УДК 681.321;322:621.395

METHODS OF ANALYSIS OF THE OPERATIONAL CYBERSECURITY LEVEL FOR SHIP'S INFORMATION SYSTEMS

МЕТОДИ АНАЛІЗУ РІВНЯ ЕКСПЛУАТАЦІЙНОЇ КІБЕРБЕЗПЕКИ СУДНОВИХ ІНФОРМАЦІЙНИХ СИСТЕМ

S.A.Mikhailov, *DSc, prof.,* **Y.S Shevtsov,** *PhD associate prof.*

С.А.Михайлов, *д.т.н., проф.,* **Ю.С. Шевцов,** *к.т.н., доц.*

National University "Odessa Maritime Academy", Ukraine

Національний університет "Одеська морська академія", Україна

ABSTRACT

An algorithm which can detect hazardous events, and the restoration and produce information and analysis of the efficacy of the protection of marine bridge integrated systems. Also, the entire complex computerized navigation equipments, such as Electronic Chart Display and Information Systems (ECDIS), Automatic Identification Systems (AIS), navigation equipments (Radar), Voyage Data Recorder (VDR) and other marine information systems.

Keywords: cyber security, audit, informational security, event, security incidents.

Постановка проблеми в загальному вигляді і її зв'язок з важливими науковими або практичними завданнями

Оцінка стану та рівня експлуатаційної інформаційної кібербезпеки (аудит інформаційної безпеки) здобуває важливе значення для суднових інформаційних систем. До них можна віднести, в першу чергу, електронні карти (ECDIS), автоматичні ідентифікаційні системи (AIS), навігаційне обладнання, реєстратор даних рейса VDR («чорний ящик»). Ці та інші суднові комплекси є комп'ютерними інформаційними системами, об'єднаними між собою локальною інформаційною мережею з можливістю виходу на глобальну інформаційну мережу Internet і, отже, доступні для дії на них з боку всіх небезпек і кібератак ззовні і усередині цих мереж.

Аудит проводиться на судні, яке є об'єктом інформаційної діяльності (ОІД), який, у свою чергу, є складною системою, що включає технічну й інфокомунікаційну інфраструктуру з її документацією та персонал, який використовує цю інфраструктуру для досягнення цілей ОІД. Оцінка роботи екіпажу, а також суднових інформаційних систем з електронними обчислювальними машинами (ЕОМ), з'єднаними у системи та мережі, можлива лише методами аудиту.

Серед процесів контролю та перевірки інформаційної безпеки особливе місце займає *аудит* (від лат. *audit – слухати*) інформаційної безпеки об'єкту інформаційної діяльності. Аудит є незалежною експертизою окремих областей функціонування організації. Його основним призначенням є формування, як правило, незалежної оцінки стану та рівня інформаційної безпеки.

Результатом аудиту є висновок про те, наскільки успішно функціонує об'єкт і наскільки він відповідає вимогам, які йому пред'являються. Вихідними документами аудиту є оціночні звіти з конкретними й твердими рекомендаціями щодо приведення внутрішніх процесів, регламентів, інструкцій до відповідності чинним стандартам та нормативно-правовим документам.

Аналіз останніх досягнень і публікацій, в яких почато рішення даної проблеми і виділення невирішених раніше частин загальної проблеми

Питання, які вирішуються в даній статті були розглянуті в роботах [1, 2, 3], де проведено аналіз та опис безперервного аудіту. Проте аналіз показує, що в алгоритмі аудиту не розглянути питання реакції на інцинденти.

Формулювання цілей статті (постановка завдання)

Метою даною роботи є розробка алгоритму спільного використання системи виявлення і обробки атак із системою постійного аудита інформаційної безпеки.

В телекомунікаційних мережах безперервний аудит інформаційної безпеки впроваджується згідно міжнародних Рекомендацій X.800 та X.816 [4, 5].

