УДК 004.056

В.Д. Хох, Є.В. Мелешко, О.А. Смірнов

Центральноукраїнський національний технічний університет, Кропивницький

ДОСЛІДЖЕННЯ МЕТОДІВ АУДИТУ СИСТЕМ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ

В роботі розглянуто поняття аудиту інформаційної безпеки, його цілі, ініціатори, принципи, фази та методи. Проведено дослідження сучасних методів аудиту систем управління інформаційною безпекою.

Ключові слова: *аудит інформаційної безпеки, системи управління інформаційною безпекою, інформаційна безпека, інформаційні технології, комп'ютерні системи та мережі.*

Вступ

Важко уявити собі сучасний бізнес, який би не підтримувався певною інформаційною системою. Зараз навіть малий бізнес опирається на інформаційні технології, використовуючи їх можливості для комунікації з постачальниками, фінансових транзакцій, ведення фінансової звітності, реклами та багато іншого. Середній та великий бізнес все частіше розгортають особисті інфраструктури, необхідні безпосередньо для здійснення підприємницької діяльності. Наприклад, для взаємозв'язку водіїв таксі з диспетчерами. Зростає ринок Інтернет-магазинів, найбільші з яких віддають перевагу розгортанню своєї інфраструктури серверів, ніж залишатися клієнтами хостинг-компаній.

Разом із збільшенням можливостей до розгортання особистих інформаційних систем: збільшенням доступності їх компонентів та із підвищенням загальної освіченості у галузях інформаційних технологій – зростає і кількість «чуттєвої» інформації, що циркулює Інтернетом або інтранетом певних компаній. Ті ж самі умови призводять і до все більшої розгалуженості інфраструктури систем та їх ускладнення. Контролювати їх стає все складніше, на плечі адміністраторів цих систем лягає все більша кількість обов'язків, і все важче стає відслідковувати джерела нових, потенційних проблем. Процеси управління такими системами та підтримка їх працездатності також ускладнюються.

Метою даної статті є дослідження основних методів проведення аудиту систем управління інформаційною безпекою.

1. Класифікація методів аудиту інформаційної безпеки

Поняття аудиту використовується у багатьох галузях людської діяльності. Розглянемо загальні відомості про процес аудиту, згодом виділивши характерні особливості для процесу аудиту систем управління інформаційною безпекою.

Цілями проведення аудиту можуть бути [1]:

• Визначення ступеня відповідності системи менеджменту об'єкту до критеріїв аудиту.

• Визначення ступенів відповідності видів робіт та процесів методикам системи керування.

• Визначення відповідності нормативним документам та нормам системи керування.

• Визначення ефективності системи керування.

• Визначення шляхів поліпшення системи керування.

Окрім цілей, аудити можливо поділити за сторонами-ініціаторами проведення аудиту. Згідно з міжнародним стандартом ISO 19011:2011 [2] їх три:

• *Аудит першої сторони* – ініціатором проведення аудиту є сама організація.

• *Аудит другої сторони* – ініціатором проведення є партнери організації або зацікавлені у діяльності організації інші організації.

• *Аудит третьої сторони* – ініціатором проведення виступають треті сторони, не задіяні у функціонуванні організації, наприклад, регулюючі органи або органи сертифікації.

У [2] надається визначення: аудит – це систематичний, незалежний та документований процес отримання доказів (свідоцтв) аудиту та об'єктивного їх оцінювання, для визначення ступеня їх відповідності критеріям аудиту. Також у [2] визначаються деякі додаткові терміни, необхідні, на думку авторів, для розуміння цього процесу, а саме:

• *Критерії аудиту* – сукупність політик, методик або вимог, що використовуються як еталон, який порівнюється з свідоцтвами (доказами) аудиту.

• *Свідоцтва аудиту* – протоколи, факти або інша інформація, яка стосується критеріїв аудиту і може бути перевірена.

• *Дані аудиту* – результати оцінки свідоцтв аудиту за критеріями аудиту.

• *Висновок аудиту* – результат аудиту, після розгляду всіх даних аудиту з врахуванням його цілей.

Визначення, що дані у [2] є дуже гнучкими і можуть бути інтерпретовані та адаптовані для тої галузі, де буде організоване проведення аудиту.

Більш специфічні для галузі захисту інформації у комп'ютерних мережах та системах визначення даються у [3]. Тут дається наступне визначення процесу *оцінки інформаційної безпеки* – це процес визначення того, наскільки ефективно сутність, що

оцінюється, відповідає певним вимогам захищеності. І виділяється три типи методів такої оцінки – тестування, експертиза та інтерв'ю.

