано певний спектр освітньо-кваліфікаційних рівнів з інформаційної безпеки, який реалізується шляхом проведення підготовки бакалаврів, спеціалістів і магістрів за формальною формою у вищих навчальних закладах (ВНЗ). Отримані знання і компетентності орієнтовані на роботу з інформаційно-комунікаційними системами, системами технічного захисту інформації та управління інформаційною безпекою. Такі дії з підготовки кадрів у ВНЗ, які проводяться з використанням формальної форми організації навчання, не можуть повною мірою вирішити постійно виникаючі різноманітні проблемні питання у сфері інформаційної безпеки через недостатність, а часом і відсутність нової неформальної форми навчання, яка дає відповідь на прийняття рішень в реальному часі і ситуації. Отже за межами формальної освіти в Україні, виходячи з європейської концепції навчання та інтеграції освіти впродовж усього життя, недостатньо розвивається гнучка форма підготовки кадрів на виробництві за неформальною формою, яка швидко реагує на запити і процеси інформаційної безпеки в підприємництві. Зазначене становище свідчить про актуальність висвітлення позитивних показників при вирішенні комплексу завдань по значному підвищенню обсягів неформальної освіти в цій галузі знань на підприємствах.

Мета роботи - показати доцільність неформальної освіти з інформаційної безпеки на обґрунтованому прикладі встановлення динаміки кількісних і якісних показників проведення вибраного науково-практичного форуму.

На сьогоднішній день проблематика неформального навчання, його визнання, участь промисловців і підприємців в підготовці кадрів практично не досліджувалася в Україні. Функціонування «неформального професійного навчання працівників» базується на Законі України «Про професійний розвиток працівників» [1]. Методичне опрацювання регулюється порівняльними вимогами щодо розвитку формальної та неформальної освіти в контексті євроінтеграції освітнього простору [2]. Також неформальне навчання з інформаційної безпеки набуває привабливості як складова професійного навчання працівників на виробництві, тому що воно не регламентується місцем набуття, строками та формою.

Базуючись на існуючому вітчизняному досвіді, розширюється підготовка кадрів з тематики інформаційної безпеки на виробництві. Вона здійснюється шляхом активізації діяльності навчальних підрозділів на підприємствах та за рахунок концентрації і консолідації зусиль по акцентуванню питань інформаційної безпеки при вивченні спеціальних профільних дисциплін на всіх рівнях національної рамки кваліфікацій. Для розвитку у працівників компетенцій з інформаційної безпеки роботодавці повинні у плановому порядку постійно виконувати низку організаційних і навчально-методичних заходів. При оцінці працівників за кваліфікаційними вимогами і посадовими обов'язками слід ураховувати їх участь у неформальному навчанні. Навчання працівників зі спеціальних курсів з інформаційної безпеки визначається з урахуванням специфіки професії, умов праці та строку навчання. Дослідження процесів становлення і розвитку неформального навчання з інформаційної безпеки виконувалося на прикладі проведення Всеукраїнської науково-практичної конференції «Стан та удосконалення безпеки інформаційно-телекомунікаційних

систем», яку проводить за денною формою «Міжнародний технологічний університет «Миколаївська політехніка». Проводилось вивчення динаміки тематичної спрямованості доповідей і виступів в плані їх орієнтації на відображення нормативного забезпечення виконання робіт з безпеки інформації, технічних аспектів реалізації інформаційно-комунікаційних систем в сферах економіки, фундаментальності математичного базису побудови комплексних систем захисту інформації. Дослідження зміни чисельності зацікавлених учасників з отримання неформальних знань наведено на рис. 1. Динаміка контингенту конференцій показана на рис. 2.

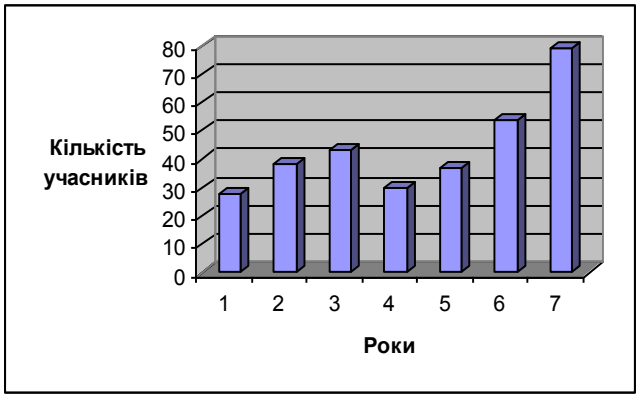

Рис. 1. Зміна чисельності зацікавлених учасників

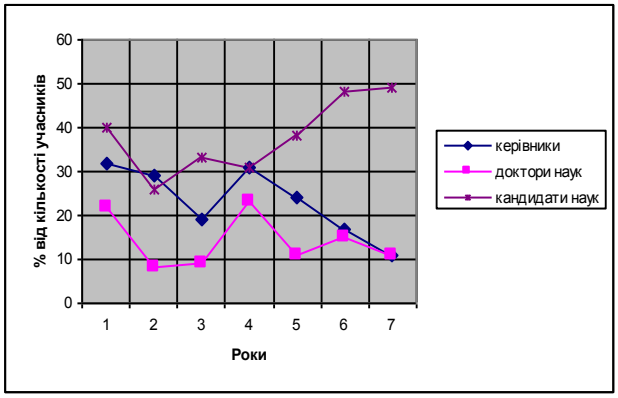

Рис. 2. Динаміка контингенту конференцій

За період 2009-2015 роки відбувалося формування колективу учасників, спостерігався експонентний характер приросту учасників, який доходив до 45%, за рахунок привабливості заходів і підвищення зацікавленості науково-педагогічних працівників ВНЗ. Істотно і діаметрально змінювалася тематика доповідей, а значить і придбання знань по фізико-математичному (фундаментальному), технічному та нормативному забезпеченням при неформальному навчанні. Процеси, які проходили наведені на рис. 3, 4.

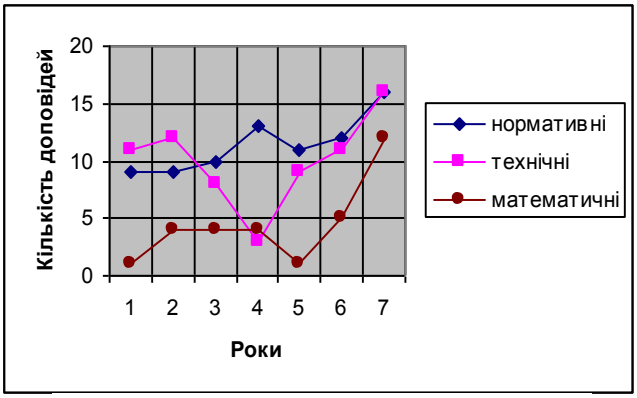

Рис. 3. Зміна тематики доповідей конференцій

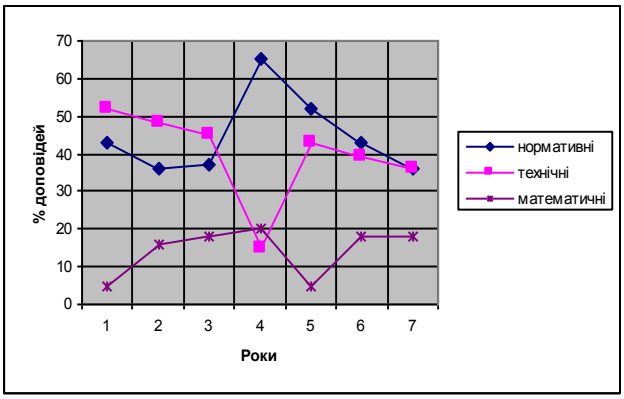

Рис. 4. Відносна зміна спрямованості доповідей

З вказаних графіків очевидно, що на протязі другого періоду проведення конференцій відбувалося абсолютне збільшення кількостей доповідей по кожній з спрямованостей та стабілізувалися відносні чисельності представлених робіт з встановленням контингенту учасників по їх науковим інтересам. Виявлена динаміка показників і проявлені тенденції характеризують позитивність процесів фундаментального, науково-прикладного, техніко-технологічного та нормативного забезпечень, спрямованих на розвиток і підвищення ефективності неформального навчання для сфери інформаційної безпеки держави.

Висновки

Обгрунтовано доцільність неформальної форми навчання з питань інформаційної безпеки. Висвітлено переваги такої освіти для працівників в умовах виробництва. Отримані

результати дослідження динаміки показників зацікавленості до науково-практичної конференції показують зміну кількості учнів з експонентним зростанням у другій половині, яке доходило до 45%, поширення професійної орієнтації контингенту і різноманітності спрямованостей навчальних доповідей.

Література

1. Закон України «Про професійний розвиток працівників» N 4312-VI від 12.01.2012.- Режим доступу: zakon.rada.gov.ua/go/4312-17
2. Возняк О. Порівняльний аналіз формальної та неформальної освіти в контексті євроінтеграції освітнього простору / О. Возняк //К.: Науково-практичне видання «Вища Школа», 2016. – № 2 (139) – С. 41-47.

Воронов В.Р., к.т.н., доцент,
Державна служба спеціального зв'язку та захисту інформації України, Київ

НОРМАТИВНІ ОСОБЛИВОСТІ ОРГАНІЗАЦІЇ ЗАХИСТУ ІНФОРМАЦІЇ ВІД ВИТОКУ ТЕХНІЧНИМИ КАНАЛАМИ

Інформація, яка є важливою для особи, суспільства та держави і втрата якої може спричинити шкоду особі, суспільству або національним інтересам держави в економічній, політичній, військової або інших сферах, повинна захищатися від несанкціонованого ознайомлення спотворення, знищення та блокування.

Захист інформації – це діяльність із забезпечення конфіденційності, цілісності та доступності важливої для особи, суспільства та держави інформації, яка обробляється в інформаційно-телекомунікаційних (автоматизованих) системах або озвучується на об'єктах інформаційної діяльності, а також із забезпечення використання інформації у відповідності з встановленими правилами. Конфіденційність, цілісність та доступність – це властивості, які характеризують інформацію як об'єкт захисту.

Конфіденційність – властивість інформації, яка характеризує захищеність інформації від несанкціонованого ознайомлення. Цілісність – властивість інформації, яка характеризує захищеність інформації від несанкціонованого спотворення, руйнування або знищення. Доступність – властивість інформації, яка характеризує захищеність інформації від несанкціонованого блокування.

Захищеність інформації – стан інформації, при якому забезпечена відповідність показників захищеності інформації нормам та вимогам захищеності інформації.

Основними загрозами для інформації, що озвучується на об'єктах інформаційної діяльності (ОІД), є витік інформації технічними каналами.

Основними загрозами для інформації, що обробляється в автоматизованих системах (АС), є витік інформації технічними каналами; несанкціоновані дії з інформацією (у тому числі з використанням комп'ютерних вірусів та кібератак); спеціальний електромагнітний вплив на засоби обробки інформації.

Для захисту інформації, що озвучується, від витоку технічними каналами на об'єкті інформаційної діяльності створюється комплекс технічного захисту інформації (комплекс ТЗІ). Для захисту інформації, що обробляється в АС, створюється комплексна система захисту інформації (КСЗІ), які складається з:

комплексу технічного захисту інформації – для захисту інформації від витоку технічними каналами;

комплексу засобів захисту від несанкціонованих дій з інформацією;

комплексу засобів захисту від спеціальних електромагнітних впливів.

Створення комплексу ТЗІ передбачає два етапи:

розроблення комплексу ТЗІ (І етап);

упровадження комплексу ТЗІ (ІІ етап).

Після створення комплексу ТЗІ здійснюється його атестація.

Розроблення комплексу ТЗІ передбачає виконання передпроектних робіт та розробку технічного проекту. Передпроектні роботи передбачають категоріювання ОІД, обстеження ОІД, (спеціальні дослідження ОІД), спеціальні дослідження ОТЗ, інженерний аналіз ДТЗС (спеціальні дослідження ДТЗС), розробку моделі загроз для інформації та технічного завдання на створення комплексу ТЗІ.

Упровадження комплексу ТЗІ передбачає придбання (закупівлю) засобів ТЗІ та іншого обладнання, монтаж та налагодження (настроювання) засобів ТЗІ, розробку технічної та експлуатаційної документації на комплекс.

Атестація комплексу ТЗІ передбачає здійснення інструментального контролю захищеності інформації та проведення перевірки повноти і відповідності реалізованих на ОІД заходів із захисту інформації від витоку властивими конкретному ОІД технічними каналами вимогам технічного завдання на створення комплексу ТЗІ, нормативно-правових актів та нормативних документів системи ТЗІ.

Вимоги до захищеності інформації від витоку технічними каналами та норми захищеності інформації визначаються нормативно-правовими актами та нормативними документами системи ТЗІ.

За результатами атестації складається акт атестації комплексу ТЗІ. Обробка технічними засобами та/або озвучення інформації, що підлягає захисту від витоку технічними каналами, без наявності чинного акта атестації комплексу ТЗІ забороняється.

Виконавцем атестації може бути підрозділ ТЗІ відповідного державного органу за наявності у цього органу дозволу на виконання робіт з ТЗІ для власних потреб або суб’єкт господарювання, який має відповідну ліцензію на провадження господарської діяльності у галузі ТЗІ.

Технічні аспекти створення комплексів ТЗІ, вимоги (рекомендації) до захисту інформації, норми захищеності інформації, методики спеціальних досліджень ОІД, ОТЗ та ДТЗС, методики інструментального контролю захищеності інформації від витоку технічними каналами визначаються відповідними нормативними документами системи технічного захисту інформації (НД ТЗІ).

В Україні на теперішній час розроблена та у встановленому порядку впроваджена система нормативного забезпечення технічного захисту інформації, що охоплює різні аспекти ТЗІ та дозволяє ефективно функціонувати всій системі ТЗІ. Проте система нормативного забезпечення ТЗІ перебуває в незавершеному стані, мають місце як загальносистемні, так і внутрісистемні проблемні питання. Зокрема, немає загальносистемного базового нормативно-правового документа – захист інформації на певних об'єктах регулюється різнорівневими за юридичною силою нормативними документами. Деякі нормативні документи системи не погоджені між собою або дублюють один одного. Правові основи окремих складових сфери захисту інформації встановлюються підзаконними актами. Певне виключення представляє правове регулювання відносин, які виникають при захисті інформаційно-телекомунікаційних системах, де правові основи встановлюються Законом України “Про захист інформації в інформаційно-телекомунікаційних системах”. Однак цей Закон не визначає поняття, принципи, норми й правила ТЗІ, загальні для всіх об'єктів, де здійснюється захист інформації. Це дозволяє зробити висновок про наявність проблемних питань у системі нормативного забезпечення ТЗІ, і як наслідок – певна необґрунтованість та неадекватність реальним загрозам вимог до захисту інформації.

Метою дослідження є виявлення та аналіз проблемних питань в системі нормативного забезпечення, зокрема захисту інформації від витоку технічними каналами.

За результатами дослідження встановлено відсутність в системі нормативного забезпечення ТЗІ обґрунтованих вимог до захисту інформації від витоку каналами "ВЧ-нав'язування", акустоелектричними каналами, візуально-оптичними каналами тощо. Виявлено застарілість методик спеціальних досліджень засобів електронної техніки, методик інструментального контролю захищеності інформації від витоку каналами побічних електромагнітних випромінювань (зокрема при використанні пасивних та активних засобів захисту інформації), каналами "ВЧ-нав'язування", акустоелектричними та візуально-оптичними каналами. Виявлені некоректності у методиках інструментального контролю захищеності інформації від витоку каналами побічних електромагнітних наведень на лінії електроживлення, заземлення та комунікації допоміжних технічних засобів та систем. Встановлено також відсутність або невідповідність сучасним вимогам та недостатність унормованих вимог до засобів ТЗІ особливо для захисту інформації від витоку лазерними акустичними каналами.

На даний момент фахівцями Адміністрації Держспецзв'язку планомірно вирішуються згадані вище проблемні питання: розроблений проект Закону України "Про криптографічний та технічний захист інформації", прийняті нове Положення та Нормативний документ системи ТЗІ, які з урахуванням сучасних реалій регламентують захист інформації від витоку технічними каналами на об'єктах інформаційної діяльності та в інформаційно-телекомунікаційних системах, обґрунтовуються методики спеціальних досліджень засобів обробки інформації та методики інструментального контролю захищеності інформації від витоку технічними каналами, які проходять процедуру погодження вимоги до засобів ТЗІ.

Список використаних джерел

1. Положення про технічний захист інформації в Україні. Затверджено Указом Президента України від 27.09.99 № 1229.

2. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.

3. НД ТЗІ 1.1-005-07 Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення.

Гавриленко О.В., к.т.н.,
Адміністрація Державної служби спеціального зв'язку та захисту інформації України, Київ

ОРГАНІЗАЦІЯ ЗАХИСТУ ІНФОРМАЦІЇ В ДЕРЖАВНИХ ОРГАНАХ НА ОСНОВІ МІЖНАРОДНИХ СТАНДАРТІВ З УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

Важливе місце у загальнодержавній системі інформаційної безпеки займають питання захисту інформації. Порядок виконання робіт з технічного захисту інформації на даний час регулюється нормативно-правовими актами, якими є: Положення про технічний захист інформації в Україні [1], Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [2], Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [3], а також нормативні документи системи технічного захисту інформації. Поточний стан розвитку нормативної бази у сфері технічного захисту інформації дозволяє здійснювати виконання усіх основних етапів робіт із захисту.

При цьому, на сьогодні у правому полі сфери питання управління організацією робіт, а тим більше встановлення певного регламенту цієї діяльності, не врегульовані в повному обсязі. Тому задля підвищення якості робіт у предметній галузі слід розглянути можливість

упорядкування й систематизації організаційних процедур забезпечення таких робіт. Відповідно, метою дослідження є удосконалення системи захисту інформації у напрямі організації робіт із захисту в інформаційно-телекомунікаційних системах (далі – ІТС) та на об'єктах інформаційної діяльності (далі – ОІД) в органах державної влади, на підприємствах, в установах, організаціях (далі – установи).

Не викликає сумніву, що продукція у галузі (а це – як окремі засоби захисту, так і комплексні системи захисту інформації (далі – КСЗІ) в ІТС і комплекси технічного захисту інформації (далі – КТЗІ) на ОІД) для виконання свої цільової функції повинні бути якісними. Вимоги до якості будь-якої продукції встановлено стандартами ISO серії 9000 (14000), якими визначено необхідні умови стосовно складу, послідовності робіт, розподілу видів діяльності, порядку організації робіт на всіх етапах створення продукції для того, щоб цю продукцію можна було визнавати якісною.

В основі якісного створення КСЗІ та КТЗІ лежить правильна організація робіт суб'єктом створення. Саме такий підхід декларується стандартами серії ISO/IEC 27000, якими визначається загальна організація робіт із захисту інформації в установі, способи класифікації ресурсів, напрями планування робіт, відповідальність керівництва та співробітників, завдання служб захисту інформації тощо. Стандарти описують системний підхід до управління захистом інформації і є тим інструментом, який дозволяє створити в установі таку систему організації робіт на всіх етапах, яка б максимально сприяла отриманню якісного кінцевого результату.

Для упровадження в сфері захисту інформації нормативної бази, яка б регламентувала процедури управління організацією робіт із захисту в установах, визначала б умови, коли такі процедури є обов'язковими, а коли можуть застосовуватися суб'єктами на власний розсуд, і нарешті, забезпечувала гармонізацію з міжнародними стандартами, пропонується запровадити технічний регламент системи управління інформаційною безпекою (далі – Технічний регламент), який повністю повторюватиме підходи, що застосовуються в ISO/IEC 27001, 27002 [4, 5].

Документом буде визначатися наступне.

СУІБ установи повинна включати: організаційну структуру, процес планування діяльності, політики реалізації заходів і виконання робіт, встановлення і розподіл відповідальності, документування всіх затверджених процедур і процесів, необхідні ресурси, інструкції і методичні рекомендації із застосування.

СУІБ в установі створюватиметься згідно з вимогами стандарту ДСТУ ISO/IEC 27001, а оцінка відповідності цього Технічного регламенту буде проводитися згідно з процедурою державної експертизи у сфері технічного захисту інформації із попереднім застосуванням, за необхідності, заходів, визначених процедурою державної експертизи у сфері криптографічного захисту інформації. При цьому можуть враховуватися також вимоги ДСТУ ISO 19011:2012 «Настанови щодо здійснення аудитів систем управління» (ISO 19011:2011 [6], IDT) (або документів, якими їх буде замінено з 2017 року).

Регламент повинен враховувати всі вимоги діючого законодавства України у сфері захисту інформації, яким регулюються безпосередньо вимоги, склад робіт та порядок створення КСЗІ в ІТС і КТЗІ на ОІД, а механізм, який застосовуватиметься для досягнення поставленої мети, не передбачатиме внесення змін до зазначеної нормативної бази. Натомість документ сприятиме підвищенню відповідальності керівників установ за якість виконання цих робіт.

Водночас, Технічний регламент встановлюватиме додаткові вимоги до фізичних та юридичних осіб, які є власниками об'єктів, де обробляється інформація, що потребує захисту згідно з законодавством, в частині організації робіт та не повинен зачіпати інтересів суб'єктів господарської діяльності, які виконують роботи за ліцензіями.

У результаті впровадження Технічного регламенту очікується підвищення якості виконання робіт із захисту державних інформаційних ресурсів, іншої інформації,

необхідність захисту якої визначено законом, підвищення відповідальності керівників установ за ефективність забезпечення захисту інформації.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Положення про технічний захист інформації в Україні, затверджене Указом Президента України від 27.09.1999 № 1229 [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/1229/99.

2. Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" [Електронний ресурс]. – Режим доступу: http://zakon0.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

3. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29.03.2006 № 373 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/373-2006-%D0%BF.

4. ISO/IEC 27001:2013 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования [Електронний ресурс]. – Режим доступу: https://www.iso.org/obp/ui/ #iso:std:iso-iec:27001:ed-2:v1:en.

5. ISO/IEC 27002:2013 Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/catalogue_detail?csnumber =54533.

6. ISO 19011:2011 Guidelines for auditing management systems [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/home/search.htm?qt=ISO +19011%3A2011& published= on&active_tab=standards&sort_by=rel.

Герганов Л.Д., к.п.н., доцент,
заступник начальника Навчального центру «Українське Дунайське пароплавство», Ізмаїл,
Герганов М.Л., к.т.н., доцент,
Київська державна академія водного транспорту

ІННОВАЦІЙНІ ТЕХНОЛОГІЇ НАВЧАННЯ В ПРОЦЕСІ ПІДГОТОВКИ ПЛАВСКЛАДУ НА ВИРОБНИЦТВІ

Соціально-економічний і психолого-педагогічний аналіз функціонування навчального закладу на виробництві з системних позицій допомагає виявити основні переваги, за яких забезпечується організація навчального процесу на сучасному рівні освітніх послуг. Це, передусім, якість, терміни, затрати ресурсів на навчання, моніторинг надання освітніх послуг на ринку праці, сучасне матеріально-технічне забезпечення, інноваційні технології навчання, гнучкість навчальних програм.

Усе це сучасна професійна освіта формує не повною мірою тому, що школа не враховувала високої динаміки економічних процесів, плинності ринку праці, насиченості інформаційними потоками. Хоча форма організації праці на флоті залишилася незмінною, однак умови праці робітника морського профілю в складі екіпажу суднової команди (іноді він є скороченим) істотно змінилися. Працівники об'єднуються для виконання певної задачі, на певному типі судна при виконанні чітко запланованого рейсу, заздалегідь заданому маршруті. Після його закінчення колектив розпадається, а окремі члени суднової команди морського судна переходять на інші судна як під національним, так і під іноземним прапором, де суднова команда часто вже має багатонаціональний склад.Така організація праці потребує здатностей працювати в єдиному екіпажі, часто багатонаціональному,

комунікабельності, толерантності, вміння ставити цілі та досягати їх. Зазначимо, що робітник, який сформований і вихований "старою школою" за радянських часів, ні приймати відповідальних рішень, ні нести за них відповідальності, частіше за все, не може та й не хоче. Все це потребує від інструкторсько-викладацького складу нових підходів до професійної підготовки робітників плавскладу, впровадження в навчальний процес сучасних інноваційних технологій і застосування сучасних ефективних методик навчання спрямованих на результат та засобів навчання.

