УДК 004.056:004.891 **Гнатюк С.О., Хохлачова Ю.Є., Охріменко А.О., Гребенькова А.К.**

ТЕОРЕТИЧНІ ОСНОВИ ПОБУДОВИ ТА ФУНКЦІОНУВАННЯ СИСТЕМ УПРАВЛІННЯ ІНЦИДЕНТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У цій статті, на основі аналізу наукових джерел, міжнародних та вітчизняних стандартів і рекомендацій, зроблено спробу систематизації принципів та формалізації процедур розробки систем управління інцидентами інформаційної безпеки. Також, на базі часткових узагальнень, визначено фази життєвого циклу інцидентів та наведено компоненти типової системи управління інцидентами інформаційної безпеки. Крім того, показано номенклатуру європейських груп реагування на інциденти інформаційної безпеки CERT/CSIRT.

Ключові слова: інцидент інформаційної безпеки, управління інцидентами, група реагування на інциденти інформаційної безпеки, система управління інцидентами інформаційної безпеки.

Вступ. Управління інцидентами є однією з найважливіших процедур управління інформаційною безпекою (ІБ). У бібліотеці кращих ІТ-практик ITIL під поняттям *«інцидент»* розуміється будь-яка подія, що не є елементом нормального функціонування певного сервісу і при цьому впливає, або здатна вплинути, на роботу цього сервісу шляхом його переривання або зниження якості. Відповідно до діючих міжнародних та вітчизняних стандартів у галузі управління інцидентами інформаційної безпеки (УІІБ) [1, 2], першим і найважливішим кроком є своєчасне та коректне усунення наслідків інциденту. Далі, необхідно розслідувати інцидент, виконати оцінку необхідності дій щодо усунення причин інциденту, якщо потрібно – реалізувати їх, а також виконати дії щодо попередження повторного виникнення інциденту (превентивні заходи). Окрім цього, важливо зберігати всі дані про інциденти ІБ, адже за допомогою статистики інцидентів можна визначити найбільш актуальні загрози для організації і, відповідно, максимально точно планувати заходи щодо підвищення рівня захищеності інформаційно-комунікаційних систем (ІКС) організації. Саме цей факт, на нашу думку, і визначає актуальність побудови та дослідження ефективності роботи систем управління інцидентами інформаційної безпеки (СУІІБ).

Метою дослідження є висвітлення основних процедур та процесів, пов’язаних із організацією та супроводженням систем менеджменту інцидентів інформаційної безпеки.

Основна частина. Відповідно до [3] *УІІБ* – це процес або набір процесів, на вхід яких подаються дані, отримані в результаті збору і протоколювання даних про події, що стосуються ІКС, а на виході цих процесів одержують інформацію про причини інциденту, що відбувся, про збиток, нанесений організації, і заходах, які необхідно прийняти для того, щоб інцидент не повторився. Таким чином, УІІБ спрямовано на вдосконалення системи забезпечення безпеки організації. Крім того, вихідні дані є, по суті, єдиним об'єктивним параметром у визначенні ймовірності реалізації загроз при аналізі ризиків. *Ефективність процесу УІІБ* залежить від: координації і узгодженості дій всіх залучених до нього осіб; наявних можливостей з отримання та аналізу інформації, пов'язаної з інцидентом; оперативності та коректності отриманих результатів. Підвищення кожного з наведених показників помітно підвищить ефективність всього процесу і, тим самим, дозволить підрозділу ІБ організації набути більш значних результатів. Використовуючи СУІІБ можна радикально змінити ситуацію щодо ефективності управління інцидентами. Таким чином, СУІІБ фактично буде системою колективної роботи, яка автоматизує процеси з УІІБ за допомогою інтеграції людей і апаратно-програмного забезпечення моніторингу і захисту, а також інформаційної інфраструктури організації.

Припущення про те, що в організації стався інцидент ІБ, має базуватися на трьох основних чинниках [3]: 1) Повідомлення про інцидент ІБ надходять одночасно з декількох джерел (користувачі, IDS, файли журналів тощо); 2) IDS сигналізують про багаторазове повторення певних подій; 3) Аналіз файлів журналів автоматизованої системи (АС) дає підставу для висновку про можливість настання інциденту.