• *Тестування* – це процес виконання одного або декількох оціночних завдань за певних умов для порівняння очікуваної (заявленої) поведінки оцінюваної сутності з реальною.

• *Експертиза* – це процес перевірки, інспектування, розгляду, спостереження, вивчення або аналізу одного або більше об'єктів оцінки для полегшення розуміння, отримання роз'яснень та доказів.

• *Інтерв'ю* – це процес проведення співбесід задля отримання роз'яснень та відомостей про можливе розташування доказів (свідоцтв) з персоналом або окремими особами організації.

Легко помітити спільне у визначеннях, і хоча [2] використовує термін *аудит*, а [3] *оцінка інформаційної безпеки*, суть процесів полягає у оцінці відповідності об'єкту перевірки до вимог або критеріїв, що визначаються стосовно цього об'єкту. Така ж спільна риса у визначенні присутня і у [4]. Окрім цього [4] визначає п'ять цілей аудиту стосовно безпеки комп'ютерної системи:

1. Забезпечити огляд моделей доступу до окремих об'єктів, історії доступу конкретних процесів і окремих осіб, використання різних механізмів захисту, які підтримуються системою, їх ефективності.

2. Механізм аудиту повинен дозволити виявити спроби обходу механізмів захисту, як зі сторони внутрішніх користувачів системи, так і з боку зовнішніх.

3. Механізм аудиту повинен надавати можливість виявлення підвищення привілеїв користувача.

4. Механізм аудиту повинен діяти як стримуючий фактор проти спроб обійти механізм захисту системи.

5. Механізм аудиту має забезпечувати можливість фіксації діяльності правопорушника.

Окрім вищезгаданого існує серія стандартів ISO27k [5] [6], яка посилається на [2], і є, по-суті, системою управління інформаційною безпекою (СУІБ). В результаті співпраці міжнародного співтовариства, що активно використовує сімейство стандартів ISO27k – була створена директива [7]. У цій директиві, окрім, згаданих визначень з [2], надається визначення *аудиту системи управління інформаційною безпекою*, як аудиту, що орієнтується на системи керування інформаційною безпекою організації. А також виділяються три принципи аудиту, що характерні саме для аудиту СУІБ:

1. Загальні принципи аудиту залишаються важливими як, наприклад, незалежна оцінка відповідно до узгоджених критеріїв, а також більш специфічні принципи, що орієнтовані на аудит СУІБ.

2. Функція аудиту СУІБ не повинна залежати від області її застосування.

3. У розпорядженні аудитора СУІБ повинні бути актуальні дані стосовно організації (штатів, бізнес процесів, технологічних процесів), а також стосовно галузі інформаційної безпеки (наприклад, останні знайдені вразливості ПЗ).

То що ж є методами аудиту СУІБ? В [3] виділяється три методи аудиту – тестування, експертиза та інтерв'ю. В [4], окрім того, що визначається п'ять цілей, також визначаються критерії аудиту до систем класів C2, B2, B3, A1, до яких згідно з [8] повинен застосовуватись процес аудиту за критеріями [4]. Важливо те, що кожен з блоків вимог до кожної з систем поділяється на три розділи:

• події, що повинні бути об'єктами аудиту;

• інформація, яка піддається аудиту;

• підстави, за якими можуть бути обрані події для аудиту.

Це перекликається з методами, вказаними у [3], оскільки завданням тестування є спроба викликати певну подію або певну їх кількість для подальшого вивчення поведінки системи, а у першому розділі вимог вказується, які саме події повинні бути досліджені. Експертиза передбачає дослідження інформації, яка зібрана із системи, що визначається у другому пункті вимог до критеріїв аудиту у [4]. У третьому розділі вказуються підстави, за якими певна подія може бути додана до розгляду в рамках аудиту, а інтерв'ю є методом пошуку додаткових свідоцтв аудиту. У [7] виділяють шість фаз аудиту:

1. *Оцінка* – аудитори визначають основну площину аудиту та його області на основі інтерв'ю з ініціатором аудиту та експертизи документів.

2. *Планування* – загальний обсяг критеріїв аудиту розбивається на більш докладні частини, створюється план аудиту.

3. *Робота на місці* – збір аудиторських свідоцтв шляхом інтерв'ю з персоналом, експертизою документів та проведенням тестів.