Зазначимо, що сучасний світовий морський флот останнім часом насичується інформаційною технікою різного класу: від простих контролерів до мультипроцесорних систем і багатомасштабних комплексів. Впродовж останніх десятиліть автоматизувалися такі процеси: розрахунок параметрів руху судна, контроль його морехідних якостей, опрацювання радіолокаційної інформації, управління технічними засобами судна, діагностика суднового електронного та радіообладнання, що потребує високого рівня організації навчального процесу, забезпеченість його спеціалізованим дидактичним матеріалом та засобами контролю якості навчання.

Аналізу сучасних педагогічних технологій відводиться значне місце у професійній педагогіці. Інноваційні педагогічні технології підпорядковані конкретній меті, дають позитивний результат при спільній роботі інструкторсько-викладацького складу й тих, хто вчиться, і спрямовані на впровадження нововведень у зміст, методи, форми та засоби професійного навчання кадрів на виробництві. Також підкреслимо, що, на відміну від новаторських методик і педагогічної майстерності викладацького складу, педагогічні технології мають гарантію кінцевого результату й можливість відтворення та проектування у майбутньому навчальному процесі, на що вказували відомі українські дослідники (І. Підласий [3], О. Пометун [1], Л. Пироженко [1], С. Сисоєва [3]). Так, Д. Чернілевський виділив вісім ознак відмінності цих термінів і довів, що поняття «технологія навчання» має більш граничне значення, ніж «методика навчання» [4, С. 50-51].

У нашому дослідженні під інноваційною педагогічною технологією будемо розуміти набір навчальних процедур, які вдосконалюють навчальний процес, упроваджують нововведення й гарантують кінцевий запланований результат, що дуже важливо у професійному становленні робітника морського профілю при його навчанні на виробництві. Розвиток і поширення інноваційних педагогічних технологій зумовлені, з одного боку, зростанням у виробничому процесі нових технологій, інформаційно-комунікаційних засобів, автоматизованого моніторингу руху суден, супутникового контролю судноплавства, електронно-картографічної технології прийняття управлінських рішень, які потребують від робітника широкого спектра професійних знань і подолання статики традиціоналізму, а з іншого – зростанням у навчальному процесі значущості таких навчальних дисциплін, в основі яких лежить вивчення різноманітних професійних ситуацій. У цьому контексті головним завданням відпрацювання цих ситуацій є не тільки отримання певного завершеного навчання, а й формування практичних навичків поведінки залежно від ситуації, що виникає.

Наукові публікації, які присвячені впровадженню інноваційних педагогічних технологій у професійну підготовку кваліфікованого робітників, здебільшого аналізують їх ефективність за умови навчання в ПТНЗ. Для професійного навчання робітників морського профілю на виробництві такі розрахунки відсутні, а вплив окремих параметрів професійної готовності моряків до роботи в умовах особистого виживання, набутої професійної компетентності на економічні показники судноплавної компанії та кар'єрне професійне зростання недостатньо досліджені.

Впровадження у процесі навчання інноваційних педагогічних технологій з використанням тренажерних комплексів та розробленого навчально-методичного забезпечення потребує підвищення кваліфікації інструкторсько-викладацького персоналу, адже навіть достатньо кваліфіковані виробничі кадри не завжди можуть передати слухачам набуті професійні знання та навички, оскільки дидактична компонента їх складової частини

слабка. У процесі використання ідеї віртуальної технології навчання для професійної підготовки робітників морської галузі було впроваджено з'єднання сучасної інформаційної технології з реальними об'єктами, які підлягають обслуговуванню, та забезпечено вихід на реально-віртуальний простір навчання моряків. Під цим терміном нами розуміється розроблення й створення такої навчально-матеріальної бази, яка поєднує переваги віртуального моделювання умов праці за допомогою комп'ютерної техніки і створює умови для використання в навчальних цілях реальних об'єктів судна. Результати наукового дослідження були враховані нами в процесі практичної реалізації результатів дослідження при вдосконаленні навчально-матеріальної бази Учбового центру «Українського Дунайського пароплавства». Навчально-тренажерне судно «Новий Донбас» (НТС «Новий Донбас») – це морське судно, що переобладнане для професійної та тренажерної підготовки моряків. спілкування між слухачами курсів на різні теми. Сучасні засоби комп'ютерної візуалізації і системи аварійної сигналізації, які розташовані на реальному навчально-тренажерному судні «Новий Донбас», дають змогу не лише відображати зображення зовнішнього і внутрішнього змісту невизначеності навігаційних та експлуатаційних процесів на різних рівнях навчального процесу, а й відтворювати навколишню обстановку, яка містить: водний простір, берегову мережу, навігаційну ситуацію, берегові об'єкти, споруди, ефекти видимості та освітленості і, таким чином, наблизити психоемоційну обстановку в процесі навчання до реальних умов.

Список використаних джерел

1. Пометун О.І., Пироженко Л.В. Сучасний урок. Інтерактивні технології навчання: науково-метод. посіб. / О.І. Пометун, Л.В. Пироженко / За ред. О.І. Пометун. – К.: Видавництво А.С.К., 2003. – 192с.

2. Сисоєва С.О. Технології педагогічної творчості в системі освітніх технологій // Освітні технології у школі та вузі: Матеріали науково-практичної конференції – Миколаїв: МФ НаУКМА, 1999. – С.25-27

3. Підласий І.П. Практична педагогіка або три технології: Інтерактивний підручник для педагогів ринкової системи освіти. – К.: Видавничий Дім «Слово», 2004. – 616с.

4. Чернилевский Д.В. Дидактические технологии в высшей школе: Учебное пособие для вузов. – М.: ЮНИТИ – ДАНА, 2002. – 437с.

Гнатюк В. О., асистент,
Іванченко І.С., асистент,
Наджі Абду Ахмед Алі,
Національний авіаційний університет, Київ

МЕРЕЖЕВО-ЦЕНТРИЧНИЙ ПІДХІД ДО МОНІТОРИНГУ КІБЕРІНЦИДЕНТІВ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ

Останнім часом термін «мережево-центричний» все частіше використовується в різних галузях, пов'язаних з використанням мережевих комп'ютерних технологій у сфері управління. Мережево-центрична (Network-centric) концепція управління виникла у військовому середовищі не стільки в процесі теоретичних досліджень, скільки внаслідок систематичного аналізу результатів впровадження в збройні сили нових бойових засобів і підвищення рівня освіченості особового складу. Характерна особливість мережево-центричної системи виражається в здатності кожної територіально-розподіленої компоненти (вузла) діяти в напрямку досягнення спільної мети і мати рівні можливості до доступу інформації, необхідної для здійснення функцій і досягнення мети, незалежно від розташування цієї інформації в системі. Зважаючи на принципи, що покладені в основу

мережево-центричного управління, воно буде ефективним, зокрема і для моніторингу кіберінцидентів в інформаційно-комунікаційних системах (ІКС).

Метою роботи є розробка методу мережево-центричного моніторингу кіберінцидентів в ІКС. Для досягнення поставленої мети необхідно вирішити наступні задачі: провести аналіз існуючих методів, моделей, систем обробки прогнозування та моніторингу кіберінцидентів в ІКС; розробити метод мережево-центричного моніторингу кіберінцидентів в ІКС; експериментально дослідити метод мережево-центричного моніторингу кіберінцидентів в ІКС.

В процесі роботи проведено аналіз методів, моделей, систем обробки прогнозування та моніторингу. А саме, розглядалися сервіси JSOC: моніторинг інцидентів (JSOC – це набір сервісів ІБ для моніторингу інцидентів і протидії сучасним загрозам); модель, метод та методика для оцінки та побудови системи моніторингу інформаційного простору; моніторинг подій і виявлення інциденту інформаційної безпеки з використанням SIEM-систем (SIEM-система вирішує завдання зі збору та зберігання інформації з різних джерел, аналізу вхідних подій, їх кореляції і обробці за правилами, виявлення інцидентів, їх пріоритетності та автоматичного оповіщення); реєстрація інцидентів з використанням кнопки допомоги ITSM (повна або часткова автоматизація процесів реєстрації, кваліфікації, маршрутизації і діагностики інциденту).

Інформаційно-комунікаційна система (ІКС) - сукупність інформаційних та комунікаційних систем, які у процесі обробки інформації діють як єдине ціле. Типовий склад ІКС: 1) серверне обладнання (комп'ютери з підвищеною продуктивністю та технічними характеристиками; зазвичай призначені для надання одного або декількох специфічних сервісів, на кшталт електронного поштового обміну, баз даних, IP-телефонії, файлового сховища тощо); 2) середовище передачі даних (оптоволоконні лінії, кабелі типу «звита пара», телефонні кабелі, бездротові канали передачі даних (Wi-Fi, Wi-MAX, Bluetooth)); 3) активне мережеве обладнання і обладнання зв'язку (комутатори, маршрутизатори, модеми, бездротові точки доступу, телефонія), а також пристрої захисту (міжмережеві екрани, системи виявлення/попередження вторгнень тощо); 4) автоматизовані робочі місця співробітників (АРМ) (стаціонарні комп'ютери, ноутбуки, мобільні пристрої).

Складові ІКС є середовищем в якому можуть виникнути кіберінциденти. Оскільки розглядається комплексне планування проведення заходів протидії прогнозованим кіберінцидентам, то залежно від сформованих умов повинні відслідковуватися параметри, що характеризують ті види кіберінцидентів, які можуть статися в системі.

Метод мережево-центричнго моніторингу кіберінцидентів реалізується у 2 етапи:

1 етап – моніторинг і оцінка ситуації на основі завчасного прогнозу, які базуються на оціночних характеристиках можливих кіберінцидентів;

2 етап – моніторинг і оцінка ситуації на основі оперативних даних про кіберінциденти;

Зазначені етапи включають відповідну організацію і використовувані засоби. Джерелами надходження інформації при проведенні моніторингу можуть бути: системи виявлення вторгнень IDS/IPS, міжмережеві екрани, honeypot системи, операційні системи, різні додатки (у тому числі спеціалізовані системи виявлення кіберінцидентів), антивірусні системи, звернення користувачів тощо.

На першому етапі основною задачею моніторингу є загальна оцінка можливих видів кіберінцидентів, які можуть виникнути, і побудова завчасного прогнозу ситуації. Для цього використовуються дані про складові ІКС, які були отримані в нормальних умовах функціонування ІКС.

На другому етапі задачею моніторингу є збір оперативних даних про кіберінциденти та, спираючись на результати першого етапу, коректування початкового прогнозу.

Загальну систему менеджменту кіберінцидентів регіону чи держави можна відобразити як складну мережу взаємопов'язаних центрів кампусного типу, кожен з яких має можливість:

– мати чітко сформульовану мету функціонування;

– діяти відповідно до закладених при його створенні правил і алгоритмів;

– керувати базою даних, що містить необхідну йому інформацію;

– вміти використовувати результати моніторингу, реагуючи на них своїми діями;

– проявляти власну ініціативу.

Розроблений метод мережево-центричного моніторингу кіберінцидентів може використовуватися у реальних практичних системах захисту інформації для визначення необхідних заходів щодо ліквідації наслідків кожного виду кіберінцидентів; формування цілей паралельної ліквідації можливих видів кіберінцидентів, їх синхронізацію, ранжування; реалізацію паралельних стратегій цілей, їх синхронізацію і взаємодію використовуваних сил і засобів; формування можливого набору паралельних оперативних впливів, їх диспетчеризацію, синхронізацію і маневрування силами і засобами в динаміці управління кіберінцидентами; попередження виникнення кіберінцидентів і, як наслідок, зниження затрат на їх ліквідацію.

Список використаної літератури

1. Гнатюк В.О. Аналіз дефініцій поняття «інцидент» та його інтерпретація у кіберпросторі / В.О. Гнатюк // Безпека інформації, 2013. – №3 (19). – С. 175-180.

2. Зацаринный А.А. Тенденции развития современных инфокоммуникационных технологий с учетом концепции сетецентрических войн / С.П. Присяжнюк, Ю.С. Ионенков // Информация и космос, 2006. – №4. – С. 85–93.

3. Синявский В.К. Влияние содержания и принципов «сетецентрической войны» на процессы управления войсками (силами) / В.К. Синявский // Наука и военная безопасность, 2010. – №4.

Гнатюк С.О., к.т.н., доцент,
Поліщук Ю.Я.,
Одарченко Р. С., к.т.н., доцент,
Національний авіаційний університет, Київ,
Сейлова Н.А., к.т.н.,
КазНДТУ імені К. І. Саптаєва, Алмати

ДОСЛІДЖЕННЯ МЕТОДУ СТВОРЕННЯ ІНФОРМАЦІЙНОЇ РЕАЛЬНОСТІ НА БАЗІ СТРУКТУРНО-АНАЛІТИЧНИХ МОДЕЛЕЙ ДЕЗІНФОРМУВАННЯ

Розвиток інформаційних систем, інформаційно-комунікативних технологій та мас-медіа, поява інформаційної зброї та спеціальних технологій впливу створили міцний фундамент для поширення маніпулятивного впливу на особу та соціальну групу. Як відомо, психологічні особливості людини та побудоване на їх основі інформаційне середовище дозволяють маніпуляторам, за допомогою маніпулятивних методів, впливати на підсвідомість, почуття, сприйняття людини з метою управління її соціальною поведінкою. З огляду на це, постає питання дослідження, вивчення та, найвагоміше, оцінювання маніпулятивного впливу, що здійснюють мас-медіа.

Метою роботи є дослідження методу створення інформаційної реальності на базі структурно-аналітичних моделей дезінформування.

Під поняттям маніпуляція розуміють процес впливу одним індивідом на іншого/інших з метою виконання волі першого [1].

На сьогодні існує велика кількість методів маніпулятивного впливу, які використовують сучасні мас-медіа; розглянемо один із них, а саме метод «Створення інформаційної реальності» [1], тобто створення псевдореальності, у якій за допомогою стереотипів маркують і закріплюють необхідну інформацію.

Реалізацію маніпулятивного впливу каналами мас-медіа для методу «Створення інформаційної реальності» можна представити за допомогою структурно-аналітичних моделей деструктивних інформаційно-управляючих впливів [2]. Метод «Створення інформаційної реальності» можна описати моделями 3 різних варіацій дезінформування: симуляційною, десимуляційною та конфузною.

Базовими характеристиками є цілісність, доступність та конфіденційність, а додатковими - адекватність, повнота, актуальність, надлишковість, адресність. Таким чином, в загальному вигляді коефіцієнт, що характеризує інформацію з точки зору безпеки можна відобразити у вигляді кортежу: $\{К_к, К_ц, К_д, К_а, К_п, К_{ак}, К_н, К_{ад}\}$.

1. Модель симуляційного дезінформування (рис. 1).

Параметри моделі: $К_д < 1; К_п < 1.$

Образ v_1 – результат перетворення оригіналу x_1, образ же v_2 не являється результатом перетворення заданого оригіналу, він появляється в результаті інших сторонніх причин. Інформація I_{v12} – симуляційне дезінформування, оскільки в множині оригіналів відсутня інформація I_{x12}.

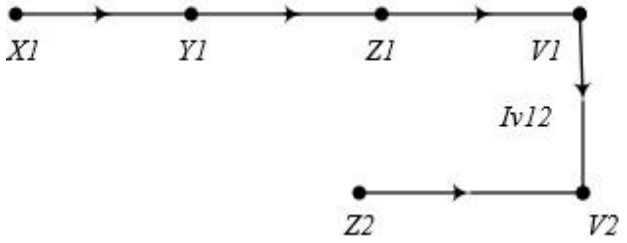

Рис. 1. Графічне зображення моделі симуляційного дезінформування

2. Модель десимуляційного дезінформування (рис. 2).

Параметри моделі: $К_{ад} = 1.$\

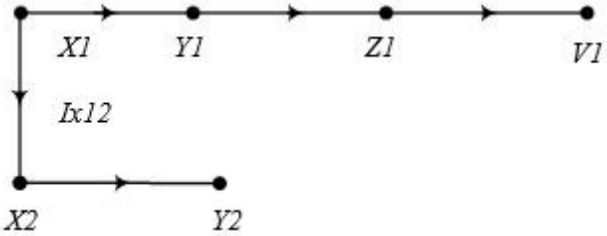

Рис. 2. Графічне зображення моделі десимуляційного дезінформування

Оригінал x_1 перетворений в образ v_1, в той же час, коли оригінал x_2 не перетворений в бажаний образ, оскільки необхідний для цього кодовий ланцюг переривається на якомусь проміжному повідомлені. Внаслідок цього в множині образів немає інформації I_{v12}.

3. Модель конфузного дезінформування (рис. 3).

Параметри $К_д < 1; К_п < 1.$

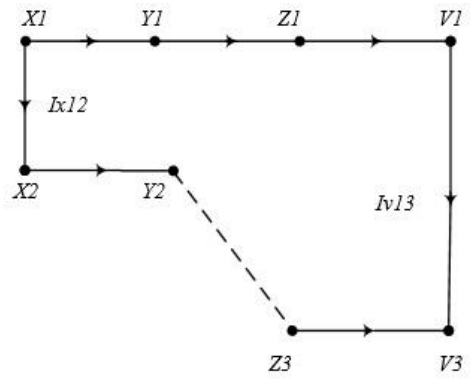

Рис. 3. Графічне зображення моделі конфузного дезінформування

Оригінал x_1 перетворений в образ v_1, в той же час, коли оригінал x_2 не перетворений в бажаний образ, в множині образів є образ v_3 , який отриманий іншим шляхом. В результаті, множина образів не містить інформацію I_{v12}(дисимуляційне дезінформування), а містить інформацію I_{v13}, хоча безліч оригіналів не містить інформацію I_{x13} (симуляційне дезінформування).

У зв'язку з інформацією, яка має гриф секретності «конфіденційно», є неможливим висвітлення деяких експериментів і інформації, яка циркулює у них. Саме тому, було прийнято рішення провести експеримент і кількісно оцінити вплив мас-медіа на особу та соціальну групу у взаємодії типу «викладач-студент», де викладач – агент впливу, а студент – особа, на яку здійснюють маніпулятивний вплив, і сукупність яких утворюють соціальну групу, спільним інтересом яких є навчання та прагнення до здобуття знань та навичок.

На прикладі моделі симуляційного дезінформування проведемо експериментальне дослідження маніпулятивного впливу мас-медіа на особу та соціальну групу в соціальній мережі «ВКонтакте».

Експеримент. В соціальній мережі «ВКонтакте» було поширено повідомлення, яке мало симуляційний дезінформуючий характер (рис. 4).

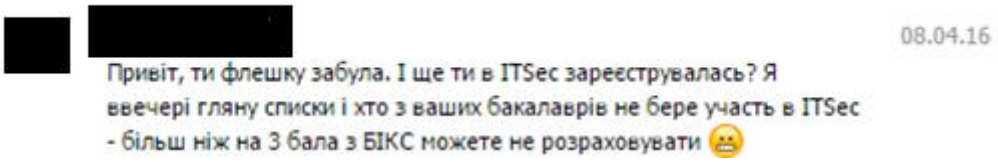

Рис. 4. Повідомлення від агента впливу

Аналізуючи повідомлення, слід виокремити, що маніпулятивна інформація посилається у комбінації з інформацією, яка не несе ніякого інформативного характеру для соціальної групи, а є важливою лише для агента, який передає цю інформацію.

Далі це повідомлення було перенаправлене соціальній групі, яка має відношення до агента впливу (взаємодія типу «викладач-студент») (рис. 5):

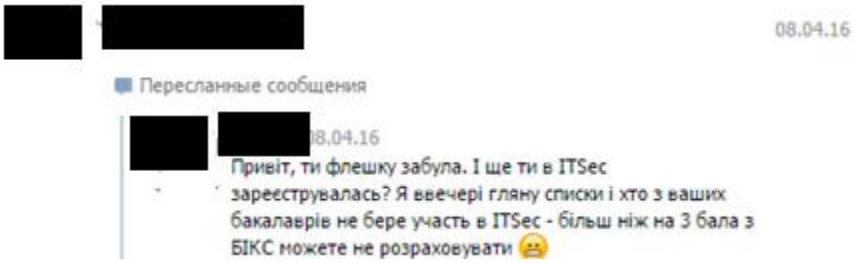

Рис. 5. Перенаправлення повідомлення

Після поширення інформації спостерігається активність в соціальній групі, що характеризує зацікавленість інформацією (повідомленням) (рис. 6):

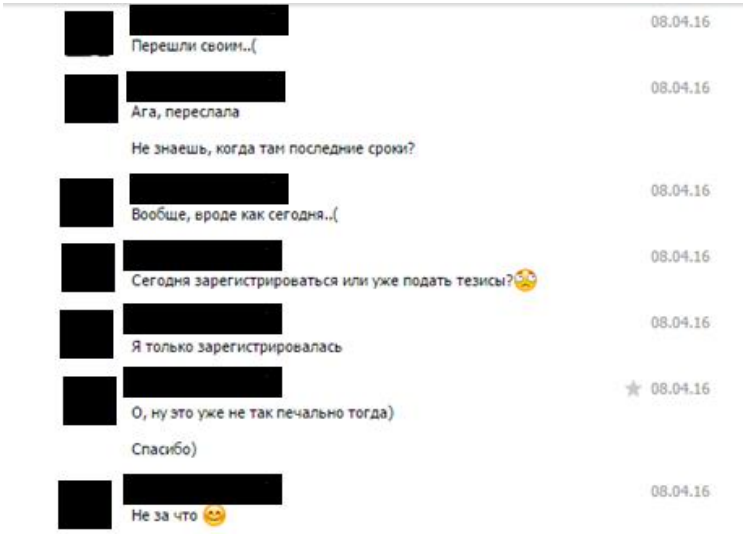

Рис. 6. Активність соціальної групи (продовження)

Загальна кількість учасників експерименту: 36 (навчальна група УБ-471 – 22 студента, навчальна група УБ-472 – 14 студентів).

Отримали контент (інформацію) – 36 чоловік.

Канал поширення: соціальна мережа «ВКонтакте».

Термін проведення конференції: 01.04.2016 – 18.04.2016.

Термін проведення експерименту: 08.04.2016 – 18.04.2016.

Зареєстрованих учасників із числа студентів груп УБ-471-472 у конференції на момент поширення інформації маніпулятивного характеру: зареєстровані відсутні.

Зареєстрованих після отримання маніпулятивного контенту: 21 (58, 3%) (рис. 7).

Рис. 7. Кількість зареєстрованих за весь період конференції

З огляду на кількісні показники експерименту, можна зробити висновок, що повідомлення з маніпулятивним змістом вплинуло на соціальну групу на 58, 3%.

Отримані у роботі результати можуть бути використаними для розробки превентивних та контрзаходів щодо протидії негативним інформаційним впливам каналами мас-медіа, розробки практичних рекомендацій для населення України в умовах інформаційної війни з метою підвищення інформаційно-психологічної безпеки громадян, суспільства та держави.

На основі результатів роботи можна розробити спеціалізоване програмне забезпечення для оцінювання та запобігання інформаційно-психологічним впливам мас-медіа на свідомість та підсвідомість людей.

Список використаної літератури

1. Polishchuk Yu., Gnatyuk S., Seilova N. Mass media as a channel of manipulative influence on society//Ukrainian Scientific Journal of Information Security, 2015.-Vol. 21. Issue 3. - P. 301-308.

2. Остапенко А. Г. Информационные операции и атаки в социотехнических системах. Учебное пособие для вузов / Под ред. чл. – корр. РАН В. И. Борисова. – М.: Горячая линия – Телеком, 2007. – 134 с.

Гнатюк С.О., к.т.н., доцент,
Шаховал О.А.,
Національний авіаційний університет, Київ,
Бекетова Г.С., докторант PhD,
Жумангалієва Н.К., докторант PhD,
Казахський національний дослідницький технічний університет ім. К.І. Сатпаєва, Алмати

ІНФОРМАЦІЙНО-ПСИХОЛОГІЧНИЙ АСПЕКТ СТРАТЕГІЇ КІБЕРБЕЗПЕКИ УКРАЇНИ

У теперішніх умовах тимчасової окупації території України Російською Федерацією, ескалації конфлікту на Сході держави, економічної кризи, поступового руйнування міжнародного іміджу та зростання ролі інформаційних технологій у повсякденному житті загалом актуальність питання інформаційно-психологічної безпеки (ІПсБ) стає безсумнівним. У зв'язку із цим, потрібно звернути увагу не лише на те, щоб знати як себе захистити від негативного впливу під час використання інформаційних технологій, а й на те, щоб це питання було врегульовано на державному рівні.