У загальному випадку, *ознаки інциденту* поділяються на дві основні категорії – повідомлення про те, що *інцидент відбувається в даний момент* і повідомлення про те, що *інцидент, можливо, відбудеться у майбутньому.*

Прийняття рішення про настання інциденту багато в чому залежить від компетентності експертів команди реагування. Вони мають чітко відрізняти випадкову помилку оператора, наприклад, від зловмисного цілеспрямованого впливу на ІКС. У документах [4, 5] наведено основні принципи організації та функціонування команд (груп) реагування на інциденти ІБ CERT/CSIRT, а рис. 1 містить перелік і місцерозташування діючих команд CERT/CSIRT за даними Європейського агентства з питань мереж та ІБ [6].

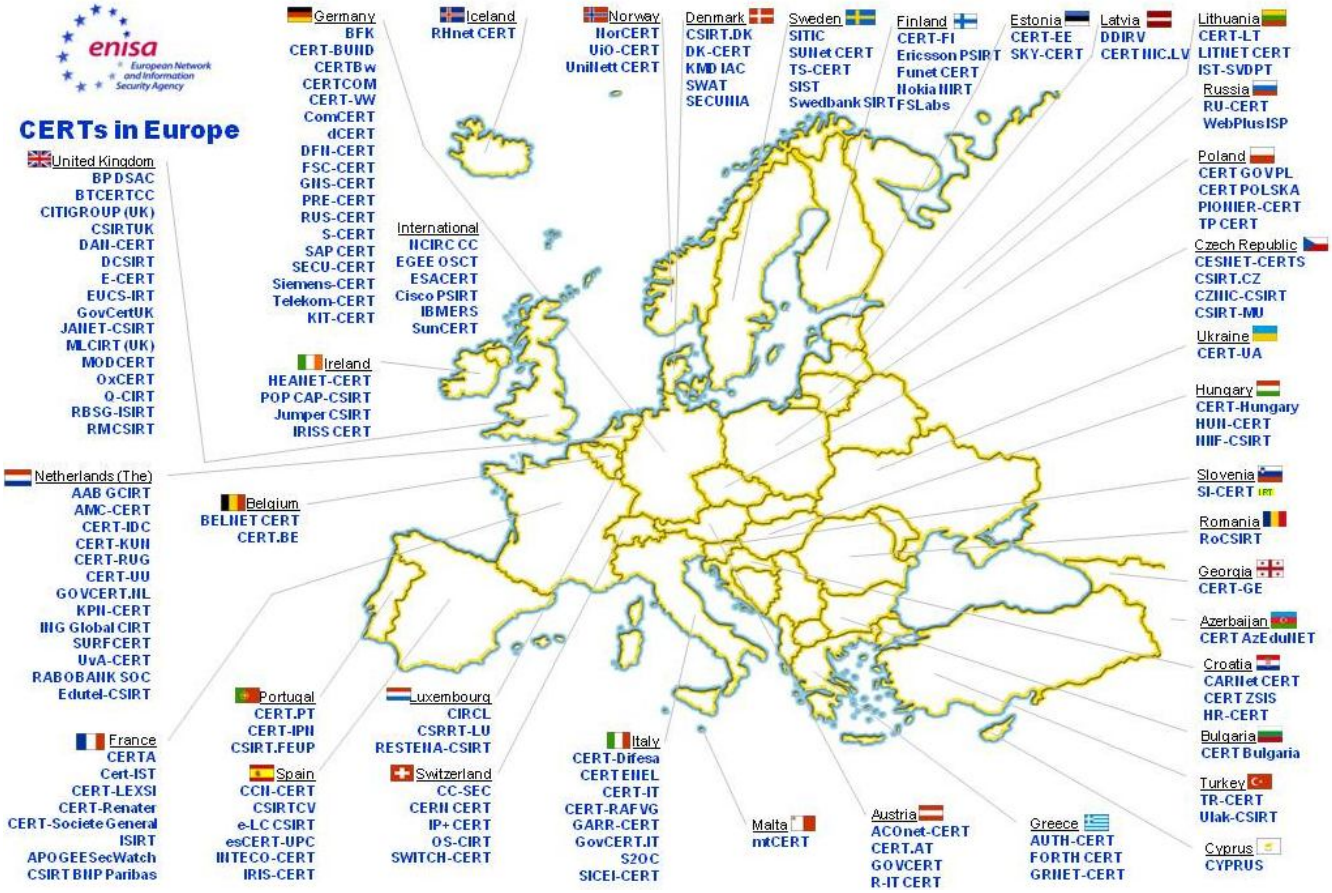

Рис.1. Мережа європейських команд CERT/CSIRT

Як показав проведений аналіз [1, 2, 7], сьогодні у міжнародній практиці розроблено достатню кількість нормативних документів різного характеру (стандарти, рекомендовані практики, керівництва тощо), що регламентують питання УІІБ. Відповідно до [3] для ефективного УІІБ необхідно організувати комплекс процесів управління інцидентами, забезпечити його належними ресурсами, відповідною нормативно-розпорядчою і робочою документацією, технічними засобами забезпечення механізмів контролю. Для обробки подій та інцидентів ІБ необхідно організувати *процес реагування на інциденти.* Потім слід розробити необхідні нормативні документи щодо управління інцидентами. Як правило, такі документи повинні описувати: 1) Визначення інциденту ІБ – перелік подій, що є інцидентами (тобто, що саме в цій організації є інцидентом ІБ); 2) Порядок сповіщення відповідальної особи про виникнення інциденту (необхідно визначити формат звіту, а також відобразити контактну інформацію осіб, яких слід оповіщати про інцидент); 3) Порядок усунення наслідків і причин інциденту; 4) Порядок розслідування інциденту (визначення причин інциденту, винних у виникненні інциденту, порядок збору і збереження доказів); 5) Внесення дисциплінарних стягнень; 6) Реалізація корегуючих і превентивних заходів.

У рамках СУІІБ необхідно збирати і обробляти велику кількість подій ІБ, які надходять з різних джерел. Ці події мають бути приведені до єдиного вигляду, що дозволяє застосовувати єдині алгоритми обробки та безпомилкового виділення з них саме інцидентів ІБ. Необхідно зберігати події ІБ протягом часу, достатнього для забезпечення розслідування інцидентів. Потрібно розробити архітектуру СУІІБ, спроектувати комплекс рішень, що

