міської ради від 30 грудня 2011 № 797-VI [Електронний ресурс]. – Режим доступу: chuguev-rada.gov.ua›doc/sesiya/39/1712.doc.

Надійшла до редколегії 29.01.2014

УДК 656.135

Концепція розвитку транспортної схеми м. Чугуєва/ Линник І. Е., Сосіпатров А. М., Никитенко Ю. В. // Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. – Х: НТУ «ХПІ», – 2014. - № 7 (1050). – С.97-103 . – Бібліогр.: 11назв. ISSN 2079-5459

Освещаются основные проблемы, существующие в транспортной сфере г. Чугуева, указаны глобальные стратегические цели развития транспортной схемы и намечены первоочередные мероприятия ее развития.

Ключевые слова: концепция, транспортная схема, международный транспортный коридор, региональный логистический центр.

Conception of transport patterns Chuguyev/ I. E. Lynnyk, A. M. Sosipatrov, J. V. Nykytenko //Bulletin of NTU "KhPI". Series: New desicions of modern technologies. – Kharkov: NTU "KhPI", 2014.- № 7 (1050).- P.97-103. Bibliogr.: 11. ISSN 2079-5459

Highlights the main challenges in the transport sector, the Chugueva, are global strategic development of the transport scheme and identified priority measures its development.

Keywords: concept, transport scheme, international transport corridor, regional logistics center.

УДК: 004.056.5

В. В. ПОЛІНОВСЬКИЙ, канд. техн. наук, дирек., Інститут комп'ютерних технологій, Відкритий міжнародний університет розвитку людини «Україна», Київ;
М. І. ОГУРЦОВ, н.с., Інститут Кібернетики ім. В. М. Глушкова НАН України, Київ

МЕТОДИ ЗАСТОСУВАННЯ УАК ПРИ ПОБУДОВІ РЕАКТИВНИХ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

В роботі проведений аналіз загроз методами експертних оцінок STRIDE та DREAD, розроблено зонно-периметральну модель безпеки, метод безпровідної адаптивної мережі безпеки, запропонований метод розділення автентифікаційних даних та розроблений метод неперервного реактивного контролю користувачів на основі УАК з вбудованим NFC-пристроєм, що базується на технології комунікації ближнього поля, застосовні для надійної багатофакторної автентифікації користувачів.

Ключові слова: аналіз загроз, модель безпеки, методи безпеки, захист інформації, реактивна система, зонно-периметральна модель, багатофакторна автентифікація.

Вступ. З кожним роком зростає кількість загроз для інформації з обмеженим доступом у сучасному суспільстві [1, 2]. Пропорційно зростає і кількість засобів захисту від цих загроз. Їх кількість настільки велика, що призводить до необхідності регулярного внесення змін у систему захисту інформації (СЗІ), включаючи зміни конфігурації та структури СЗІ для адаптації та адекватного реагування сучасним загрозам [3]. Можливе також застосування проактивного підходу, протилежності реактивного, коли відбувається попередження реалізації можливих загроз а не реагування на їх реалізацію [3, 4], але зі зростанням кількості загроз такий підхід втрачає актуальність.

Мета даної роботи. Розробка нових методів та алгоритмів, застосовних для побудови реактивних систем захисту інформації, призначених як для великих корпорацій та державних структур, так і для високотехнологічного домашнього оточення, так званого «розумного дому» [5].

Методика експериментів. Приступаючи до аналізу архітектури побудови реактивних систем захисту інформації та контролю доступу, слід перш за все формалізувати об'єкт захисту. При цьому слід розуміти, що реактивна система захисту інформації

повинна відстежувати місцезнаходження кожного суб'єкта в сфері її дії і відстежувати його як санкціоновані так і несанкціоновані дії, видаючи відповідну реакцію на кожен варіант цих дій. На основі розробленої моделі загроз можна створювати архітектуру та конкретні рішення, що дозволять захиститись від потенційних небезпек.

Огляд результатів. Проведемо розробку моделі загроз для розробки архітектури реактивних систем захисту інформації для формального об'єкту, що потребує захисту, враховуючи при цьому всю сукупність загроз, цінність інформації та її носіїв, вразливості в системі захисту інформації, аудит засобів безпеки [3]. Щоб унеможливити успішні атаки на ІзОД об'єкту, слід організувати комплексну реактивну систему [2] технічного захисту інформації на базі архітектури реактивних систем захисту інформації. Загальна схема проведення робіт по ЗІ. Проведення робіт по ЗІ повинно бути наступним [5]:

1. Необхідно визначити на об'єкті інформацію, яку необхідно захищати, визначити вартість витоку чи втрати цієї інформації [6].

