УДК 004.056
DOI: 10.31673/2409-7292.2018.035157

Толубко В.Б., Курченко О.А., Шевченко А.В.

СТАБІЛІЗАЦІЯ ФУНКЦІОНАЛЬНОЇ СТІЙКОСТІ ІНФОРМАЦІЙНОЇ СИСТЕМИ ШЛЯХОМ УПРАВЛІННЯ ДИНАМІКОЮ РОЗВИТКУ ПРОФІЛІВ ЗАХИЩЕНОСТІ

Мета роботи: на основі аналізу нормативних документів проаналізувати основні профілі захищеності для різних станів розвитку на прикладі інформаційних систем медичного призначення та надати рекомендації щодо доцільних переходів між означеними станами. Для цього проаналізовані особливості спеціалізованого програмно-апаратного комплексу «Імедіс-Експерт». Визначено, що потрібно не тільки прогнозувати небезпеки, враховувати вимоги діючого нормативного поля, але й прогнозувати можливі шляхи розвитку системи управління інформаційною безпекою в умовах існуючих обмежень. В роботі запропонована логічна послідовність нарощування стандартних функціональних профілів захищеності, які відповідають певним етапам розвитку системи.

Ключові слова: дисфункціональний стан, функціональна стійкість, профілі захищеності.

Зростання дисфункціональних станів інформаційних систем у вигляді інцидентів інформаційної безпеки (ІБ) має **епідеміологічний характер** [1, 2] і, як мінімум, вдвічі перевищує темпи росту мобільного ринку і росту світового ВВП [3, 4, 5, 6]. Ситуація погіршується тим, що 71% атак залишається невиявленим [6, 7]. Як би не зростала якість технологій захисту, але нові атаки з'являются раніше ніж засоби протидії проти них. Такий стан справ потребує роботи на упередження, що, в свою чергу, потребує **прогнозування** розвитку атак. Теоретичні основи прогнозування процесів, які носять епідеміологічний характер розглянуті в роботах [1, 2, 8, 9]. Для управління інцидентами ІБ необхідно вбудовувати процеси прогнозування в систему управління ІБ (**СУІБ**). Без системи управління в умовах інформаційних та кібернетичних атак ми не можемо забезпечити **функціональну стійкість** інформаційної системи [4].

Системам управління ІБ присвячені стандарти ISO 27001, 27002 [10]. СУІБ будь-якої організації розвивається разом з організацією відповідно до змін умов функціонування, нарощування масштабів інформаційної діяльності, підвищення кількості та складності функцій організації та суттєвого збільшення цінності інформації після її агрегування, узагальнення та аналітичної обробки. Тобто потрібно не тільки спрогнозувати небезпеки, врахувати вимоги діючого нормативного поля, але й спрогнозувати можливі шляхи розвитку СУІБ в умовах вищенаведених обмежень. Виходячи з цього, питання управління динамікою розвитку профілів захищеності, в рамках діючого нормативного поля, є **актуальним.**

Мета роботи – на основі аналізу діючих нормативних документів сформулювати основні профілі захищеності для різних станів розвитку інформаційной систем організації на прикладі інформаційних систем медичного призначення та надати рекомендації щодо доцільних переходів між означеним станами.

Аналіз особливостей комп'ютерної системи, що підлягає захисту

Загальні підходи. Інформатизація медицини розвивається від автономних вузькопрофільних систем до складних інтегрованих мережних рішень на кшалт автоматизованих систем управління підприємством (АСУП) (Enterprise Resource Planning - ERP), які забезпечують сумісну роботу багатьох користувачів за великою кількістю функцій. **Впровадження інтегрованих** систем йде одночасно із поглиненням автономних систем та, зазвичай, проходить **три фази** [11, 12]:

1. Універсальні адміністративно-господарчі рішення: кадри, фінанси, логістика тощо..
2. Впровадження у стандартні універсальні рішення певні специфічні функції.
3. Глибоко специфічні медичні рішення.

Основні напрямки впровадження інформаційних технологій у медицині [11, 12]:

- Підтримка управлінських рішень, адміністративно-господарська діяльність.
- Обліково-звітна діяльність.

