УДК 004.45; 004.91

С. В. Гладиш
Одеська національна академія зв'язку ім. О.С. Попова
вул. Кузнечна, 1, 65029 Одеса, Україна

Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах

Розглянуто проблему автоматизації та інтелектуалізації керування інцидентами інформаційної безпеки в організаційно-технічних системах. Визначено постановку завдання, чинники, критерії та показники автоматизованих процедур підтримки прийняття рішень. Запропоновано функціональну схему відповідної інтелектуальної системи.

Ключові слова: *інформаційна безпека, інцидент, обробка, реагування, система керування.*

Вступ

Інциденти інформаційної безпеки (ІБ) є окремим підкласом кризових і надзвичайних ситуацій [1], що можуть відбутися в інфо-соціо-технічній інфраструктурі держави, і, як окремий випадок, — в організаційно-технічних системах (ОТС) та інфокомунікаційних мережах (ІКМ) [2], впливаючи на стан державних інформаційних ресурсів і національної безпеки [3, 4].

Підтримку прийняття рішень під час інцидетів ІБ [5, 6] в такому аспекті можна розглядати як частину більш загальної проблеми підтримки прийняття управлінських рішень у кризових ситуаціях [1]. В Україні останнє завдання вирішується згідно з [7] створенням відповідної урядової інформаційно-аналітичної системи [8]. У дослідженні [1] описано результати роботи ІПРІ НАН України в данному напрямку.

Дослідженню процесів реагування, обробки, керування інцидентами ІБ присвячено багато публікацій, зокрема науково-теоретичного [9–12], науково-прикладного [2, 5, 6, 13–15] та виробничо-практичного [16–19] змісту. Існує стандартизована міжнародна нормативно-методологічна база, зокрема [20–25], класифікацію та аналіз якої проведено в [2, 14–16, 19]. Відмітимо, що найбільшу кількість стандартів, рекомендацій і технічних звітів у цій проблемній підгалузі розроблено в США, наприклад [26, 27], та інші.

Стосовно України детально проаналізовано й оцінено як недостатній [2–4, 14, 15, 19] стан робіт, пов'язаних зі створенням відповідних нормативно-методологічних засад й організаційно-технічних інфраструктур, які повинні дозволяти на за-

гальнодержавному, галузевому та/або відомчому (корпоративному) рівнях вирішувати завдання, пов'язані з інцидентами ІБ. Державою поступово здійснюються ***окремі*** організаційні, правові та технічні заходи, ***частково*** спрямовані на підготовку до реагування, обробки та ліквідації наслідків інцидентів ІБ [28–31], керування телекомунікаційними мережами (ТМ) в умовах надзвичайних ситуацій, надзвичайного та воєнного стану [32, 33]. Зокрема, в рамках Адміністрації Держспецзв'язку України створено підрозділ — Державний центр безпеки інформаційно-телекомунікаційних систем (український аналог CSIRT), діяльність якого має бути спрямована на вирішення завдань реагування та обробки інцидентів, що порушили безперебійне функціонування ІКМ органів державної влади [3, 34].

Але на сьогодні все ще існує цілий ряд наукових, технічних, організаційних і нормативно-правових завдань, які є недостатньо вирішеними.

Як в Україні, так і в світовій практиці завдання підтримки прийняття рішень й автоматизації керування інцидентами ІБ потребує подальшого дослідження. В жодному з міжнародних чи вітчизняних нормативно-технічних документах, які частково торкаються або повністю присвячені керуванню інцидентами ІБ, не визначено, що саме можна/треба розуміти під автоматизацією процесу, з яких функцій та елементів ця автоматизація повинна складатися, та як її проводити.

Метою статті є розробка пропозицій щодо організації та інформаційного забезпечення системи підтримки прийняття рішень з керування інцидентами ІБ.

Постановка завдання

Реалізація будь-яких процесів, що повинні бути реалізовані в сучасних ОТС, неможлива без інформаційного забезпечення. Більшість процесів сучасної ОТС забезпечуються однією або декількома прикладними інформаційними системами корпоративного рівня з використанням корпоративної ІКМ або ІКМ загального використання.