реалізують дану архітектуру, вибрати комплекс технічних засобів, здійснити впровадження системи. При розробці технічних рішень необхідно враховувати особливості функціонування інфраструктури інформаційних технологій (ІТ-інфраструктури) організації, наявні засоби автоматизації тощо. Для ефективного функціонування СУІБ необхідно, на стадії впровадження, забезпечити ряд ключових чинників. У першу чергу, система управління має бути забезпечена вхідним потоком подій ІБ, що адекватно відображає стан в рамках обраної області дії. При виявленні і реагуванні на інцидент, необхідно мати дані щодо задіяних ресурсів (активів), їх власників і ступінь критичності, а також мати доступ до даних про події, що вплинули на інцидент ІБ, таких як дані аудиту дій користувачів і адміністраторів. При наданні звітності про інциденти керівництву, необхідно мати можливість зіставлення ресурсів, що підпали під вплив в результаті інциденту і ризиків для основних бізнес-процесів організації.

Відповідно до [3] *роботи з впровадження СУІБ пропонується проводити у декілька етапів:* обстеження об'єкту; розробка процедур та процесів системи управління, написання відповідних документів; впровадження СУІБ; впровадження АС моніторингу й управління інцидентами ІБ. Для візуалізації результатів аналізу подій, що відбуваються в інформаційній системі, використовується складання діагностичних матриць. Матриця формується з рядків потенційних ознак інциденту та стовпців – типів інцидентів. Дається оцінка події за шкалою пріоритетів – «високий», «середній», «низький». Діагностична матриця покликана документувати хід логічних висновків експертів в процесі прийняття рішення і, поряд з іншими документами, служить свідченням розслідування інциденту. *При аналізі інцидентів ІБ організація повинна виконати такі дії:* своєчасно ідентифікувати невдалі та успішні порушення і інциденти ІБ; допомогти у виявленні подій безпеки, таким чином запобігти інцидентам безпеки шляхом використання індикаторів. *Управління інцидентами ІБ повинно включати такі дії:* повідомлення про уразливі місця ІКС та події ІБ; відповідальність і процедури; навчання на інцидентах ІБ; збір доказів. Документування подій інциденту ІБ необхідне, перш за все, для збору і консолідації технологічних та операційних свідчень розслідування. Документуванню підлягають усі факти та докази зловмисного впливу, типовою практикою є ведення журналу розслідування інциденту, який не має стандартної форми і розробляється командою CERT/CSIRT.