- Лікарська практика.
- Електронні консультанти, довідково-пошукові системи та штучний інтелект.
- Дистанційна медична консультація, відео- (аудіо-) конференції.
- Автоматизація навчання, дистанційне навчання медичних спеціалістів тощо.

В нашому випадку в якості основної інформаційної системи розглядаємо спеціалізований **програмно-апаратний комплекс «Імедіс-Експерт»** призначений для реєстрації, зберігання, обробки та наочного представлення вимірювальних даних при наявності додаткового інтерфейсного модуля. Дані, отримуються в процесі вимірювання електричних показників за методом Р.Фолля з біологічно-активних точок (БАТ) і біологічно-активних зон (БАЗ), в ході медікаментозного тестування, діагностики за методом вегето-резонансного теста (ВРТ), а також в ході проведення сегментарної експрес-діагностики, біорезонансної або резонансно-частотної терапії. Крім того, апаратно-програмний комплекс може слугувати джерелом великого об'єму довідкової інформації.

Наявність програмного забезпечення «Імедіс-Експерт» є необхідним для функціонування апарата «Імедіс-Експерт». Програмне забезпечення комплекса дозволяє:

- вести картотеку пацієнтів, в якій зберігаються дані, в тому числі вимірювання по кожному візиту;

- реєструвати вимірювальні дані по БАТ та БАЗ в автоматичному режимі або в режимі ручного вводу;

- відображати та виводити на друк первинні вимірювальні дані та результати їх обробки;

- на основі автоматичного аналізу вимірювальних даних виявляти найбільш вражені органи та системи організму, найбільш вірогідні захворювання;

- здійснювати підбір препаратів для тестування і терапії за допомогою вбудованої підсистеми реперторизації, включаючої інформацію і можливості всіх програм «Провізор»;

- керувати вбудованим медикаментозним селектором апарата;

- керувати системою біорезонансної терапії.

Програмне забезпечення постачається на компакт-диску CD-ROM та захищено від несанкціонованого доступу електронним ключом з USB-інтерфейсом.

При проведенні вимірювань в програмі використовується принцип віртуального пристроя. Пристрій представлений вікном індикатора вимірювань (підблок програмного забезпечення з відповідним інтерфейсом користувача). Дані, що надходять по інтерфейсному кабелю з апарата, приймаються цим вікном, в ньому ж відображається положення стрілки вимірювача і стан апарата. В подальшому вже вікно індикатора (підблок програмного забезпечення) розсилає інформацію про стан апарата іншим вікнам (підблокам) програми, які, щоба отримати цю інформацію, повинні підключитися (встановити з'єднання) з вікном індикатора вимірювань.

У методі ВРТ використовується спеціальна техніка вимірювання електропроводності в одній відтворюваній точці вимірювання при підключенні тест-препаратів, тест-вказівок, маркерів, маркуючих наявність або відсутність у пацієнта тих, чи інших порушень.

Для оцінки динаміки стану хворих по інтегральним показникам організму в ВРТ використовується ряд тест-вказівок, представлений у вигляді шкал. Під діагностичними шкалами розуміється впорядкована більшість (множина) тест-вказівників в різних потенціях, відповідних певному ступеню вираженості діагностичного процесу (стану захворюваності).

Загальні висновки щодо потреби захисту інформації

Таким чином, розглянутий об'єкт захисту **програмно-апаратний комплекс «Імедіс-Експерт»** представляє собою компьютерну систему, яка виконує всі види роботи з делікатною інформацією: отримання даних з сенсорів, отримання паспортних даних від пацієнтів в результаті опитування або через мережу (залежно від ступеню автономності роботи системи), зберігання, упорядкування, обробка інформації з сенсорів та паспортних даних, робота з довідковими системами, бізнес-аналітика, щодо отриманої інформації,

розподіл первинної та опрацьованої отриманої інформації. Всі розглянуті етапи обробки інформації є дуже чуттєвими з точки зору вразливості інформації як той, що отримується з сенсорів, так й той, що належить вбудованим довідковим системам, а також інформації, що відноситься до персональних даних пацієнта. Рейтинг загроз інформації (в порядку убування значущості) для розглянутої системи має такий вигляд: 1. Цілісність. 2. Доступність. 3. Конфіденційність.