4. *Аналіз* – вивчаються свідоцтва, що були зібрані під час роботи на місцях, визначаються можливі прогалини у плані аудиту.

5. *Звітування* – важлива фаза аудиту. Формується звіт, в якому відображається вся необхідна інформація.

6. *Завершення аудиту* – якщо аудит був ініційований третьою стороною, то СУІБ отримує необхідні дозволи та сертифікати. Окрім цього готуються документи з помітками для наступних аудитів.

Отже, як видно з описів кожної з фаз, інструменти, якими оперують аудитори незмінні: методи тестування; методи експертизи; методи інтерв'ю.

Розглянемо детально зазначені методи аудиту СУІБ та способи їх реалізації.

2. Методи тестування

Методи тестування полягають у виконанні одного або декількох оціночних завдань за певних умов, для порівняння очікуваної (заявленої) поведінки оцінюваної сутності з реальною.

Якщо розглядати метод тестування у розрізі [7], то він застосовується лише у третій фазі проведення аудиту – роботі на місці. У [7] метод тестування

пов'язують з суто технічним процесом, завдяки якому визначається правильність конфігурування інформаційних систем відносно політики інформаційної безпеки, стандартів та технічних керівництв. Також, вказується на можливість використання автоматизованих засобів перевірки та виявлення вразливостей системи і конфігурацій, але попереджається про те, що, незважаючи на підвищення швидкості цього процесу, є велика вірогідність того, що у звітах автоматизованих засобів буде і спотворена інформація, що обумовлено помилками у самих засобах.

У [3] тестування СУІБ поділяють на три групи:

• *Перегляд методів (технік).* Ця група тестів зосереджена на оцінці систем, додатків, мереж і процедур для виявлення вразливих місць і, як правило, проводяться вручну. Група включає у себе перегляд документації, лог-записів, набори правил (наприклад, брендмауеру), конфігурацій, сніфінг мережі, а також перевірку цілісності файлів.

• *Ідентифікація та аналіз технік.* Ці методи націлені на визначення систем, портів, сервісів і потенціальних вразливостей, можуть бути проведені вручну, але зазвичай використовуються автоматизовані засоби. Вони включають у себе ідентифікацію мережі, портів, сервісів, сканування на вразливості, сканування бездротової мережі та вразливостей застосунків.

• *Валідація вразливостей.* Ці техніки можуть бути застосовані із залученням автоматизованих засобів чи вручну, в залежності від техніки та рівня спеціалізації тест-команди. Цілями цієї техніки є злам паролів, тести на проникнення, соціальна інженерія та тестування застосунків на вразливості.

Варто зупинитися на останній групі, а саме на тестах на проникнення. Головним завданням тестів на проникнення є визначення вразливостей у контрольованих умовах, для того щоб їх можливо було позбутися до того, як ними скористуються зловмисники. Фахівці використовують тест на проникнення для вирішення проблем, пов'язаних з оцінкою ризиків, зосереджуючись на найнебезпечніших вразливостях [9]. Тестування на проникнення полягає у тому, щоб моделювати поведінку зловмисника, який намагається обійти засоби безпеки організації. Цей метод, зазвичай, включає застосування реальних атак на реальні системи та дані організації з використанням справжніх засобів, що застосовуються зловмисниками. Метод тестування на проникнення передбачає не лише технічні засоби, наприклад, під час тесту може бути прийнята спроба фізично дістатися носіїв даних чи викрасти їх [3]. Тестування на проникнення дає змогу зібрати необхідні для аудиту свідчення відповідності або невідповідності вимогам [10]. Існують три стратегії проведення тесту на проникнення [10]:

• *Чорна скринька.* Стратегія реалізується у випадку, коли у фахівця немає жодної інформації про ціль. В такому випадку він збирає інформацію з чистого листа, і проводяться усі дії та процедури, які б поводив реальний зловмисник.

• *Сіра скринька.* Фахівець має певну інформацію про ціль, але недостатню, що змушує його шукати далі.

• *Біла скринька.* Реалізується, коли фахівцю надають всю необхідну інформацію щодо цілі.

Тест на проникнення складається з трьох фаз: підготовка, тест, аналіз. Під час підготовки визначаються цілі та стратегії, у другій фазі виконується збір інформації про цілі, пошук та аналіз вразливостей, спроби використати вразливості, у випадку якщо вразливість використана вдало, тест переходить у фазу аналізу отриманих даних [9].