Як відомо, кіберпростір – це сукупність апаратних, програмних засобів та користувачів, що взаємодіють між собою. Невід'ємним компонентом функціонування будь-якої системи є людина та її свідомість, яка стає об'єктом інформаційно-психологічного впливу (ІПсВ). Вона є елементарною складовою суспільства та держави загалом. Забезпечення ІПсБ та контрзаходи для протидії ІПсВ мають бути закріплені на законодавчому рівні. Стратегія кібербезпеки України [1] передбачає не лише заходи захисту від технічного впливу, а й від психологічного. *Метою* цієї роботи є саме аналіз зазначеного документу з позицій виявлення шкідливих ІПсВ та забезпечення ІПсБ України.

Для проведення спеціальних інформаційних операцій (СІО) використовують такі методи як дезінформування, пропаганда, диверсифікація громадської думки, психологічний тиск, поширення чуток [2]. Саме недопущення їх реалізації забезпечує ІПсБ держави. Тому розглянемо дане питання у контексті вітчизняної стратегії кібербезпеки. Дезінформування найяскравіше розкривається у формі термінологічного «мінування», який полягає у викривленні первинно правильної суті принципово важливих, базових термінів і тлумачень. У зв'язку із тим, що у вітчизняній стратегії відсутній понятійний апарат, це може

спричинити до неправильного визначення понять, що може призвести до хибних дій в забезпеченні кібербезпеки. Стратегією передбачено використання позитивної пропаганди, що виконує виховну та інформативну функції, спрямовану на користь тих, кому адресована. Застосовується не для підриву ІПсБ, а для захисту населення від СІО. Метод проявляється в підвищення цифрової грамотності громадян та культури безпекового поводження у кіберпросторі, проведення кібернавчань для суб'єктів кіберпростору, проходження обов'язкової періодичної атестації спеціалістів на предмет відповідності вимогам та підвищення кваліфікації, залучення до співпраці волонтерів, підтримка використання програмних та інформаційних продуктів вітчизняного виробництва.

Психологічний тиск, поширення чуток, диверсифікація громадської думки у контексті Стратегії кібербезпеки Украни є проявами впливу, якому піддається Україна з боку Російської Федерації. Здійснюються агресивні дії з метою ліквідації держави та загарбання її території, а саме: військова агресія, розвідувальна діяльність і диверсійні дії, нарощування військових об'єднань на кордоні з Україною, торгівельно-економічна війна, інформаційно-психологічна війна, пригноблення української мови та культури, фальсифікування історії та інформації, яка подається російськими засобами масової інформації [3].

Окремим проявом психологічного тиску у документі є обмеження участі у заходах, що спрямовані на забезпечення інформаційної безпеки та кібербезпеки будь-яких суб'єктів господарювання, які знаходяться під контролем держави-агресора, або держав чи осіб, стосовно яких діють обмежувальні заходи. Також у стратегії введено поняття активного кіберзахисту, який застосовуватиметься як засіб стримування військових конфліктів та загроз у кіберпросторі.

Сьогодні фіксується все більше випадків діяльності іноземних спецслужб у кіберпросторі та атак на урядові і приватні веб-сайти в мережі Інтернет, що мають політичний підтекст та здійснюють вплив на суспільну свідомість і можуть здійснюватися з метою диверсифікації громадської думки, поширення чуток, дезінформації. Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Проте важко досягнути поставленої мети за відсутності врахування всіх можливих аспектів ІПсВ та контрзаходів. Це викликає необхідність створення та затвердження окремого документу, який регулював би діяльність, яка стосується ІПсБ, зокрема у кіберпросторі. Окрім цього, доцільним є формування та розповсюдження системи знань про основні способи забезпечення ІПсБ і навчання населення виявленню шкідливого ІПсВ та захисту від нього.

Список використаної літератури

1.Стратегія кібербезпеки України [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/962016-19836.
2.Петрик В.М., Присяжнюк М.М, Мельник Д.С. Інформаційна безпека держави: підручник в 2 т. – Т.1 / За заг. ред. Остроухова В.В. – К.: ДНУ «Книжкова палата України», 2016. – 264 с.
3.Стратегія національної безпеки України [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015

Голубев В.А., к. юр. н., доц.,
Юридическая компания «Кодекс Чести»,
Департамент Противодействия
Киберпреступности, Запорожье

КИБЕРПРЕСТУПНОСТЬ: СКРЫТАЯ И ЯВНАЯ УГРОЗЫ

Ограбление с помощью компьютера — уже не просто популярный сюжет голливудского фильма, а вполне реальная угроза, с которой сталкиваются финучреждения и их клиенты по всему миру. Согласно оценкам комиссии по внутренним делам британского парламента, потери мировой экономики от преступлений, совершенных с помощью Интернета, достигли 388 млрд. долл. в год. Тем самым киберпреступность обошла по своему размаху мировой наркорынок, годовой оборот которого оценивается в 288 млрд. долл. Таким образом, стремительное развитие информатизации в Украине несет в себе потенциальную возможность использования компьютерных технологий из корыстных и других мотивов, что в известной мере ставит под угрозу национальную безопасность государства.

Проблема преступлений, совершение которых связанно с использованием компьютерных технологий стоит довольно широко, это в первую очередь обусловлено временем, а именно способностью человечества привлечь себе на помощь электронно-вычислительную технику.

Точно также как был период создание и внедрение в повседневную жизнь транспорта, и возникла необходимость в защите прав всех участников этого процесса. Так происходит и в настоящее время, если в момент появления компьютерных технологий, не было четкого регулирующей законодательной базы, так как человек еще не представлял где его изобретение найдет себе применение, а следовательно не был определен круг участников данного процесса и не вставал риторический вопрос о законодательной защите их интересов, то сейчас изобретения в области компьютерных технологий затрагивают и втягивают в круговорот отношений, все большее количество участников. Отсюда и вытекает необходимость более детального и тщательного регулирования этой области человеческих достижений.

С целью оградить добросовестных пользователей компьютерных технологий, которые до конца могут и не понимать принцип их работы, от лиц, которые благодаря своим глубинным знаниям в этой области, имеют корыстную цель, например кражи с кредиток, завладение кодами доступа либо совершение иных преступлений против собственности с использованием компьютерных технологий. Анализируя сказанное, получается, что ничего нового в психологии людей не произошло, как и 100 и 1000 лет назад люди, совершавшие преступления против собственности, имели своей целью наживу, личное обогащение, обращение в свою пользу чужого имущества.

Но необходимо отметить, что сейчас появилась новая сфера, культура, подвигнутая прогрессом, толчком для которого стала человеческая лень. Существующий мир компьютерных технологий открывает огромнейшие возможности, в нем можно общаться, искать и хранить информацию, совершать покупки в интернет-магазинах и рассчитываться за них при помощи электронных средств расчетов, работать и получать за это вознаграждение. Следовательно, человек теперь способен полноценно, реализовано жить и в виртуальном пространстве.

Однако не только само по себе массовое распространение компьютеров формирует информационную сферу. Значительную, если не главную, роль в этом процессе играют различные постоянно совершенствующиеся виды компьютерных технологий.

Таким образом, естественной причиной возникновения, существования и увеличения преступлений против собственности с использованием компьютерных технологий является совершенствование информационных технологий, расширение производства их поддерживающих технических средств и сферы их применения, а также появление в этой

сфере виртуальных форм расчетов как потенциальных объектов преступного посягательства, и все большая доступность подобных устройств.

Так в результате проведенного независимого опроса, проведенного Департаментом противодействия киберпреступности, 100 респондентов, которые более одного года активно пользовались сетью интернет, совершали покупки с помощью электронных средств расчетов (банковские карточки, электронные кошельки), были выявлены следующие процентные соотношения: а) Лица, в отношении имущества которых были совершены преступные посягательства при помощи компьютерных технологий – 87 %; б) Лица, которые осознали факт утраты имущества в течении первых часов – 2% ; в) Лица, которые осознали факт утраты имущества в течении первого месяца – 5 % ; г) Лица, которые осознали факт утраты имущества в период больше одного месяца - 93%.

Выводы. Из сказанного следует, что общественная опасность подобных преступлений заключается в их латентности, которая в свою очередь образуется в результате того, что потерпевший зачастую и не понимает, что в отношении него совершенно преступление. Получается, что злоумышленник уже заранее уверен в своей безнаказанности, и тем самым ставит себя выше общества и закона.

Для предупреждения мошенничеств в системах дистанционного банковского обслуживания специалисты советуют соблюдать, по крайней мере, несколько элементарных правил безопасности. В частности, использовать лицензионное программное обеспечение; не передавать коды доступа другим лицам (в т.ч. сотрудникам банка); не использовать компьютер системы "клиент—банк" для других целей, кроме проведения операций со счетами; не применять системы дистанционного управления компьютером.

Дудатьєв А.В., к.т.н., доцент,
Дудатьєва В.М., асистент,
Літушко О.А.,
Вінницький національний технічний університет

КОМПЛЕКСНИЙ МЕТОД ПРОТИДІЇ СПЕЦІАЛЬНИМ ІНФОРМАЦІЙНИМ ОПЕРАЦІЯМ

В умовах ведення інформаційної війни зростає роль ефективного управління комплексною інформаційною безпекою, що забезпечує стійке функціонування соціотехнічних систем (СТС). Спеціальні інформаційні операції, до яких відносяться інформаційно-психологічні операції (ІПО) та інформаційно-кібернетичні операції (ІКО) можуть проводитись на різних етапах життєдіяльності СТС з використанням різних джерел та технологій. Практично невирішеною проблемою залишається формалізація або алгоритмізація процесу ведення інформаційної війни, що накладає певні труднощі при побудові ефективного захисту від проведення ІПО та ІКО.

Для рішення даної проблеми авторами пропонується комплексний метод протидії спеціальним деструктивним інформаційним операціям, який дозволяє мінімізувати зазначені проблеми. Головною метою проведення спеціальних інформаційних операцій є вплив на соціальну частину СТС з метою перепрограмування її свідомості. При цьому процес проведення ІПО складається з підготовки ІПО та її реалізації. Тому запропонований метод передбачає організацію двохетапного захисту. Комплексний метод використовує технології інформаційного мем-впливу. Річард Доукінс вперше ввів поняття культурного гена – мема, призначеного для культурної еволюції соціума. Мем визначається як мінімальна кількість інформації у свідомості людини. Іншими словами, мемом можна назвати спеціально створене інформаційне повідомлення, яке розповсюджується у інформаційному просторі з використанням різних джерел і яке призначене для формування необхідної моделі

свідомості соціальної частини СТС і, як наслідок, прийняття відповідних або “потрібних” рішень людиною. З точки зору інформаційної безпеки, спеціально підготовлена одиниця інформація або мем використовується саме для проведення інформаційного впливу або для “інфікування” соціальної частини СТС [1,2] .

Використовуючи теорію меметики, будемо вважати зміну стану інформаційного середовища результатом наявності у ньому нового мема або мема, на факт присутності якого відсутня адекватна реакція. Результатом обслуговування нового мема будемо вважати його нейтралізацію або формування відповідного захисту.

І-й етап запропонованого методу передбачає проведення власних спеціальних інформаційних операцій та організаційних заходів, метою проведення яких є випередження ймовірних інформаційних операцій з боку потенційних конкурентів і, як наслідок, мінімізація ризиків проведення спеціальних деструктивних операцій з боку конкурентів.

Авторами запропонована модель реалізації І-го етапу захисту, яка враховує умови для проведення власних попереджувальних спеціальних інформаційних операцій, доступні ресурси, специфіку соціуму, на який спрямований інформаційний вплив, механізми реалізації інформаційних операцій тощо. Відомо, що гарантованого захисту не існує, тобто під деструктивний інформаційний вплив підпаде певна частина соціальної частини СТС, яку також необхідно мінімізувати після так званого “інформаційного інфікування”. Для рішення цієї задачі ІІ-й етап комплексного методу передбачає реалізацію захисту після проведення спеціальних інформаційних операцій з боку конкурентів за рахунок так званих компенсуючих мемів [3]. Запропонована модель для реалізації ІІ–го етапу комплексного методу враховує кількість джерел впливу, що розповсюджують деструктивні меми, кількість об’єктів соціальної частини СТС, на які спрямований деструктивний інформаційний вплив, а також відповідну кількість джерел розповсюдження компенсуючого мема та кількість об’єктів соціальної частини, на які спрямовані саме компенсуючі меми. Запропонована спеціальна шкала стійкості, що дозволяє за отриманими ймовірнісними значеннями визначити інформаційну стійкість СТС. Отримані співвідношення дозволяють визначити загальний стан захищеності соціотехнічної системи від проведення ймовірних ІПО та ІКО, а також визначити стійкість СТС в умовах інформаційної війни.

Для перемоги у сучасній інформаційній війні необхідно застосування ефективних інформаційних технологій. Методи та засоби ведення інформаційної війни постійно розширюються, механізми проведення деструктивних інформаційних впливів постійно покращуються, що приводить до збільшення ефективності зовнішнього інформаційного впливу на соціальну частину СТС. Запропонований комплексний метод протидії спеціальним інформаційним операціям дозволяє формалізувати процес проведення інформаційного впливу з боку ймовірного конкурента та організувати ефективний захист від проведення інформаційно-психологічних та інформаційно-кібернетичних операцій. Метод представляє систематизовану сукупність моделей, множину різноманітних засобів і заходів.

Список використаної літератури

1. Артёмов А.А. Теоретические основы информационного управления / А.А. Артёмов // Информационные войны, 2015. – № 3. – С. 83-97.
2. Дудатьєв А. В. Інформаційна обфускація: Методи і моделі / А. В. Дудатьєв // Сучасний захист інформації, 2015. – № 4. – С.56-61.
3. Дудатьев А.В., Лужецкий В.А., Коротаев Д.А. Метод оценки информационной устойчивости социотехнических систем в условиях информационной войны / А.В. Дудатьев, В.А. Лужецкий, Д.А. Коротаев // Восточно–Евпропейский журнал передовых технологий, 2016. – № 2 (80). – С.4-11.

Ісмайлов К.Ю., к.юр.н.,
Косаревська О.В., к.пед.н., доцент,
Одеський державний університет внутрішніх справ

АКТУАЛЬНІ ПИТАННЯ ІНФОРМАЦІЙНО-ТЕХНОЛОГІЧНОЇ ПІДГОТОВКИ МАЙБУТНІХ ФАХІВЦІВ ПРАВООХОРОННОЇ СФЕРИ У ВНЗ З ОСОБЛИВИМИ УМОВАМИ НАВЧАННЯ

В сучасних умовах реформування та розвитку підрозділів МВС України, що забезпечують підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності, особливо актуальною постає проблема вдосконалення інформаційно-технологічної підготовки майбутніх фахівців правоохоронної сфери у ВНЗ з особливими умовами навчання.

Основні чинники у сфері вищої юридичної освіти спрямовані на вдосконалення механізмів управління системою вищої юридичної освіти, методології та стратегії відбору змісту методів і організаційних форм навчання та виховання; створення нових методичних систем навчання та діагностуючих методик проведення поточного та підсумкового контролю знань [1;2;3].

Огляд сучасної юридичної, педагогічної, психологічної наукової думок стосовно впровадження інноваційних технологій в навчально-виховний процес, а саме робіт таких авторів: Албула С.В.,Галіциної Л.,Гуревича Р.С.,Іванова І.І.,Користіна О.Є.,Меркулової В.О., Моргуна О.М., Орехової В.А, Радула В.В, Сергєєвої Т.А., Селевка В.Г., Узлова Д.Ю., Шолоховича В.Ф,, Цехана Д. М., Яковенко С.І. та ін. дає підставу наголосити на основні важливі, на наш погляд, аспекти.

І. Вдосконалення початкового загальноосвітнього рівня підготовки курсантів та студентів з «комп'ютерної грамотності» за рахунок інформаційно-технологічної фахової підготовки у ВНЗ з особливими умовами навчання.

Інформатизація навчання в своїй структурі передбачає: засвоєння основних понять інформатики та обчислювальної техніки, знання сучасних операційних систем та оволодіння їх основними командами, початкове уявлення про алгоритми мови і пакети програмування. Для цього доцільно використовувати такі методи інтерактивного навчання як: інтерактивний діалог, інтерактивне моделювання та інтерактивна дошка [7, С. 44-45].

Використання інтерактивної технології в навчальному процесі дає можливість вирішення певних завдань: оволодіння курсантами та студентами практикою використання різних інтерактивних презентаційних технологій (Flash-анімація, Gif-анімація, комп'ютерні презентації); вивчення сфер їх застосування; опанування взаємодії в діалоговому режимі між суб'єктами навчального процесу; стимулювання розвитку їх самостійної роботи.

В сучасних умовах реформування всієї системи МВС особливого значення набувають такі якості майбутніх правоохоронців, як: професіоналізм, компетентність, творча активність, здатність навчатися протягом усього життя. Інноваційна модель сучасного поліцейського за європейськими стандартами вимагає розвитку творчого мислення, формування відчуття самостійності, рішучості, відповідальності, вміння гнучко адаптуватися у різноманітних правоохоронних ситуаціях, бути комунікабельним та високоморальним у спілкуванні з населенням, а також високої інформаційної культури.

Враховуючи, що майбутні фахівці правоохоронної сфери будуть стикатися з величезним потоком інформації дуже важливим постає питання ознайомлення їх з різною технікою та прийомами мислення, що буде сприяти розвитку їх комунікативних здібностей, розвивати їх загальні та спеціальні вміння за рахунок використання інтеграційної освітньої технології. Міжпредметна вертикальна та горизонтальна інтеграційна освітня технологія

зорієнтована на розвиток особи на базі засвоєного наочного матеріалу нормативних юридичних дисциплін. Обидві концепції передбачають комп'ютеризацію та інформатизацію навчального процесу, широке застосування мультимедійних засобів. В світлі сучасних технологій навчання інтеграція вигідна тим, що вона дозволяє науково-педагогічному складу ВНЗ формувати у курсантів та студентів загально-навчальну компетенцію, що не можливо при ізольованому вивчені предметів.

Поряд з традиційними формами та методами юридичної освіти за вимогою часу в ВНЗ з особливими умовами навчання повинні застосовуватись такі інтерактивні методи активного навчання як: ділові ігри, мозкові штурми, конференції-диспути. Одним з ефективних інтерактивних методів є проблемне навчання за рахунок розв'язання ситуаційних кейсових завдань з метою розв'язання алгоритмів професійних дій в окремих правоохоронних ситуаціях.

II. Підвищення якості професійної компетентності науково-педагогічного складу ВНЗ з особливими умовами навчання, на наш погляд, слід розглядати в наступних напрямках.

По-перше, опанування методологією інтерактивного навчання, за рахунок: тренінгової підготовки з розв'язання алгоритмів дій між суб'єктами інформаційних правовідносин у сфері протидії кіберзлочинності у інформаційно-телекомунікаційних системах.

По-друге, забезпечення проходження перепідготовки педагогічних кадрів з ІКТ та новітніх технологій за програмою Intel® «Навчання для майбутнього». Ця програма виступає каталізатором реформування освіти; сприяє широкому включенню освітніх закладів України у світовий інформаційних простір [6].

По-третє, спрямування проходження стажування науково-педагогічного складу ВНЗ у практичних територіальних органах національної поліції в рамках підвищення кваліфікації [8, С.135].

По-четверте, активізація наукового потенціалу науково-педагогічного складу ВНЗ в рамках міжнародної співпраці з вищими навчальними закладами з підготовки поліцейських.

III. Впровадження комп'ютерних технологій в навчально-виховний процес ВНЗ з особливими умовами навчання.

Новітні методи надання інформації.

- Презентаційний прийом навчання передбачає інтегрування традиційної системи особистісно-орієнтованого навчання з використанням комп'ютерної техніки
- Електронний підручник, як інформаційна система комплексного призначення для реалізації дидактичних можливостей засобів інформаційно-комп'ютерних технологій у всіх ланках дидактичного циклу процесу навчання.

Запровадження електронних навчальних посібників є самостійною дидактичною ланкою в інформаційно-комунікаційній технології навчання з додержанням принципів наочності, адаптованості, комп'ютерної підтримки, мобільності наповнення дидактичних інтегрованих пакетів. Комп'ютерна техніка використовується як: джерело інформації, наочний посібник, тренажер, засіб контролю та творчості.

IV. Створення практико-зорієнтованого навчального середовища організації навчального процесу в ВНЗ зі спеціальними умовами навчання.

Фахова підготовка майбутнього правоохоронця передбачає впровадження в навчальний процес інноваційних виробничих технологій пов'язаних з інтеграцією понять соціального партнерства та модернізації професійно-технічної освіти під час проходження виробничої практики у практичних підрозділах національної поліції.

В рамках реалізації державної політики у сфері протидії кіберзлочинності та забезпечення безпеки інформаційно-телекомунікаційних систем курсанти повинні детально

ознайомитись з методами протидії кіберзлочинам у сферах: використання платіжних систем; електронної комерції та господарської діяльності; інтелектуальної власності; технологіями: соціальної інженерії, мальваре, рефайлінга, протиправного контента.

Система самоосвіти практичних працівників національної поліції передбачає наступні форми: віртуальне навчання, метод проектів, сертифікаційне навчання.

Таким чином, інформаційні технології у вищій юридичній освіті слід розглядати: як предмет вивчення, як засіб навчання, як інструмент автоматизації навчально-виробничої діяльності у правоохоронній сфері.

Література

1. Закон України «Про Національну поліцію»: від 07.11.2015 № 580-VII // Відомості Верхової Ради України (ВВР), 2015. - №40-41.-С. 379.

2. Про вищу освіту:Закон України від 01.07.2014№4 1556-VII // [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/ laws/ show/1556-18.

3. Стратегія та сучасні тенденції розвитку університетської освіти України в контексті Європейського простору вищої освіти/ Офіційний сайт міністерства освіти і науки, молоді та спорту України [Електронний ресурс]. - Режим доступу: http://www.mon.gov.ua/ education/higher.

5. Юридична освіта в Україні // [Електронний ресурс]. – Режим доступу: http://law-edu.dp.ua/yurudychna-osvita-v-ukrajini.html.

6. Навчання для майбутнього в Україні: // [Електронний ресурс]. – Режим доступу: http://iteach.com.ua.

7. Галіцина Л. Ігри дорослих. Інтерактивні методи навчання / Л. Галіцина. – К.: «Редакція загально педагогічних газет», 2005. – 128с.

8. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія / Д. М. Цехан; за наук. ред. О. О. Подобного. – О.: Юрид. л-ра, 2011. – 216 с.

Карпинский Н.П., д.т.н., профессор,
Университет в Бельско-Бялой, Польша,
Корченко А.А., к.т.н., доцент,
Казмирчук С.В., к.т.н., доцент,
Национальный авиационный университет, Киев

ФАЗЗИФИКАЦИЯ ПАРАМЕТРОВ В КОРТЕЖНОЙ МОДЕЛИ ДЛЯ ВЫЯВЛЕНИЯ КИБЕРАТАК

Одной из базовых задач в области информационной безопасности является создание систем защиты сетевых и системных ресурсов, основанных на аномальном принципе. Для построения и расширения функциональности такого рода систем используется метод выявления аномалий, порожденных кибератаками в информационных системах [1]. В этом методе процесс фаззификации параметров практически не формализован, что понижает эффективность его использования. Для эффективного применения метода выявления аномалий необходима формальная реализация этапа 5 – фаззификация параметров [1], посредством которого формируются требуемые для последующих вычислений текущие значения нечетких параметров в моделируемой среде окружения. Исходя из этого, создание методов, позволяющих фаззифировать текущие значения параметров для систем выявления кибератак, есть актуальной задачей.

С этой целью предлагается метод фаззификации параметров на лингвистических эталонах (МФПЛЭ), позволяющий сформировать текущие значения переменных в нечеткой форме, посредством которых формализуются параметры характерные для конкретной среды окружения при решении задач выявления кибератак в компьютерных системах.