2. Далі будується модель об'єкту (включаючи інформаційні потоки) [7-8].

3. Розробляється модель загроз та модель порушника.

4. Виконується аналіз та вибір конкретних заходів ЗІ об'єкту.

2. Аналіз ризиків та модель загроз

Для того, щоб перейти до проектування архітектури реактивних СЗІ і визначити вимоги до її створення, слід визначити множину загроз – побудувати модель загроз. Потрібно визначити цінності інформації, щоб можна було порівняти витрати на ЗІ і розмір збитків у разі успішних атак [6]. В різних джерелах [3,6] мають різні підходи до визначення найбільш небезпечних порушень. Небезпечність та шкідливість тих чи інших порушень може визначатись на основі експертних оцінок [8]. Далі на основі даних, наведених в [3,6, 9-11] проводимо аналіз можливої множини загроз, яким необхідно протистояти, та виділяємо найбільш ймовірні та найбільш небезпечні з них (табл. 1).

Таблиця 1 – Множини ймовірних загроз

Категорії загроз	Ймовірність реалізації	Ступінь втрат
1.Непрямі Z1 – Програмні, вірусні методи, троянські коні	Висока	Дуже висока
Z2 – Перехоплення електромагнітних випромінювань	Низька	Середня
Z3 – Акустичний контроль приміщень (засобами телефонного та централізованого зв'язку)	Висока	Середня
Z4 – Прослуховування приміщень за допомогою лазерного чи інфрачервоного зондування віконного скла, напрямлених мікрофонів	Нижче середньої	Середня
Z5 – Перехоплення виводу на екран	Низька	Низька
Z6 – Перехоплення відходів діяльності	Середня	Низька
2. Прямі Z7 – Зловмисна передача інформації	Висока	Дуже висока
Z8 – Крадіжка, пошкодження, знищення, підробка, блокування, копіювання інформації в результаті НСД до її носіїв чи засобів обробки, передачі й зберігання	Висока	Дуже висока
Z9 – Зміна параметрів підсистеми захисту або інформаційних засобів задля порушення конфіденційності/цілісності/доступності	Середня	Дуже висока
Z10 – Встановлення пристроїв несанкціонованого знімання інформації	Середня	Середня
Z11 – Ненавмисне розголошення інформації або пошкодження носіїв інформації	Дуже висока	Середня
Z12 – Стихійні лиха	Дуже висока	Висока

На основі наведених статистичних даних побудуємо таблицю множини загроз з виділенням ймовірності їх реалізації (у вигляді атаки) та приблизного обсягу фінансових втрат при виконанні такої атаки.Ризик загрози трактується як добуток ймовірності здійснення загрози на величину потенційних втрат. Виявлення загроз та присвоєння ним рейтингу здійснюється на основі методик експертних оцінок DREAD та STRIDE.

STRIDE-методика якісної оцінки вразливості. STRIDE дозволяє типізувати загрози за цілями і задачами. За STRIDE методикою експерт оцінює можливість шести основних атак, відображених на отриманих з дерева загроз вразливостях, або точках застосування атаки (було обрано 4 статистично ймовірні – I – несанкціонований фізичний доступ до носіїв ІзОД, II – помилкові дії легітимних суб'єктів при роботі ІзОД, III –віддалений мережевий доступ до ІзОД, IV – перехоплення виводу на екран) за допомогою діаграм інформаційних потоків, процесів, сутностей та файлів за двозначною логікою. Отриманий перелік атак [3] з експертизою можливості їх проведення дозволяє перейти до розробки стратегії їх протидії. Отримані результати зводяться в таблицю STRIDE (табл. 2).

DREAD-методика оцінки ваги ризиків. Загальна проблема з рейтинговими системами оцінки загроз полягає в тому, що команді експертів важко дійти згоди в призначенні пріоритету загрозам. Тому було запропоновано методику обчислення значущості ризиків. DREAD-методика дозволяє отримати кількісну оцінку значимості загрози на основі опитування експертів, які ставлять бали рівню загроз таким характеристикам атаки: D – Damage potential, втрати при успішній атаці; R – Reproductively, складність атаки; E – Exploitability, рівень супротивника і ресурси для виконання атаки; A – Affected users, кількість користувачів, яким буде нанесено збитки; D – Discoverability, простота виявлення атаки. Отримані результати зводяться у таблицю DREAD і усереднюються (табл. 3).