Оскільки вимоги безпеки впливають на функціонування інфо-соціо-технічної інфраструктури ОТС, вони повинні бути відбиті в угодах про рівень сервісу (SLA — Service Level Agreement). Будь-яка подія, що може перешкодити виконанню вимог SLA, згідно [22] класифікується як «*інцидент*». Передбачається, що «*інцидент*» менш серйозний, ніж «*інцидент безпеки*», а «*інцидент ІБ*» є певним типом «*інциденту безпеки*». Термін «*інцидент безпеки*» визначений у [20] як злом, загроза, слабке місце та несправність системи безпеки, які можуть вплинути на безпеку організаційних ресурсів. Останній похідний термін «*інцидент ІБ*» визначається в [21, 23] як одинична небажана чи непередбачена подія ІБ (або сукупність таких подій), котра може скомпрометувати бізнес-процеси компанії або загрожує її ІБ.

Отже пропонується: ***першим кроком у прийнятті рішень щодо керування інцидентами ІБ повинна бути систематизація та включення до SLA визначень класів інцидентів.*** Завдання керування інцидентами ІБ у даному контексті — постійне забезпечення *критеріїв* і *показників* інформаційних процесів у ОТС на узгодженому рівні SLA. Втілення такого підходу під час прийняття рішень щодо керування інцидентами ІБ буде сприяти інтеграції аспектів ІБ в інфо-соціо-технічну інфраструктуру ОТС.

При цьому будемо вважати, що головне ***завдання*** дослідження полягатиме в розробці математично формалізованої моделі, яка дозволятиме в режимі реально-

го часу формувати функцію виділення підмножини оптимальних стратегій щодо вибору варіанта адаптивного динамічного розподілу та перерозподілу ресурсів у відповідь на інцидент ІБ. Методика реагування на інциденти ІБ повинна давати можливість динамічно в режимі реального часу прогнозувати, враховувати та адаптуватися до можливих інцидентів, змін у множині загроз і вразливостей.

Чинники, критерії, показники та складнощі

Інциденти ІБ спричинені багатьма зовнішніми чинниками (загрозами) та внутрішніми вразливостями сучасних інформаційних і телекомунікаційних технологій (обробки, зберігання, передачі інформації). Складний розподілений характер, багатомодульність, помилки та недоліки в програмно-апаратній архітектурі автоматизованих (інформаційних) систем обробки та зберігання даних, які для інформаційного обміну використовують транспортні послуги вразливих і не завжди достатньо захищених ІКМ, наприклад Internet, — створюють додаткові вразливості та можливості для реалізації загроз ІБ у вигляді інцидентів.

Крім того, розвиток високих технологій (Hi-Tech), таких як *нанотехнології, робототехніка, сенсорні мережі, радіочастотна ідентифікація, телебіометрія, штучний інтелект, інформаційна зброя, нові засоби впливу* тощо, — все це несе за собою ***нові проблеми, ризики, побічні негативні явища***. Тому, незважаючи на своє вирішальне значення для розвитку інформаційного суспільства, в найближчому майбутньому ІКМ виявляться слабо захищеними від зловживань, вторгнень, зовнішніх і внутрішніх впливів, стаючи ареною інформаційних війн, діяльності кіберзлочинців і Hi-Tech-хакерів. Для інформаційної та національної безпеки України це є особливо актуальним у зв'язку з відставанням нашої держави в критичних напрямках Hi-Tech.

За думкою відомого фахівця, одного з перших учених-дослідників у галузі ІБ — професора Ленса Хофмана (George Washington University, США): «*необхідно осучаснити як закони, методики, так і відповідні інститути в галузі керування інформаційними технологіями та ІБ*» [35].

Уже сам факт існування та постійної появи інцидентів ІБ є найбільш очевидним доказом актуальності проблеми захисту інформації та керування ІБ. Як цілеспрямований процес — керування інцидентами ІБ характеризується множиною *критеріїв* і *показників*. Головними комплексними критеріями є *якість, надійність і безпечність інформаційного обміну* [2, 3]. Можна виділити множину показників, пов'язаних з інцидентами (*кількісні* [10, 13, 27]: частота й кількість появи інцидентів, середній час реагування, відсоток успішно вирішених інцидентів, величина збитків; *якісні* [2, 15, 20–26]: термінологія, ступінь критичності, плин інциденту тощо).