Окрім цього у групі з тестуванням на проникнення стоїть *соціальна інженерія*, вона передбачає використання соціальних навичок для отримання паролів, даних про кредитні картки або компромату. Методів соціальної інженерії багато, люди, що їх використовують надзвичайно винахідливі і швидко адаптуються. Цей метод використовує внутрішню природу людей, щоб маніпулювати ними і отримувати конфіденційну інформацію. Було визначено п'ять моделей переконання, які засновані на: простоті, цікавості, розбіжності, впевненості в собі і співпереживанні [11]. Навіть потужні системи безпеки не можуть протистояти цій загрозі, оскільки люди легко «ламаються», що робить їх телефони, комп'ютери, сторінки соціальних мереж легкими цілями, що у подальшому призводить до заражень або встановлення бекдорів у корпоративних мережах. Серед засобів протидії методам соціальної інженерії є поліпшення обізнаності робітників організації та їх підготовка в рамках інформаційної безпеки. А також формування грамотної політики безпеки, що робить методи експертизи та інтерв'ю не менш важливими, ніж методи тестування [12].

3. Методи експертизи

Методи експертизи полягають у перевірці, інспектуванні, розгляді, спостереженні, вивченні або аналізі одного чи більше об'єктів оцінки. Якщо завдяки методам інтерв'ю аудитор отримує дані про можливе існування свідоцтв аудиту від персоналу організації, а завдяки тестуванню перевіряє наявність свідоцтв – то метод експертизи дозволяє отримати інформацію про існування свідоцтв аудиту, найчастіше шляхом вивчення документації організації. Більш того, вивчення документації організації може вносити серйозні корективи у цілі аудиту. Одним з найважливіших документів організації, стосовно інформаційної безпеки, є документ політики безпеки.

Зазвичай, організація, що зацікавлена у забезпеченні інформаційної безпеки своєї інфраструктури, визначає вимоги до її забезпечення у документі політики безпеки організації. У цьому ж документі може визначатись і порядок проведення аудитів. Добре розроблена політика безпеки визначає, що необхідно зробити для забезпечення безпеки інформації організації і які заходи для цього необхідні. Політика також може складатися з документів високого рівня та до-

кументів низького, які визначають більш детально певні аспекти забезпечення безпеки інформації організації [14].

Згідно з ISO/IEC 27002:2005 [6] політика інформаційної безпеки повинна переглядатись у заплановані терміни або за появи істотних змін з метою забезпечення її актуальності. При розробці політики інформаційної безпеки необхідно враховувати не лише інтереси організації, а й інші нормативні документи та закони країни, в якій вона функціонує. Також у ній повинні бути відображені інциденти інформаційної безпеки, рекомендації уповноважених організацій і, звісно ж, – результати минулих аудитів.

Згідно з ISO/IEC 27001:2005 [5] документація організації повинна містити записи управлінських рішень. Дані документації повинні бути відтворювані та відображати зворотній зв'язок, тобто обрані заходи проаналізовано з точки зору результатів оцінки і процесу обробки ризиків. Також [5] визначає, які саме записи повинні бути у документації:

- Законодавчі положення щодо політики та цілей СУІБ.
- Визначення сфери застосування.
- Перелік процедур та заходів безпеки, що підтримується системою.
- Опис методології оцінки ризиків.
- Звіт та план оцінки ризиків.
- Положення щодо застосовності.
- Процедури, що необхідні для ефективного планування і контролю процесів СУІБ, а також опис вимірювання ефективності заходів безпеки.

У [7] процес вивчення документації, у тому числі політики безпеки, відноситься до першої фази – оцінювання, під час якої аудитори визначають основну площину аудиту та його області. Також процес експертизи документації згадується як типовий процес для першої частини фази роботи на місці.

Окрім вищезгаданих документів, організація може розробити правила безпечної роботи [13]. Це документ, в якому зібрані всі необхідні користувачам правила. Він складається з фрагментів правил всієї організації і відображає обов'язки користувачів у галузі інформаційної безпеки. Правила безпечної роботи повинені бути чіткими і короткими, а сам документ, в ідеалі, складатися з декількох сторінок.

У [8] для деяких систем передбачаються чіткі керівництва щодо того що, як, ким і коли повинно бути задокументовано. Такі дані мають велику цінність для аудиторів у тому числі і тому що це дозволяє проводити аудит певного проміжку часу. Окрім цього, такий підхід до ведення документації дозволяє частково автоматизувати процес аудиту [15], [16]. У спеціальній публікації NIST [4] були внесені зміни щодо інформації, яка підлягає аудиту.