Виклад основного матеріалу дослідження з обгрунтуванням отриманих наукових результатів

Розглянемо аудит інформаційної безпеки найбільш критичної ланки суднових інформаційних систем, а саме інформаційної безпеки систем технологічного управління (СТУ), зупинка яких викликає переривання процесу управління, дозволяє також враховувати дії суб'єктів, контролювати правильність використання ресурсів, виявляти спроби пошкодити інформаційну систему. На судні до них можна віднести, перш за все, інтегровані системи містка, весь комп'ютеризований комплекс навігаційного обладнання.

Безперервний аудит безпеки – це незалежний перегляд та дослідження системних даних, протоколів і подій для перевірки адекватності управління системою, для забезпечення відповідності між встановленою політикою та діючими процедурами, для виявлення виломів безпеки і для цілеспрямованого вдосконалення політики та процесу функціонування системи.

Механізми аудиту безпеки хоч і не здатні безпосередньо запобігати порушенням безпеки, але виконують важливі функції запису та аналізу подій, що трапляються в системі, сприяють правильній реакції на ситуації порушення безпеки системи шляхом зміни робочих процедур. При виникненні неприпустимої загрози безпеці, коли параметри системи перевищують встановлені межі, в системі генерується сигнал тривоги.

Ієрархічна модель реалізації послуг аудиту

Серед множини процедур аудиту можна виділити робочі фази, кожна з яких характеризується своєю тривалістю:

t_1 - визначення події, що стосується безпеки системи;

t_2 - прийняття рішення щодо запису події або генерацію тривожної сигналізації;

t_3 - опрацювання прийнятого рішення, тобто створення повідомлень аудиту безпеки або тривожної сигналізації;

t_4 - аналіз та оцінка, згідно з визначених критеріїв, події, що стосується безпеки системи, а також визначення реакції на подію, тобто послідовності дій;

t_5 - накопичення (збирання) розподілених в системі записів в журнали реєстрації аудиту (*security audit trail*);

t_6 - формування звіту із записів журналів реєстрації аудиту;

t_7 - архівація, тобто переміщення записів в журналах реєстрації аудиту.

Усі наведені вище фази не розділені за часом, тобто можуть перекриватись, тривати одночасно.

На рис.1 наведено ієрархічну модель послуг аудиту та тривожної сигналізації в СТУ, що будується у відповідності з рекомендацією ITU-T X.816.

На найнижчому рівні *S*1 відбувається, згідно з визначених критеріїв, визначення подій, що стосуються безпеки СТУ, та реакції на події. При прийнятті рішення вхідними параметрами дискримінатора події є тип події, що стосується безпеки, час доби та деякі особливі характеристики об’єкта-чинника події. Вихідною реакцією дискримінатора є повідомлення про дію у відповідь на подію, генерування тривожної сигналізації та повідомлення аудиту безпеки.

На рівні *S*1 відсутні можливості ведення стеження та аналізу подій, тому тривожні повідомлення направляються до *S*2, а повідомлення аудиту безпеки – до *S*3 для подальшого включення до журналів реєстрації аудиту. Журнал реєстрації аудиту містить дані, що збираються та потенційно використовуються для полегшення аудиту безпеки.

На рівні *S*3 відбувається поновлення журналів реєстрації аудиту, забезпечується для рівня *S*6 доступ до журналів реєстрації та до їх архівів з можливістю сортувати та вибирати потрібні записи журналів згідно з визначених критеріїв з подальшим занесенням цих записів до звіту безпеки. При формуванні звітів з безпеки інформації ці критерії враховуються при обробленні інформації, що міститься в одному чи більше журналах реєстрації аудиту. Рішення приймається на основі таких параметрів: тип аудит-запису; тип події, що стосується безпеки; тривалість події, що розглядається; тип об’єкту, інформація, котра потрібна для прийняття рішення. Кінцеве рішення видається у вигляді списку вибраних записів.