Таблиця 2 – Результати якісної оцінки загроз за методикою STRIDE

Вразливість	S	T	R	I	D	E
I	x	x	x	x	x	
II		x	x		x	
III	x	x		x	x	x
IV			x	x		x

На основі аналізу розробленої моделі загроз можна зробити висновок, що першочерговим завданням є захист процесу автентифікації користувача та реактивні дії по виявленню програмних атак та крадіжок носіїв інформації.

Таблиця 3 – Результати оцінки ваги загроз за методикою DREAD

Загроза	D	R	E	A	D	∑/5
Z1	5	2	3	4	3	4
Z2	1	2	1	1	5	2
Z3	4	1	1	4	1	2
Z4	2	2	2	2	4	2
Z5	2	4	5	1	2	3
Z6	1	4	5	2	5	3
Z7	5	3	5	4	3	4
Z8	5	2	4	3	2	3
Z9	2	1	1	5	2	2
Z10	2	3	3	2	4	3
Z11	2	4	5	2	1	3
Z12	5	4	5	5	1	4

Таким чином, найбільш небезпечними серед категорій загроз за експертними оцінками можна назвати стихійні лиха, необережні дії легітимних користувачів, програмні засоби несанкціонованого доступу (НСД) до інформації, та зловмисна передача інформації легітимними користувачами стороннім особам. Для цього частіше за усе ці користувачі намагаються отримати доступ до інформації, права доступу до якої за своїми повноваженнями вони не мають. Тобто виконаний аналіз можливої множини загроз показав збільшення ролі захисту інформації від несанкціонованого доступу і автентифікації користувачів при виконанні всіх операцій з ІзОД.

Концепція периметральної безпеки. Практично будь-який об'єкт піддається розбиттю на окремі сектори з різним рівнем захисту [2], розділених периметрами безпеки,відрізнятись в залежності від об'єкту буде лише кількість цих секторів, або зон безпеки. Тому пропонується застосування концепції периметральної безпеки – використовуючи розбиття об'єкту на зони з різним рівнем доступу до них, можна сконцентрувати засоби захисту на кордонах цих зон, на периметрах доступу. Метою застосування концепції є те, щоб жоден користувач не мав змоги отримати доступ до зони, права доступу до якої він не має.

На основі аналізу експертних та статистичних даних були розраховані приблизні ймовірності виконання конкретної атаки в кожній зоні та ймовірність її своєчасного виявлення службою безпеки. Для розрахунку ймовірності атаки була використана наступна формула:

$$I_z = \frac{\frac{\sum_{i=1}^{m} S_{zi}}{m} \times \partial_S + \frac{\sum_{i=1}^{n} E_{zi}}{n} \times \partial_E}{2} \quad (1)$$

де Szi– статистичні дані по ймовірності реалізації загрози Z з джерела i;

Ezi – експертні оцінки ймовірності реалізації загрози Z з джерела i;

δ – коефіцієнти довіри експертним оцінкам та статистичним даним (сума δS та δЕдорівнюєодиниці);

m – кількість джерел статистичних даних;

n – кількість експертних оцінок.

Аналогічна формула використовувалась і для розрахунку ймовірності своєчасного виявлення атаки:

$$I_{vz} = \frac{\frac{\sum_{i=1}^{m} S_{zi}}{m} \times \partial_S + \frac{\sum_{i=1}^{n} E_{zi}}{n} \times \partial_E}{2} \quad (2)$$

В результаті проведених розрахунків було доведено емпірично отримані висновки – найбільш небезпечними порушниками є внутрішні, особливо системні адміністратори та співробітники служби безпеки. Таким чином, побудова ефективної реактивної архітектури з мінімізацією привілеїв зовнішніх користувачів дозволить захиститись від найбільш небезпечної множини загроз.

На основі формул (1-2) визначимо усереднений рівень небезпеки кожної зони (у вигляді середньої ймовірності реалізації атаки саме в цій зоні) для визначення того, на яку з зон треба звертати особливої уваги при побудові СЗІ. Для цього використаємо наступну формулу:

$$H_{zone} = \frac{\sum_{i=1}^{l} \sum_{k=1}^{q} \left(P_{ik} / q \right)}{l} \quad (3)$$

де l – кількість загроз в даній зоні;

q – кількість ймовірних категорій порушників для кожної з загроз даної зони;

Pik – ймовірність реалізації атаки в даній зоні по даній загрозі для даної категорії порушників.