Як один з найважливіших показників — постійне зростання *кількості* зареєстрованих інцидентів ІБ, зокрема в системах, які підключені до мережі Internet, відмічається [13], починаючи з 1998 року, причому темп приросту кількості інцидентів ІБ продовжує прискорюватися за останні роки швидше, ніж це було раніше. У той же час, заходи протидії не встигають за ростом кількості інцидентів. З цих спостережень робимо логічний висновок про недостатню ефективність існуючих підходів до захисту інформації та керування ІБ. Більшість дослідників [2, 13, 18] сходяться на думці, що й надалі, принаймні в найближчій перспективі, в гонці між атакуючою стороною та захисниками інформації випереджатимуть ата-

куючі. Такі невтішні тенденції спонукають вести пошук нових методів вдосконалення процесів реагування, обробки, розслідування та запобігання, які в сукупності складають *керування інцидентами ІБ*.

У чому недоліки існуючих підходів до керування інцидентами ІБ, у чому причини постійного погіршення становища, які заходи необхідно запровадити та які є можливості й передумови щодо його поліпшення?

Процес прийняття будь-якого рішення щодо керування інцидентами ІБ супроводжується попереднім аналізом альтернатив можливих варіантів. Під час аналізу альтернатив виникає необхідність розрахунку, порівняння, розподілу ресурсів ІБ. Якщо в процесі прийняття рішень, оцінки та вибору альтернатив в умовах невизначеності початкових даних і нечіткості постановки завдання — обов'язково буде вноситися додаткова некоректність, що збільшуватиме тим самим початкову невизначеність.

У дослідженнях [9, 11, 12, 36] доведено, що пряме використання традиційних математичних підходів, таких як апарат теорії ймовірностей, математична статистика, теорія систем масового обслуговування, теорія черг, марківські процеси, теорія телетрафіка, класичні методи багатокритеріальної оптимізації — на сьогодні не дає прийнятних результатів під час вирішення завдань ІБ. Причина тому — недостатній період спостереженнь за процесами, відсутність репрезентативних статистичних даних, невідповідність математичного інструментарію рівню складності, невизначеності й нечіткості досліджуваних процесів захисту інформації та керування ІБ.

Отже, розробку ефективної математично формалізованої та обгрунтованої методики підтримки прийняття рішень щодо керування інцидентами ІБ ускладнює ряд особливостей:

— недостатність знань про природу та структуру нових інцидентів ІБ;

— невизначеність законів розподілу ймовірностей появи інцидентів ІБ через нестохастичні чинники та непередбачувані умови їхнього здійснення;

— необхідність врахування надвеликої кількості неістотних на перший погляд чинників, які можуть суттєво вплинути на процес обробки інциденту ІБ;

— вирішальний вплив антропогенного фактору на процеси керування інцидентами ІБ;

— відсутність репрезентативної кількості інформації стосовно інцидентів ІБ;

— недостатньо тривалий період спостережень за інцидентами ІБ;

— отримання необхідної інформації виявляється складним, трудомістким або навіть неможливим завданням;

— множина загроз, що можуть спричинити інцидент ІБ, постійно розширюється й динамічно змінюється, причому швидшими темпами, ніж множина засобів захисту;

— еволюційний розвиток ІТМ у напрямку конвергентності, мультисервісності, гетерогенності, використання технологій, які значально не створювались як захищені та безпечні (наприклад IPv4, Bluetooth), призводить до збільшення складності систем і спричиняє виникнення нових вразливостей.

Загальні принципи автоматизації підтримки прийняття рішень

Керування інцидентами ІБ є проблемою, яку необхідно вирішувати не перманентно, а постійно мати в полі уваги як послідовний безперервний процес, що ди-

мічно протікає в режимі реального часу на всіх етапах життєвого циклу ОТС або ІКМ, починаючи з розробки вимог безпеки та складання технічного завдання на проектування комплексної системи захисту інформації (КСЗІ), технічної експлуатації, наступної модернізації та вдосконаленнями, і не закінчуючи, а й надалі продовжуючи на наступних життевих циклах.

Організація процесу керування інцидентами ІБ без використання засобів ***автоматизації*** являє собою складне й трудомістке завдання. Необхідно збирати та консолідувати надвелику кількість даних у різних форматах, вести централізований архів. Для ручної обробки даних щодо подій та інцидентів ІБ потрібна велика кількість висококваліфікованих фахівців-аналітиків. Через великий обсяг рутинної роботи обробка подій найчастіше буває неповною, що не відбиває всього змісту поточної ситуації. Може статися, що інциденти ІБ, критичні для надійного й захищеного функціонування системи, виявляються поза полем зору аналітиків, і через це не приймаються відповідні превентивні заходи.