Тобто важливі всі розлянуті складові, але в першу чергу треба допомогти людині, потім важливо це зробити швидко, і в останню чергу, зробити це конфіденційно. Хоча правозахисники з питань захисту прав людини скоріше перевернули би цю ієрархію до гори дригом. Конкретизуємо технології захисту та можливі підходи до їх можливої еволюції у вигляді фунціональних профілів захищеності.

Обрання рівню захищеності системи виходячи з вимог до функціональності

Комп'ютерні системи зазвичай проходять декілька етапів в своєму розвитку. У нашому випадку щодо програмно-апаратних систем ці етапи можуть бути пов'язані з послідовним вдосконаленням програмной, апаратної та організаційної компонент. Відповідним чином має розвиватись і система захисту інформації. Але, якщо при первинному проектуванні використання лікувально-діагностичного комплексу не передбачити можливі майбутні вимоги до функціонального профілю захищеності [13], то в подальшому їх реалізація може бути дуже ускладненої або зовсім неможливою. Розглянемо бажану послідовність нарощування рівнів захищеності нашої системи як послідовність зміни варіантів стандартних функціональних профілів захищеності.

Варіант 1 (мінімально можливий). Забезпечує функціональність без врахування втрат часу. Відповідно до проведеного аналізу було визначено, що у штатному режимі ми маємо справу із автоматизованою системою класу 1. Найбільш важливим видом загроз, якому має відповідати профіль захищеності такої системи є **цілісність**. Тому що, часові обмеження щодо використання системи дозволяють витрачати певний додатковий час на усунення проблем із функціональністю системи. Зрозуміло, що будь-які затримки в роботі погіршують якість роботи системи, але не унеможливлюють її. Краще втратити певний час на відновлення, а потім все ж таки виконати основні задачі щодо медичної діагностики та терапії. Отже у якості стандартного функціонального профілю захищеності можна обрати 1.Ц.1 або 1.Ц.2 [13, 14].

1.Ц.1 = { НР-1, НИ-1, НК-1, НО-1, НЦ-1, НТ-1 }
1.Ц.2 = { ЦА-2, ЦО-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }

Варіант 2 (основний робочий). Забезпечує функціональність за всіма вимогами. На другому місці стоять загрози щодо **доступності**. Якщо система захисту буде забезпечувати захист від загроз **як цілісності, так й доступності**, то це буде забезпечувати практично повну функціональність системи. Отже для переходу на більш високий рівень захищеності бажано використовувати стандартний функціональний профіль захищеності 1.ЦД.1 або 1.ЦД.2-4 [13, 14].

1.ЦД.1={ЦА-1,ЦО-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
1.ЦД.2={ЦА-1,ЦО-1, ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }
1.ЦД.3={ЦА-1,ЦО-1, ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }
1.ЦД.4={ЦА-1,ЦО-1, ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }

Варіант 3 (основний конфіденційний). Забезпечує повну функціональність та захист персональних даних пацієнтів. Взагалі то захист персональних даних в АС класу 1 забезпечується відносно легко, оскільки для цього можна обмежити доступ до системи на фізичному рівні. В АС класу 1 таке обмеження ніяк не вплине на функціональність. Але все ж таки слід враховувати, що при роботі з системою поряд з лікарем знаходиться пацієнт (пацієнти), який (які) потенційно може бути порушником інформаційної безпеки. Отже в

цьому випадку доцільно використовувати один з таких стандартних функціональних профілів захищеності 1.КЦД.1-4 [13, 14].

1.КЦД.1 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-1 }
1.КЦД.2 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-2, ДС-1, ДЗ-1, ДВ-2, НР-2, НИ-2, НК-1, НО-1, НЦ-1, НТ-2 }
1.КЦД.3 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-2, ДС-2, ДЗ-2, ДВ-2, НР-3, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }
1.КЦД.4 = { КА-1, КО-1, ЦА-1, ЦО-1,
ДР-2, ДС-3, ДЗ-3, ДВ-3, НР-4, НИ-2, НК-1, НО-1, НЦ-2, НТ-2 }

Варіант 4 (локально мережевий). Забезпечує повну функціональність та захист персональних даних пацієнтів при наявності підключення до локальної мережі. Оскільки сучасні медичні інформаційні системи об'єднують свої дані, то в цьому випадку доцільно використовувати один з таких стандартних функціональних профілів захищеності 2.КЦД.1-5 [13, 14].