Метод базируется на кортежной модели формирования набора базовых компонент для выявления кибератак [2, 3], в которой для формализации процесса их формирования вводится множество возможных кибератак $\mathbf{CA}$, которые могут воздействовать на ресурсы информационных систем за определенный временной промежуток τ_f, т.е.: $\mathbf{CA}^{\tau_f} = \{\bigcup_{i=1}^{n} \mathbf{CA}_i^{\tau_f}\} = \{\mathbf{CA}_1^{\tau_f}, \mathbf{CA}_2^{\tau_f}, \ldots, \mathbf{CA}_n^{\tau_f}\}$, где n определяет количество возможных кибератак, каждая из которых отображается обобщенным кортежем $\mathbf{CA}_i^{\tau_f} = < CA_i, \mathbf{P_i}, \mathbf{T_i^e}, \mathbf{P_i^{\tau_f}}, \mathbf{DR_i} >$, а фаззификация параметров на лингвистических эталонах реализуется посредством трех базовых этапов.

Этап 1 – формирование частот встречаемости параметров. Для реализации этого этапа введем множество всех возможных сенсоров $\mathbf{S}$ и подмножества таких сенсоров $\mathbf{S_{ij}} \subseteq \mathbf{S}$: $\mathbf{S_{ij}} = \{\bigcup_{k=1}^{r_j} S_{ijk}(t_\eta)\} = \{S_{ij1}(t_\eta), \; S_{ij2}(t_\eta), \; \ldots, \; S_{ijr_j}(t_\eta)\}$, используемых для контроля текущего состояния физических параметров, отображаемых посредством $\mathbf{P_i^{\tau_f}}$ в $\mathbf{CA_i^{\tau_f}}$ [2].

Здесь $S_{ijk}(t_\eta)$ $(i = \overline{1,n}, \; j = \overline{1,m_i}, \; k = \overline{1,r_j})$ является сенсором N_{ijk}-го интервала [4], отражающем значение (на соответствующем интервале) физического параметра $P_{ij}(t_\eta)$ в момент t_η, а r_j – количество сенсоров.

Сенсор $S_{ijk}(t_\eta)$ представляет собой бинарную функцию, которая эквивалентна единице только в случае, когда значение $P_{ij}(t_\eta)$ относительно кортежной модели [2] в момент t_η (момент наступления ожидаемого события) будет находиться в интервале N_{ijk} т.е.: $S_{ijk}(t_\eta) = \begin{cases} 1, \text{ при } P_{ij}(t_\eta) \in N_{ijk} \\ 0, \text{ при } P_{ij}(t_\eta) \notin N_{ijk} \end{cases}$, $(k = \overline{1,r_j})$.

Далее, введем множество всех возможных счетчиков сенсоров $\mathbf{CS}$ и подмножества таких счетчиков $\mathbf{CS_{ij}} \subseteq \mathbf{CS}$, которые согласно выражения (1), на основе данных сенсоров $S_{ijk}(t_\eta)$, характеризующих текущее состояние *j*-х физических параметров относительно *i*-й атаки в моменты t_η, формируются частоты встречаемости значений $P_{ij}(t_\eta)$ на каждом из интервалов N_{ijk} $(k = \overline{1,r_j})$ [4] посредством подмножеств

$$\mathbf{CS_{ij}} = \{\bigcup_{k=1}^{r_j} CS_{ijk}\} = \{\bigcup_{k=1}^{r_j} \sum_{\eta=1}^{\eta_{max}} S_{ijk}(t_\eta)\}, \qquad 1)$$

где CS_{ijk} является счетчиком сенсора $S_{ijk}(t_\eta)$, а η_{max} соответствует общему количеству возможных t_η.

Далее, указанные частоты встречаемости, отображаемые счетчиками CS_{ijk} $(k=\overline{1,r_j})$ представим в виде таблицы (табл. 1), т.е. каждый CS_{ijk} счетчик отвечает за контроль состояния соответствующего параметра на интервале N_{ijk} $(k=\overline{1,r_j})$.

Таблица 1

Типовая таблица для $\mathbf{CS_{ij}}$

Счетчик сенсора	$\mathbf{N_{ij}}$ $(k=\overline{1,r_j})$			
	N_{ij1}	N_{ij2}		N_{ijr_j}
CS_{ij}	CS_{ij1}	CS_{ij2}		CS_{ijr_j}

Этап 2 – формирование поправочных эталонов. Для реализации этого этапа введем подмножества поправочных эталонов $\mathbf{T_{ij}^E} \subseteq \mathbf{T^E}$, ($\mathbf{T^E}$ – множество всех возможных поправочных эталонов), каждое из которых основывается на $\mathbf{T_{ij}^e}$ [4] и определяется как $\mathbf{T_{ij}^E} = \{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^E\} = \{\underset{\sim}{T}_{ij1}^E,\ \underset{\sim}{T}_{ij2}^E,\ \ldots,\ \underset{\sim}{T}_{ijr_j}^E\}$,

где $\underset{\sim}{T}_{ijs}^E$ $(s=\overline{1,r_j})$ – поправочные эталонные нечеткие числа (НЧ). Эти числа строятся на основе преобразования соответствующих НЧ (см. выражение (12) в [4]) из подмножества $\mathbf{T_{ij}^e} \subseteq \mathbf{T^e}$ с помощью счетчиков сенсоров из $\mathbf{CS_{ij}} \subseteq \mathbf{CS}$, согласно выражения

$$\{\bigcup_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^E\} = \{\bigcup_{s=1}^{r_j} (\underset{\sim}{T}_{ijs}^e \cdot CS_{ijs})\} = \{\underset{\sim}{T}_{ij1}^e \cdot CS_{ij1},\ \underset{\sim}{T}_{ij2}^e \cdot CS_{ij2},\ \ldots,\ \underset{\sim}{T}_{ijr_j}^e \cdot CS_{ijr_j}\}.$$

Этап 3 – формирование нечетких параметров. Реализация этого этапа осуществляется по следующему выражению

$$\underset{\sim}{P}_{ij}^{\tau_f} = (\sum_{s=1}^{r_j} \underset{\sim}{T}_{ijs}^E) / \eta_{max} = (\underset{\sim}{T}_{ij1}^E \tilde{+} \underset{\sim}{T}_{ij2}^E \tilde{+} \ldots \tilde{+} \underset{\sim}{T}_{ijs}^E \tilde{+} \ldots \tilde{+} \underset{\sim}{T}_{ijr_j}^E) / \eta_{max},$$

где $$\underset{\sim}{P}_{ij}^{\tau_f} = \{\bigcup_{q=1}^{\rho} \mu_{ijq} / x_{ijq}\} = \{\mu_{ij1} / x_{ij1}, \mu_{ij2} / x_{ij2}, \ldots, \mu_{ij(\rho-1)} / x_{ij(\rho-1)}, \mu_{ij\rho} / x_{ij\rho}\}$$

$(q=\overline{1,\rho})$, ρ – количество компонент в текущем НЧ $\underset{\sim}{P}_{ij}^{\tau_f}$.

Предложенный в работе МФПЛЭ, за счет преобразования введенных множеств сенсоров, счетчиков сенсоров и поправочных эталонов, а также использования множеств лингвистических эталонов и соответствующих подмножеств интервалов для формирования частот встречаемости значений физических параметров в заданные моменты наступления ожидаемого события, позволяет фаззифировать текущие значения параметров для последующего выявления аномального состояния в компьютерных системах.

Следует также отметить, что имея обобщенные описания процесса фаззификации текущих параметров и построения лингвистических эталонов, можно формализовать процесс поиска эталонного значения наиболее близкого к текущему параметру и таким образом повысить эффективность решения задач определения уровня аномального состояния в компьютерных системах.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Стасюк А.И. Метод выявления аномалий порожденных кибератаками в компьютерных сетях / А.И. Стасюк, А.А. Корченко // Захист інформації, 2012. – №4 (57). – С. 129-134.

2. Корченко А.А. Кортежная модель формирования набора базовых компонент для выявления кибератак / А.А. Корченко // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2014. – Вип.2 (28). – С. 29-36.

3. Anna Korchenko, Kornel Warwas, Aleksandra Kłos-Witkowska. The Tupel Model of Basic Components' Set Formation for Cyberattacks // Proceedings of the 2015 IEEE 8th International Conference on «Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications» (IDAACS'2015). – Warsaw. Poland, 2015. - September 24-26. - Vol. 1.– P. 478-483.

4. Корченко А.А. Метод формирования лингвистических эталонов для систем выявления вторжений / А.А. Корченко//Захист інформації, 2014. – Т.16. №1. – С. 5-12.

Кінзерявий В. М., к.т.н., доцент,
Кінзерявий О.М., к.т.н., асистент,
Гізун А.І., к.т.н., доцент,
Національний авіаційний університет, Київ,
Рябий М.О., к.т.н.,
ПАТ "МХП", Київ

АЛГОРИТМ ПРИХОВУВАННЯ ІНФОРМАЦІЇ У ВЕКТОРНІ ЗОБРАЖЕННЯ

Розвиток глобальної мережі Інтернет та поширення її використання серед населення планети сприяє збільшенню обсягів інформації, що передається, обробляється, зберігається та знищується. Використовуючи можливості і ресурси мережі Інтернет можна організувати резервний канал зв'язку (наприклад, із дипломатичними установами, що знаходяться на території іноземних держав) для передачі секретних даних, коли штатні захищені канали зв'язку недоступні або виведені з ладу. Скритність передачі інформації по таким каналам може забезпечуватися стенографічними засобами захисту.

Більшість сучасних стеганографічних досліджень присвячені приховуванню інформації в графічних зображеннях. Враховуючи той факт, що шлюзи доступу в мережу Інтернет знаходяться під контролем спецслужб розвинутих країн, то при передачі зображень можуть застосовуватися активні фільтри, які візуально непомітно модифікують їх і таким чином знищують приховане повідомлення. До таких атак слід віднести різного роду трансформації на основі афінних перетворень [1, 4]. Проведені дослідження, показують, що стеганографічні методи, які використовують растрові та фрактальні типи зображення в якості контейнерів, не забезпечують достатнього рівня стійкості до афінних перетворень [1]. У той час, як методи приховування у векторні зображення, завдяки властивостям побудови векторної графіки, можуть успішно протистояти їм.

Відомими стеганографічними методами, що використовують векторні зображення є методи Канга, Обуші, Шульца-Войта, Карпінцева-Яремчука та інші [1, 2]. Проведений аналіз стійкості даних методів показав їх слабку здатність протидії до афінних перетворень. Крім того, вони базуються на просторових та частотних перетвореннях векторних зображень, які при зміні контурів векторних об'єктів погіршують якість самого зображення та утворюють видимі відхилення ліній в них, що не дозволяє в повній мірі їх використовувати для передачі секретної інформації резервними каналами зв'язку. Тому розробка нових та удосконалення існуючих стеганографічних методів і алгоритмів для підвищення ефективності приховування інформації є *актуальним* завданням.

Метою роботи є підвищення стійкості стеганографічного захисту інформації на основі застосування нового алгоритму приховування інформації у векторні зображення.

Основним елементом у векторній графіці є лінія, якій притаманні деякі властивості: форма, колір, товщина та інші. Задається кожна лінія за допомогою аналітичної формули з

певним числом параметрів необхідних для її представлення. Будь-який об'єкт (прямокутник, еліпс, пряма лінія тощо) сприймається і подається як криві лінії. Досить великий клас кривих, які відрізняються різним ступенем гладкості, можна побудувати за сукупністю точок, заданих за допомогою проективних координат. Такий клас кривих називається точково-заданими, а до їх складу відносяться ламана лінія та різноманітні сплайнові криві.

Будуються дані криві за допомогою множини точок (вершин) $\mathrm{P} = \{P_i\}$, $i = \overline{0,n}$, n – ступінь кривої, та параметра побудови кривих t, $t \in [a,b]$, що при послідовному з'єднані утворюють ламану, яку називають опорною, а її вершини – опорними.

Кожне значення параметра побудови кривих t строго визначає положення точки на кривій. Зафіксувавши певний крок Δt зміни параметра t буде здійснюватися перехід між його значеннями $t_{i+1} = t_i + \Delta t$ під час побудови кривої в межах визначеного проміжку $[a,b]$. Використовуючи значення t_i можна здійснювати приховування інформації у точково-задані криві шляхом їх розбиття на сукупності сегментів в даних точках. За допомогою властивості афінно-інваріантності, якою володіє ряд кривих даного класу, буде забезпечуватися стійкість до атак на основі афінних перетворень.

При роботі з векторними зображеннями можуть використовуватися різні формати представлення даних: AI, CDR, CDW, CDT, DWG, DXF, WMF, FLA, FH, SVG, SWF, 3DM та інші, в структурі яких використовуються різні типи точково-заданих кривих. Для приховування інформації у векторні зображення запропоновано використання найпоширеніших кривих, що підтримуються більшістю графічними пакетами, а саме кривих Без'є. Дані криві володіють необхідними властивостями для приховування інформації, а саме: будь-яка крива Без'є є афінно-інваріанта відносно афінних перетворень; будь-яку криву Без'є можна розбити та подати у вигляді довільної сукупності сегментів.

На основі роботи [3] і властивостей кривих Без'є реалізовано алгоритм StegoTEMPL, що дозволяє вбудовувати дані у криві Без'є третього ступеня векторних зображень. Псевдокод процедури вбудовування інформації даним алгоритмом представлено на рис. 1.

Під операцією $SplitMessage(x, y)$ мається на увазі побітове розбиття вхідного повідомлення x на частини розмірністю y біт. Операція $SelectImage(x, y, z)$ виконує відбір допустимих контейнерів з множини x необхідних для вбудовування y частин прихованого повідомлення, в структурі яких містяться криві Без'є ступеня z. Операція $SelectCurves(x, y, z, h)$ визначає з множини зображень x кількість кривих Без'є ступеня z необхідних для вбудовування y частин прихованого повідомлення, що відповідають мінімальній допустимій відстані h між опорними точками. Операція $GetPoints(x)$ використовується для одержання координат опорних точок кривої x. Операція $CreateCurve(x, y, z, h)$ використовується для побудови кривої Без'є за координатами опорних точок x, y, z та h. Операція $ReplaceCurve(x, y, z)$ виконує заміну в зображеннях x початкових кривих y на сукупності сегментів z, що містять приховану інформацію.

Input: Секретне повідомлення $a = \{a_i\}$, $a_i \in \{0,1\}$, $i = \overline{1,h}$, $h \in N$; множина векторних зображень (контейнерів) $I = \{I_b\}$, $b \in N$; множина параметрів приховування $V = \{V_u\}$, $u = \overline{1,4}$, $V_u \in N$, $V_1 = 3$; таблиця шаблону $TV_l[w]$, що виступатиме стеганоключем, $w = \overline{0, 2^l - 1}$, $TV_l[w] \in (0,\ l/V_3)$, $l \in N$, $c = V_3 / l$.

Output: множина стеганоконтейнерів $S = \{S_x\}$, $x \in N$.

1. $\{a^j\} = SplitMessage(a, V_3)$, $a^j = \{a_1^j, ..., a_{V_3}^j\}$, $a_i^j \in \{0,1\}$, $i = \overline{1, V_3}$, $j = \overline{1, m}$, $m = \lceil h/V_3 \rceil$;

2. $S = SelectImage(I, m, V_1)$, $S = \{S_x\}$, $x \in N$, $x \le m$, $m = \lceil h/V_3 \rceil$;

3. $D = SelectCurves(S, m, V_1, V_2)$, $D = \{D_j\}$, $j = \overline{1, m}$, $m = \lceil h/V_3 \rceil$;

4. $For\ (j = 1; j \le m; j{+}{+})$

4.1. $\{A_i^j\} = SplitMessage(a^j, l)$, $A_i^j \in \{0,1\}^l$, $i = \overline{1, c}$;

4.2. $w = 0$; $t = 0$; $D_{V_1}^w = D_j$;

4.3. $For\ (i = 1; i \le c; i{+}{+})$

4.3.1. $t = t + TV_l[A_i^j]$;

4.3.2. $\{P_e\} = GetPoints(D_{V_1}^w)$, $e = \overline{0, 3}$;

4.3.3. $P_0^1 = (1-t) \cdot P_0 + t \cdot P_1$;

4.3.4. $P_1^1 = (1-t) \cdot P_1 + t \cdot P_2$;

4.3.5. $P_2^1 = (1-t) \cdot P_2 + t \cdot P_3$;

4.3.6. $P_0^2 = (1-t) \cdot P_0^1 + t \cdot P_1^1$;

4.3.7. $P_1^2 = (1-t) \cdot P_1^1 + t \cdot P_2^1$;

4.3.8.. $P_0^3 = (1-t) \cdot P_0^2 + t \cdot P_1^2$;

4.3.9. $D_{V_1}^w = CreateCurve(P_0, P_0^1, P_0^2, P_0^3)$;

4.3.10. $D_{V_1}^{w+1} = CreateCurve(P_0^3, P_1^2, P_2^1, P_3)$;

4.3.11. $w = w + 1$;

4.4. $D_j = ReplaceCurve(S, D_j, \{D_{V_1}^i\})$, $i = \overline{0, w}$;

5. $Return\ S$;

Рис. 1. Псевдокод процедури приховування інформації алгоритму StegoTEMPL

Стійкість запропонованого алгоритму StegoTEMPL до атак на основі афінних перетворень була перевірена у ході експериментального дослідження. Було обрано 30 контейнерів формату SVG в які вбудовувалась інформація розміром 2^{10} біт при різних стеганоключах та параметрах приховування: $V_1 = 3$ (кубічні криві), $V_2 \ge 1$, $V_3 \in \{40, 60, 80\}$ біт, $V_4 = \{5, 6\}$, $V_5 \in \{2 \cdot 10^{-5}, 4 \cdot 10^{-5}\}$, $l = 4$. Всього проведено 36 експериментів, в кожному з яких визначено стійкість розробленого алгоритму до афінних перетворень. Перевірка стійкості до афінних перетворень здійснювалася за допомогою наступної загальної формули:

$$S_k = F\left(S_{k-1}, \alpha_{1,1}^k, \alpha_{1,2}^k, \alpha_{2,1}^k, \alpha_{2,2}^k, \beta_1^k, \beta_2^k, \varepsilon_1^k, \varepsilon_2^k, \varepsilon_3^k, \varepsilon_4^k, \varepsilon_5^k, \varepsilon_6^k\right),\ k = k + 1,$$

де F – функція здійснення афінного перетворення, S_0 – початковий стеганоконтейнер, $\alpha_{1,1}^k, \alpha_{1,2}^k, \alpha_{2,1}^k, \alpha_{2,2}^k, \beta_1^k, \beta_2^k$ – коефіцієнти накладання перетворення перенесення, повороту, зсуву і масштабування, $\varepsilon_1^k, \varepsilon_2^k, \varepsilon_3^k, \varepsilon_4^k, \varepsilon_5^k, \varepsilon_6^k$ – коефіцієнти спотворення перетворення повороту (для здійснення майже афінного повороту),

$\alpha_{1,1}^k, \alpha_{1,2}^k, \alpha_{2,1}^k, \alpha_{2,2}^k, \beta_1^k, \beta_2^k, \varepsilon_1^k, \varepsilon_2^k, \varepsilon_3^k,\ \varepsilon_4^k, \varepsilon_5^k, \varepsilon_6^k \in R,\ k \in \overline{1,100}$. Для кожного $S_k,\ k > 0$ виконувалося вилучення прихованих даних з обробленого стеганоконтейнера для його аналізу.

Одержані результати дослідження свідчать, що розроблений алгоритм StegoTEMPL завдяки властивостям кривих Без'є забезпечує гарну стійкість до атак на основі афінних перетворень. Максимальний коефіцієнт втрат при багаторазовому застосуванні даних перетворень до стеганоконтейнерів при різних параметрах склав: до атаки перенесення 1,52%, повороту 3,87%, майже повороту 2,16%, масштабування 5,29% та зсуву 55,33%.

Висновки. У роботі запропоновано новий стеганографічний алгоритм приховування інформації у векторні зображення StegoTEMPL. Проведено експериментальні дослідження для перевірки його стійкості до атак основі афінних перетворень. Експерименти показали, що запропонований алгоритм забезпечує гарні показники стійкості до атак на основі афінних перетворень (перетворень перенесення, повороту, майже повороту, масштабування і зсуву) та може бути застосований у стеганографічних системах для підвищення їх ефективності.

Список використаної літератури

1. Niu X. A survey of digital vector map watermarking / X. Niu, C. Shao, X. Wang // International Journal of Innovative Computing, Information and Control ICIC International, 2006. — vol.2. №6. — P. 1301-1316.

2.Карпінець В.В. Методи захисту векторних зображень цифровими водяними знаками : [монографія] // В.В. Карпінець, Ю.Є. Яремчук, 2013. — 156 с.

3.Кінзерявий О.М. Метод шаблонного приховування даних у векторні зображення / О.М. Кінзерявий, В.Ю. Ковтун, О.Л. Стокіпний // Захист інформації, 2014. — Т.16, №2. — С. 139-146.

4.Конахович Г.Ф. Компьютерная стеганография. Теория и практика / Г.Ф. Конахович, А.Ю. Пузыренко. — К. : МК-Пресс, 2006. — 288 с.

Корнейко О.В., к.т.н., профессор,
ИСЗЗИ НТУУ «КПИ», Киев

ТЕОРИЯ РАЗРЯДНЫХ ПРЕОБРАЗОВАНИЙ В СОВРЕМЕННОЙ КРИПТОГРАФИИ

В настоящее время широкое применение в современной криптографии нашли асимметричные криптоалгоритмы (АКА). Они используются, как правило: при распределении ключей, шифровании передаваемых ключей и формировании общего секретного ключа; обеспечения аутентификации абонентов и электронной цифровой подписи (ЭЦП); генерации криптографически сильных псевдослучайных последовательностей; генерации параметров ключевых массивов, используемых для создания ключей и др.

Актуальность использования АКА обусловлена также тем, что с их помощью достаточно просто реализовываются разнообразные электронные услуги в соответствии с Директивой 1999/93/ЕС и Регламента 2014 года Европейского Парламента и Совета по вопросам электронной идентификации и доверительных услуг (сервисов) для электронных операций на внутреннем рынке ЕС. И здесь особое место принадлежит АКА шифрования, а также обеспечения ЭЦП, криптостойкость которых основывается на сложности факторизации (разложения на множители) многоразрядных чисел (МРЧ), которые формируют криптомодули этих АКА.

К таким современным АКА шифрования относятся: «классический» алгоритм RSA (авторов Райвеста, Шамира и Адлемана), операции шифрования и дешифрования которого в некоторой литературе называют также криптопримитивами RSAEP (IFEP-RSA) и RSADP (IFDP-RSA) соответственно; его усовершенствованная версия RSAES-OAEP, сочетающая примитивы RSAEP и RSADP с методом предварительного кодирования EME-OAEP, основанном на алгоритме оптимизированного дополнения асимметричного шифрования OAEP, а также алгоритм RSAES-PKCS1-v1.5, который сочетает примитивы RSAEP и RSADP с методом кодирования EME-PKCS1-v1.5.

В качестве таких ЭЦП в международном стандарте ISO/IEC 14888-2:2008, который принят в Украине как национальный ДСТУ ISO/IEC 14888-2:2014, предлагается использовать криптосхемы RSA и RW (Рабина и Вильямса), которые позволяют не только удостоверить документ с помощью ЭЦП, но и при необходимости ознакомиться с его содержанием, а также криптосхемы так называемого «слепого» ЭЦП GQ1 и GQ2 (Гилоу и Квисквотера), GPS1 (Гиро, Попарда и Штерна), GPS2 (Гиро и Пайе) и ESIGN (Фуджийока, Окамото и Мягучи), котрые разрешают лишь подписать или проверить подпись, наложенную на электронный документ, без ознакомления и разглашение его содержания.

Поэтому или при оценке криптостойкости этих АКА, или при их дешифровании неизбежно возникает задача необходимости использования для этих целей эффективного метода факторизации, позволяющего разложить криптомодуль АКА длиной Z на два больших (многоразрядных) простых числа P и Q.

В настоящее время разработано достаточно большое число математических методов факторизации, из которых асимптотически самыми быстрыми для реализации на классических компьютерах являются вероятностные методы факторизации с субэкспоненциальной сложностью – методы квадратичного решета (QS) и решета числового поля (GNFS).

Однако эти методы факторизации многоразрядных чисел не учитывают особенности структурного построения числа, которое необходимо разложить на множители. Вместе с тем, известным математиком и криптографом Брюссом Шнайером (B. Schneier) была выдвинута гипотеза о том, что «могут появится новые методы разложения на множители, которые лучше работают с числами, обладающими определенной структурой» и, следовательно, учет особенностей структуры факторизируемых чисел может повысить эффективность алгоритмов факторизации и снизить показатели их вычислительной сложности. Но пути решения этой проблемы Б. Шнайер не показал.