Під час проектування інтелектуальної системи підтримки прийняття рішень (ІСППР) щодо керування інцидентами ІБ потрібно дотримуватися деяких уже встановлених ***загальних принципів*** побудови інтелектуальних систем керування [37] будь-якими об'єктами та процесами в особливих ситуаціях.

Доцільно взяти до уваги результати досліджень у суміжних проблемних галузях. У [38] для збору, реєстрації та обробки інформації щодо екстремальних станів ТМ пропонується впроваджувати інтегровану систему, дається її загальна структура та оптимізований алгоритм виконання запитів. У [39] визначається перелік завдань, що їх здатна виконувати ІСППР під час експлуатації та ремонту засобів і комплексів зв'язку. Підхід до створення моделі візуалізації параметрів складних систем під час нештатних ситуацій пропонується в [40].

В якості одного зі шляхів зменшення витрат на створення, експлуатацію й модернізацію КСЗІ в ТМ, у [5] запропоновано на всіх етапах життєвого циклу використовувати методи штучного інтелекту, зокрема ІСППР, нечіткі мережі Петрі та нечіткі нейронні мережі.

Для того, щоб розробник, проектувальник, оцінювач або інженер мали можливість приймати дійсно раціональні рішення, що будуть технічно, математично й економічно обґрунтованими, доцільно створити ІСППР. При створенні ІСППР повинні бути розроблені: сукупність математичних моделей функціонування об'єкта (ОТС або ІКМ), модель представлення знань та алгоритм виводу в ІСППР, сукупність критеріїв оцінки ефективності керування інцидентами ІБ, методика оптимізації розподілу ресурсів ІБ. ІСППР також повинна забезпечувати функції верифікації та тестування, отримання нових знань на основі даних моніторингу та аудиту, адаптивного керування інцидентами ІБ в ОТС.

Функції інтелектуальної системи підтримки прийняття рішень у рамках процесного підходу ISO/IEC та моделі PDCA

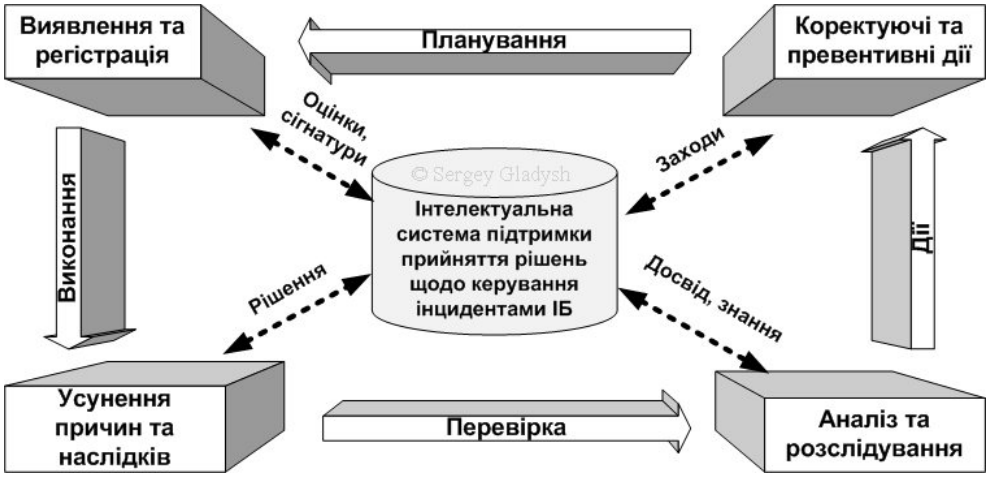
Неможливо в рамках окремого проектного підходу врахувати всі наявні методологічні рекомендації щодо керування інцидентами ІБ, і цілком ймовірно, що найбільш ефективним для окремої ОТС або ІКМ може бути використання якої-небудь іншої методології, в тому числі й розробленої самостійно. Але на думку автора доцільно, щоб будь-яка використовувана методологія була ***сумісна*** з відпо-

відними міжнародними стандартами ISO [20–23].