2.КЦД.1 = { КД-2, КО-1, ЦД-1, ЦО-1, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }
2.КЦД.2 = { КД-2, КА-2, КО-1, ЦД-1, ЦА-2, ЦО-1, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2 }
2.КЦД.3 = { КД-2, КА-2, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, ДР-2, ДС-1, ДЗ-1, ДВ-2,
НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2 }
2.КЦД.4 = { КД-3, КА-3, КО-1, КК-1, ЦД-1, ЦА-3, ЦО-2, ДР-3, ДС-2, ДЗ-2, ДВ-2,
НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2 }
2.КЦД.5 = { КД-4, КА-4, КО-1, КК-2, ЦД-4, ЦА-4, ЦО-2, ДР-3, ДС-3, ДЗ-3, ДВ-3,
НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2 }

Варіант 5 (глобально мережевий). Забезпечує повну функціональність та захист персональних даних пацієнтів при наявності підключення до глобальної мережі. Часто сучасні медичні інформаційні системи мають розподілену структуру. В цьому випадку доцільно використовувати один з таких стандартних функціональних профілів захищеності 3.КЦД.1-5 [13, 14].

3.КЦД.1={КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }
3.КЦД.2={КД-2, КА-2, КО-1, КВ-2, ЦД-1, ЦА-2, ЦО-1, ЦВ-2, ДР-1, ДВ-1,
НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 }
3.КЦД.3={КД-2,КА-2,КО-1,КК-1, КВ-3, ЦД-1,ЦА-3,ЦО-2,ЦВ-2, ДР-2,ДС-1,ДЗ-1,ДВ-2,
НР-3, НИ-2, НК-1, НО-2, НЦ-3, НТ-2, НВ-2 }
3.КЦД.4={КД-3,КА-3,КО-1,КК-1,КВ-3, ЦД-1,ЦА-3,ЦО-2,ЦВ-2, ДР-3,ДС-2,ДЗ-2,ДВ-2,
НР-4, НИ-2, НК-1, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1 }
3.КЦД.5={КД-4,КА-4,КО-1,КК-2,КВ-4, ЦД-4,ЦА-4,ЦО-2,ЦВ-3, ДР-3,ДС-3,ДЗ-3,ДВ-3,
НР-5, НИ-2, НК-2, НО-3, НЦ-3, НТ-2, НВ-2, НА-1, НП-1 }

Для порівняльного аналізу обраних стандартних функціональних профілів захищеності узагальнимо їх характеристики в таблиці 1. Найбільший рівень функціональності забезпечує АС класу 3 (**варіант 5**), оскільки дозволяє залучати до роботи зовнішні інформаційні ресурси. Але вона ж є найбільш уразливою для інформаційних атак. Використання АС класу 2 (**варіант 4**) мало що додає до функціональності лікувально-діагностичного комплексу у порівнянні з варіантами 1-3, але може гарно забезепечити роботу АСУ лікувального заходу відповідною інформацією щодо пацієнтів. При цьому економія на засобах захисту є незначною. АС класу 1 (**варіанти 1-3**) дозволяє забезпечити повну функціональність лікувально-діагностичного комплексу, але в автономному режимі без взаємодії із

зовнішними інформаційними ресурсами. На відміну від варіанту 1, варіанти 2 та 3 забезпечують високий ступінь захисту при збереженні високого рівня функціональності системи. Отже можна казати, що за ознакою функціональної стійкості найбільшу функціональну стійкість для автономной системи забезпечує варіант 3. Але з урахуванням економічних показників оптимальним є варіант 2. Нажаль, всі розглянуті варіанти не мають абсолютного захисту від кібернетичних атак. Навіть у випадку від'єднання від інформаційної мережі залишається можливість потрапляння в комп'ютер зловмисного програмного забезпечення, наприклад через флеш-накопичувачі. Тому задача прогнозування розповсюдження зловмисного програмного забезпечення залишається актуальною. Розглянуті 5 варіантів побудови профілів захищеності можна вважати базовими для найбільш типових ситуацій. У випадку виникнення ситуацій, в яких до об'єкту складно застосувати один або інший варіант можливе використання проміжних варіантів, які обираються за допомогою таблиці 1. Наприклад в варіанті 5 перехід із стандартного функціонального профілю захищеності 3.КЦД.3 в 3.КЦД.4 вимагає одночасного нарощування відразу двох послуг конфіденційності: КД2, КА2, КО1 замінити на КД3, КА3, КО1. Якщо виявляється, що така заміна вимає надмірну кількість ресурсів (матеріали, гроші, люди, час), то в даному досліджені пропонується на підставі таблиці 1 наочно обрати один з проміжних варіантів КД2, КА3, КО1 або КД3, КА2, КО1, а вже на наступному етапі перейти до наступного стандартного фукнціонального профілю захищеності КД3, КА3, КО1.