Поэтому в докладе показано, что так как названные выше современные методы факторизации (QS и GNFS) используют вычислительные операции просеивания в факторных базах (которые являются одними из самых трудоемких в этих методах факторизации), то за счет применения математического аппарата разрядных преобразований можно усовершенствовать этап просеивания в факторных базах с целью понижения вычислительной сложности этих методов факторизации.

Показано, как за счет использования математического аппарата разрядных преобразований для определения простых множителей P и Q числа Z, которые представлены в двоичной форме, формируется система нелинейных логических уравнений, в которой переменные соответствуют разрядам каждого из чисел P или Q, последующее решение которой дает возможность найти значения разрядов P или Q.

Предложено также использовать математический аппарат разрядных преобразований для синтеза комбинационных схем (логических сетей, битовых моделей), выполняющих процедуру нелинейной рандомизации для схем кодирования RSA, позволяющих повысить криптографическую стойкость этого АКА.

Кузнецова А.В.,
Василиу Е.В., д.т.н., профессор,
Одесская национальная академия связи им. А.С. Попова

ПЕРСПЕКТИВЫ РАЗВИТИЯ КВАНТОВЫХ ПРОТОКОЛОВ С НЕПРЕРЫВНЫМИ ПЕРЕМЕННЫМИ

На сегодняшний день классические телекоммуникационные системы уязвимы для перехвата информации из канала связи злоумышленником. Решением данной проблемы являются современные технологии квантовой связи, которые, благодаря своим физическим свойствам, позволяют обнаружить злоумышленника.

Также, производя ряд квантовых измерений, два легитимных пользователя могут оценить, как много информации злоумышленник крадет из канала.

Первоначально, дискуссии и экспериментальные исследования QKD были сосредоточены на дискретных переменных (DV). Существовали две основные схемы для DV QKD: те, которые основаны на отправке состояний ортогональных базисов, так как это описано в оригинальном «BB84 протоколе», предложенном в 1984 году Беннетом и Брассардом, и те, которые основаны на обмене запутанными фотонами между отправителем и получателем, например, схема Экерта в «E91-протоколе». К настоящему моменту большое количество схем QKD с DV были представлены и их возможное использование в безопасной связи было экспериментально показано [1, 5, 6]

Наряду с классической квантовой криптографией, параллельно развивается квантовая криптография с непрерывными переменными (CV), которая в свою очередь имеет ряд особенностей.

Многие из первых предложений по использованию CV QKD включали перепутанные пучки света [1, 2], однако, эти состояния трудно производить. Некоторые другие протоколы используют более традиционные процедуры подготовки и измерения, где Алиса готовит состояние и посылает его Бобу без сохранения запутанных подсистем [2].

Тем не менее, генерация сжатых состояний довольно затруднительна. Гораздо проще генерировать когерентные состояния. Несмотря на то, что когерентные состояния являются частными случаями сжатых состояний. Гроссханс и Грангиер разработали первый протокол, в котором когерентные состояния модулированы в обоих квадратурах одновременно - протокол GG02 [2]. В GG02 также используется идея гауссовой модуляции. Этот протокол позволяет облегчить реализацию и обеспечить высокую скорость генерации секретного ключа[2] - это следует из того, что гомодинное детектирование, используемое в GG02, может работать быстрее, чем детекторов фотонов в BB84.

Возможные стратегии (атаки) перехвата информации в QKD делятся на три категории: индивидуальные, коллективные и совместные.

Индивидуальная атака является стратегией, в которой Ева исследует каждое из квантовых состояний независимо друг от друга. В этом случае результаты измерений Евы могут быть смоделированы как случайные величины.

В коллективной атаке Ева также исследует каждое квантовое состояние независимо, но при этом она может измерять целый набор таких «проб» совместно. Кроме того, Ева может ждать, пока открытая передача данных не будет завершена. В этом случае результаты действий Евы не могут быть смоделированы как случайная величина, зависящая от элемента ключа, так как не известно, какую стратегию измерения секретного ключа она выбрала.

При совместной атаке Ева может исследовать все квантовые состояния совместно. Это наиболее общий вид атаки на квантовый канал. Конечно, как и для коллективных атак, Ева может сделать измерение после того как вся открытая передача данных будет завершена

В описанных выше стратегиях перехвата, предполагалось, что Ева атакует только квантовый протокол распределения ключей. Но ничто не мешает ей дождаться использования ключа Алисой и Бобом, например, для шифрования секретного сообщения,

прежде чем произвести измерение. Знание того, какие операции легитимные стороны совершают с их ключом, может помочь Еве в разрушении криптографический системы, в которой Алиса и Боб используют данный ключ. Например, она может захотеть определить секретное зашифрованное сообщение. Это проблема компонуемости QKD протоколов с другими криптографическими протоколами.

Неформально, протокол QKD является компонуемым, если сгенерированный им ключ также хорош, как если бы он был сгенерирован идеальным протоколом распределения ключей.

Выводы

Таким образом ключ QKD протокола должен выполнять три условия. Во-первых, ключ должен иметь распределение, близкое к равномерному. Во-вторых, случай несовпадения ключей между Алисой и Бобом на этапе просеивания должен быть редким. Наконец, взаимная информация между Евой и сгенерированных ключей должна быть мала. Ожидается, что эти условия должны быть выполнены после усиления конфиденциальности.

Важным, в контексте безопасности QKD против совместных подслушивающих атак, является то, что информация Евы о ключе должна быть мала, даже если она держит квантовую информацию, пока Алиса и Боб не использовали свой ключ. Если злоумышленник задерживает измерение перехваченной квантовой информации пока Алиса и Боб не раскроют то, как они собираются использовать сгенерированный ключ - выбранный криптографический алгоритм может быть взломан, но если перечисленные выше три условия будут выполняться в присутствии злоумышленника с неограниченным технологическим потенциалом и без каких-либо ограничений, кроме законов квантовой механики.

Список литературы

1. Gilles Van Assche. Quantum cryptography and secret-key distillation / Gilles Van Assche // Cambridge University Press, 2006.

2. Cerf N.J. Quantum information with continuous variables of atoms and light / N.J. Cerf, G. Leuchs, E.S. Polzik // Imperial College Pres, 2007.

3. Kok P. Quantum information processing / P. Kok, B.W. Lovett // Cambridge University Press, 2010.

4. Cerf N.J. Quantum information with continuous variables of atoms and light / N.J. Cerf, G. Leuchs, E.S. Polzik // Imperial College Pres, 2007.

5. Bouwmeester D. The Physics of Quantum Information / D. Bouwmeester, A. Ekert, A. Zeilinger//M: Postmarket, 2002.

6. Nielsen M.A. Quantum Computation and Quantum Information / M.A. Nielsen, I.L. Chuang// M:“Mir“, 2006.

Лахно В.А., д.т.н., доцент,
Європейський університет, Київ,
Корченко О.Г., д.т.н., професор,
Національний авіаційний університет, Київ,
Бекетова Г.С.,
Інститут інформаційних і телекомунікаційних технологій,
Казахський національний дослідницький
технічний університет імені К.І. Сатпаєва, Алмати

ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІНТЕЛЕКТУАЛЬНОГО РОЗПІЗНАВАННЯ КІБЕРЗАГРОЗ

Ефективність функціонування сучасних КС та технологій виявлення кібератак істотно залежить від оперативності та достовірності моніторингової інформації активності кіберзлочинців на попередніх стадіях реалізації кібернападів на інформаційні ресурси державних установ та приватних компаній. Як показав світовий досвід, на сьогодні найбільш ефективним методологічним підходом до побудови інноваційних інтелектуальних моніторингових систем кібернападів є шлях створення ієрархічних багаторівневих структур розпізнавання кібератак на початкових стадіях їхньої реалізації. При цьому, ієрархічний підхід дає змогу розв'язувати складні задачі управління процесом захисту інформації від кібератак в розподілених інформаційних системах критичної інфраструктури держави як послідовність локальних задач, скоординованих між собою.

Розробка і використовування інтелектуальних систем моніторингу, розпізнавання кібератак та управління подіями інформаційної безпеки (ІБ) в даний час є одним з найбільш перспективних напрямків в області забезпечення кіберзахисту в КС і мережах. Подібні системи дозволяють на основі збору і оперативного аналізу даних про події ІБ, зокрема кібератаки, виявляти і попереджувати мережеві вторгнення, оцінювати і прогнозувати рівень захищеності об'єктів інформатизації, наприклад, інформаційно-комунікаційних систем (ІКС) критичної інфраструктури держави. Тому вирішення задач, пов'язаних із здійсненням інтелектуального моніторингу інцидентів ІБ і формуванням оперативних рішень по кіберзахисту в інтегрованих територіально-розподілених інформаційних системах, є актуальним.

В США, державах ЄС, Китаї, Південній Кореї та Японії дослідженням проблематики створення інтелектуальних систем виявлення кібератак приділяється багато уваги, про що свідчить велика кількість публікації з цієї тематики [1-5]. На пострадянському просторі питанням розробки розподілених систем виявлення кібератак (РСВК) в різний час теж займалися різні вчені [6-11]. Однак в галузі кіберзахисту побудову моделей РСВК засновано на різнорідних підходах, вони носять точковий характер відповідно до об'єктів кібернападу. Моделі та алгоритми розпізнавання кібернападів часто не взаємопов'язані, що наразі ускладнює їх використання при створенні ефективних РСВК. Таким чином, розробка та застосування інноваційних РСВК стримується недостатньою ефективністю функціонування моделей та алгоритмів розпізнавання загроз у межах відомих та нових класів кібератак, що викликано низькою точністю моделей об'єктів моніторингу кіберзахисту. На наш погляд, основними причинами є:

1.Низька ефективність управління системами виявлення кібератак пов'язана із недостатньою кількістю інформації про стан об'єктів кіберзахисту, особливо, для критичної інфраструктури держави.

2.Значна кількість непов'язаних між собою об'єктів моніторингу, що у свою чергу ускладнює формалізацію задач виявлення складних кібератак та традиційних математичних методів опису шаблонів кібернападів. Для синтезу адекватних моделей РСВК необхідне підсилення можливостей традиційних статистичних підходів [4, 5, 7] методами, які є менш чутливими до вимоги незалежності параметрів.

Аналіз методів визначення причиново-наслідкових зв’язків між вхідними параметрами та вихідною величиною при розробці РСВК, дозволяє дійти висновку, що жоден з них з притаманними їм перевагами і недоліками не може окремо повною мірою відповідати моделі "багатовимірний вхід – вихід". Отже, існує велика кількість неформалізованих задач кібербезпеки, які не можуть бути розв’язані за допомогою лише одного методу, а необхідний консорціум методологій, які забезпечили б основи конструювання та розвитку інтелектуальних РСВК або ІРСВК. Першим шляхом комплексного використання таких напрямків, як нечітка логіка, нейро- і генетичні обчислення та інших інтелектуальних технологій ідентифікації стали м’які обчислення (Soft Computing), які більшою мірою пристосовані до роботи з неточними та невизначеними даними, що дозволяє розв’язати проблему лінгвістичної невизначеності. Однак, наряду з подоланням труднощів використання нечітко заданої вхідної інформації необхідно також забезпечити можливість урахування відмінностей між різними класами кібератак за важливістю контрольованих параметрів і врахувати їх взаємодії необхідного порядку. Ця проблема може бути вирішена методами нечіткої логіки та регресійного аналізу.

Метою даної роботи є апробація методу інтелектуального розпізнавання кібератак на основі дискретних процедур для побудови адаптивних систем кіберзахисту інформаційно-комунікаційних систем, в умовах збільшення кількості дестабілізуючих впливів на схоронність, доступність і цілісність інформаційних ресурсів.

Неповнота інформації про загрози для ІБ у ІКС є двоякою. По-перше, це часткова відсутність апріорної інформації, навіть на рівні уявлення про структуру всього об'єкта нападу на інформацію, що має, як правило, стохастичну природу. По-друге, обмежена можливість спостереження об'єкта нападу й розпізнавання загроз, що належать певному класу. У граничному випадку заздалегідь відома лише загальна множина загроз ІБ і способів їх реалізації.

Однак, як показує практика, одна з основних характеристик сучасних загроз полягає у тому, що вони довгий час не активуються, іноді до двох-трьох років [7, 8]. Цільові атаки, зокрема, спрямовані на ІС підприємств, об'єкти інфраструктури, енергетики, транспорту тощо, зазвичай розробляються з урахуванням того середовища, на яке вони будуть націлені. Сучасні загрози створюються таким чином, щоб обійти захист, і, як правило, вже не виявляються за допомогою сигнатур. Розробка сценаріїв кібератак виконується з дотриманням всіх стандартів і технологій, з технічним завданням, робочим проектом, тестуванням, підтримкою і оновленням.

Оцінка можливості реалізації загрози залежить від багатьох факторів. У багатьох джерелах можливість реалізації загрози визначається як певна ймовірність [1, 4, 11]. Однак, загроза, яка є джерелом потенційного збитку, а тому представляє деяку небезпеку, будь-яким чином повинна бути виміряна. Фактично, мова йде про формування моделі загроз для ІКС. Безумовно, вимірювання загрози слід почати з оцінки можливості її виникнення. Така оцінка може бути зроблена на основі даних по відомим фактам появи загрози, вираженим через статистичну частотність. Дану оцінку можна розглядати як оцінку, засновану на наявному досвіді експлуатації СЗІ ІКСТГ.

Другим фактором оцінки можливості реалізації загрози є оцінка витрат, що неминуче виникають при введенні тих чи інших засобів захисту.

Таким чином, нові моделі розпізнавання кіберзагроз для ІКС не тільки становлять самостійний практичний інтерес, але і є прикладом можливої формалізації опису нових, ще невідомих класів кібератак.

Перспективи подальших досліджень полягають у тому, щоб визначити найбільш критичні об’єкти ІКС, що підлягають захисту, а також дослідити запропонований метод інтелектуального розпізнавання загроз на більш широкому класі задач кількісного і якісного розпізнавання кібернападів.

Література
1. U.S. Department of Transportation, Research and Innovative Technology Administration, “Intelligent Transportation Systems (ITS) Strategic Plan: Background and Processes,” January 8, 2010, http://www.its.dot.gov/strat_plan/pdf/ IntelliDriveBook_Jan2010.pdf.
2. Maras Marie-Helen. Cybercrime Laws: Which Statute for Which Crimes. (2012). *Computer Forensics: Cybercriminals, Laws, and Evidence*. Sudbury, MA: Jones & Bartlett Learning. – P. 104-06.
3.Adel W. Sadeka, Byungkyu “Brian” Parkb & Mecit Cetinc (2014). Special Issue on Cyber Transportation Systems and Connected Vehicle Research. Journal of Intelligent Transportation Systems: Technology, Planning, and Operations. Volume 20, Issue 1, 2016. DOI:10.1080/15472450.2014.889914
4.Teodor Sommestad, Henrik Karlzén, Jonas Hallberg (2015). A Meta-Analysis of Studies on Protection Motivation Theory and Information Security Behaviour. *International Journal of Information Security and Privacy* (IJISP). Volume 9. – P. 26-46.
5.Sumeet Dua. Data Mining and Machine Learning in Cybersecurity / Sumeet Dua, Xian Du. — Taylor & Francis Group, 2011. — 223 p.
6.Дудикевич В. Б. Проблеми оцінки ефективності систем захисту /В. Б. Дудикевич, І. А. Прокопишин, В. Ф. Чекурін // Вісник Національного університету "Львівська політехніка". – Сер.: Автоматика, вимірювання та керування. – Львів : НУ "Львівська політехніка", 2012. – № 741. – С. 118–122.
7.Корченко А. А. Система формирования нечетких эталонов сетевых параметров / А. А. Корченко // Захист інформації, 2013. – Т. 15, №3. – С. 240 –246.
8.Грищук Р. В. Атаки на інформацію в інформаційно-комунікаційних системах / Р. В. Грищук // Сучасна спеціальна техніка, 2011. – №1(24). – С.61-66.
9.Харченко В. П. Кибертерроризм на авиационном транспорте / В. П. Харченко, Ю. Б. Чеботаренко, О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк // Проблеми інформатизації та управління: Зб. наук. пр. : Вип. 4 (28). – К. : НАУ, 2009. – С. 131-140.
10.Корченко О. Г. Ознаковий принцип формування класифікацій кібератак / О. Г. Корченко, Є. В. Паціра, С. О. Гнатюк, В. М. Кінзерявий, С.В. Казмірчук // Вісник Східноукраїнського національного університету імені Володимира Даля, 2010. – №1. – С. 32–38.
11.Lahno V. Ensuring of information processes’ reliability and security in critical application data processing systems/ V. Lahno // MEST Journal. – Belgrade, 2014. –Vol. 2, No 1. – P. 71–79.

Мельник С.В., к.е.н., доцент,
заслужений економіст України,
позаштатний консультант
Комітету ВРУ з питань науки і освіти, Київ

НОВІ ПІДХОДИ ЩОДО ЗАКОНОДАВЧО-НОРМАТИВНОГО ЗАБЕЗПЕЧЕННЯ РЕФОРМИ ОСВІТИ

Питання реформування освіти у контексті змін, що задекларовані або дійсно відбуваються на теренах розбудови про європейської держави на заміну збанкрутілих тоталітарних методів розвитку, є вкрай нагальним та випитаним часом. У цьому контексті на перший план виступає формування ефективного та зрозумілого законодавчо-нормативного базису для супроводження відповідних перетворень.

За останні два роки в країні відбулося багато знакових освітянських подій: запроваджено з вересня 2014 року новий ЗУ «Про вищу освіту», який імплементовано менш ніж на 20,0%; прийнято новий перелік спеціальностей, що інтегрував «попередника» майже в

5 разів; обрано персональний склад Національного агентства з оцінювання вищої освіти, який не став дієздатним через цілу низку суб'єктивних (обрали не зовсім тих, на кого розраховувало тодішнє керівництво МОН України) та об'єктивних (відсутність попереднього досвіду, підготовчих заходів) причин; розроблено та подано на повторне перше читання досить інноваційний проект ЗУ «Про освіту»; підготовлено та знято як невдалий варіант законопроект «Про професійну освіту» тощо. Ключовими публікаціями цього періоду виступають результати відповідних обговорень експертним та громадським середовищем, наукові дослідження зарубіжного та міжнародного досвіду реформування сфери освіти, матеріали міжнародних та вітчизняних науково-практичних конференцій тощо. Серед великого числа авторів публікацій можна виділити Вітренка Ю.М., Гриневич Л.М., Калашнікову С.А., Ковтунця В.В., Лугового В.І., Фінікова Т.В. та ін. Разом з тим, питанням навчання дорослого населення освітня реформа приділяє вкрай мало уваги. Спроба систематизувати ключові завдання саме у цій царині виступає метою цієї роботи.

Участь автора в роботі над окремими питаннями законотворчо-нормативної діяльності у сфері реформування системи освітніх послуг дає можливість визначити його особисту думку щодо можливих реформаторських досягнень, а саме:

- законодавче закріплення нових понять, термінів, підходів, механізмів та процедур (національна рамка кваліфікацій, типи кваліфікацій (освітні, професійні, повні, часткові), кваліфікаційні центри, агентство з професійних кваліфікацій, реєстр кваліфікацій, незалежне (зовнішнє) оцінювання результатів навчання тощо);
- визнання як рівнозначних складових, що надають освітні послуги формальної, неформальної та спонтанної (інформальної) освіт;
- рівність у правах, можливостях та доступі до ресурсів навчальних закладів усіх типів та форм власності;
- запровадження механізму фінансово – господарської діяльності в освітній сфері, як окремого рентабельного ринкового виду економічної діяльності – економіки знань;
- визнання освіти дорослих, як взаємопов'язаного сегменту освіти в цілому, та навчання на протязі всього життя, зокрема.

Серед проблемних, дискусійних питань, що виникають (виникнуть найближчим часом) слід виділити:

- проблемність застосування на практиці освітнього рівня молодший бакалавр, складність у визначенні освітніх кваліфікацій 0 та 9 рівнів НРК, та в інтерпретації професійних кваліфікацій 1-3 рівнів НРК;
- відхід освітніх кваліфікацій 6 та 7 рівнів НРК (бакалавр та магістр) від професійних кваліфікацій цих рівнів. Європейський механізм прив'язування цих двох типів кваліфікацій за оптимістичним сценарієм можна сформувати в країні для всіх спеціальностей не раніше 2020 року;
- винесення левової частки коледжів за межі вищої освіти та відірваність їх від профтехосвіти. Така ситуація буде залишатися конфліктною певний період, який характеризуватиметься формуванням нових інтеграційних інституцій до університетського рівня, в тому числі шляхом укрупнення ВНЗ до 100-120 одиниць.

Висновки. Проведений короткий огляд піднятого питання дозволяє зробити декілька узагальнюючих висновків, а саме:

- освітня реформа, як і всі інші, повинна здійснюватися системно та комплексно .У нашому випадку відсутня чітка взаємодія з розробкою проекту Трудового кодексу України, переглядом ЗУ «Про професійний розвиток працівників», «Про формування державного замовлення на підготовку кадрів», «Про стандартизацію», «Про ліцензійну діяльність», «Про оплату праці» тощо;

- для успішної імплементації нових актів законодавства потрібна попередня клопітка експертно-дослідницька робота, розробка превентивних заходів із визначенням зисків та ризиків, втрат та переваг;
- для запровадження на практиці нових інноваційних освітянських складових необхідні чималі фінансові, матеріальні, кадрові, інституціональні, інформаційні та інші ресурси або їх перерозподіл у межах наявних. Без цього будь-які прогресивні задуми та намагання приречені на поразку чи «недоуспіх», яких у країні, на превеликий жаль, переважна більшість.

Нємкова О.А., к.ф.-м.н., доцент,
Львівський інститут ДВНЗ «Університет банківської справи»,
Шандра З.А., к.т.н., с.н.с.,
Національний університет «Львівська політехніка»,
Костирко Т.М., аспірант,
Львівський інститут ДВНЗ «Університет банківської справи»

ТОПОЛОГІЯ МУЛЬТИФРАКТАЛІВ ШУМІВ ПРИСТРОЮ В ЗАДАЧАХ ДИНАМІЧНОЇ ІДЕНТИФІКАЦІЇ

За останні роки в науці сформувався новий напрям, який має назву кібер-фізичні системи [1]. По суті, це означає впровадження в навколишній світ інтелектуальних пристроїв, які об'єднані в єдине ціле за допомогою мережевих технологій. Кожний пристрій діє в комплексі з іншими пристроями системи. В такому випадку роль інформаційної безпеки зростає багаторазово, зокрема, посилюється значення ідентифікації кожного пристрою, що входить в систему. Питання ідентифікації пристроїв в інформаційних мережах не є новим, добре відомо, що для цих цілей використовуються дві адреси пристрою - фізичний (MAC адреса) і логічний (IP). Ці адреси досить легко змінити, особливо логічну адресу - до нещодавнього часу адреси були потрібні тільки для пересилання інформаційних пакетів. У кібер-фізичних системах пристрої мають виконавчий механізм, їх мета - вплив на навколишній реальний світ. Вони приймають рішення на підставі отриманої інформації від інших пристроїв і передавачів, і самі можуть керувати іншими пристроями. Тому дуже важливо, щоб інформація, на підставі якої приймаються рішення та здійснюються дії в фізичному світі, прийшла саме від тих пристроїв і передавачів, які є в системі, а не в результаті кібератаки. Легкість зміни адресації мережевих пристроїв призводить до необхідності пошуку іншого способу їх надійної ідентифікації, яка пов'язана з конкретним пристроєм і не може бути надана йому зовні. Така можливість обумовлена відмінністю пристроїв один від одного на мікроскопічному рівні. Ці відмінності фіксуються практично тільки на рівні шумів пристрою.