Сертифікація систем керування інцидентами вітчизняних ОТС за ISO/IEC 27001 [21] могла би підвищити ступінь їхньої привабливості та надійності для іноземних інвесторів і партнерів. Враховуючи це, будемо використовувати стандарти ISO/IEC [20–23] та інші як методологічні засади для створення системи керування інцидентами ІБ, яка б цілком вписувалася та була б логічним продовженням уже існуючих і сертифікованих систем керування бізнес-процесами ОТС, зокрема, таких як система технічної експлуатації та система менеджменту якості ISO 9001. Якщо в ОТС уже впроваджено системи менеджменту у відповідності до стандартів ISO 9001 та ISO 14000, то доцільно забезпечити виконання вимог стандарту ISO 27001 [21] у рамках існуючих систем менеджменту.

Стандарти ISO серій 9000, 14000, 20000, 27000 описують правила створення систем керування різними процесами та гармонійно поєднуються один з одним. Усі вони, як основу керування підконтрольними процесами, використовують процесний підхід, що розглядає керування як процес, а саме як набір взаємозалежних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, що витрачені для цього. Стандарти зазначених серій використовують єдину модель PDCA як структуру життєвого циклу всіх процесів системи менеджменту.

Уже ставши класичною, модель безперервного поліпшення процесів, одержала назву від циклу Шухарта–Деминга — PDCA (Плануй, Plan — Виконуй, Do — Перевіряй, Check — Дій, Act). Доцільно, щоб алгоритм роботи ІСППР щодо керування інцидентів ІБ ТМ також вписувався в цикл моделі PDCA (див. рисунок).



Функціональна схема ІСППР щодо керування інцидентами ІБ

Виявлення та реєстрація інциденту. Оперативні дані сенсорів безпеки повинні аналізуватися та оцінюватися на предмет наявності сигнатур відомих інцидентів за допомогою бази знань ІСППР. Після чого кожний адміністратор, користувач чи співробітник повинен одержати інструкцію, що визначатиме, які повинні бути його дії. Звіт про виявлення та реєстрацію інциденту ІБ в ОТС повинен містити докладний опис інциденту, перелік залучених співробітників, прізвище співробітника, що зафіксував інцидент, дату виникнення та реєстрації.

Усунення причин, наслідків інциденту і його розслідування. ІСППР на підставі звіту повинна надавати інструкцію щодо усунення причин і наслідків інциденту ІБ, включаючи опис загальних заходів, які необхідно розпочати, та конкретні дії для кожного інциденту ІБ, а також терміни, протягом яких варто усунути наслідки та причини інциденту ІБ. Варто розробити класифікацію інцидентів ІБ — визначити рівні критичності інцидентів, описати інциденти кожного рівня й терміни їхнього усунення.

Під час розслідування інциденту ІСППР повинна надавати інформаційно-аналітичну підтримку у вигляді досвіду та знань, що містять у собі визначення винних у виникненні інциденту, збір доказів, визначення дисциплінарних стягнень тощо.

Коригувальні та превентивні дії. Після усунення наслідків інциденту й відновлення нормального функціонування бізнес-процесів ОТС, доцільно виконати дії щодо запобігання повторного виникнення інциденту ІБ. Для визначення необхідності реалізації таких дій ІСППР повинна провести аналіз ризиків, у рамках якого визначити доцільність коригувальних і превентивних дій.

Для того щоб процедура виконувалася правильно й ефективно, всі ці етапи повинні безупинно й послідовно повторюватися.

Висновки

Таким чином, у статті розглянуто завдання підтримки прийняття рішень під час інцидетів ІБ в ОТС, яке можна розглядати як частину більш загальної проблеми підтримки прийняття управлінських рішень у кризових ситуаціях. У ході вирішення даного завдання визначено головні чинники, критерії і показники автоматизованих процедур підтримки прийняття рішень щодо керування інцидентами ІБ.

Організація процесу керування інцидентами ІБ без використання засобів автоматизації являє собою складне й трудомістке завдання. Розробку формалізмваної методики підтримки прийняття рішень щодо керування інцидентами ІБ ускладнює ряд особливостей, про які йдеться мова в даній статті. Однак все ж таки можна визначити загальні принципи, якими зможе користуватися розробник такого классу ІСППР.

Першим кроком у прийнятті рішень щодо керування інцидентами ІБ повинна бути систематизація та включення до SLA визначень класів інцидентів. Пропонується постійно осучаснювати як закони, методики, так і відповідні інститути в галузі керування інформаційними технологіями та ІБ.