Таблиця 1.

Порівняльний аналіз обраних стандартних функціональних профілів захищеності

	Варіант 1		Варіант 2				Варіант 3				Варіант 4					Варіант 5				
	1.Ц.		**1.ЦД.**				**1.КЦД.**				**2.КЦД.**					**3.КЦД.**				
	1	**2**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**1**	**2**	**3**	**4**	**5**	**1**	**2**	**3**	**4**	**5**
Послуги конфіденційності:																				
КД — довірча конфіденційність;											2	2	2	3	4	2	2	2	3	4
КА — адміністративна конфіденційність;							1	1	1	1		2	2	3	4		2	2	3	4
КО — повторне використання об'єктів;							1	1	1	1	1	1	1	1	1	1	1	1	1	1
КК — аналіз прихованих каналів;													1	1	2			1	1	2
КВ — конфіденційність при обміні.																	2	3	3	4
Послуги цілісності:																				
ЦД — довірча цілісність;											1	1	1	1	4	1	1	1	1	4
ЦА — адміністративна цілісність;		2	1	1	1	1	1	1	1	1		2	3	3	4		2	3	3	4
ЦО — відкат;		1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	2	2	2
ЦВ — цілісність при обміні.																				
Послуги доступності:																				
ДР — використання ресурсів;			1	2	2	2	1	2	2	2	1	1	2	3	3	1	1	2	3	3
ДС — стійкість до відмов;				1	2	3		1	2	3			1	2	3			1	2	3
ДЗ — гаряча заміна;				1	2	3		1	2	3			1	2	3			1	2	3

ДВ — відновлення після збоїв.			1	2	2	3	1	2	2	3	1	1	2	2	3	1	2	2	2	3
Послуги спостережності:																				
НР — реєстрація;	1	2	2	2	3	4	2	2	3	4	2	2	3	4	5	2	2	3	4	5
НИ — ідентифікація и автентифікація;	1	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
НК — достовірний канал;	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2
НО — розподіл обов'язків;	1	1	1	1	1	1	1	1	1	1	2	2	2	3	3	2	2	2	3	3
НЦ — цілісність КЗЗ;	1	1	1	1	2	2	1	1	2	2	2	2	3	3	3	2	2	3	3	3
НТ — самотестування;	1	1	1	2	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2	2
НВ — автентифікація при обміні;																1	1	2	2	2
НА — автентифікація відправника;																			1	1
НП — автентифікація одержувача.																			1	1

Висновки

1. Для забезпечення функціональної стійкості інформаційної системи в умовах дій інформаційних та кібернетичних атак потрібно забезпечити прогнозування розвитку атак, яке буде функціонувати в межах СУІБ, яка, в свою чергу, будується в рамках діючого нормативного поля.

2. СУІБ розвивається разом з організацією відповідно до змін умов функціонування, нарощування масштабів інформаційної діяльності, підвищення кількості та складності функцій організації та суттєвого збільшення цінності інформації після її агрегування, узагальнення та аналітичної обробки. Тобто потрібно не тільки спрогнозувати небезпеки, врахувати вимоги діючого нормативного поля, але й спрогнозувати можливі шляхи розвитку СУІБ в умовах вищенаведених обмежень.

3. В якості практичних рекомендацій запропонована логічна послідовність нарощування стандартних профілів захищеності, які відповідають певним етапам технічного розвитку інформаційної системи, що підлягає захисту. Розглянуті варіанти: Варіант 1 (мінімально можливий). 1.Ц.1-2. Варіант 2 (основний робочий). 1.ЦД.1-4. Варіант 3 (основний конфіденційний). 1.КЦД.1-4. Варіант 4 (локально мережевий). 2.КЦД.1-5. Варіант 5 (глобально мережевий). 3.КЦД.1-5.