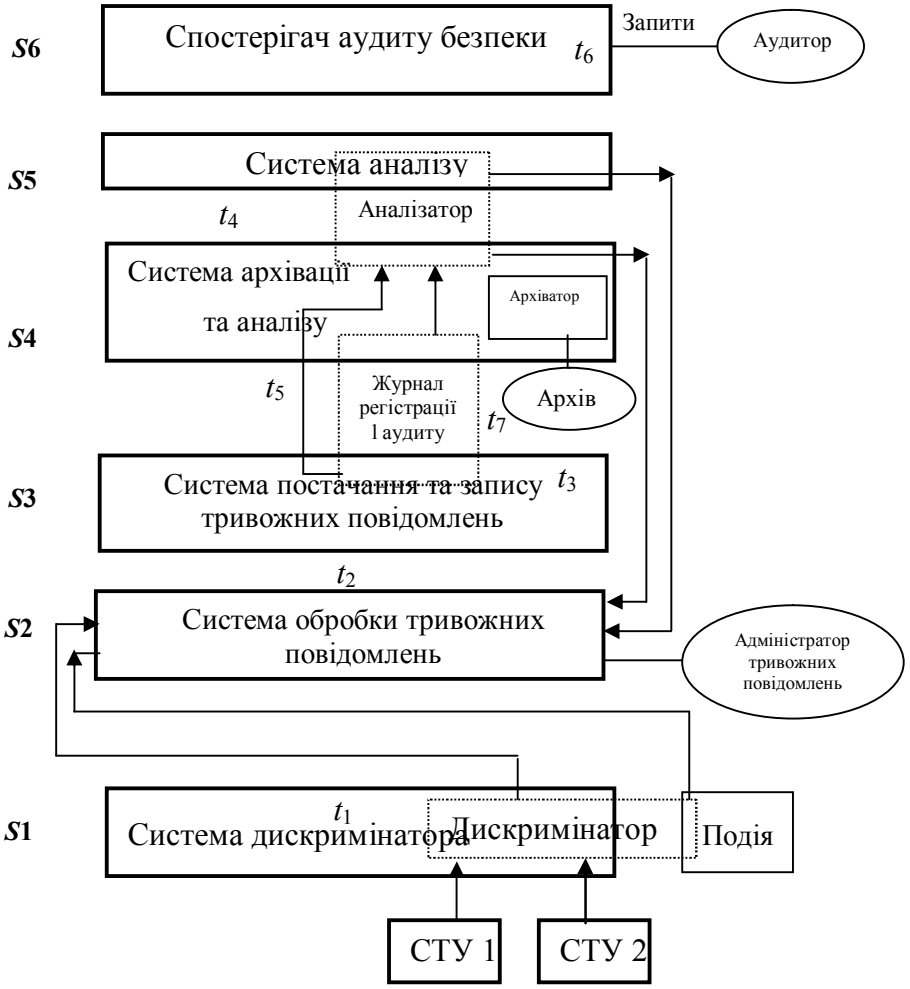

Рис.1. Модель реалізації послуг аудиту та тривожної сигналізації в СТУ

На рівні *S*4 відбувається архівація записів журналу реєстрації та пошук потрібних записів в архівах.

Програмне забезпечення (ПЗ) рівня *S*5 здійснює аналіз записів журналів реєстрації, а також архівних записів, згідно з визначених критеріїв, а також пересилає сигнали тривоги до *S*2 при перевищенні певних граничних значень параметрів системи або визначених умов роботи системи, що можуть трактуватись як ненормальні.

Критерії в даному разі визначають, яким чином аналізатор аудиту буде обробляти записи журналів реєстрації. В загальному випадку аналіз записів журналу реєстрації аудиту відбувається шляхом оцінки частоти появи подій та типу подій до того, як буде визначено реакцію системи на подію. Прийняття рішення базується на таких параметрах: тип події, частота появи події, тривалість події. Після ретельного аналізу події визначається, яка дія потрібна у відповідь.