Запропоновано функціональну схему ІСППР щодо керування інцидентами ІБ в ОТС. Дана схема цілком вписується в модель PDCA та процесний підхід, визначений у відповідних міжнародних стандартах ISO/IEC.

1. *Додонов О.Г., Путятін В.Г., Валетчик В.О.* Інформаційно-аналітична підтримка прийняття управлінських рішень у кризових ситуаціях // Реєстрація, зберігання і оброб. даних. — 2006. — Т. 8, № 1. — С. 37–54.

2. *Гладиш С. В., Кононович В. Г., Тардаскін М. Ф.* Розподіл відповідальності щодо реагування та обробки інцидентів безпеки в інформаційно-телекомунікаційній мережі загального користування // Зв'язок. — 2007. — № 8. — С. 28–31.

3. *Колобов С.О.* Концепція створення та забезпечення функціонування інфраструктури захисту державних інформаційних ресурсів в інформаційно-телекомунікаційних системах // Computer World. — 29.07.2002. — № 33(377). — http://www.dstszi.gov.ua/dstszi/control/uk/publish/article?art_id=38814&cat_id=38712

4. *Гладиш С. В.* Формування вимог щодо безпеки державних інформаційних ресурсів у телекомунікаційній мережі загального користування // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2007. — № 14. — С. 33–40.

5. *Гладиш С.В.* Інтелектуальна система керування інцидентами інформаційної безпеки телекомунікаційних мереж // Матеріали міжнародної науково-практичної конференції «Інформаційні технології та інформаційна безпека в науці, техниці та освіті ІНФОТЕХ-2007». — Севастополь: СевНТУ, 2007. — С. 53–57.

6. *Gladysh S.* Decision Support System on Telecommunications Security Incidents Response and Handling // Збірник тез доповідей першої Міжнародної науково-практичної конференції «Методи та засоби кодування, захисту й ущільнення інформації». — Вінниця: ВНТУ, 2007. — С. 65–66.

7. Постанова Кабінету Міністрів України № 250 від 7 квітня 1995 р. «Про Програму створення Урядової інформаційно-аналітичної системи з питань надзвичайних ситуацій».

8. Електронний ресурс. Режим доступу: — http://www.ipri.kiev.ua/ukr/index.php?id=/rozrobki/uiasns/index

9. *Гладыш С.В.* Представление знаний об управлении инцидентами информационной безопасности посредством нечетких временных раскрашенных сетей Петри // Інформаційні технології та комп'ютерна інженерія. — 2008. — № 1 (у друці).

10. *Гладиш С.В. Кононович В.Г.* Реагування та обробка інцидентів інформаційної безпеки мультиагентною системою // Наукові праці Одеської національної академії зв'язку ім. О.С. Попова. — 2007. — Вип. 2 (у друці).

11. *Гладыш С.В.* Иммунная мультиагентная система управления инцидентами информационной безопасности // Информация & Безопасность. — 2008. — № 1 (у друці).

12. *Гладыш С.В.* Иммунокомпьютинг в управлении инцидентами информационной безопасности // Искусственный интеллект. — 2008. — № 1. — С. 123–130.

13. *Howard J.* An Analysis of Security Incidents on the Internet. — CERT/CC, 2000. Електронний ресурс. Режим доступу: http://www.cert.org/research/JHThesis/Start.html.

14. *Гладиш С.В., Кононович В.Г., Тардаскін М.Ф.* Порівняльний аналіз стандартів ISO/IEC та української нормативної бази в частині керування інцидентами інформаційної безпеки // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. — 2007. — № 15. — С. 31–39.

15. *Gladysh S.* Distribution of responsibility on telecommunication incidents in Ukraine // Матеріали ІІІ Міжнародної науково-практичної конференції «Інформаційні технології в наукових дослідженнях і навчальному процесі», Луганськ: ЛНПУ, 2007.

