праці / Ю. Маршавін // Україна: аспекти праці. – 2006. – № 1. – С. 26–29.

4. Капелюшников Р. Структура российской рабочей силы: особенности и динамика / Р. Капелюшников // Вопросы экономики. – 2006. – № 10. – С. 19–40.

5. Гільорме Т.В. Інноваційні зрушення у кваліфікаційно-професійному складі регіонів: регіональний аспект / Т.В. Гільорме // Економічний вісник національного гірничого університету. – 2004. – № 1(5). – С. 17–23.

6. Caroleo F.E. The European Labour Market. Regional dimensions (AIEL Series in Labour Economics) / Floro Ernesto Caroleo, Sergio Destefanis. – Mörlenbax: Physica-Verlag HD A Springer Company, 2006. – 341 p.

7. Anderton R. Globalisation and the Labour Market. Trade, technology and less-skilled workers in Europe and the United States/ Robert Anderton, Paul Brenton, John Whalley. –New York: Routledge, 2004. – 193 p.

8. Atkinson T., Cantillon B., Marlier E., Nolan B. Social indicators. The EU and social inclusion / Tony Atkinson, Bea Cantillon, Eric Marlier, Brian Nolan. – New York: Oxford University press inc., 2002. – 240 p.

9. Cobet Aaron E. Comparing 50 Years of Labor Productivity in U.S. and Foreign Manufacturing / Aaron E. Cobet, Gregory A. Wilson // Monthly Labor Review. – 2002. – Num. 6. – Pp. 51–65.

10. Fleck S. International comparisons of hours worked: an assessment of the statistics / Susan Fleck // Monthly Labor Review. – 2009. – Num. 5. – Pp. 3–31.

11. Sawchuk P. Labour perspectives on the new politics of skill and competency formation: International reflections / Peter Sawchuk //Asia Pacific Education Review. – 2008. – Vol. 9. – Num. 1. – Pp.50–62.

12. OECD Employment Outlook. Boosting jobs and incomes. – Paris: OECD, 2006. – 281 p.

13. Klaus F. Zimmermann. European Labour Mobility: Challenges and Potentials / F. Klaus // De Economist, Springer. – 2005. – Vol. 153. – Num. 4. – Pp.425–450.

14. Bijak J. Population and labour force projections for 27 European countries, 2002-052: impact of international migration on population ageing / Jakub Bijak, Dorota Kupiszewska, Marek Kupiszewski, Katarzyna Saczuku, Anna Kicinger // European Journal of Population. – 2007. – Vol. 23. – Num. 1. – Pp.1–31.

15. Labour market outlook. Quarterly survey report. Summer 2009. Focus: migrant workers. – London: CIPD, 2009. – 15 p.

16. Raynor J. Comparative civilian labor force statistics, 10 countries: a visual essay / Jennifer Raynor // Monthly Labor Review. – 2007. – Num. 12. – Pp. 32-37.

17. ДК 003:2005 Національний класифікатор України. Класифікатор професій // Українська інвестиційна газета. – травень 2006р. – № 19.

18. Довідник кваліфікаційних характеристик працівників. Випуск 23. Загальні професії хімічних виробництв, затверджений Наказом Міністерства промислової політики України від 15.04.2008 № 229.

19. Довідник кваліфікаційних характеристик професій працівників. Випуск 1. Професії працівників, що є загальними для всіх видів економічної діяльності. Розділ 1. Професії керівників, професіоналів, спеціалістів та технічних служблвців / Уклад. Я. Кавторєва. – 5-те вид., перераб. і доп. – Харків: Фактор, 2007. – 384 с.

РОЗРОБКА ТА ДОСЛІДЖЕННЯ МЕТОДИКИ ПЕРЕДПРОЕКТНОГО АУДИТУ НА ОСНОВІ ЧИННОЇ НОРМАТИВНОЇ ДОКУМЕНТАЦІЇ

О.М. Данілін, *студент*

Керівник: **О.Є. Архипов,** *д.т.н., професор*

Фізико-Технічний інститут Національного технічного університету України «Київський політехнічний інститут»

В даній доповіді розглянута методика передпроектного аудиту. Дана методика розроблена на основі чинних стандартів (як українських, так і міжнародних) у галузі інформаційної безпеки. Ціль розробки даної методики – побудова послідовності дій, згідно яких може бути проведена процедура аудиту типового об'єкта щодо побудови комплексу засобів захисту інформації. Методика визначає послідовність проведення передпроектного аудиту та представлення його результатів. Комбінація вимог нормативних документів проведена на основі існуючих у них припущень і визначення області та характеру їх дії

Проведення передпроектного аудиту є однією з найважливіших умов побудови комплексу засобів захисту інформації (КЗЗІ). Результатом його проведення є технічне завдання, згідно якого і будується КЗЗІ. Передпроектний аудит дає можливість оцінити всі вимоги до КЗЗІ на стадії його розробки і врахувати можливі впливи (як зовнішні, так і внутрішні) на об'єкт аудиту.