Згідно формули (3), найбільшу небезпеку мають атаки в зоні 5 та в зоні 4.

Архітектура побудови реактивних систем захисту інформації. При побудові системи захисту не треба покладатися лише на одну лінію захисту, якою б надійною вона не була. За засобами фізичного захисту (зони 1-2) повинні йти програмно-технічні засоби, за ідентифікацією та автентифікацією – керування доступом (зони 3-5), і як останній механізм, – протоколювання та аудит (зона 5) [3].

Розглянемо запропоновану авторами архітектуру реактивних систем захисту інформації (див. рис. 1). Її ключовою частиною є зонно-периметральна модель безпеки, згідно якої кількість периметрів безпеки залежить від кількості зон організації.

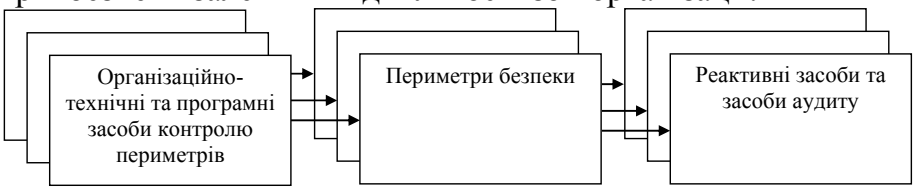

Рис. 1 – Архітектура реактивних систем захисту інформації

Якщо користувач системи або зовнішній зловмисник намагається перетнути периметр безпеки, не маючи на це повноважень, спрацьовують інтелектуальні реактивні засоби захисту, що видають реакцію на цю несанкціоновану спробу – блокування доступу, відстеження зловмисника, повідомлення служби безпеки, ввімкнення додаткових засобів захисту, здатних більш адекватно реагувати на зловмисні дії цього типу та ін.

Побудова безпровідної адаптивної мережі безпеки та базі технології NFC. Архітектуру реактивних систем захисту інформації пропонується реалізовувати на базі методу безпровідної адаптивної мережі безпеки на основі технології комунікації ближнього поля – Near Field Communication (NFC) [12]. Її застосування забезпечить просте розгортання системи безпеки будь-якої складності в практично будь-яких умовах.

Технологія NFC передбачає три основних ролі:

1) безконтактні віртуальні платіжні картки;

2) зчитувач RFID міток;

3) P2P обмін даними між двома NFC пристроями.

Отож, засіб захисту встановлюється у необхідному місці системи, використовуючи NFC він зв’язується з сусідніми засобами захисту, повідомляє про свою присутність, реєструючи себе у системі захисту. Засіб захисту також повідомляє про свій тип та починає обмінюватись необхідною інформацією з сусідніми засобами. У випадку порушення безпеки засіб захисту повідомляє про це, використовуючи NFC, що дозволяє вважати цю систему такою, що відповідає парадигмі архітектури, орієнтованої на події (Event-driven architecture — EDA) [13].

Використання методу безпровідної адаптивної мережі безпеки дозволить просто змінювати конфігурацію системи захисту та розміщення її елементів, спростить масштабування системи. Загалом у реактивній системі захисту інформації пропонується застосовувати пристрої трьох типів:

Пристрої основної ланки. Обмінюються інформацією про себе та своє функціонування з сусідніми пристроями, регулярно повідомляючи про себе.

Роутери. Відстежують конфігурацію ближнього оточення та її зміни, здатні брати на себе роль основного серверу безпеки у випадку його виходу з ладу.

Ретранслятори. Обладнані більш потужними приймачами та передавачами для об’єднання територіально віддалених сегментів системи захисту.

На основі P2P ролі технології NFC або інших методів безпечної передачі інформації з обмеженим доступом пропонується створити канал передачі секретних автентифікаційних даних для роботи алгоритмів захисту інформації від несанкціонованого доступу.

При цьому, як засіб персоналізації обрано вітчизняні (розроблені та впроваджуються авторським науковим колективом) пристрої, а саме український ключ-автентифікатор УАК [14].