16. *Мелехин И.* Управление инцидентами // Jet Info. — 2006. — № 7. — Електронний ресурс. Режим доступу: http://www.jetinfo.ru/2006/7/3/article3.7.2006.html

17. *Куканова Н.* Управление инцидентами информационной безопасности // Открытые системы. — 2006. — № 10. — Електронний ресурс. Режим доступу: http://www.osp.ru/os/2006/10/3910101/_p1.html

18. *Голов А.* Реагирование на инциденты информационной безопасности // Intelligent Enterprise. — 2005. — № 22. — Електронний ресурс. Режим доступу: http://www.topsbi.ru/default.asp?artID=807

19. *Гладиш С.В.* Реагування та обробка інцидентів інформаційної безпеки в мережі GSM // Вісник Державного університету інформаційно-комунікаційних технологій. — 2008. — № 1. — С. 58–72.

20. ISO/IEC 17799:2005. Information Technology. Security Techniques. Code of Practice for Information Security Management.

21. ISO/IEC 27001:2005. Information Technology. Security Techniques. Information Security Management Systems. Requirements.

22. ISO/IEC 20000:2005. Information Technology. Service Management. — Part 2: Code of Practice.

23. ISO/IEC TR 18044:2004. Information Technology. Security Techniques. Information Security Incident Management.

24. ITU-T E.409 Recommendation. Organization on Security Incidents Response and Handling: Guide for Telecommunication Companies. — Geneva, 2004.

25. *Brownlee N., Guttman E.* Expectations for Computer Security Incident Response. (RFC 2350, BCP 21). — The Internet Society, 1998. — http://www.ietf.org/rfc/rfc2350.txt?number=2350

26. *Grance T., Kent K., Kim B.* Computer Security Incident Handling Guide. (NIST SP 800-61). - Recommendations of the National Institute of Standards and Technology. — U.S. Department of Commerce, 2004. — http://csrc.nist.gov/publications/nistpubs/800-61/sp800-61-pdf.zip

27. *Dorofee A., Killcrece G., Ruefle R., Zajicek M.* Incident Management Capability Metrics. Version 0.1. Technical Report CMU/SEI-2007-TR-008. — CMU, 2007. — 221 p.

28. Порядок захисту державних інформаційних ресурсів у інформаційно-телекомунікаційних системах. — Затв. наказом ДСТСЗІ СБУ № 76 від 24.12.2001 р. — 4 с.

29. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» № 2594-IV від 31.05.2006. — 3 с.

30. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено постановою КМУ від 29.03.2006 р. № 373. — 4 с.

31. Порядок взаємодії органів виконавчої влади з питань захисту державних інформаційних ресурсів в інформаційних та телекомунікаційних системах. Затв. постановою КМУ від 16.11.2002 р. № 1772. Із змінами, внесеними згідно з Постановою КМУ від 08.12.2006 р. № 1700. — 2 с.

32. Постанова КМУ від 29.06.2004 р. № 812. Деякі питання оперативно-технічного управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану.

33. *Кільчицький Є.В., Колченко Г.Ф., Слюсар В.О., Смирнова О.В.* Знову про оперативно-технічне управління телекомунікаційними мережами в умовах надзвичайних ситуацій, надзвичайного та воєнного стану // Вісник УБЕНТІЗ. — 2004. — № 2. — С. 15–19.

34. Офіційний сайт Державної служби спеціальних телекомунікаційних систем і захисту інформації. Електронний ресурс: «Біла книга Держспецзв'язку». — http://www.dstszi.gov.ua/dstszi/. — 47 с.

35. Електронний ресурс. — http://www.seas.gwu.edu/~lanceh/writings.html

36. *Малюк А.* Информационная безопасность: концептуальные и методологические основы защиты информации. — М.: Горячая линия – Телеком, 2004. — 280 с.

37. Интеллектуальные системы управления организационно-техническими системами / Под ред. проф. А.А. Большакова. — М.: Горячая Линия – Телеком, 2006. — 160 с.

38. *Коробко В.В., Скоропаденко А.П., Задоя Г.М., Вовк В.М.* Интегрированная система сбора информации об экстремальных состояниях телекоммуникационных сетей и их защиты // Зв'язок. — 2004. — № 1. — С. 39–45.

39. *Сакович Л.М., Політов В.І.* Використання системи підтримки прийняття рішення під час експлуатації та ремонту засобів і комплексів зв'язку // Зв'язок. — 2000. — № 5. — С. 37–39.

40. *Єрохін А.Л.* Модель візуалізації нештатних подій у складних інформаційних системах // Зв'язок. — 2005. — № 6. — С. 52–56.

Надійшла до редакції 20.12.2007