У даній роботі розглянута можливість ідентифікації з використанням фрактальних властивостей динамічного ряду шуму, який характерний для аудіоплати стаціонарного комп'ютера. Шум аудіоплати у першому наближенні можна вважати білим шумом. Відмінності шуму кожної аудіоплати проявляються у відхиленнях від моделі білого шуму. Для візуалізації цих відмінностей були побудовані фазові портрети динамічних спектральних компонент ряду шуму. Розпізнавання конкретного аудіопристрою (використання методики ідентифікації аудіоплат за допомогою портрета Хьорста [2]) базується на розрахунку коефіцієнта Хьорста для кожної спектральної компоненти шуму. В результаті проведених експериментів та подальших розрахунків було виявлено динамічний характер портрета – коефіцієнти змінюються у часі, причому ці зміни не однакові для різних спектральних компонент. Враховуючи цей факт, а також неоднозначність вибору ділянки графіка при RS -

аналізі шумового процесу, за яким власне обраховується коефіцієнт Хьорста [3,4], в даній роботі наведено спробу ідентифікації за топологічними ознаками мультифрактала шуму. В якості тестових сигналів для перевірки розрахунків було обрано синусоїдальний сигнал та білий шум, які було згенеровано за допомогою програми Soundcard Scope, частота дискретизації 44,1 кГц. Паралельно з'ясувалось, що досліджуваний синусоїдальний сигнал являв собою набір амплітудно змодульованих ділянок синусоїд з деякими відхиленнями від ідеальної форми. Тестові сигнали складались з трьох характерних ділянок: відсутності сигналу (≈ 0.02 сек), перехідного процесу (≈ 0.02 сек), сигналу синусоїди або білого шуму. Аналогічні ділянки спостерігались для вимірюваного шуму аудіоплати. Для розрахунків використовувались ділянки розвинутого процесу. На рис.1 наведено фазові портрети модельних сигналів для 8-спектральної компоненти (було використано швидке перетворення Фур'є для 128 точок).

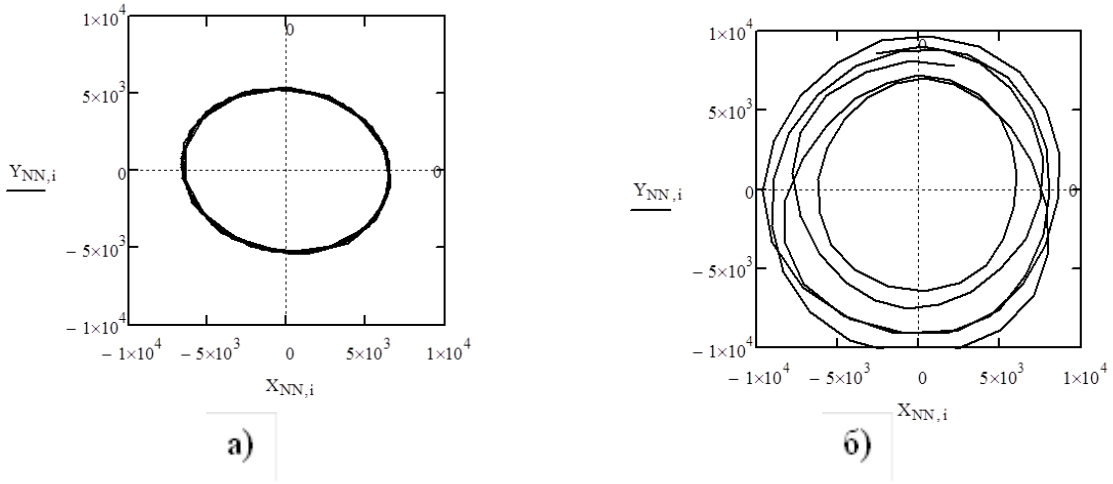

Рис.1. Фазові портрети спектральної компоненти (n=8) модельних сигналів: а) синусоїдального сигналу, б) білого шуму

На рис.2 наведено фазові портрети двох спектральних компонент мульти-фрактала шуму аудіоплати.

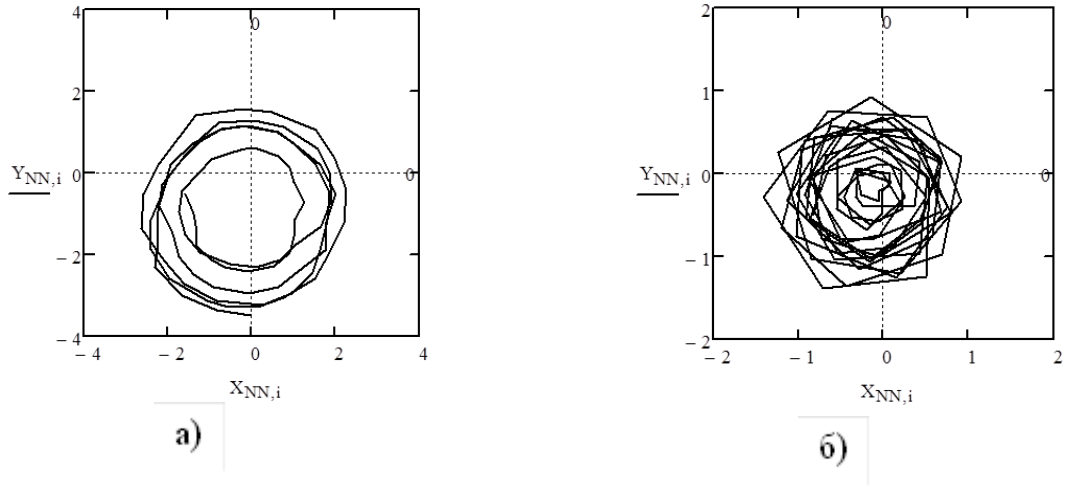

Рис.2. Фазові портрети спектральних компонент шуму аудіоплати стаціонарного комп'ютера: а) n=8, б) n=24

По осях абсцис та ординат на графіках обох рисунків відкладено амплітуди дійсної та уявної частин спектральної щільності потужності, які утворюються при швидкому перетворенні Фур'є динамічного ряду шуму. Для синусоїдального сигналу отримано добре відомий результат – граничний цикл. Фазові траєкторії для модельного білого шуму та реальних шумів представляють собою дивні атрактори. Для низьких частот дивні атрактори частково нагадують граничний цикл, а зі збільшенням частоти область атрактора виявляється більш заповненою траєкторіями. Тим не менш, область, яку займає атрактор, дуже подібна до кола. Для модельного білого шуму координати кіл атракторів різних спектральних компонент співпадають з початком координат. Для реального шуму координати кіл атракторів мають зміщення відносно початку координат, причому кожна спектральна компонента характеризується власним зміщенням.

Висновки. За допомогою фазового портрету спектральної щільності потужності показана відмінність модельного білого шуму і реального шуму аудіоплати комп'ютера. Дивний атрактор різних спектральних компонент реального шуму пояснює нерегулярну (хаотичну) частину шуму, а також вказує на наявність циклів різних періодів.

Література

[1] Куприяновский В.П. Кибер-физические системы как основа цифровой экономики. / В.П. Куприяновский, Д.Е. Намиот, С.А. Синягов // International Journal of Open Information Technologies ISSN: 2307-8162, 2016. - vol. 4. no. 2. – P.18-25.

[2] Нємкова О.А. Методика вимірювання ідентифікаційних параметрів аудіозаписувальних пристроїв. / О.А. Нємкова, З.А. Шандра // Вісник національного університету "Львівська політехніка" "Комп'ютерні системи та мережі", 2015. - № 821. – С.94–100.

[3] Антипов О.И. Сравнение скорости и точности фрактальных методов детерминированного хаоса применительно к распознанию стадий сна. / О.И.Антипов, А.В.Захаров, В.А.Неганов. // Бюллетень ВСНЦ СО РАМН, 2013.-№2 (90). Част. 1. - С.9-14.

[4] Кириллов Д.С. Распределения показателя Херста нестационарного маркированного временного ряда / Д.С.Кириллов [и др.] // Препринты ИПМ им. М.В.Келдыша, 2013. - № 11. - 16 с.

Ogbu J.O., PhD student,
Shestak Y.V., PhD student,
Taras Shevchenko National University, Kyiv

MONITORING of DATA PROCESSING CENTER (DPC) IN INFORMATION PROTECTION FROM CYBER ATTACKS

Огбу Д.О., Шестак Я.В. Моніторинг обробки даних центру (ОДЦ) в інформаційному захисті даних від кібератак. У цій статті розглянуті найбільш важливі цілі безпеки в системі автоматизації розподілу і запропоновані ефективні способи досягнення цих цілей. Основними моментами тут є питання безпеки кіберсистеми і енергетичної комунікаційної системи (PSC), які виділені в цій роботі. Проаналізовані основні чинники, які сприяють збільшенню уразливості конфіденційних даних. На основі проведеного аналізу виявлена і обгрунтована необхідність захисту інформаційних даних від кібератак.

***Ключові слова*:** інформація, інформаційна безпека, інформаційні загрози, кібератака, кібербезпека, кіберзагроза, стратегія, інформаційний захист.

In the current conditions, the issues in operation of data processing centers (DPC) become particularly urgent, which can significantly reduce the availability and the quality of DPC services. These issues are crucial to the success of customers and owners of DPC.

Monitoring of the network of data processing center is a systematic control over basic parameters of operation of the network and network applications to provide high levels of quality of user service and network performance [1]. The systems of network monitoring accelerate the detection and analysis of the network problems encountered, and allow identifying potential problems and fix them before they impact the work of the customers of data processing center. The operators of data processing centers should invest in net flow monitoring tools to enable analysis of incidents and threats. Using a variety of tools — from Net Flow analysis to correlation of events using SIEM systems —the operators need to understand and assess the source and types of internal and external threats. Comprehensive monitoring of processes and net flow helps identify unauthorized access to data, and timely identify threats of its accessibility before the customer notifies of the problem.

Today, as part of the international community, some areas (methodologies) of the network monitoring are singled out. One of them is SNMP monitoring (SNMP — Simple Network Management Protocol) —this is a widely used technology, which is generally intended to manage networking equipment (routers, switches, servers, etc.) [2]. SNMP monitoring provides details on the networking equipment and creates an overall picture of the network usage. However, despite the functions performed, this technology with a large number of controlled devices of SNMP inquiry may create a great net flow, that is an additional load on the controlled network. It is also worth noting that SNMP monitoring is provided by Simple Network Management Protocol which information is generally not sufficient to determine the root cause of the networking problems.

The second area of network monitoring is flow-based monitoring. Flow-based monitoring is an advantageous area due to its low-cost solutions, because routers and switches are usually used as sensors, eliminating the need to purchase additional devices for capturing traffic [2]. As a result of this area of monitoring, the user receives useful statistical information about the network operation, applications and network bandwidth used. However, such monitoring methodology, depending on the type of technology used (xFlow) and the load on the networking equipment, can exercise sampled control of batches, reducing accuracy of generated information on the network.

Batch-based monitoring is also a relevant monitoring methodology of the network of data processing center. Batch-based monitoring systems analyze all parts of each IP batch (including its payload). These systems are able to generate the same statistics generated by SNMP- and flow-based solutions, thereby providing the most detailed analysis of the network operation [1]. The use of batch-based systems is the only way to quickly and effectively solve networking problems with no impact on the operation of controlled network.

The usefulness of the data processing center network monitoring is to accelerate the response to failures in the network and diagnose problems in the applications that are interspersed; investigation of network incidents and monitoring of compliance with the rules of using the customer's applications; optimization of network operation and acceleration of return on such IT initiatives as VDI and SDN; notification of traffic spikes and bandwidth planning.

Conclusion

A data center (sometimes-spelled datacenter) is a centralized repository, either physical or virtual, for the storage, management, and dissemination of data and information organized around a particular body of knowledge or pertaining to a particular business. A data center is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls and various security devices. Large data centers are industrial scale operations using as much electricity as a small town.

Introduced the novel concept of stochastic cyber-attack process, which offers a new perspective for studying cyber-attack sand, in particular, can be instantiated at multiple resolutions

such as network-level, victim-level and port-level. Then proposed a statistical framework that is centered on identifying. In this paper, we identified the most critical security goals in the distribution automation system and proposed efficient ways of achieving these goals.

References

1. Zasetskyi A., Shelgov B. Data Processing Center Network Monitoring // Journal of Networking Solutions/LAN, 2013. - No. 05. - 68 p.
2. Barskov A. The World of Data Processing Center 2015: under “M” Sign // Journal of Networking Solutions/LAN, 2015. - No. 05-06. - 76p.

Павленко В.Н., д.т.н., профессор,
Зряхов М.С., к.т.н., доцент,
Пономаренко Н.Н., д.т.н., доцент,
Национальный аэрокосмический университет им. Н. Е. Жуковского «ХАИ», Харьков

МЕТОДИКА ВЫЧИСЛЕНИЯ РЕЙТИНГОВЫХ БАЛОВ В ИНФОРМАЦИОННОЙСИСТЕМЕ ХАИ

Интенсивность научной деятельности сотрудников высших учебных заведений (ВУЗ) зависит от квалификации НПР [1, 2]. Совокупность программ мотивации и методик контроля качества услуг, предоставляемых высшими учебными заведениями способны существенно повысить эффективность труда. Следовательно, реализованная автоматическая система контроля позволяет определить не только лучших НПР и структурные подразделения ВУЗа, но и мотивировать к дальнейшему развитию и совершенствованию НПР, что, в целом, приведет к улучшению качественных показателей работы ВУЗа и повышению его рейтинга среди учебных заведений.

К основным видам нагрузок в ВУЗе относятся: учебная, научная и учебно-методическая работы [3] на основании которых и формируется рейтинг. Остальные виды деятельности (например, организационно-методическая работа, воспитательная работа) можно отнести к второстепенным, однако, без них работа ВУЗа будет неполноценной, а в некоторых случаях полностью/частично заблокированной.

Чтоб обеспечить надежное и качественное функционирование автоматизированной системы оценивания труда необходимо удовлетворить ряд требований (зачастую противоречивых) или искать разумные компромиссы. Примером автоматизированной системы оценивания труда сотрудников ВУЗа может быть информационно-рейтинговая систем оценивания эффективности труда НПР Национального аэрокосмического университета «ХАИ» (ИРС ХАИ), в которой успешно решены основные требования и реализован взвешенный подход к начислению баллов за каждый вид деятельности.

Составными частями рейтинга в ИРС ХАИ являются: прошлые заслуги НПР (ученая степень, ученое звание, стаж, публикации с высоким уровнем цитирования и др.), учебная нагрузка, учебно-методическая работа (подготовка к занятиям, сопровождение учебных дисциплин, обеспечение лабораторных и практических занятий, издание учебных пособий, учебников и другой учебно-методической литературы), научно-исследовательская работа (публикации на конференциях и в журналах, монографии, патенты, руководство студентами, защиты диссертаций, руководство защитившимися, оппонирование диссертаций, выполнение научных исследований и др.), организационно-методическая и воспитательная работы. Подробный перечень пунктов рейтинга приведен в [4].

Предложено баллы рейтинга в ИРС ХАИ условно привязывать к трудоемкости работы в часах. При этом, каждому достижению НПР в ИРС соответствует скорректированный весом определенный вид работ, указанный в индивидуальном плане преподавателя и полезный при учете в рейтинге ВУЗов в соответствии со следующими принципами:

– рейтинговые баллы за работу, выполненную в соавторстве, делятся поровну между соавторами;

– рейтинговые баллы уменьшаются, если публикация не присутствует в электронном каталоге библиотеки ХАИ или общепризнанных наукометических базах;

– количество рейтинговых баллов зависит от языка публикации, присутствия в базе Scopus, SNIP индекса научного журнала, места проведения конференции, присутствия среди соавторов студента ХАИ, объем публикации (в печатных листах) и др.

– каждый вид работы в ИРС ХАИ подтверждается документально;

– рейтинг формируется по категориям НПР и подразделениям (аспирант, молодой преподаватель до 35 лет, ассистент, старший преподаватель, доцент, профессор, заведующий кафедры, кафедра, факультет, докторант, аспирант).

Предлагается для каждого НПР вычислять его индивидуальный рейтинг (*ИР)* и его вклад в рейтинг кафедры (*РК)*, учитывая баллы рейтинга по индивидуальному плану (*И),* остальные баллы рейтинга *Д*, ставку в единицах, на которую оформлен НПР (*С)*. Таким образом, балы вычисляются следующим способом:

– рейтинг штатных НПП, работающих на полную ставку или более:

$$ИР = \min(1548, И/С) + Д,$$
$$РК = \min(1548*С, И) + Д.$$

– рейтинг преподавателей-совместителей (С<1):

$$ИР = \min(1548, И/С) + Д,$$
$$РК = \min(1548*С, И) + Д*С.$$

– рейтинг аспирантов и докторантов:

$$ИР = \max[\ \min(100, И), \min(1548, И/С)\ ] + Д,$$
$$РК= \min(100, И) + Д*(1-С).$$

– рейтинг кафедр: $РКаф = \frac{\sum РК_i}{К}$, где $РК_i$ - рейтинг i-го НПР кафедры, $К$ - число штатных преподавательских единиц на кафедре;

– рейтинг заведующего кафедры вычисляется из личного рейтинга заведующего (*ИРЗ*) с коэффициентом 0,3, и рейтинга кафедры с коэффициентом 0,7:

$$РЗ = 0{,}3 * ИРЗ + 0{,}7 * РКаф.$$

– рейтинг факультета вычисляется как взвешенная сумма рейтингов кафедр

$$РФак = \frac{\sum Р_{Каф\ j} К_j}{\sum К_j}$$

где $Р_{Кафj}$ - рейтинг j-й кафедры, $К_j$ - число штатных преподавательских единиц на j-й кафедре.

Практическая эксплуатация ИРС ХАИ показала ее высокую эффективность и соответствие целям и требованиям, поставленных на начальных этапах ее разработки. Тем не менее существует ряд проблем, которые требуют от руководства выработки технологии мотивации регулярного заполнения и ответственного отношения НПР к ИРС.

Литература

1. Комплексный инновационный подход к оценке деятельности вузов / В.В. Крюков, Р. А. Луговой, Ю. А. Солдатова, В. О. Карпова // Управление эконом. системами: электрон. науч. Журнал, 2015. № 2 (74).

2. Автоматизация рейтинговой оценки деятельности преподавателей /

Е.Н. Архипова, О.В. Кононова, В.В. Крюков, К.И. Шахгельдян // Университетское управление: практика и анализ, 2010. – № 5 – С. 51– 62.

3. Павленко В.Н. Оценивание эффективности труда научно-педагогических работников высших учебных заведений [Текст] / В. Н. Павленко, Н. Н. Пономаренко, М. С. Зряхов // Вісник. Тестування і моніторинг в освіті, 2016. - № 2/3. - С. 25-30.

4. Положение о рейтинге научно-педагогических работников ХАИ [электронный ресурс] - http://rating.khai.edu/docs/rating_khai_polozhenie.pdf

Пядишев В.Г., к.т.н., доцент, с.н.с.,
Одеський державний
університет внутрішніх справ

КІБЕР-ТЕРОРИЗМ: ЙОГО МІСЦЕ У СТРУКТУРІ КІБЕР-ЗЛОЧИННОСТІ ТА КОМПЛЕКСНИЙ ПІДХІД ДО БОРОТЬБИ З НИМ У США

Сьогодні серед інших кібер-злочинів [1], та навіть усіх злочинів, кібер-тероризм уявляється фахівцями, як найбільша загроза суспільству.

Через розвиток комп'ютерних технологій відбувається розвиток кібер-злочинності, яка, як і інші види прибуткових злочинів, має тенденцію до переростання в організовану та, у решті-решт, у транснаціональну. Згадаємо, що кібер-злочинність можна поділити на низку нових злочинів, які принципово не існували без сучасних досягнень у галузі інформаційно-телекомунікаційних систем, та сукупність давно відомих злочинів, які набули нової могутності через застосування останніх досягнень кібер-технологій в якості підтримки.

Особливого розвитку у зазначених умовах здобула сукупність злочинів під назвою "тероризм", яка має вельми непросту структуру, та прояви якої відомі світу з часів прадавньої історії. З одного боку, чисельні злочини з цієї сукупності підсилилися через набуття сучасної інформаційної підтримки, з іншого — виник новий кримінальний феномен — кібер-тероризм, який демонструє можливості свого негативного впливу на всі галузі використання інформаційно-телекомунікаційних технологій у суспільстві, починаючи від приватного листування і до керування підприємствами атомної енергетики.

Паралельно одним з феноменів розвитку сучасної злочинності стало те, що в зонах сучасних, тобто внутрішньодержавних збройних конфліктів, де за природними причинами послаблений правоохоронний контроль, стрімко розвиваються всі види організованої злочинності, включаючи торгівлю зброєю, наркотиками, людьми, людськими органами, природними ресурсами, награбованими витворами мистецтва, тощо.

Нещодавно ситуація погіршилася виходом на світову арену транснаціонального тероризму. Феномен останнього, на нашу думку, характеризують наступні важливіші компоненти: 1) геноцид, як звичайна практика, 2) використання насильницького екстремізму, 3) активне вербування, підготовка і впровадження своїх професіоналів в усі страти суспільства; 4) активне використання, захист і вдосконалення організованої злочинності, 5) своєю діяльністю він пов'язує держави різного рівню розвитку, а саме:

- зони збройних конфліктів, в яких загартовуються кадри терористів;
- розвинені держави, до яких прямують потоки біженців і які є основною ціллю терористів;
- країни проміжного рівню розвитку, в яких терористи здобувають "гарматне м'ясо".

Отже сучасний транснаціональний тероризм, відрізняючись крайньою жорстокістю і нещадністю, з одного боку намагається пов'язати у своїй системі всі країни світу, з іншого — підпорядковує собі, захищає і розвиває всю організовану злочинність. При цьому до його арсеналу потрапляє і кібер-тероризм.

Слід зазначити, що сьогодні через низку причин не створено єдиного універсального, міжнародно узгодженого визначення для поняття тероризм [2, 6], [3]. Безумовно, це не сприяє створенню визначення для поняття ”кібер-тероризм”. Проте він існує як явище, і у зазначених вище умовах саме кібер-тероризм посідає верхній щабель у шкалі небезпеки для суспільства. Саме тому правоохоронна система найбільш розвинутої країни сучасного світу не шкодує сил і засобів для боротьби з кібер-тероризмом. Розглянемо комплексний підхід до боротьби з цим явищем у США, викладений у промові Р. Андерсона, виконуючого обов’язки помічника директора ФБР (Відділ злочинності, реагування та обслуговування) [4].

Держава стикається з кібер-загрозами від проплачених іншими державами хакерів, хакерів за найманням, глобальних кібер-синдикатів і терористів. Вони шукають державні та торгові секрети, технології та ідеї. Вони прагнуть вразити критичну інфраструктуру держави і завдати шкоди економіці. Через масштаби кібер-загрози агентства федерального уряду надають кібербезпеці вищий пріоритет. ФБР та наші партнери в Департаменті внутрішньої безпеки (DHS), Агентства національної безпеки, а також інше. Розвідувальне співтовариство США і правоохоронні органи зробили зусилля загальнодержавного масштабу по боротьбі з кібер-загрозами. У ФБР приділяється головного значення втручанням високого рівня — здійснюваним найбільшими і найнебезпечнішими ботнетами, хакерами, проплаченими іншими державами, і глобальними кібер-синдикатами. Сумісна робота з партнерами спрямована на те, щоб здійснювати не просте реагування на факт, але своєчасне прогнозування і запобігання атакам.

Агенти ФБР, аналітики і комп'ютерні вчені для боротьби з кіберзлочинністю використовують технічні можливості і традиційні методи розслідування, такі як джерела і прослуховування телефонних розмов, спостереження і криміналістичні дослідження. Праця здійснюється сумісно з федеральними, державними і місцевими партнерами з Кібернетичних сил спеціального призначення в кожному з 56 територіальних офісів ФБР і в Національному Кібернетичному Слідчому Об'єднаному Відділі спеціального призначення (NCIJTF). В разі значних кібер-атак, через цілодобовий командний центр кібер-спостереження (CyWatch) об'єднуються ресурси ФБР і NCIJTF, що дозволяє забезпечувати зв'язок з федеральними кібер-центрами, урядовими установами, офісами ФБР на місцях, юридичними аташе, а також з приватним сектором.

Здійснюється обмін інформацією про кібер-загрози з приватним сектором на основі партнерських зв'язків, таких як Рада Альянсу внутрішньої безпеки, ІнфраГард і Спілка Національної кібер-криміналістики та навчанняе (NCFTA). Для наших партнерів в державних і місцевих правоохоронних органах, започатковано Спілку Кібер-Шит на www.leo.gov, яка забезпечує доступ до можливостей кібернетичного навчання та інформації, а також можливість повідомляти ФБР про кібер-інціденти. Юридичні відділення ФБР за кордоном працюють над координацією кібер-розслідувань і усуненням перешкод через юрисдикційні відмінності в законах між країнами. Здійснюється співпраця з новоствореними кібер-центрами злочинності в Інтерпол і Європол. Продовжується оцінювання інших локацій, щоб представники кібер-персоналу знаходилися в найбільш відповідних місцях по всій земній кулі.