Окрім цього, метод експертизи може бути застосовано відносно лог-записів. Лог-записи можливо поділити на дві групи: лог-записи систем безпеки та записи операційної безпеки. Лог-записи можуть зберігати широкий спектр різноманітної інформації про події. В рамках аудиту лог-записи використовуються як додатковий матеріал [17].

4. Методи інтерв'ю

Завданням методів інтерв'ю є збір інформації про можливе розташування свідоцтв аудиту, роз'яснення певної поведінки системи, роз'яснення щодо процесів організації шляхом опитування персоналу організації.

Інформаційна безпека – це не лише питання технологій та процесів, вона пов'язана і з людьми, і тому не можна автоматизувати кожен її аспект [18]. Варто зауважити, що найчастіше спеціалісти з інформаційної безпеки вказують на персонал як на найслабкішу ланку в інформаційній безпеці.

У [2] наголошується на необхідності проведення наради на самому початку проведення аудиту, обов'язково з головуванням лідера групи аудиту (якщо аудит проводить група). На цій нараді, бажана, якщо вона доцільна, присутність всіх або певної частини персоналу, який відповідає за об'єкти організації, що проходять аудит або частково залучені у проведенні аудиту. Нараду слід проводити за присутності керівництва організації. Необхідно надати можливість задавати питання учасникам наради. Під час фази збору даних група аудиту повинна розглядати інформацію, яка отримана шляхом інтерв'ю, з такої позиції, що враховуватись повинна лише та інформація, яку точно можливо перевірити. У ISO/IEC 27001:2005 [5] в розділі про відповідальність керівництва зазначається, що організація повинна забезпечити, щоб весь персонал, для якого встановлено визначені в СУІБ відповідальності, був компетентним для виконання необхідних завдань. Така вимога, що визначена у стандарті, сама по собі може стати об'єктом аудиту, а у випадку, якщо компанія приймає відповідний стандарт або країна, в якій функціонує організація прийняла цей стандарт як державний, то аудит третьої сторони обов'язково буде включати перевірку компетентності персоналу, для отримання відповідних сертифікатів або дозволів з боку регулюючих органів.

У [4] пропонується розділити персонал, який залучено у користуванні СУІБ, на дві категорії – системні адміністратори та користувачі. До того ж, у разі проведення внутрішніх аудитів або у випадку, коли аудит має постійний характер – у ролі аудитору виступає сам системний адміністратор. В такому випадку завданням інтерв'ю буде збір даних про використання системи, роз'яснень щодо певних подій та певної діяльності користувачів у системі.

У [19] розглядається п'ять категорій персоналу – старший, керування СУІБ, програмні та функціональні менеджери, постачальники технологій, користувачі. Кожній з категорій відповідає своя роль у системі безпеки та свої обов'язки. Тут же звертається увага на небезпеку з боку "ображених" співробітників та комерційного шпіонажу. Виявити потенційну загрозу такого роду можливо, якщо компанія постійно веде внутрішній аудит.

Висновки

В процесі вивчення документів [2, 5-8], стає зрозумілим, що незалежно від різної термінології, яка в них використовується, основна мета аудиту СУІБ – систематичне та якомога більш повне визначення актуального стану СУІБ та його відповідності вимогам. Для досягнення цієї мети використовуються різноманітні методи, їх можна розділити на три групи – методи тестування, експертизи та інтерв'ю. Методи інтерв'ю охоплюють область, яка стосується персоналу організації і дозволяють визначити рівень кваліфікації персоналу та отримати додаткову інформацію, яка може бути критично важливою для процесу аудиту. Методи експертизи дозволяють сформувати загальну картину стану СУІБ, знайти критично важливі вузли системи. Методи тестування дозволяють ефективно перевірити адекватність системи, здатність її працювати як в рамках штатного режиму, так і в режимі атак. Методи тестування дають змогу визначити прогалини у СУІБ, про які не було зазначено в документації, а персонал про них міг і не здогадуватись. Така класифікація методів аудиту дає змогу більш чітко визначати ті роботи, які необхідно провести в рамках певного аудиту. До того ж такий підхід до класифікації методів аудиту дає змогу розглядати способи автоматизації процесу аудиту системи управління інформаційною безпекою, визначити джерела інформації для системи автоматизації та джерела зворотного зв'язку, а також області впливу системи автоматизації.