Архітектура типової СУІБ має включати такі основні компоненти [3, 8, 9]: інтеграційну платформу; апаратно-програмні засоби моніторингу і аудиту; апаратно-програмні засоби захисту інформації; сховище інформації про інциденти ІБ; аналітичні інструменти і засоби генерації звітів; засоби управління та користувацькі інтерфейси. *Інтеграційна платформа* є ядром системи, вона покликана забезпечувати чітку і оперативну координацію та взаємодію осіб, що відповідають за реакцію на події, пов'язані з інцидентами ІБ. *Апаратно-програмні засоби моніторингу і аудиту* – засоби, що реалізують функції з протоколювання, збору, накопичення та обробки інформації функціонування ІКС організації. Вони складають підсистему збору інформації про інциденти ІБ. Результатом їх роботи є дані, на основі яких системою приймається рішення щодо настання інциденту. *Апаратно-програмні засоби захисту в контексті СУІБ* – засоби, які забезпечують локалізацію інцидентів або зниження збитку. Ці засоби мають механізми, що дозволяють проводити швидку і дистанційну зміну своєї конфігурації або мати в своєму складі наперед розроблені автоматизовані сценарії дій з мінімізації можливого збитку від інцидентів ІБ. Також, в організації повинна бути розроблена та впроваджена система сповіщення про інциденти.

Узагальненою метою забезпечення ІБ організації є зниження ризиків, діючих відносно інформаційних ресурсів, і як наслідок запобігання або мінімізація збитку від можливих інцидентів ІБ. *Основною задачею процесу УІБ* є усунення інцидентів в гранично стислі терміни. У ході процесу управління інцидентами ІБ проводиться виявлення, реєстрація, класифікація і початкова підтримка запитів, а також пошук рішення, його застосування, контроль, інформування і підготовка звітності. Оскільки, як ми вже визначили, інцидентом, в першу чергу, є певна недозволена подія, то вона має бути кимось заборонена. Отже, існує

необхідність розробки та затвердження документів, що чітко описують всі дії, які можна виконувати в ІКС і які виконувати заборонено.

Однією з кращих СУІБ серед присутніх на вітчизняному ринку є програмний продукт для обробки подій – *netForensics nFX Open Security Platform* [3], зображений на рис. 2:

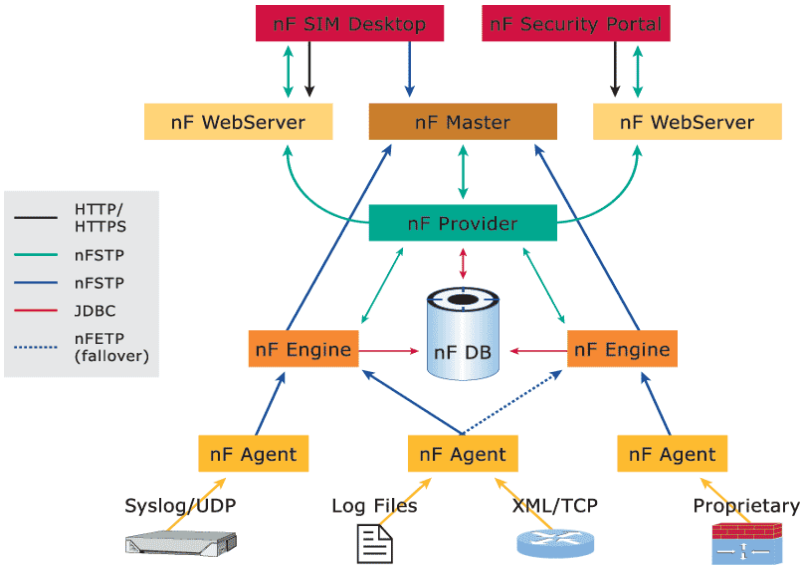

Рис. 2. СУІБ netForensics

Система netForensics призначена для роботи з гетерогенним середовищем продуктів забезпечення ІБ і реалізує безперервний збір, обробку та відображення подій безпеки. Система може працювати на платформах Windows, Linux або Solaris, використовуючи в якості сховища даних повнофункціональну СУБД Oracle. Ця СУІБ має широкі можливості щодо роботи в розподіленому режимі, підтримку різних відмовостійких конфігурацій тощо. СУІБ netForensics реалізована на базі технології Java за модульним принципом. Основними модулями системи є сервер додатків (реалізує основну логіку обробки подій, представлення даних, взаємодії з користувачами); база даних (забезпечує зберігання інформації, що надходить до системи); модуль кореляції (здійснює кореляцію зібраних даних); модуль автоматизації УІБ (здійснює автоматизацію процесів УІБ); агенти (збирають інформацію безпосередньо з пристроїв). До складу системи також входять засоби щодо написання агентів збору даних з нестандартних систем захисту, засоби формалізації користувацьких правил кореляції і створення звітів.

Для опису *процедури УІБ* відповідно до [1, 9, 10] можна використати класичну модель безперервного поліпшення процесів, що отримала назву від *циклу Шухарта-Демінга – модель PDCA (плануй – «Plan», виконуй – «Do», перевіряй – «Check», дій – «Act»).* Стандарт [1] описує модель PDCA як основу функціонування всіх процесів системи управління інформаційною безпекою. Ця модель об'єднує 4 взаємозв'язані процеси: розробка, впровадження, моніторинг і розвиток. *Життєвий цикл системи управління* буде визначатись такими стадіями: *1) Планування і підготовка.* Здійснюється розробка схеми УІБ, розробка і затвердження ряду організаційно-регламентуючих документів, виділення людських і матеріальних ресурсів, проведення необхідного навчання та апробація обраної схеми управління. *2) Експлуатація.* Здійснюється виявлення та ідентифікація інциденту ІБ, реагування, розслідування й аналіз. *3) Аналіз.* Здійснюється аналіз системи управління інцидентами інформаційної безпеки, виявляються ділянки щодо поліпшення та міри з поліпшення. *4) Поліпшення.* Реалізуються рекомендації, розроблені на етапі аналізу. Загалом, ця процедура регулюється стандартом [1], що прийшов на зміну BS 15000:2002, який, у свою чергу, взяв за основу бібліотеку ITIL. Слід зазначити, що всі стандарти ISO/IEC серій 9000, 14000, 20000, 27000 та ін., що описують правила створення систем управління різними процесами, гармонійно поєднуються один з одним, і в якості основи управління підконтрольними процесами використовують *процесний підхід,* який розглядає управління як

процес, тобто як набір взаємозв'язаних безперервних дій. Процесний підхід акцентує увагу на досягненні поставлених цілей, а також на ресурсах, витрачених для цього.

Процес УІІБ, як правило, покладається на службу ІТ-підтримки, яка обробляє інциденти ІБ (у випадку, якщо така служба існує в організації). Це ще раз доводить факт доцільності розробки єдиної системи управління всіма процесами в компанії, так як управління подібними процесами в різних галузях її діяльності часто виконується за однією схемою. Варто також розуміти, що УІІБ не попереджує нанесення збитку компанії, проте розслідування інциденту ІБ та своєчасне впровадження превентивних і корегуючих заходів знижує ймовірність його рецидиву. Робота організації без СУІІБ може обернутися рядом неприємностей. У результаті впровадження процесу управління проблемами організація отримує такі важливі і *корисні властивості* як якість сервісів, скорочення числа інцидентів та безперервне функціонування. В умовах зростання впливу ІТ на діяльність сучасних організацій, значна увага приділяється організації підтримки та супроводу ІТ-систем. Світовий досвід щодо управління ІТ-організаціями та їх взаємодією із замовниками описаний у, згаданій раніше, бібліотеці ITIL. Вона містить комплекс необхідних для побудови СУІІБ рекомендацій. По-перше, в ITIL з певним ступенем деталізації описаний *процес управління безпекою (Security Management)*. По-друге, надання ІТ-послуг, включаючи сервіси ІБ, відноситься до відповідальності служб ІТ та ІБ організацій. Для ефективного розслідування інцидентів ІБ необхідні не просто диференційований інструментарій, а *спеціалізований уніфікований комплекс таких інструментів,* так званий *toolkit.* Необхідність дотримання вимог стандартів, а також законів щодо проведення розслідувань, накладає певні складності у роботі слідчих, приводить до нагромадження неструктурованих даних, а також збільшує витрати на проведення розслідування. Все це стало підґрунтям розробки інтегрованих спеціалізованих наборів інструментів для проведення розслідувань, що включають в себе такі можливості як аналіз смартфонів, мобільних телефонів, розподілені обчислення, планування задач тощо. Тобто, основними вимогами, для ефективного проведення розслідувань інцидентів, мають бути інтегрованість всіх інструментів, розподілення обчислень, оперування великими об’ємами даних без збоїв, оперативне виявлення спроб вторгнення та вразливих місць ІКС, можливість розширення функціоналу, створення деталізованих звітів, швидкий доступ до пов’язаних даних, а також можливість взаємодії з іншими групами CERT/CSIRT. Також, для підвищення ймовірності ідентифікації зловмисника, відстеження активності та виявлення його істинних намірів слід проводити аналіз мережевої активності та здійснювати візуалізацію інформаційних потоків.