4. Напрямками подальших досліджень є розвиток шляхів математичної формалізації переходів між стандартними функціональними профілями захищеності для подальшого включення в загальну прогноз-модель засобів атаки та засобів захисту від атак.

Список використаних джерел

1. Shevchenko A. The Epidemiological Approach to Prognosis and Management of Information Incidents / Shevchenko V., Shcheblanin Ju., Shevchenko A. // Наука і техніка Повітряних Сил Збройних Сил України. – 2017. - № 4 (29). – p.145-150.

2. Shevchenko A. The Epidemiological Approach to Information Security Incidents Forecasting for Decision Making Systems. / Shevchenko V., Shevchenko A. // 13-th International Conference Perspective Technologies and Methods in MEMS Design (MEMSTECH). Proceeding. – Polyana. – 2017. - pp.174-177.

3. Управление киберрисками во взаимосвязанном мире. Основные результаты глобального исследования по вопросам обеспечения информационной безопасности. Перспективы на 2015 год. Январь 2015. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers- Режим доступу: http://www.pwc.ru/ru/riskassurance/publications/assets/ managing-cyberrisks.pdf

4. Шевченко В.Л. Кращі світові практики управління інформаційною безпекою та їх вплив на економічну стабільність держави // Сучасний захист інформації. - №4. – Київ: ДУТ, 2015. – С. 4-9.

5. PwC представляет результаты глобального исследования по вопросам обеспечения информационной безопасности, перспективы на 2015 год. [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers - Режим доступу: http://www.pwc.ru/ru/press-releases/2015/cyber-security-press-release.html

6. The Global State of Information Security® Survey 2016. Turnaround and transformation in cybersecurity [електронний ресурс] // Офіційний сайт PricewaterhouseCoopers - Режим доступу https://www.pwc.com/gx/en/ issues/cyber-security/information-security-survey.html

7. Healthcare cybersecurity challenges in an interconnected world. [електронний ресурс] // Key finding from The Global State of Information Security. Survey 2015. - Режим доступу: http://www.pwc.ru/en/ riskassurance/publications/assets/healthcare.pdf

8. Шевченко А.В. Грубі моделі розвитку в медицині / Шевченко А.В., Шевченко В.Л. // Медична інформатика та інженерія. - 2009. - №4, с.52-55.

9. Шевченко В.Л. Оптимізаційне моделювання в стратегічному плануванні. – К.: ЦВСД НУОУ, 2011. – 283с.

10. ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. Галузевий стандарт України. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. (ISO/IEC 27002:2005, MOD)

11. Шевченко А.В. Основні напрями інформатизації військової медицини. - зб. матеріалів другого науково-практичного семінару / Шевченко А.В., Бадюк М.І., Румянцев Ю.В., Савицький В.Л., Закалад М.А. // "Актуальні проблеми управління проектами інформатизації в сфері безпеки і оборони" (27.10.09) - Київ: ЦВСД НАОУ. - 2009. - с.43.

12. Шевченко А.В. Потенціал рішень SAP AG HEALTH CARE та DFPS для автоматизації діяльності військово-медичних закладів. / Шевченко А.В., Закалад М.А., Савицкий В.Л. / 1-й Всеукраїнський з'їзд "Медична та біологічна інформатика і кібернетика" з міжнародною участю: 23-26.06.2010: Зб.праць. - К.: НМАПО ім.П.Л.Шупика, с.46.

13. НД ТЗІ 2.5-005 -99. Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу. Затверджено нак. Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від 28 квітня 1999 р. № 22. Зі Зміною №1, затвердженою наказом Адміністрації Держспецзв'язку від 15.10.2008 № 172. 20с.

14. НД ТЗІ 2.5-004-99. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу. Затверджено нак. Департаменту спеціальних телекомунікаційних систем та захисту інформації СБ України від " 28 " квітня 1999 р. № 22 із змінами згідно наказу Адміністрації Держспецзв'язку від 28.12.2012 № 806. - 61 с.

Надійшла: 11.07.2018 Рецензент: к.т.н. Довбешко О.А.