Участь операторів у процесі аудиту передбачається на двох рівнях. Аудит-адміністратор здійснює загальне управління аудитом, а оперативне управління покладається на адміністратора тривожних повідомлень.

З вище сказаного можна зробити висновок, що функціями аудита є тільки аналіз подій та виявлення й реєстрація тривожних повідомлень. Це є недостатнім для забезпечення надійного захисту тому що не здійснює функцію боротьби з несанкціонованою подією - інцидентом. Для рішення даного завдання передбачається ввести додаткову функцію - реакція на інцидент, в алгоритм безперервного аудита, що спричинить розширення обов'язків адміністратора тривожних повідомлень або створення нового підрозділу по адмініструванню і реакції на інциденти (ПАРІ).

Для того щоб використати загальну і обґрунтовану термінологію по обробці у Рекомендації ITU-T E.409 [6] визначаються наступні терміни.

Подія – це спостережуване явище, що неможливо передбачувати (цілком) або яким неможливо управляти.

Інцидент – це подія, що може привести до явища або епізоду, що не є серйозним.

Інцидент безпеки – це будь-яка несприятлива подія, у результаті якого якийсь аспект безпеки може піддатися погрозі.

Інцидент безпеки інфокомунікаційних мереж (ICN) – це будь-яка фактична або передбачувана несприятлива подія відносно безпеки ICN. Це охоплює:

– проникнення в комп'ютерні системи ICN через мережу;

– появу комп'ютерних вірусів;

– зондування через мережу уразливість ряду комп'ютерних мереж;

– витік викликів установчих АТС;

– будь-які інші небажані події, що є результатом несанкціонованих внутрішніх або зовнішніх дій.

Криза – це стан, викликаний деякою подією, або знанням про подію, що наближається, що може викликати серйозні негативні наслідки. Під час кризи можна, у найкращому разі, мати можливість вжити заходів для запобігання переходу кризи в катастрофу. Коли відбувається катастрофа, звичайно є План поновлення роботи (ППР), а також група кризового керування для подолання цієї ситуації.

По суті інцидент безпеки ICN є будь-якою небажаною несанкціонованою подією. Це значить, що інцидент безпеки ICN охоплює проникнення в комп'ютер, атаку "відмова в обслуговуванні" або вірус залежно від мотивування, досвіду й доступних добре обізнаних ресурсів в організації. В організаціях, що мають ефективну групу по боротьбі з вірусами, віруси можуть розглядатися не як інциденти безпеки ICN, а скоріше як інциденти.

Таблиця 1. Приклад утворення похідних термінів

Інциденти	Порушення мережного етикету Інтернет (розсилання спама, шкідливий контент і т.д.) Порушення стратегії забезпечення безпеки Окремі віруси
Інциденти безпеки ICN	Сканування й зондування Проникнення в комп'ютер Комп'ютерні диверсія й ушкодження (атаки на готовність, такі як "бомбардування", атаки на DoS) Зловмисне програмне забезпечення (віруси, програми "троянський кінь", хробаки і т.д.) Крадіжка інформації і шпигунство Маскування під законного користувача.

Структура обробки інциденту

Щоб зрозуміти роль обробки інциденту і організації по реагуванню на інциденти усередині певної організації, рекомендується використовувати структуру обробки інциденту. Ця структура дає огляд перебіг інциденту, описуючи виникнення інциденту, дії/міри з метою обмеження інциденту, відновлення й перевірку виконання.

Структура (рис. 2) показує, що всі події, інциденти, інциденти безпеки і кризи виникають із нормального стану, тобто з нормально функціонуючої справи.