Інтеграція УАК та NFC. УАК –це ключ-автентифікатор (рис. 2) – засіб для набору та введення кодової інформації, що забезпечує ідентифікацію/автентифікацію користувачів. Основною особливістю конструкції ключа-автентифікатора є можливість набору на ньому коду за допомогою обертання навколо осі та фіксації в певних положеннях секретних елементів, з яких він складається. Ключ складається з об'ємних секретних елементів, які можуть мати будь-яку форму та містять кодові отвори, що перекривають гвинти, фіксатори та кодові символи.

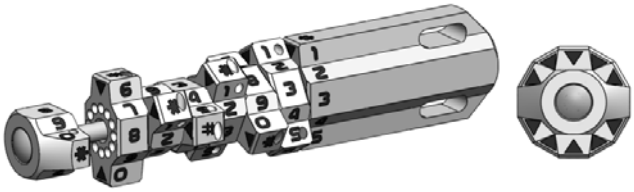

Рис. 2 – Обертання секретних елементів УАК навколо осі

Основні характеристики УАК детально розписані [14]. Розглянемо, як можна підвищити рівень захисту периметральної системи контролю доступу на основі УАК з використанням NFC. Авторами пропонується метод неперервного реактивного контролю користувачів, для якого слід вбудовувати NFC пристрій всередину УАК (RC-контури вбудовуються всередину сегментів УАК). Відповідно до функціонування алгоритмуреалізації методу неперервного реактивного контролю користувачів, NFC-пристрої, вбудовані в елементи системи захисту, будуть постійно відстежувати наявність та місцезнаходження кожного з користувачів, визначаючи при цьому його рівень повноважень (рис. 3).

В результаті якщо хтось спробує, наприклад, відкрити двері до приміщення, при цьому не маючи біля дверей відповідного NFC-пристрою, вони не відчиняться. І навпаки, для некритичних перевірок безпеки факту наявності NFC-пристрою буде достатньо, і користувачеві не доведеться вводити паролі або відкривати замки – тобто запропонований метод також призведе до спрощення функціонування системи безпеки для користувачів. При переході ж в іншу зону безпеки наявності автентифікатора з відповідним NFC-пристроєм буде недостатньо – його могли поцупити, тому користувач буде додатково вводити до зчитувача вірну комбінацію, набрану на УАК. При реалізації цього методу користувачі будуть вводити комбінацію УАК лише приходячи на роботу, а далі їм досить буде мати його при собі, щоб отримувати доступ в рамках своїх повноважень. При цьому система безпеки в режимі реального часу відстежує присутність, місцезнаходження та дії кожного користувача, перевіряючи за необхідності його права доступу в автоматичному режимі.

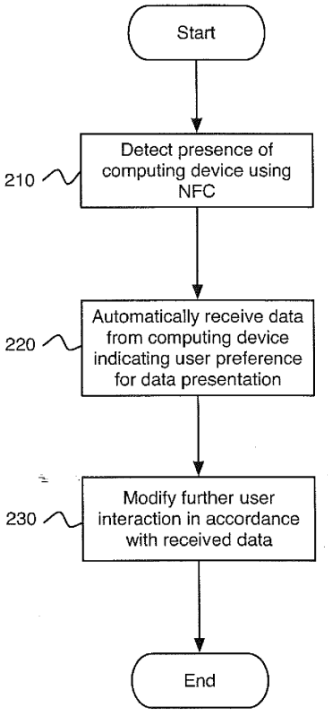

Рис. 3 –Алгоритм реалізації методу неперервного реактивного контролю користувачів

Можливо також не вбудовувати NFC-пристрій в УАК, а використовувати запропонований метод розділення автентифікаційних даних, зберігаючи частину даних автентифікації, наприклад, у NFC стільникового телефону – так зване «розділення секрету».

В якості прикладу такої апаратно-програмної персоналізації пропонується наступна схема (див. рис. 4), автентифікації на базі мобільного телефону.

Перевага цієї схеми в тому, що не потрібно розробляти нову версію зчитувача УАК, необхідно буде лише замінити програмні налаштування NFC-протоколу для передачі секретного коду і використовувати звичайні NFC-зчитувачі. Застосування подібних схем можливе й для інших автентифікаторів, наприклад, USB-автентифікації.