Щоб підтримувати успіх в боротьбі з кіберзлочинністю, слід продовжувати набирати, розвивати і утримувати висококваліфікований персонал. З цією метою розроблено низку інноваційних програм з підготовки кадрів і спільних партнерств з приватними підприємствами.

Література

1. Конвенція про кіберзлочинність. Міжнародний документ від 23.11.2001. Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV (2824-15) від 07.09.2005 // ВВР, 2006. – № 5-6. - С.71.

2. Jeffrey Record J. Bounding the Global War on Terrorism / Jeffrey Record. – New York: Oxford University Press,1999. – P. 312.

3. Martyn A. The Right of Self-Defence under International Law-the Response to the Terrorist Attacks of 11 September [Електронний ресурс] / Angus Martyn // Australian Law and Bills Digest Group, Parliament of Australia Web Site, 2002. – February 12. – Режим доступу: http://www.aph.gov.au/About_Parliament/ Parliamentary_Departments/Parliamentary_ Library/ Publications_Archive/CIB/cib0102/02CIB08

4. Anderson R. Jr. Statement Before the Senate Committee on Homeland Security and Governmental Affairs [Електронний ресурс] / Robert Anderson, Jr. // the Federal Bureau of |Investigation, 2014. - September 10. – Режим доступу: https://www.fbi.gov/ news/ testimony/cyber-security-terrorism-and-beyond-addressing-evolving-threats-to-the-homeland

Сахно А.П., начальник відділу ТЗІ,
Жепало А.С., провідний інженер,
Науково-виробничий комплекс газотурбування «Зоря-Машпроект», Миколаїв

ОСОБЛИВОСТІ ПРОВЕДЕННЯ РОБІТ З ВИЯВЛЕННЯ ЗАКЛАДНИХ ПРИСТРОЇВ НА ОБ'ЄКТАХ ІНФОРМАЦІЙНОЇ ДІЯЛЬНОСТІ

Відповідно до положення про захист інформації від витоку технічними каналами на об'єктах інформаційної діяльності та в інформаційно- телекомунікаційних системах (затвердженого 19 червня 2015 р. наказом № 023 Адміністрації ДССЗЗІ України) на об'єктах інформаційної діяльності під час атестації комплексів ТЗІ та при здійснені періодичного інструментально контролю захищеності інформації проводяться роботи з виявлення закладних пристроїв (ЗП). Результатом таких робіт є висновок про відсутність або наявність пристроїв негласного зйому інформації. До того ж результати таких робіт вносяться до паспорту на КТЗІ.

Нормативним документом, що безпосередньо встановлює вимоги до розробки, змісту та оформлення Методик виявлення закладних пристроїв, як документів, що визначають методи (способи) та порядок проведення робіт з виявлення закладних пристроїв є НД ТЗІ 2.7-011-2012. Згідно п. 6.3 цього документу «…Методика за змістом має визначати конкретні способи (методи) та порядок виявлення ЗП, а також містити перелік видів і демаскувальні ознаки ЗП, перелік технічних засобів, приладів та обладнання матеріально-технічного та іншого забезпечення робіт з виявлення ЗП та методики (інструкції) з особливостей застосування цих засобів та приладів при виявленні ЗП, перелік документів, які мають бути оформлені при проведені та за результатами робіт з виявлення ЗП. Методика не повинна містити загальнотеоретичних і довідникових матеріалів щодо ЗП і способів (методів) їх виявлення, а також загальних матеріалів інструкцій з експлуатації технічних засобів і приладів…».

Багаторічний досвід проведення робіт з пошуку ЗП на об'єктах засвідчує, що декілька вимог чинної нормативно-правової бази в сфері технічного захисту інформації, зокрема НД ТЗІ 2.7-011-2012, є надлишковими та по суті не виконуються або виконуються формально. Зокрема, це стосується вимог щодо розробки та погодження Плану проведення робіт з виявлення закладних пристроїв (на конкретному ОІД), у тому числі легенду прикриття робіт з виявлення ЗП. Однак об'єктивно проведення таких робіт проводяться безумовно у випадках, коли є підозра у витоку інформації завдяки встановленим пристроям негласного отримання інформації або виключені всі інші, та саме такий канал є найбільш вірогідним. Зрозуміло, що проведення підготовчого етапу (який зокрема повинен включати

обстеження ОІД, визначення заходів та способів з активації ЗП і вимог до тестових сигналів, вибір технічних засобів, розробку плану проведення робіт, розробку легенди прикриття і т.д) є щонайменше надлишковим. При цьому необхідно зазначити, що все це має відображатися у документі «План проведення робіт з виявлення закладних пристроїв» та бути погодженим з відповідальною за ТЗІ особою організації замовника, керівником організації виконавця, затвердженим керівником організації замовника та підписаний співробітниками, що безпосередньо будуть здійснювати відповідні роботи. До того ж цей документ повинен бути відповідним чином прийнятий та зареєстрований, тобто пройти ще ряд осіб, які відповідно до специфіки робіт не можуть бути ознайомлені із зазначеними матеріалами. Всі ці встановлені нормативними документами необхідні вимоги, навіть за умови легендування, повністю дискредитують скритність, неупередженість, та реальність кінцевого результатвву робіт з виявлення ЗП або місць можливого встановлення (як у минулому, так і в майбутньому).

Найскладнішим випадком при проведені зазначених робіт є обстеження на ОІД, при якому доступ до суміжних приміщень є обмеженим або неможливим. При цьому пошукова група має не тільки керуватися легендою щодо доступу до ОІД, але й скритністю робіт відповідно до суміжних приміщень, обмежуючи при цьому свою роботу у виборі тестових сигналів та методах пошуку. Звісно, що про проведення підготовчого етапу в таких випадках не може й мови, а про розробку, погодження та затвердження Плану проведення робіт й говорити не доводиться. Тому був розроблений інноваційний метод проведення пошукових робіт із використанням фізичних властивостей щодо теплоємності жорстких конструкцій та нерівномірного розподілу надлишкової теплової енергії.

Суть методу полягає в наступному:

Всі об’єкти на ОІД мають температуру, що співвідносна із температурою навколишнього середовища або навколишнього простору, із рівномірно розподіленим градієнтом збільшення або зменшення температури від засобів випромінення теплової енергії (батареї, працююча техніка, засоби, що за своїм прямим призначенням мають бути із температурою, більшою за оточуючу). При цьому це є замкнутий простір із своєю картою температурного спектру. Тому при обстеженні жорстких конструкцій та предметів інтер’єру виявити змонтований закладний пристрій або місце його встановлення майже неможливо. Однак, при швидкій зміні температури на об’єкті (локально зосереджено або в цілому на об’єкті), можливо встановити неоднорідності та пустоти, що спричинені більш швидкою або, навпаки, більш повільною зміною температури. Це обумовлено тим, що будь-який пристрій або місце для нього повинно мати простір для розміщення та заповнюється повітрям або із-зовні (сусіднього приміщення), або внутрішнім (самого ОІД), або суміші (коли наприклад отвір наскрізний). В будь-якому випадку при різниці температури, яка змінюється у часі, значення градієнта температури буде відчутне для пристроїв пошукової групи. До таких пристроїв звісно відносяться тепловізори різних типів, такі, наприклад, як Fliri3, при цьому достатньо термочутливості $< 0.15°$ C.

При цьому обов’язковою вимогою є проведення робіт безпосередньо під час максимальної швидкості зміни градієнта, тобто коли температурна різниця між повітрям всередині ОІД та навколишніми предметами є максимальною. Звісно, цей метод працює як із підвищенням температури, так і з її зниженням, та на практиці найбільш сприятливе для пошукової групи є саме збільшення температури. Це можливо досягти побутовими пристроями, особливо якщо це безшумні – такі, наприклад, як інфрачервоні лампи UFO. Безумовною перевагою саме інфрачервоних нагрівачів є мобільність, компактність, простота у використанні, швидкість нагріву та прогрів на достатню для визначення товщину матеріала.

Використання запропонованого методу із використанням зниження температури обумовлено використанням лише системи охолодження самого приміщення та можливе лише для системи кондиціонування.

Метод температурного градієнта є складовим в пошукових роботах, однак вирізняється своєю візуальністю для оператора, безшумністю, може бути використаний як для елементів інтер'єру, так і для огороджувальних конструкцій, хоча і має ряд недоліків: необхідність у додатковому обладнанні, енерговитратний, некомфортний для пошукової групи (особливо в літній період).

Стайкуца С.В., к.ф.н., доц.,
Семенов О.С.,
ОНАЗ ім. О.С.Попова, Одеса

АНАЛІЗ ЗАГРОЗ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНИХ КОМПАНІЙ З РОЗРОБКОЮ МЕТОДОЛОГІЇ ЗАХИСТУ

Телекомунікаційна мережа (Telecommunication Network) – це системоутворювальна сукупність засобів телекомунікацій, що надає територіально рознесеним об'єктам можливість інформаційної взаємодії шляхом обміну сигналами [1]. Це основа діяльності будь-якої компанії, яка надає свої послуги в сфері телекомунікацій. Саме на основі мережі оператор надає комплекс послуг для своїх абонентів. Працездатність телекомунікаційної мережі в сукупності з її елементами - запорука успішної роботи всієї компанії, її репутація та перспективи роботи на ринку телекомунікацій в умовах жорсткої конкуренції. Адже, навіть у разі виходу з ладу всього однієї базової станції без сервісу можуть залишитися сотні абонентів, не кажучи про випадки, коли пошкоджується магістральний волоконно-оптичний кабель або апаратно-програмні частини ЦАТС. Саме з цієї причини застосування оптимальних методів захисту компонентів телекомунікаційних мереж - важлива і актуальна задача. Незважаючи на велику кількість об'єктів телекомунікаційної компанії, глобально їх можна розподілити на такі групи:

1. Інформаційна мережа телекомунікаційної компанії;
2. Будівлі та споруди телекомунікаційної компанії (приміщення інфраструктури);
3. Інфраструктура телекомунікаційної компанії;
4. Офісні будівлі;
5. Персонал

Розглянемо більш докладно загрози, які можуть бути спрямовані на ті чи інші компоненти телекомунікаційної компанії. Отже, потенційні загрози щодо безпеки телекомунікаційних мереж можуть включати відмову в обслуговуванні, аналіз трафіку, крадіжку послуг, непривілейований доступ, а також, з більш масштабного погляду, загальне порушення цілісності та конфіденційності інформації. Перелік загроз неодноразово наводився у численних публікаціях, але він продовжує постійно змінюватись та уточнюватись. Загальний перелік загроз телекомунікацій наведено в міжнародній рекомендації *ITU-T* E.408 [2].

Загрози можуть буди направлені на елементи інфраструктури телекомунікаційної мережі, а саме – на приміщення та будівлі. За класом приміщення можуть бути як з персоналом, так без нього. До основних класів приміщень інфраструктури телекомунікаційних компаній можна віднести:

- Центри моніторингу та реагування на інциденти;
- Приміщення ЦАТС та ЦОД;
- Приміщення електричних підстанцій та генераторних;
- Територіальні пости охорони;
- Інші технічні приміщення в будівлях та спорудах.

Кількісний та якісний склад будівель і споруд може змінюватися, виходячи з поставлених при проектуванні телекомунікаційної мережі завдань.

Інженерна інфраструктура, інженерні мережі, системи або комунікації - комплекс систем і комунікацій, що забезпечують нормальну життєдіяльність споживачів. До складу інженерної інфраструктури можуть включатися:

– зовнішні системи електропостачання (лінії електропередачі, трансформаторні і тягові підстанції і т. д.);

– внутрішні системи електропостачання (будинкові мережі з напругою до 380 В);

– системи вентиляції та кондиціонування повітря (житлових та громадських будівель і споруд та об'єктів інженерного забезпечення);

– технічні системи охорони.

Деструктивні дії зловмисника можуть бути направлені на зовнішні та внутрішні інженерні мережі з метою виведення з ладу останніх. Гірше, коли завданням порушника стає не фізична лінія зв’язку, а інформація, яка нею передається. В такому разі потенційний порушник має можливість отримувати інформацію фактично без створення самого інциденту (наприклад, в системах інженерного забезпечення та ТЗО). Велику шкоду компанії може нанести внутрішній порушник або ”інсайдер”, а саме, особа, що має в силу свого службового становища доступ до конфіденційної інформації. Небезпека інсайдерської загрози полягає в тому, що співробітник підприємства, на відміну від зовнішнього порушника, володіє ланкою характеристик [3].

На рис. 1 представлено гіпотетичну модель загроз телекомунікаційної мережі для компанії, що надає послуги в даній сфері. Представлена модель загроз, звичайно, не відображає всі загрози, які спрямовані на мережу. Проте, при цьому зображено основні загрози. Детальний опис загроз наведений в табл.1.

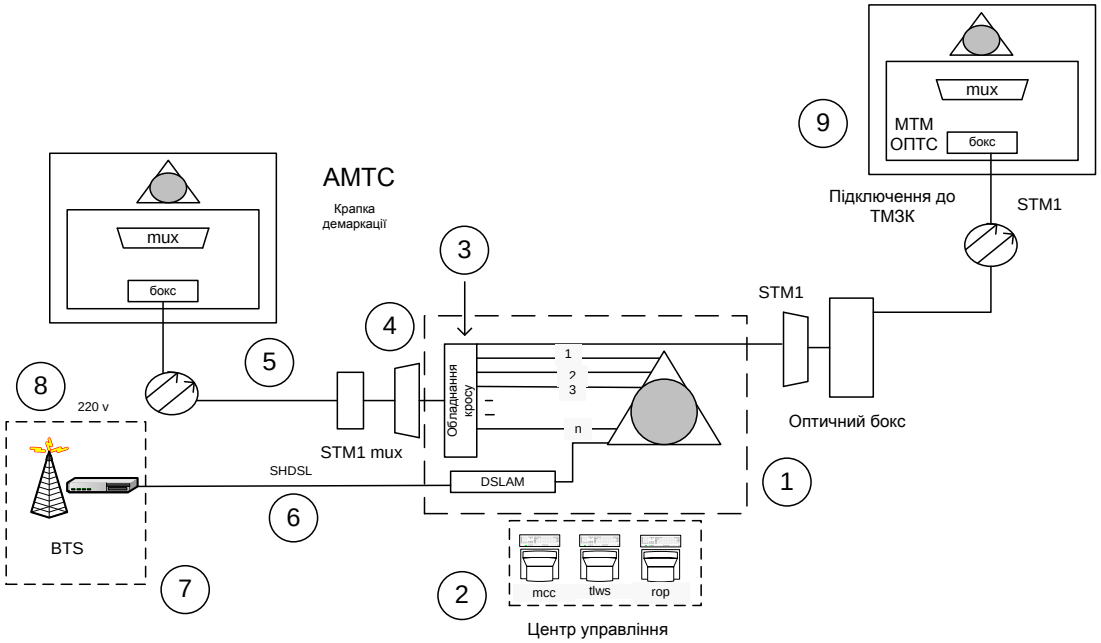

Рисунок 1 ─ Модель загроз мережі телекомунікаційної компанії.

Таблиця 1 - Основні загрози телекомунікаційної мережі

	Загроза
	Загроза, направлена на середовище ЦАТС або ЦОД
	Загроза, направлена на блокування або перехват управління телекомунікаційною мережею
	Загрози, направлені на пошкодження обладнання кросу. Несанкціонована перекомутація ліній зв’язку
	Атаки, направлені на обладнання транспортних мереж телекомунікаційної

	компанії (мультиплексор)
	Несанкціонований доступ до волоконно-оптичних ліній зв’язку
	Порушення цілісності ліній та обладнання при організації DSL-доступу
	Загроза, направлена на порушення синхронізації базової станції мережі
	Деструктивні дії, направлені на дестабілізацію енергоживлення мережі та її компонентів
	Загрози НСД в крапках демаркації мереж

Звичайно, що телекомунікаційна компанія - це не тільки телекомунікаційна мережа, хоча остання і виступає основним ядром. Але для роботи компанії необхідні офіси для роботи відділів компанії, центри обслуговування абонентів, робота з віддаленими представництвами і т.д. Відповідно, на дані елементи телекомунікаційної компанії також поширюються загрози безпеки.

Наприклад, приміщення ЦАТС, ЦОД, ЦОА та офісів потрібно обладнати технічними засобами охорони. При цьому застосовуються як традиційні засоби, так і інтегровані рішення [4], а також як системні, так і позасистемні методи та засоби захисту [5]. Автоматизовані робочі місця та мережеве обладнання (загалом - корпоративна мережа) необхідно захищати від внутрішніх і зовнішніх порушників [6]. Всі ці питання вирішуються при комплексному підході до формування політики безпеки компанії. Отже, при проведенні оцінки усіх ризиків на мережі телекомунікаційної компанії необхідно провести чималий обсяг роботи, а саме, уважно вивчити схему організації зв'язку, виявити всі слабкі місця, опрацювати документальну базу, провести роботу з персоналом. Одним словом, для виявлення всіх ризиків і загроз необхідно, першочергово, провести аналіз ризиків інформаційної безпеки. Зрозуміло, що СЗІ, яка буде створюватися на підприємстві, повинна буди економічно доцільною. Тому при проведенні аналізу ризиків необхідно пройти ланку етапів від інвентаризації інформаційних ресурсів компанії до визначення прийнятних рівнів ризику та побудови системи управління ризиками.

Для виявлення ризиків в рамках телекомунікаційної компанії можливе використання наступних інструментів:

- SWOT – аналіз;
- Аналіз документації;
- Мозковий штурм;
- Метод Делфі;
- Інтерв'ю;
- Причинно-наслідкові діаграми.

Для полегшення проведення аналізу інформаційних ризиків існують автоматизовані засоби аналізу та управління інформаційними ризиками - CRAMM (Central Computer and Telecommunications Agency, Великобританія), Risk Watch (Risk Watch, США), Digital Security Office (Digital Security, Росія). Вказані програмні продукти дозволяють змоделювати інформаційну систему компанії і розрахувати інформаційні ризики. Крім того, вони генерують звіт, що містить рекомендації щодо зниження рівня ризику відповідно до особливостей інформаційної системи.

Отже, наведемо основні підсистеми захисту інформації [7], які направлені на блокування чи попередження інформаційних загроз телекомунікаційних компаній (табл. 2).

Таблиця 2 – Основні підсистеми ЗІ телекомунікаційної компанії

№	Підсистема	Можливі елементи підсистеми
1	Організаційна	– Захист комерційної та конфіденційної інформації підприємства; – Захист від шахрайства;

		– Супровід персоналу з моменту влаштування на роботу до звільнення; – Оптимізація роботи служби безпеки підприємства; – Формування моделі загроз; – Організація повного циклу документообігу; – Застосування методові та засобів конкурентної розвідки; – Розробка інструкцій, рекомендацій, проведення навчання.
2	Технічного захисту інформації	– Перевірка приміщень на наявність закладних пристроїв; – Захист від комерційного шпигунства; – Захист переговорів; – Захист телефонних мереж; – Побудова "захищеної переговорної кімнати".
3	Технічних засобів охорони та систем комплексного моніторингу	– Автоматична система пожежної сигналізації, система автоматичного пожежогасіння та сповіщення про пожежу; – Система відеоспостереження; – Система охоронно-тривожної сигналізації; – Система контролю і управління доступом; – Система охорони периметру. – Система комплексного моніторингу показників.
4	Захисту корпоративних мереж	– Розмежування доступу до ресурсів системи; – Захист автоматизованих робочих місць; – Налаштування і конфігурація серверу; – Впровадження VPN, RDP, технологію "тонких клієнтів"; – Застосування DLP-систем; – Розробка правил та норм корпоративної комп'ютерної етики; – Впровадження систем резервування інформації.

Приведені підсистеми можуть стати основою методології захисту телекомунікаційних компаній та забезпечити прийнятні рівні ризиків на всі свої компоненти.

Література

1 Довгий С.О., Воробієнко П.П., Гуляєв К.Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / За загальною редакцією члена-кореспондента НАН України С.О. Довгого / Київ: “Азимут-Україна”, 2013. – 607 с.

2 Рекомендація ITU-T E.408 Telecommunication networks security requirements

3 Журин С.И. Инсайдер: основная характеристика и комплексность противодействия. Безопасность информационных технологий, 2011. - №4. - С.176-183.

4 Дворський М.Н., Палатченко С.Н. – Технічна безпека об’єктів підприємництва, 1 том, К.: “А-ДЕПТ”, 2006. – 304 с. (“ Концепція безпеки ”).

5 Кононович В.Г., Стайкуца С.В., Лемеха Т.М., Копитін Ю.В. // Інформаційна безпека цифрових програмно-керованих АТС // Навчальний посібник для студентів вищих навчальних закладів. – Одеса: ОНАЗ ім. О.С. Попова, 2013. – 242 с.

6 Richard Kissel, Hyunjeong Moon DRAFT NISTIR 7621 Rev.1 Small Business Information Security: The Fundamentals, 2014.

7 Стайкуца С.В., Плотна О.М. // Дослідження методів та рішень при впровадженні системи захисту інформації на прикладі медичної установи // Матеріали третьої міжнародної наукова-практичної конференції молодих вчених “Інфокомунікації – сучасність та майбутнє”. - Одеса: ОНАЗ ім. О.С.Попова, 20-23 жовтня 2013. – 557 с.

Ткач Ю.М., к.п.н., доцент,
Чернігівський національний технологічний університет,
Казмирчук С.В., к.т.н., доцент,
Національний авіаційний університет, Київ

ЗАСТОСУВАННЯ СТАТИСТИЧНОГО ІНСТРУМЕНТАРІЮ У ПРОЦЕСІ ОЦІНЮВАННЯ ІНФОРМАЦІЙНИХ РИЗИКІВ

Проблема оцінювання інформаційних ризиків в умовах невизначеності або настання несприятливих подій, що призводять до значних втрат, займає одне з ключових місць у сучасній системі захисту інформаційних ресурсів.

Оцінювання ризиків являє собою процес систематичного контролю та оцінки ефективності діяльності установи. Крім того, цей процес спрямований на запобігання та згладжування ризиків [2].

Для оцінювання інформаційних ризиків використовуються різноманітні методи, методики та методології. Зокрема, статистичний та аналітичний методи та метод експертних оцінок.

Зазначимо, що статистичний та аналітичний метод можна використовувати у випадку наявності досить великої кількості даних про результати діяльності установи, для якої здійснюється аналіз.

У зв'язку із недостатністю достовірної статичної інформації або взагалі її відсутністю щодо загроз інформаційній безпеці найбільш поширеним методом оцінювання інформаційних ризиків є метод експертних оцінок.

Метод експертних оцінок – це евристичний метод, який застосовується у випадках, коли ускладнено знаходження розв'язку математичними методами.

Суть цього методу полягає у оцінюванні ризику на основі суб'єктивних думок експертів-фахівців у конкретній галузі діяльності. Метод експертних оцінок полягає в тому, що команда проекту виділяє певну групу ризиків і розглядає, яким чином вони впливають на діяльність підприємства. Цей розгляд зводиться до подачі бальних оцінок за ймовірність виникнення того чи іншого виду ризику, а також ступеня його впливу на діяльність проекту [1].

Процес оцінювання ризиків передбачає визначення об'єкта дослідження. Представимо схематично послідовність дій згідно з методом експертних оцінок (рис.1).

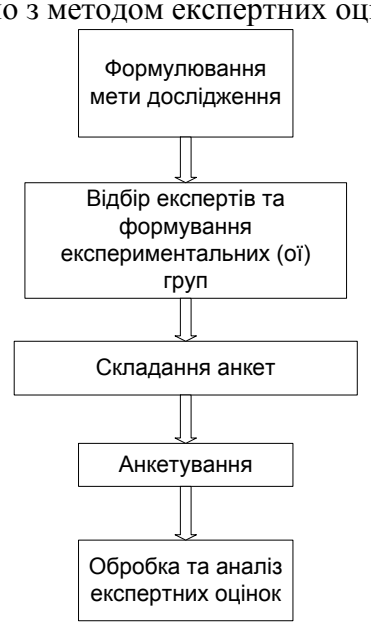

Рис. 1. Схема методу експертних оцінок

Зупинимось на обробці та аналізі експертних оцінок.