Коли виявлена індикація активності, що може привести до інциденту або інциденту безпеки, вона обробляється постійною організацією, як описується нижче. Час між індикацією й появою інциденту або інциденту безпеки може бути дуже коротким. Типом індикації окремого інциденту може бути вірус на одному робочому місці, помилка в мережі і т.д. Що стосується інцидентів безпеки, їхні індикатори можна знайти в реєструємих файлах, фільтрах брандмауера і т.д. Індикаціями можуть бути аварійні сигнали, що також спрацьовують, індикації від камер спостереження та інші.

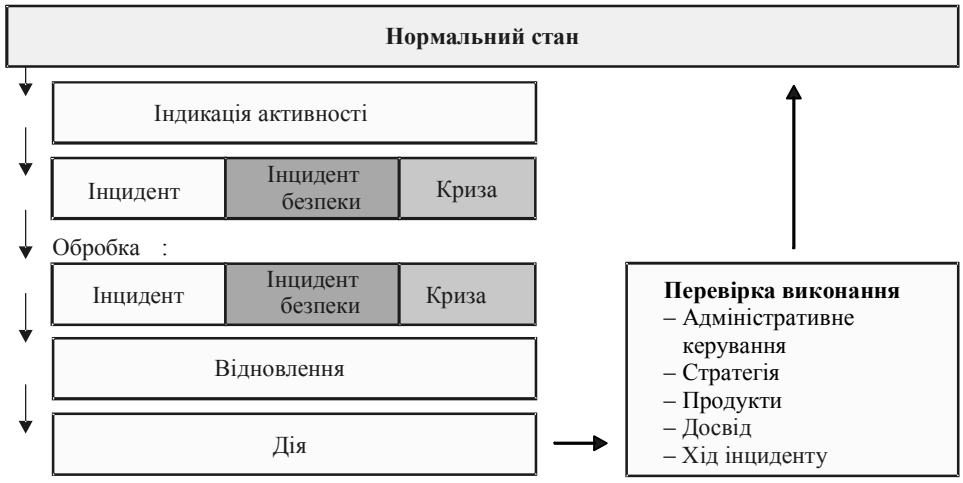

Рис. 2. Структура обробки інцидента

Коли відбувається інцидент або інцидент безпеки, він оцінюється по його області дії і наслідкам. Інцидент може розвитися в інцидент безпеки або кризу. Постійна організація обробляє інциденти, а інциденти безпеки обробляє спеціальна група реагування на інциденти (Група реагування на комп'ютерні інциденти). Кризи обробляє спеціально створювана група кризового керування.

Група реагування може входити до складу групи безпеки в організації електрозв'язку або бути повністю відділеною від такої групи безпеки в організації. Як варіант, хоча організація електрозв'язку може не мати окремої Групи реагування, цю роль може фактично виконувати неявно група безпеки даної організації.

Дії/міри, що вживаються, відповідають установленій методиці або стандартній процедурі. У випадку серйозних інцидентів безпеки або криз міри будуть залежати від області дії і наслідків такого інциденту. Міри здійснюються групою безпеки або групою реагування на інциденти.

Під час відновлення приймаються міри для повернення до нормальної діяльності. Залежно від виниклої події це може означати перезапуск комп'ютерних або мережних систем, повторну установку програм, відновлення резервних ресурсів. Такі міри можуть охоплювати установку аварійних сигналів у вихідне положення, відновлення ушкодженої властивості і т.д.

Обговорення

Під час цієї роботи також виробляється оцінка того, повинне чи ця подія мати правовий наслідок. Це може зажадати більше ретельного аналізу, надійних даних і т.д.

Важлива перевірка виконання тієї роботи, що вироблялася під час обробки інциденту і інциденту безпеки, а також при кризі. Метою перевірки виконання є поліпшення стандартних операцій і процедур, щоб запобігти повторній появі інциденту і мінімізувати будь-які наслідки і витрати.