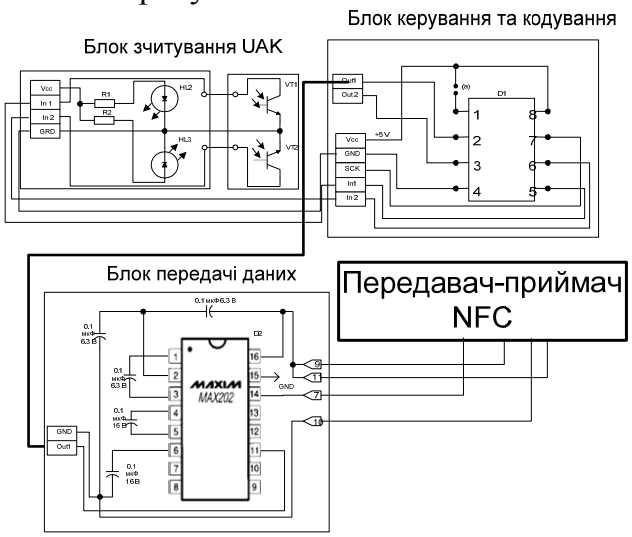

Рис. 4 – Приклад схеми автентифікації з використанням стільникового телефону

Використання вбудованих в УАК RC-контурів надає наступні переваги:

збільшення комбінаторики з базового значення 2256;

забезпечення багатофакторної автентифікації;

Водночас це поєднання має ряд недоліків:

значне зростання вартості УАК;

зростання вартості зчитувача УАК;

можливість обмеженого використання вкраденого УАК всередині тієї ж зони безпеки для проходження некритичних перевірок автентифікації;

складність заміни УАК при його втраті або ротації;

поява електромагнітного каналу витоку даних.

Таким чином, застосування УАК з вбудованим NFC-пристроєм в загальному випадку не рекомендується, воно допустиме лише для систем, що вимагають максимально високого рівня надійності завдяки забезпеченню додаткового рівня захисту.

Висновки. В даній роботі була побудована модель загроз та виконано експертну оцінку втрат методами STRIDE та DREAD. Були виділені найбільш небезпечні загрози та категорії порушників, до яких відносяться в першу чергу ненавмисні та зловмисні дії співробітників та адміністраторів безпеки.

Розроблено концепцію периметральної безпеки, запропонована зонно-периметральна модель безпеки, що передбачає розбиття об’єкту захисту на зоні з різним рівнем доступу до них та концентрацію на контролі доступу на кордонах цих зон. Було розроблено архітектуру периметральних реактивних СЗІ, яку пропонується виконувати на основі розробленого методу бездротової адаптивної мережі безпеки, що базується на технології NFC, що дозволить легке та гнучке розгортання, масштабування та оновлення системи захисту.

Для надійного контролю користувачів пропонується застосувати розроблений метод неперервного реактивного контролю користувачів, згідно якого місцезнаходження та дії користувачів будуть постійно відстежуватись СЗІ в автоматичному режимі. В якості засобу автентифікації пропонується застосовувати УАК з вбудованим NFC-пристроєм, що дозволить реалізувати цей метод та забезпечить багатофакторну автентифікацію. Також можна застосувати запропонований метод розділення автентифікаційних даних, згідно якого частина даних автентифікації буде зберігатись на іншому пристрої, наприклад, мобільному телефоні з NFC-пристроєм.

Список літератури: **1.** *Хорошко В. А.*, Методы и средства защиты информации[Текст] /*В. А Хорошко, А. А. Чекатков* //– К.: “Юниор”, 2003 р. – 504 с. **2.** *Бардаченко В. Ф.* Побудова політики безпеки для