Зауважимо, що мінімальну кількість експертів ми визначили на основі статистичного підходу. Для цього використали загальноприйняту формулу для визначення мінімального обсягу вибірки:

$$N = \frac{t_\alpha^2 \cdot \sigma^2}{\square^2},$$

де t_α - довірче число, що залежить від ймовірності результату оцінювання, σ - дисперсія, $\square$ - відносна гранична похибка.

Тоді для рівня значущості $\alpha = 0,05$ критерій $t_\alpha = 1,96$. Зауважимо, що це значення критерію t_α для невеликої вибірки, а саме до 30 одиниць.

Дисперсію визначимо як добуток $p \cdot q$, де p - доля одиниць, що володіють певною ознакою, а q - доля одиниць, що не володіють певною ознакою.

В умовах відсутності інформації про значення p та q приймаємо їх рівними 0,5. Оскільки цей показник відповідає найбільшій можливій варіації сукупності.

Для оцінки відносної граничної похибки нами було використано статистичне правило, що похибка не повинна перевищувати 5%.

Під час виставлення балів експертами можуть бути використані різні шкали, наприклад, п'ятибальна шкала Лайкерта (1-абсолютно неймовірно, 2-неймовірно, 3-не визначився, 4–ймовірна, 5-дуже ймовірна) або семибальний семантичний диференціал, або десятибальна шкала Степела (1-5 – ймовірність настання ризику незначна, 6-10 – найбільш ймовірний ризик).

Отже, мінімальна кількість експертів в групі за умови використання десятибальної шкали оцінювання має становити 4 людини, за умови обрання семибальної шкали мінімальна кількість експертів мала б становити 8 осіб, а для п'ятибальної – 16.

Сукупність відповідей експертів необхідно дослідити на нерівномірність.

Це можна зробити за допомогою таких статистичних показників:

1) середнє ($\bar{x}$) – покаже зведену (інтегровану) оцінку опитаних експертів,
2) стандартне відхилення (σ) – покаже зведене відхилення думки експертів від середніх значень (при цьому дане відхилення має бути в межах $\bar{x} \pm 3\sigma$),
3) коефіцієнт варіації ($V = \frac{\sigma}{M}$) – охарактеризує співвідношення середньоквадратичного відхилення та математичного сподівання (середнього), що покаже міру ризику притаманного досліджуваному явищу.

Щодо думок експертів, то зауважимо, що показник варіації засвідчить:

- 0-33% - сукупність однорідна, середня є типовою, варіація незначна,
- 34-66% - сукупність однорідна, середня є типовою, варіація значна,
- 67-100% - сукупність неоднорідна, середня не є типовою, варіація висока.

Отже, якщо за високого або значного рівня варіативності за однією з груп досліджуваних ризиків спостерігається значна варіація, то це вказує на неспівставність відповідей експертів по заданому питанню і потребує вирішення у двох напрямах:

1) вилучення одиниць, що деформують сукупність (усунути одного з експертів, чиї відповіді найбільш неузгоджені із відповідями інших),
2) вилучення досліджуваних факторів із переліку питань (вилучення певного ризику з переліку або проведення додаткового дослідження із такими ризиками, але за участі інших експертів, оскільки у даному питанні сформована група експертів може виявитись некомпетентною).

У випадку незначної варіації, як у наведеній нами ситуації, можна говорити про співставність думок експертів щодо досліджуваного процесу.

Наступним етапом аналізу результатів оцінювання інформаційних ризиків має стати визначення міри узгодженості думок експертів.

Оскільки кількість ранжованих ознак (експертів) більша двох, то для оцінки міри узгодженості думок експертів використаємо коефіцієнт конкордації:

$$W = \frac{12\sum_{j=1}^{n} d_j^2}{m^2(n^3 - n)},$$

де n - кількість факторів; m - кількість експертів; d_j - відхилення суми від середньої суми. При цьому

$$d_j = S_j - \frac{\sum_{j=1}^{n} S_j}{n},$$

де S_j - сума рангів.

Коефіцієнт конкордації змінюється в межах від 0 до 1. Чим ближче коефіцієнт до одиниці, тим більший ступінь узгодженості думок експертів, і навпаки. У випадку, коли коефіцієнт конкордації дорівнює одиниці, то це означає, що всі експерти надали однакові ранги ризикам, якщо він дорівнює 0, то думки експертів не узгоджені. Зазвичай вважається, що думки експертів узгоджені, якщо $W \geq 0{,}7$.

Разом з тим, розрахований коефіцієнт конкордації треба перевірити на статистичну значущість. Якщо кількість можливих ризиків, що пропонуються для оцінки експертам, більша за сім, то перевірити статистичну значущість коефіцієнта конкордації можна за допомогою критерію Пірсона ($\chi^2_{розрах}$), а якщо їх кількість менша семи, то за допомогою F - розподілу.

Після встановлення узгодженості думок експертів та її статистичної значущості варто визначити, у якій мірі кожний експерт впливає на узгодженість думок. Для цього потрібно послідовно, одного за одним, виключати з розрахунку експертів та обчислювати коефіцієнт конкордації, а також встановлювати його статистичну значущість. Це дасть можливість визначити експерта, який надавав найбільш неординарні відповіді. Але це не є приводом для його вилучення з експертної групи.

Також, отримані за допомогою методу експертних оцінок результати можна використати для кількісного оцінювання зон ризику установи, що характеризують певний рівень можливих втрат. За міру ризику можна прийняти показник стандартного відхилення (σ). Загальноприйнято вважати, що прийнятним є ризик до 0,125, витратам у розмірі половини чистого прибутку відповідає коефіцієнт ризику від 0,125 до 0,25, у випадку, якщо ризик становить 0,25 і більше, то це свідчить про втрату усього чистого прибутку підприємства.

Отже, метод експертних оцінок є дуже поширеним методом оцінювання інформаційного ризику. Результати опитувань експертів мають бути проаналізовані за допомогою різноманітного статистичного інструментарію. Обираючи інструментарій під час застосування методу експертних оцінок для оцінювання інформаційних ризиків, треба враховувати різні фактори, а саме: мету дослідження, шкалу вимірювання відповідей експертів, кількість ризиків тощо.

Запропонований нами перелік статистичного інструментарію для оцінювання інформаційних ризиків не є вичерпним і може бути змінений або доповнений.

Список використаних джерел

1. Проектні ризики та методи їх зменшення [Електр. ресурс]. – Режим доступу: www.info-works.com.ua/referats/finansi/5.html

2. Ткач Ю.М. Побудова нечітких когнітивних карт для оцінки інформаційних ризиків вищого навчального закладу / Ю.М.Ткач // Вісник Чернігівського державного технологічного університету. Серія «Технічні науки»: науковий збірник / Чернігів. нац. технол. ун-т. – Чернігів : ЧНТУ, 2014. - №2 (73). – С.149-153.

Толюпа С.В., д.т.н., професор,
Розум'як М.В.,
Національний університет імені Т.Г. Шевченка, Київ

ЗАХИСТ ВІД НЕСАНКЦІОНОВАНОГО ДОСТУПУ В МЕРЕЖЕВУ ІНФРАСТРУКТУРУ

Архітектура системи обробки даних і технологія її функціонування дозволяє зловмисникам знаходити або спеціально створювати лазівки для прихованого доступу до інформації. Таких лазівок існує або може бути створено багато. Тому протидія таким загрозам є і буде актуальною. Метою данного дослідження є розгляд можливостей попередження несанкціонованого доступу та використання апаратно-програмних можливостей захисту та безпеки мережевої інфраструктури *Cisco*.

З розвитком інформаційних технологій збільшується різноманіття пристроїв і засобів зберігання, обробки та передачі інформації, хмарних технологій та Інтернет мереж. Слабким місцем стає будь-який елемент, що підключений до мережі організації як в апаратній, так і в програмній частинах. Відповідно причинами несанкціонованого доступу до інформації та корпоративної мережі можуть бути такі фактори, як: необережність чи неграмотність співробітників, навмисна крадіжка інформації як своїми співробітниками, так і зловмисниками.

Багато організацій досі будують свою систему захисту спираючись на застарілий периметровий підхід, зосереджуючи всі засоби безпеки в кількох контрольних точках мережі, повністю забуваючи про наявність обхідних каналів – *WiFi, USB flash* носіїв інформації, 3*G, ActiveSync*. Необхідно також не забувати і про внутрішнього порушника, який може виконувати свою ”чорну справу”, не боячись бути виявленим периметровими засобами захисту. Можна виділити три варіанти вирішення проблеми [1]:

Перший – побудувати у внутрішній мережі ще одну, створену із міркувань засобів безпеки. Багато виробників засобів захисту надають пропозиції для даного варіанту, включаючи в нього багато *IPS* сенсорів та мережевих екранів, які будуть контролювати внутрішні мережеві потоки та виявляти шкідливий код та заборонені додатки.

Другий часто рекомендований варіант – встановлення засобів захисту на сервери та робочі станції, виявляючи та блокуючи несанкціоновану активність користувачів чи проти користувачів.

Третій варіант – перенести рішення на те у що вже інвестовано кошти, а саме на мережеву інфраструктуру. Маршрутизатори, комутатори та точки доступу, які можуть не лише передавати трафік з точки А в точку Б, але й ефективно захищати цей трафік, виконуючи одночасно роль сенсору, захисної стіни та інструменту реагування на інциденти безпеки.

Власне всі ці можливості надає *Cisco* в своїй мережевій інфраструктурі, виступаючи не лише як сенсор системи захисту, але і як система захисту і система розслідування інцидентів інформаційної безпеки. Мережева інфраструктура в ролі “Мережа як сенсор” дозволяє проактивно виявляти загрози по наступних категоріях: пристрої; трафік; додатки; користувачі; зловмисне програмне забезпечення. Це можна використовувати як інструмент

інвентаризації та в рамках політик. За рахунок вбудованого в безпровідну інфраструктуру функціоналу, можна на фізичній карті будови відмічати з точністю до 1-2-х метрів місце положення несанкціонованих точок доступу, несанкціонованих безпровідних клієнтів і при необхідності їх подавляти. Можна відповідні дії додатків дозволяти чи забороняти в визначений час чи для визначених облікових записів користувачів в певних напрямках з певних вузлів, тобто використовувати будь-які комбінації в політиках безпеки. За рахунок доступу до мережевого трафіку можна створювати білі та чорні списки того, що можна робити в мережі. Ще один елемент мережевої інфраструктури *NetFlow* – з самого початку призначався для визначення проблем в мережі [2]. За рахунок того що *NetFlow* являється потужним джерелом інформації для кожного мережевого з'єднання, ми можем його використовувати для ідентифікації атак, зломів, витоків даних, тощо [3].

Виявлення зловмисності робиться на платформі коду *Advanced Malware Protection,* яка включає в себе емуляцію атак, пісочницю а також: репутаційний аналіз (ідентична сигнатура; нечіткі ідентифікуючі мітки; машинне навчання); поведінковий аналіз (ознаки компрометації; динамічний аналіз; розширена аналітика; співставлення потоків пристроїв). На маршрутизатори, сервери, міжмережеві екрани, *IPS, WSA/ESA*, персональні комп'ютери, мобільні пристрої можуть встановлюватися засоби платформи AMP. Підхід базується на виділенні і правильному описанні "Що значить нормально", а будь-які відхилення від "нормально" сприймаються як аномалії з послідуючим реагуванням, блокуванням, розміщенням в карантин чи іншими діями. «*Мережа як захисна стіна»* надає наступні можливості [4]: сегментувати мережу для локалізації атак; шифрувати трафік для захисту даних в процесі передачі; захистити філіали при прямому доступі в Інтернет. *«Мережа як інструмент реагування»* може: зменшити час відновлення і прискорити реагування; автоматизувати налаштування і динамічно його змінювати, виходячи з ситуації в мережі; інтегрувати з іншими рішеннями для захисту інвестицій і росту якості захисту. Для покращення реагування потрібно автоматизувати багато функцій. Для цього також розроблено *APIC Enterprise Module.* Він дозволяє автоматизувати *ACL* : виявлення дублікатів політик; виявлення конфліктів політик; оцінка відповідності політик; автоматизація *ACLs* для мобільності. Відслідковування руху шкідливого ПО і зловмисника по мережі дозволяє робити вбудована система кореляції подій *FireSIGHT* , яка збирає дані щодо: *події виявлення зловмисників: події аналізу ІБ:* які системи були інфіковані?; хто був інфікований?; коли це відбулось?; який процес був відправною точкою?; чому це трапилось?; що ще трапилось? Таким чином, на основі проведеного аналізу, виділено 5 принципів для побудови справжньої захищеної мережі: увімкнення NetFlow (виділення ознак нормального функціонування мережі); впровадження TrustSec / сегментації (локалізація атак, надання ролевого керування, що не залежить від топології чи типу доступу); шифрування трафіку і увімкнення *CISF*; впровадження *Intelligent WAN* (захист філіалів, додаткових офісів, тощо); впровадження APIC-EM (прискорення конфігурування і усунення проблем). Користуючись наявною інфраструктурою мережі можна перетворити її в систему захисту, яка виступатиме в наступних ролях – сенсора, захисної стіни, інструменту реагування.

Список використаних джерел

1. 2012 DATA BREACH INVESTIGATIONS REPORT [Електронний ресурс] // - Режим доступу: http://www.verizonenterprise.com/ - (25.03.2016).

2. Jesse Russell, Ronald Cohn. Netflow. - P. 75-81.

3. Introduction to Cisco IOS NetFlow. - A Technical Overview. - P. 101-110.

4. Казаков Д.С. Управление доступом в архитектуре Cisco TrustSec [Електронний ресурс] // - Режим доступу: http://gblogs.cisco.com/ - (29.03.2016).

Хохлачева Ю.Е., к.т.н.,
Скворцов С.А., к.т.н., доцент,
Национальный авиационный университет, Киев

ОСОБЕННОСТИ ОЦЕНКИ БЕЗОПАСНОСТИ ИНФОРМАЦИОННЫХ СИСТЕМ

Темпы развития современных информационных технологий значительно опережают темпы разработки рекомендаций и нормативно-правовой базы руководящих документов в Украине. Поэтому проблемы оценки уровня безопасности информационной системы обязательно приводят к возникновению следующих вопросов: согласно каким критериям проводить оценку эффективности защиты, как оценивать и переоценивать информационные риски? В результате, дополнительно к требованиям рекомендаций и нормативно-правовых документов, приходится адаптировать к нашим условиям и применять методики международных стандартов, а также использовать методы количественного анализа рисков в совокупности с оценками экономической эффективности обеспечения безопасности и защиты информации [1].

Сегодня современные методы работы по анализу рисков информационной безопасности, проектирования и сопровождения систем безопасности должны позволять:

- выполнить количественную оценку текущего уровня безопасности, задать допустимые уровни рисков, разработать план мероприятий по обеспечению необходимого уровня безопасности на организационно-управленческом и техническом уровнях с использованием современных методик и средств;
- рассчитать и экономически обосновать размер необходимых вложений в обеспечение безопасности на основе технологий анализа рисков, соотнести расходы на обеспечение безопасности с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередные блокировки наиболее опасных уязвимостей к осуществлению атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц по обеспечению информационной безопасности, создать необходимый пакет организационно-распорядительной документации;
- обеспечить поддержку внедренного комплекса защиты в соответствии с условиями работы объекта, изменяющимся регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модификацией технических средств защиты.

Исходя из уровня воплощения информационных технологий современности и рассматривая информацию как объект деятельности, следует отметить, что в зависимости от ее важности и значения для пользования им тратятся соответствующие ресурсы. Но важность и значение информации для тех и других субъектов информационных отношений в условиях коммерческого, ведомственного и государственного интереса определить сложно. Поэтому понятно, что удовлетворение информационных потребностей находится в пропорциональной зависимости от условий и методов (средств) практической деятельности соответствующих субъектов, а высокий уровень автоматизации, к которому стремится человечество, ставит его в зависимость от уровня безопасности информационных технологий, используемых ими. В связи с этим информационные ресурсы требуют разграничения доступа, в соответствии с этим информацию по рангу доступа и правовым режимом [2].

Современные информационные технологии сублимируют в себе качества всех форм, различные текущие формы могут трансформироваться между собой.

Условно, все трансформации данных в ИС определены как трансформации информационных потоков, модификация которых вызывает вопросы нарушения целостности и достоверности данных.

Главной целью любой системы информационной безопасности является обеспечение устойчивого функционирования объекта, предотвращение угроз его безопасности, защита законных интересов пользователя ИС от противоправных посягательств, недопущение хищения финансовых средств, разглашения, утраты, утечки, искажения и уничтожения информации, обеспечения нормальной производственной деятельности всех подразделений объекта. Другой целью системы информационной безопасности является повышение качества предоставляемых услуг и гарантий безопасности прав и интересов клиентов. Достижения заданных целей возможно в ходе решения следующих основных задач:

- отнесения информации к категории ограниченного доступа (служебной тайны);
- прогнозирование и своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению материального и морального ущерба, нарушению этого нормального функционирования и развития;
- создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба;
- создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное прекращение посягательств на ресурсы на основе правовых, организационных и технических мер и средств обеспечения безопасности;
- создание условий для максимально возможного возмещения и локализации ущерба, который может быть нанесен неправомерными действиями физических и юридических лиц, ослабление негативного влияния последствий нарушения безопасности ИС на достижение стратегических целей.

Ориентируясь на защиту ведомственных, коммерческих, государственных интересов следует заметить, что на всех этапах трансформации информации тратится данный промежуток времени, то есть информация имеет свой жизненный цикл.

Жизненный цикл информации на объекте зависит от оценки ее ценности, а также соответственно от способности санкционированных пользователей обеспечить ее надежную защиту, и, таким образом, не допустить "обесценивание" информации. Он предусматривает, что информация добывается, обрабатывается (анализируется), сохраняется, охраняется, используется, транслируется, разворовывается и уничтожается. Поэтому рассмотрим этапы жизненного цикла информации с позиции целевого признака ИС подробно, чтобы отделить уязвимые звенья трансформации, которые требуют рассмотрения (защиты). Подчеркнем, что процесс модификации информации охватывает все этапы жизненного цикла. Под термином "модификация" будем понимать любое изменение прежнего содержания исключительно этапа создания объекта.

Процессы создания и уничтожения информации, то есть отражение или стирание на некотором материальном носителе, бумаге, или электронной копии накопленных данных с учетом определенных задач к разработке документов осуществляются авторизованными пользователями. После создания документа производиться его оценка на предмет соответствия абстрактным и конкретным требованиям для последующего направления и использования в определенных и разрешенных пределах. Процесс хранения включает как разработку порядка и правил подготовки к хранению, так и само хранение информации на различных носителях с последующей технологией (ограничения) доступа. Выборка объекта и последующая оценка выбора обусловлены конкретностью поставленной задачи. Критичность по отношению к данным наступает с момента выборки и дальнейшей их обработки.

Обработка и использование информационного объекта субъектами распределенной системы, обуславливающих практическое использование информации при принятии решений и реализации тех или иных жизненных процессов, позволяет выделить наиболее уязвимое звено защищенной системы - этап ее передачи, где имеет место возможность несанкционированных действий со стороны неавторизованных пользователей.

При выполнении работ на объекте можно использовать различные модели построения системы информационной безопасности, основанные на адаптации нормативных документов и проведении анализа риска.

Разработанная модель информационной безопасности - это совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранение материальных или информационных ресурсов [3].

Рассматриваются следующие объективные факторы:

- угрозы информационной безопасности, характеризующихся вероятностью возникновения и вероятностью реализации;

- уязвимости ИС или системы контрмер (системы информационной безопасности), влияющие на вероятность реализации угрозы;

- риск-фактор, отражающий возможный ущерб организации в результате реализации угрозы информационной безопасности: утечки информации и ее неправомерного использования (риск в конечном итоге отражает вероятные финансовые потери - прямые или косвенные).

Для построения сбалансированной системы информационной безопасности предполагается сначала провести анализ рисков в области информационной безопасности. Затем определить оптимальный уровень риска для организации на основе заданного критерия. Систему информационной безопасности должно быть построено таким образом, чтобы достичь заданного уровня риска [4].

В ходе работ должны быть установлены границы исследования. Для этого необходимо выделить ресурсы ИС, для которых в дальнейшем будут получены оценки рисков. При этом нужно разделить рассмотренные ресурсы и внешние элементы, с которыми осуществляется взаимодействие. Ресурсами могут быть средства вычислительной техники, программное обеспечение, данные. При построении модели будут учитываться взаимодействия между ресурсами. Например, выход из строя какого-либо оборудования может привести к потере информации или выходу из строя другого критически важного элемента системы. Подобные взаимосвязи определяют основу построения модели организации с точки зрения информационной безопасности.

Эта модель, в соответствии с предлагаемой методикой, строится следующим образом: для выделенных ресурсов определяется их ценность, описываются взаимосвязи ресурсов, определяются угрозы безопасности и оцениваются вероятности их реализации.

На базе предложенной модели можно выбрать и обосновать систему контрмер, снижая риски до допустимых уровней, которые имеют наибольшую ценовую эффективность. Частью системы контрмер будут рекомендации по проведению регулярных проверок эффективности системы защиты. Управление рисками - обеспечение повышенных требований к информационной безопасности предполагает соответствующие меры на всех этапах жизненного цикла информации и информационных технологий. Планирование этих мероприятий осуществляется по завершении этапа анализа рисков и выбора контрмер. Обязательной составной частью этих планов является периодическая проверка соответствия существующего режима информационной безопасности, политики безопасности, сертификация ИС (технологии) на соответствие требованиям определенного стандарта безопасности.

В завершении работ, можно будет определить степень гарантии безопасности информационно-вычислительной среды, основанную на оценке и, с которой можно доверять информационно-вычислительной среде объекта.

Таким образом, жизненный цикл информации на объекте зависит от оценки ее ценности, а также от способности санкционированных пользователей обеспечить ее надежную защиту, и, таким образом, не допустить "обесценивание" информации. Он предусматривает, что информация добывается, обрабатывается (анализируется), сохраняется, охраняется, используется, транслируется, разворовывается и уничтожается. Поэтому было целесообразным рассмотреть этапы жизненного цикла информации с позиции целевых

признаков ИС подробно, чтобы отделить уязвимые звенья трансформации, которые нуждаются в защите.

Разработанная модель информационной безопасности представляет совокупность объективных внешних и внутренних факторов и их влияние на состояние информационной безопасности на объекте и на сохранение материальных или информационных ресурсов. На базе предложенной модели можно обоснованно выбрать и обосновать систему контрмер, которая снижает риски до допустимых уровней, и которые имеют наибольшую ценовую эффективность. В завершении работ, можно будет определить степень гарантии безопасности информационно-вычислительной среды, основанную на оценке, с которой можно доверять информационно-вычислительном среде объекта.

Литература

1) Хорошко В.А. Стратегия, методы и модели управления безопасностью информационных технологий / В.А. Хорошко, Ю.Е. Хохлачева // Информационные технологии и защита информации в информационно-коммуникационных системах, 2015. – Раздел 19. – С. 265-280.

2) Голубенко О.Л. Політика інформаційної безпеки / О.Л. Голубенко, В.О. Хорошко, О.С. Петров, С.М. Головань, Ю.Є. Яремчук. – Луганськ: Вид. СНУ ім. В. Даля, 2009. – 300 с.

3) Хорошко В.О. Методичний підхід щодо оцінки рівня безпеки інформації / В.О. Хорошко, В.С. Чередниченко // Збірник наук. праць Військового інституту Київського національного університету ім. Т. Шевченка, 2008. - №14. – С. 176-181.

4) Ленков С.В. Методы и средства защиты информации. В 2-х томах/С.В. Ленков, Д.А. Перегудов, В.А. Хорошко. – К.: Арий, 2008.

Наукове видання

СТАН ТА УДОСКОНАЛЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ (SITS'2016)

VIII Всеукраїнська науково-практична конференція

09 – 12 червня 2016 року

ЗБІРНИК НАУКОВИХ ПРАЦЬ

(*українською, російською та англійською мовами*)

Відповідальний за випуск

Михалишин Б.Є.

Підписано до друку 25.05.2016. Папір офсетний. Формат 60×84$^{1}/_{16}$.
Гарнітура Таймс. Друк офсетний. Ум. друк. арк. 4,4.
Обл.-вид. арк. 3,5. Тираж 50 прим. Зам. № 2745.

Надруковано в типографії ДП НВКГ «Зоря-Машпроект»,
м. Миколаїв, пр. Жовтневий 42А, тел. (0512)-491909