Звіт про перевірку виконання може привести до зміни процесів обробки інциденту, зміні продуктів і стратегії. Керівникам надаються короткі відомості про інциденти, що відбулися, і інцидентах безпеки, їхньої області дії, наслідках і витратах. Ці відомості повинні також включати ефективність роботи організації по обробці інцидентів. Варто створити файл витягнутих уроків/досвіду, щоб мати можливість порівнювати різні інциденти з метою знаходження більше ефективних методів і практики виявлення й обробки інцидентів і інцидентів безпеки.

При появі інциденту приступає до відповідної реакції підрозділ ПАРІ. Підрозділ реагування є віртуальною групою, що формується під час інциденту безпеки. Хазяїн інциденту повідомляє про інцидент безпеки у ПАРІ, що відповідає за підрозділ реагування, у якому буде виконуватися правильна оцінка і ініціюватися контакт із відповідальними підрозділами.

Хазяїн інциденту – це особа, що відповідальна за порушене відділення, або власник порушеної системи. Хазяїн інциденту є особою, що повинна взяти на себе відповідальність за втрати і витрати.

Хазяїн інциденту в консультації з ПАРІ ініціює і створює віртуальну і тимчасову групу реагування на інцидент. Вибирається також керівник по

інциденту. Це може бути будь-яка особа з порушених підрозділів підтримки, групи спостереження або ПАРІ. Група реагування на інцидент формується з урахуванням відповідних осіб і їхніх умінь і навичок. Алгоритм адміністрування і реакції на інциденти представлен на рис. 3.