інформаційних систем з використанням ВІК-ВАК технологій [Текст] / *В. Ф. Бардаченко, В. В. Поліновський, О. В. Костенко* // Вісті Академії інженерних наук України. – 2007. – № 1 (31). – с. 3-9. **3.** *Поліновський В. В.* Методи та рекомендації побудови комплексних систем захисту інформації [Текст] / *В. В. Поліновський, М. І. Огурцов* // Вісті Академії інженерних наук України. – 2008. – № 3 (37). – с.12-18. **4.** *Н. И. Алишов,* Самоподобная архитектура подсистемы информационной безопасности [Текст] / *Н. И. Алишов, М. И. Огурцов*//. – К.: УСиМ, 2006, №3. – с. 82-92. **5.** *Харке В.* Умный дом. Объединение в сеть бытовой техники и системы коммуникаций в жилищном строительстве [Текст] / *В. Харке* //. М.: Техносфера, 2006 р. – 416 с. **6.** *Задірака В. К.* Методи захисту фінансової інформації [Текст] / *В. К. Задірака, О. С. Олексюк* // – Київ. Вища школа, 2000. – 460с. **7.** *Корченко А. Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения. [Текст] / *Корченко А. Г.* //– К: МК-Пресс. – 2006. – 320 с. **8.** *Поліновський В. В.* Використання вітчизняних засобів персоналізації мобільних комп'ютерних та телекомунікаційних пристроїв для сучасних хмарних сервісів [Текст] / *В. В. Поліновський, В. Ю. Корольов* // Інформатика, обчислювальна техніка та кібернетика: Вісник університету «Україна». — № 2.К.: Університет «Україна», 2011. — С. 135– 140. **9.** *Поліновський В. В.* Аналіз змін архітектури аутентифікації в ОС Microsoft Vista та розробка засобів підвищення рівня безпеки при аутентифікації користувачів [Текст] / *В. В. Поліновський, В. А. Герасименко* // Інформатика, обчислювальна техніка та кібернетика: Вісник університету «Україна». — № 8.К.: Університет «Україна», 2010. — С. 167 – 173. **10.** *Корченко А. Г.* Логико-лингвистический подход в задачах оценки уровня безопасности информации в компьютерных системах [Текст] /*А. Г. Корченко, В. П. Щербина, Л. Г. Черныш*// Збірник наукових праць ІП-МЕ НАН України. Випуск 10.- Львів: НВМ ПТ УАД.- 2000.- С. 41 - 46. **11.** *Корольов В. Ю.* Концепція побудови персоналізованих флеш-накопичувачів даних з апаратним-захистом інформації [Текст] / *В. Ю. Корольов, В. В. Поліновський* // Математичні машини та системи. –2009. – № 4. – С.96 -105. **12.** *Tiruvilwamalai Venkatraman Raman*Personalized access using near field communication. [Патент] / *Tiruvilwamalai Venkatraman Raman*// *Google Inc.* US20120311019 / EP 2530664 A1 http://www.google.com/patents/EP2530664A1. **13.** *K. Mani Chandy* Event-Driven Applications: Costs, Benefits and Design Approaches [Текст] / *K. Mani Chandy //* California Institute of Technology, 2006. **14.** *Поліновський В. В.* Спосіб автентифікації і введення кодової інформації та автентифікатор зі зчитувачем кодової інформації для його здійснення [Патент на винахід] / *В. В. Поліновський, О. М. Ходзінський, Т. М. Нипорка, О. В. Усатенко* // Патент на винахід UA 89745 Україна, МПК (2009) Е 05В 19/00 Заявл. 06.08.2009; Опубл. 25.02.2010, Бюл. № 4.

Поступила в редколлегию 30.01.2014

УДК: 004.056.5

Методи та алгоритми застосування УАК при побудові реактивних систем захисту інформації/ Поліновський В. В., Огурцов М. І.// Вісник НТУ «ХПІ». Серія: Нові рішення в сучасних технологіях. – Х: НТУ «ХПІ», – 2014. - № 7 (1050). – С.103-110 . – Бібліогр.:14 назв. ISSN 2079-5459

В работе проведен анализ угроз методами экспертных оценок STRIDE и DREAD, разработана зонно-периметральная модель безопасности, метод беспроводной адаптивной сети безопасности, предложен метод разделения аутентификационных данных и разработан метод непрерывного реактивного контроля пользователей на основе УАК со встроенным NFC-устройством, базирующимся на технологии коммуникации ближнего поля, применимые для надежной многофакторной аутентификации пользователей.

Ключевые слова: анализ угроз, модель безопасности, методы безопасности, защита информации, реактивная система, зонно-периметральная модель, многофакторная аутентификация.

Methods for use UAKey in the construction of the reactive systems for information Security/ Polinovskyi V. V., Ogurtsov M. I. //Bulletin of NTU "KhPI". Series: New desicions of modern technologies. – Kharkov: NTU "KhPI", 2014.-№ 7 (1050).- P.103-110. Bibliogr.: 14. ISSN 2079-5459

Paper analyzes possible threats on the basis of expert assessments methods – STRIDE and DREAD. Created concept of perimeter security based on proposed zone-perimeter security model. Developed a method for efficient wireless adaptive network security, a method for the separation of authentication data and a method of continuous control of reactive users based on UAK with integrated NFC-device based on the technology of near field communication, applicable for robust multi-factor authentication of users.

Keywords: analyzes possible threats, security model, method of security, informationsecurity, reactive systems, zone-perimeter security model, multi-factor authentication.