Методика передпроектного аудиту розроблена на основі чинної нормативної документації. Вона вирішує питання поєднання вимог і рекомендацій стандартів у галузі, внаслідок чого не суперечить жодному з них. За основні її положення обрано комбінацію положень з нормативної документації технічного захисту інформації (НД ТЗІ), ГОСТ Р ИСО/МЭК та ISO/IEC. Дана комбінація побудована при умові обмеження витрат (з економічної точки зору та з точки зору використаного часу) на саму процедуру проведення аудиту.

Перш за все специфікується типовий об'єкт дослідження. Визначаються структурні складові даного об'єкта, способи взаємодії між ними, а також межі проведення процедури аудиту для даного об'єкта. Для побудови моделі об'єкта доцільно використовувати дані з технічних характеристик його складових.

Після визначення типового об'єкту дослідження будується модель порушника. Вона повинна відображати максимальний рівень можливостей порушника щодо реалізації його дій на даному типовому об'єкті. Для цього доцільно скористатися існуючими класифікаторами характеристик порушника. Можливості порушника доцільно вважати максимальними для того, щоб врахувати всі його можливості щодо реалізації загроз щодо інформаційно-телекомунікаційної системи (ІТС) через її вразливості.

Наступним етапом є оцінка активів типового об'єкта. Згідно рекомендацій ISO/IEC FDIS 27005 методикою передбачене використання 26 критеріїв оцінювання активів. Внаслідок застосування методики до типового об'єкта виникає необхідність введення вагових коефіцієнтів для врахування важливості кожного з критеріїв для даного об'єкта. Найбільш зручним способом визначення вагових коефіцієнтів для критеріїв є використання методу аналізу ієрархій, сутність якого викладена в [8]. Всі критерії розбиваються на три категорії: вплив на технічні засоби, вплив на людей, вплив на репутацію та інші нематеріальні цінності. У кожній категорії визначаються вагові коефіцієнти для кожного з критеріїв і, враховуючи вагові коефіцієнти кожної категорії, обчислюється загальні вагові коефіцієнти. Після їх отримання всі активи оцінюються за спеціально введеною шкалою з урахуванням вагових коефіцієнтів для критеріїв.

На основі отриманих оцінок активів приймається рішення щодо введення базового рівня захищеності (згідно ГОСТ Р ИСО/МЭК 13335). Маючи базовий рівень захищеності, визначається перелік засобів захисту, які задовольняють вимогам цього рівня, згідно існуючих каталогів засобів захисту.

Для всіх систем, захищеність яких потребує додаткових засобів, проводиться детальний аналіз ризиків.

Спочатку будується модель загроз. Для ідентифікації загроз можна використовувати існуючі у нормативних документах та довідкових матеріалах переліки загроз, а також попередній досвід організації. Загрози мають наступні характеристиками, які встановлюють їх взаємозв'язок з іншими компонентами безпеки: джерело (внутрішні або зовнішні), мотивація, частота виникнення, правдоподібність, шкідливий вплив. Деякі загрози можуть вражати не один вид активів. У цьому разі загрози можуть завдавати збитки в залежності від того, які саме активи пошкоджені.

Навколишні умови і соціальне середовище, в яких функціонує організація, можуть мати велике значення і суттєво впливати на ставлення до загроз й активів. Деякі загрози в організаціях можуть

взагалі не розглядатися. Коли мова йде про загрози, необхідно враховувати вплив зовнішнього середовища.

Після побудови моделі загроз будується модель існуючих засобів захисту. Побудова моделі існуючих засобів захисту необхідна для аналізу можливості реалізації загроз через існуючі вразливості. Для її побудови використовуються наступні джерела: документація по засобам захисту. попередній досвід, порівняння з іншими засобами захисту, попередні результати аудиту.

Наступним етапом є побудова моделі вразливостей. Пов'язані з активами вразливості включають в себе слабкості фізичного носія, організації, процедур, персоналу, управління, адміністрування, апаратного/програмного забезпечення або інформації. Загрози можуть використовувати уразливості для нанесення збитку ІТС або цілям бізнесу. Уразливість може існувати і за відсутності загрози. Вразливість сама по собі не завдає шкоди, але це є тільки умовою або набором умов, що дозволяє загрозі впливати на активи. Слід розглядати уразливості, що виникають з різних джерел, наприклад, внутрішніх і зовнішніх по відношенню до конкретного активу. Уразливість може зберігатися, поки сам актив не зміниться так, щоб уразливість вже не змогла проявитися. Вразливість необхідно оцінювати індивідуально і в сукупності, щоб розглянути ситуацію, що склалася в цілому.

У конкретній системі або організації не всі уразливості відповідають загрозам. У першу чергу слід зосередитися на вразливостях, яким відповідають загрози. Але в силу того, що навколишнє середовище може непередбачувано змінюватися, необхідно вести моніторинг всіх вразливостей для того, щоб вчасно виявляти ті з них, які можуть використовувати нові загрози.

Оцінка вразливостей – це перевірка слабкостей, які можуть бути використані існуючими загрозами. Ця оцінка повинна враховувати навколишнє середовище і існуючі захисні заходи. Мірою вразливості конкретної системи або активу по відношенню до загрози є ступінь того, з якою легкістю системі або активу може бути завдано шкоди.