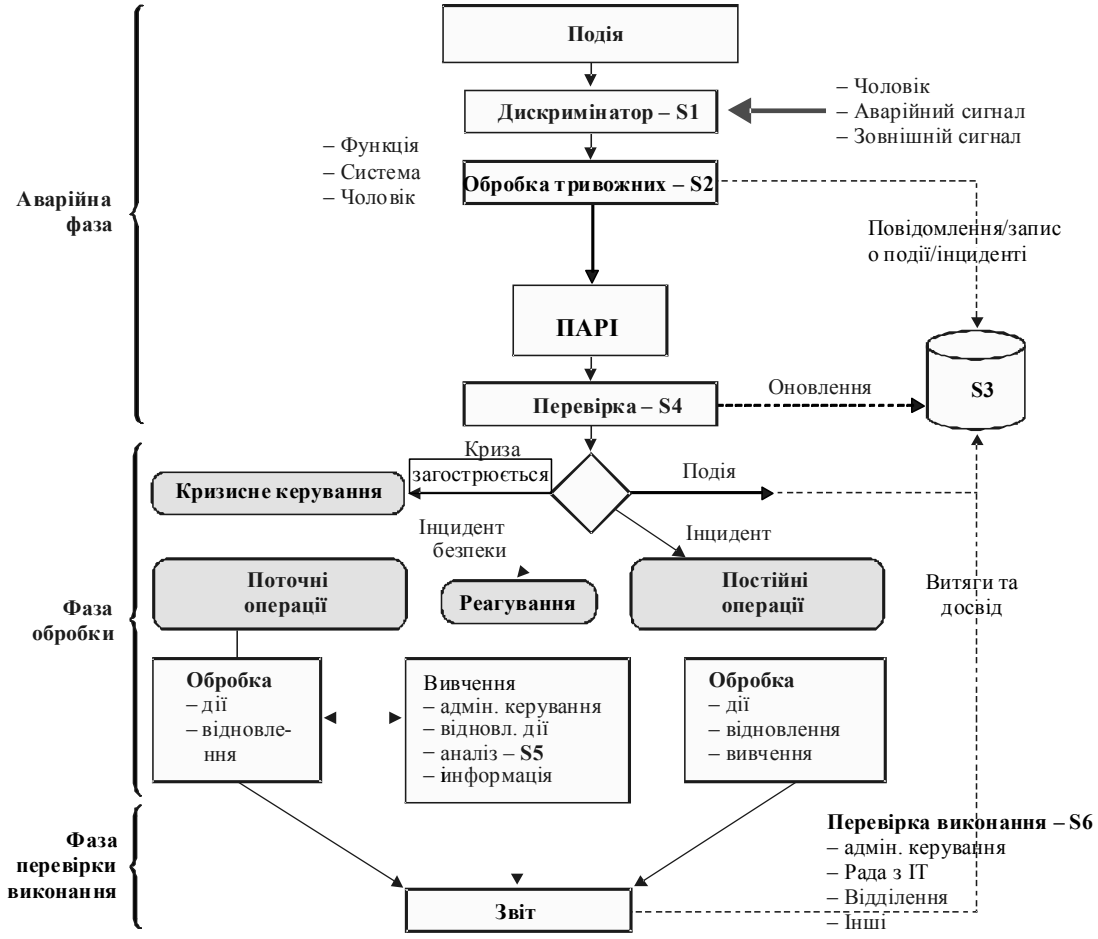

Рис. 3. Алгоритм адміністрування і реакції на інциденти

Висновки

Одержаний алгоритм дозволяє не тільки виявляти небезпечні події, а і проводити відновлення інформації та аналіз ефективності методів захисту суднових інтегрованих систем містка, всього комп'ютеризованого комплексу навігаційного обладнання, у т.ч. електронних карт, автоматичних ідентифікаційних систем, навігаційного обладнання, реєстратора даних рейса та інших суднових інформаційних систем [8, 9].

У висновку відзначимо, що одержаний результат може бути використаний в системах інформаційної безпеки та дозволяє підвищити надійність функціонування процесів управління.

ЛІТЕРАТУРА

1. Михайлов С.А. Нові функції аудиту та моніторингу у забезпеченні кібербезпеки підприємств / С. А. Михайлов, Ю.С. Шевцов – Інформатика та математичні методи в моделюванні. - Одесса, - ОНПУ, 2011, том 1, № 3. – С. 243-247с.
2. Шевцов Ю.С. Функції керування кібербезпекою на морському транспорті / Ю.С. Шевцов // В кн.:"Актуальні питання суднової електротехніки і радіотехніки". - Національний університет «Одеська морська академія», 2016, - с. 101-104.
3. Менеджмент інформаційної безпеки: Навчальний посібник / Тардаскіна Т.М., Кононович В.Г. - Одеса: ОНАЗ ім. О.С. Попова, 2009. – 265 с.
4. ITU-T Recommendation X.800. Security architecture for Open Systems Interconnection for CCITT applications. – Geneva, 1991. – 48 с. – Режим доступу: http://www.itu.int/net/home/index.aspx
5. ITU-T recomendation X.816. Information technology – Open System Interconnection – Security frameworks for Open systems: Security audit and alarms framework.
6. Рекомендация ITU-T E.409. Организация по реагированию на инциденты и обработка инцидентов безопасности: Руководство для организаций электросвязи. (Серия E: Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы. Управление сетью - Управление международной сетью.). - Женева, 2004. – 13 с.
7. Модель спільного використання системи виявлення і обробки атак із системою постійного аудиту інформаційної безпеки. Шевцов Ю.С., Кононович В.Г., Кільдішев В.Й. Вісник Східноукраїнського національного університету імені Володимира Даля. – Луганськ, 2010. – №9 (151). – С. 52–58.
8. Михайлов С.А. Информационная безопасность программных и аппаратных средств судових компьютерных систем / С.А. Михайлов, Д.В. Мельникова // В кн.: "Актуальні питання суднової електротехніки і радіотехніки". - Одеська національна морська академія, 2014 р., с. 120-122.
9. Михайлов С.А. Электронные компьютерные «облачные» технологии в реализации концепции e-Navigation / С.А. Михайлов, Д.А. Салабутина // "Актуальні питання суднової електротехніки і радіотехніки". - Національний університет «Одеська морська академія», 2016 р., с. 84-87.