Висновки. Таким чином, аналіз науково-методичних та нормативно-правових джерел показав необхідність та дозволив систематизувати теоретичні засади розробки СУІІБ. У роботі також визначено фази життєвого циклу інциденту ІБ та наведено компоненти типової СУІІБ. Ефективне функціонування останньої дозволить акумулювати інформацію щодо інцидентів ІБ, категоризувати їх та визначити найбільш актуальні загрози і, як результат, максимально ефективно впроваджувати превентивні заходи, що дасть можливість підвищити рівень захищеності ІКС організації в цілому.

ЛІТЕРАТУРА

1. Information technology. Security techniques. Information security incident management (ISO 18044:2004) : ГОСТ Р ИСО/МЭК 18044:2004. — [Чинний від 2008-07-01]. — М. : Федеральное агенство по техническому регулированию и метрологии 2007. — 50 с. — (Нац. стандарт РФ).

2. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою (ISO/IEC 27002:2005, MOD) ГСТУ СУІБ 2.0/ISO/IEC 27002:2010. — [Чинний від 2010-07-01]. — К.: Національний банк України 2010. — 163 с. — (Галузевий стандарт України).

3. Звіт «Розробка та впровадження типових рішень щодо комплексної системи захисту інформації в АІС НАНУ» (КСЗІ АІС НАНУ): Система управління інцидентами інформаційної безпеки. Керівництво адміністратора. 05540149.90000.043.ИЗ-06. — К.: НАН України 209. — 149 с.

4. Пошаговое руководство по созданию CSIRT (Европейское агентство по сетевой и информационной безопасности (ENISA) в рамках программы WP-2006), 2006. — 86 с.

5. Moira J.W.-B. Handbook for Computer Security Incident Response Teams (CSIRTs) / Moira J.W.-B., Stikvoort D., Kossakowski K.-P. et al. — Pittsburgh, 2003. — 223 p.

6. European Network and Information Security Agency [Electronic resource] : ENISA. — Electronic data. — Heraklion, Greece: ENISA, [04.02.2012]. — Mode of access: World Wide Web. — URL: http:// www.enisa.europa.eu. — Description based on screen.

7. Організація щодо реагування на інциденти та обробка інцидентів безпеки: Керівництво для організації електрозв'язку. Рекомендація МСЭ-Т Е.409 (ITU-T E.409. — [Чинне від 2004-28-05]. — Женева. — 22 с. — (Рекомендація Міжнародної організації телекомунікацій (ITU)).

8. Кононович В.Г. Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Ч. 4. Інформаційна безпека комунікаційних мереж та послуг. Реагування на атаки. Навчальний посібник / В.Г. Кононович, С.В. Гладиш. — Одеса : ОНАЗ ім. О.С. Попова, 2009. — 208 с.

9. Модель підсистеми моніторингу інцидентів безпеки інформації в інформаційних системах організацій / І.А. Пількевич, В.І. Котков, Н.М. Лобанчикова, І.І. Сугоняк // Восточноевропейский журнал передовых технологий. — 2012. — № 2 (56). — С. 18–21.

10. Гладиш С.В. Підтримка прийняття рішень щодо керування інцидентами інформаційної безпеки в організаційно-технічних системах / Гладиш С.В. // Реєстрація, зберігання і обробка даних. — 2008 — Т. 10, № 1. — С. 116–124.

Надійшла 01.02.2012

Рецензент: д.т.н., проф. Корченко О.Г.