Вразливості можуть бути ідентифіковані в наступних сферах: організація, процеси та процедури, порядок управління організацією, персонал, фізичне середовище, конфігурація ІТС, програмне та апаратне забезпечення, залежність від третіх сторін. Для ідентифікації загроз використовуються спеціальні довідники (у відповідній сфері) та попередній досвід організації.

Після побудови всіх цих моделей проводиться аналіз ризиків з урахуванням введеного базового рівня захищеності. Корисним апаратом для аналізу ризиків є побудова повної групи подій для загроз, вразливостей і цінності активів. На основі такої характеристики ризиків для даного типового об'єкту робиться висновок щодо введення додаткових засобів захисту і визначення найбільш критичних для системи її компонентів. Ці компоненти потребують найбільшого рівня захищеності.

Результатом застосування методики є сформований набір вимог безпеки для даного об'єкта, на основі якого існує можливість побудови профілю захищеності або завдання безпеки. Важливим моментом у застосуванні методики є чітке визначення меж проведення дослідження на етапі специфікації типового об'єкта. При невірному визначенні меж можуть бути не враховані вразливості системи і загрози, а в протилежному випадку їх кількість може бути занадто великою, що викликатиме додаткові витрати (матеріальні і нематеріальні) на застосування методики.

Загальна схема розробленої методики має наступний вигляд (рис. 1).

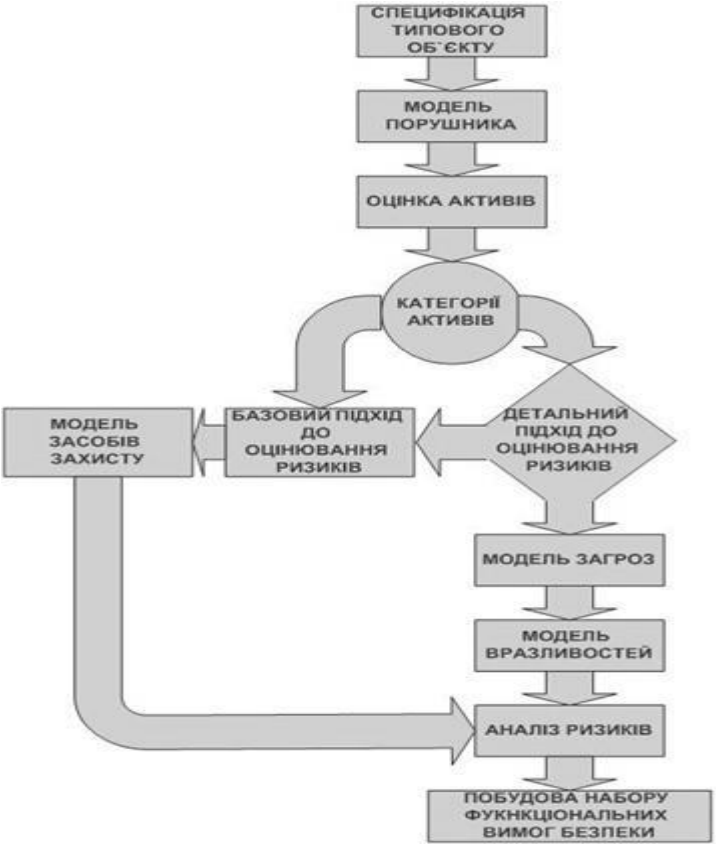

Рис. 1. Методика передпроектного аудиту типового об'єкта щодо побудови комплексу засобів захисту інформації

РОЛЬ ІНФОРМАЦІЙНИХ РЕСУРСІВ У РОЗВИТКУ ПІДПРИЄМСТВА

С.П. Дунда, *старший викладач*
Національний університет харчових технологій, м. Київ

Розглянуто джерела виникнення інформаційних ресурсів підприємства. Визначено вплив інформаційних ресурсів на ефективність діяльності підприємства

Наявність інформації передбачає розвиток підприємства. Діяльність підприємства багато в чому залежить від інформованості його персоналу і керівництва та здатності ефективно використовувати інформацію. Кожна дія підприємства базується на управлінських рішеннях, яким, в свою чергу, передує проведення великої роботи по збиранню, обробці та аналізу необхідної інформації.

Інформація обертається в економіці як ресурс і товар. З найбільш загальних позицій інформаційний ресурс може бути визначений як сукупність накопиченої інформації, зафіксованої на матеріальному носії в будь-якій формі, що забезпечує її передачу у часі та просторі для рішення наукових, виробничих, управлінських та інших задач [1, с. 9]. Інформаційні ресурси займають все більш важливе положення поряд з іншими ресурсами підприємства. Інформаційні ресурси пов'язані з функціями управління, тож по відношенню до фінансових, природних, матеріальних, трудових та інших ресурсів підприємства інформація грає об'єднуючу роль.

Для роботи підприємства важливе значення має економічна інформація, оскільки безпосередньо пов'язана з управлінням соціально-економічними процесами та персоналом у виробничій та невиробничій сферах. Характеристиками економічної інформації є [2, с. 15]:

- великі обсяги;