Список літератури

1. Teck-Heang L. The evolution of auditing: An analysis of the historical development / L. Teck-Heang, A. Azham. // Journal of Modern Acc. and Auditing. – 2008. – №12. – P. 1-8.

2. ISO 19011:2011 Guidelines for auditing management systems (Міжнародний стандарт)

3. Scarfone K. Technical Guide to Information Security Testing and Assessment: Recommendations of the National Institute of Standards and Technology (NIST Special Publication 800-115) / K. Scarfone, M. Souppaya, A. Cody, A. Orebaugh. – Gaithensburg: NIST, 2008. – 80 p.

4. A Guide to Understanding Audit in Trusted Systems – Fort Feorge G. Meade: Nat. comp. security center, 1987.– 25 p.

5. ISO/IEC 27001:2005 Information technology – Security techniques – Information security management systems – Requirements (Міжнародний стандарт).

6. ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management (Міжнародний стандарт)

7. ISMS Auditing Guideline // ISO27k Forum. – 2008. – №1. [Електр. ресурс]. – Режим доступу: http:// www.iso 27001security.com/ISO27k_Guideline_on_ISMS_audit_v1.docx.

8. Trusted computer system evaluation criteria, 1985. – (Department of defense standard).

9. Bacudio A. An overview of penetration testing / A. Bacudio, Y. Xiaohon, C. Bei-Tseng. // Int. Journal of Network Security & Its Appl. (IJNSA). – 2011. – №6. – P. 19-38.

10. Tewai A. Evaluation and Taxonomy of Penetration Testing / A. Tewai, K. M. Arun. // International Journal on Recent and Innovation Trends in Computing and Communication. – 2015. – №3. – P. 5297-5302.

11. Greavu-Şerban V. Social Engineering a General Approach / V. Greavu-ŞErban, O. Şerban. // Informatica Economică. – 2014. – №18. – P. 5-14.

12. Conteh N.Y. Cybersecurity: risks, vulnerabilities and countermeasures to prevent social engineering attacks / N.Y. Conteh, P.J. Schmick. // International Journal of Advanced Computer Research. – 2016. – №6. – P. 31-38.

13. Бармен С. Разработка правил информационной безопасности / Скотт Бармен // М.: Издательский дом "Вильямс", 2002. – 208 с.

14. Tuyikeze T. An Information Security Policy Development Life Cycle / T. Tuyikeze, D. Pottas. // Proceedings of the South African Information Security. – 2010. – P. 165-176.

15. Tsudik G. AudES – An Expert System for Security Auditing / G. Tsudik, R. Summers. // IAAI-90 Proceedings. – 1990. – P. 221-232.

16. Sodiya A. S. An Expert System-based Site Security Officer / A. S. Sodiya, O. Adeniran, R. Ikuomola. // Journal of Computing and Information Technology – CIT. – 2007. – №15. – P. 227-235.

17. Karen K. Guide to Computer Security Log Management / K. Karen, M. Souppaya. // Computer Security Division Information Technology Laboratory National Institute of Standards and Technology. – 2006.

18. Montesino R. Information security automation: how far can we go? / R. Montesino, S. Fenz. // Sixth Int. Conf. on Availability, Reliability and Security. – 2011. – P. 280-285.

19. Guttman B. An Introduction to Computer Security: The NIST Handbook / B. Guttman, R. A. Edward. – Gaithersburg, MD 20899-0001: National Institute of Standards and Technology, 1995. – (U.S. Government printing office).

Надійшла до редколегії 30.01.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

ИССЛЕДОВАНИЕ МЕТОДОВ АУДИТА СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

В.Д. Хох, Е.В. Мелешко, А.А. Смирнов

В работе рассмотрено понятие аудита информационной безопасности, его цели, инициаторы, принципы, фазы и методы. Проведено исследование современных методов аудита систем управления информационной безопасностью.

Ключевые слова: *аудит информационной безопасности, системы управления информационной безопасностью, информационная безопасность, информационные технологии, компьютерные системы и сети.*

RESEARCH OF METHODS OF AUDITING INFORMATION SECURITY MANAGEMENT SYSTEMS

V.D. Khokh, E.V. Meleshko, O.A. Smirnov

In this paper we considered the concept of information security audit, its objectives, initiators, principles, phases and methods. Modern methods of auditing information security management systems were researched.

Keywords: *information security audit, information security management system, information security, information technology, computer systems and networks.*