УДК 004.056.3

Хорошко В.О., Хохлачова Ю.Є.

ОСОБЛИВОСТІ ОЦІНКИ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

У даній статті приведені задачі сучасних методів роботи з аналізу ризиків інформаційної безпеки, проектування і супроводу систем безпеки; різновид аналітичних і консалтингових робіт в області інформаційної безпеки об'єкта. Розглянуто етапи життєвого циклу інформації з позиції цільової ознаки ІС з метою відокремлення вразливих ланок трансформації, котрі потребують захисту.

Розроблено модель інформаційної безпеки, яка являє собою сукупність об'єктивних зовнішніх і внутрішніх факторів та їх вплив на стан інформаційної безпеки на об'єкті і на збереження матеріальних чи інформаційних ресурсів. На базі запропонованої моделі можна обґрунтовано вибрати та обґрунтувати систему контрзаходів, що знижує ризики до припустимих рівнів, які мають найбільшу цінову ефективність.

Ключові слова: захист інформації, безпека інформаційних систем, модель побудови системи інформаційної безпеки, життєвий цикл інформації, аналіз ризиків інформаційної безпеки.

Вступ.

Темпи розвитку сучасних інформаційних технологій значно випереджають темпи розробки рекомендацій та нормативно-правової бази керівних документів в Україні. Тому питання оцінки рівня безпеки інформаційної системи обов'язково спричиняє виникнення наступних питань: відповідно до яких критеріїв проводити оцінку ефективності захисту, як оцінювати і переоцінювати інформаційні ризики? Внаслідок цього, додатково до вимог рекомендацій і нормативно-правових документів, приходиться адаптувати до наших умов і застосовувати методики міжнародних стандартів, а також використовувати методи кількісного аналізу ризиків у сукупності з оцінками економічної ефективності забезпечення безпеки і захисту інформації.

Сьогодні сучасні методи роботи з аналізу ризиків інформаційної безпеки, проектування і супроводу систем безпеки повинні дозволяти:

- виконати кількісну оцінку поточного рівня безпеки, задати припустимі рівні ризиків, розробити план заходів щодо забезпечення необхідного рівня безпеки на організаційно-управлінському і технічному рівнях з використанням сучасних методик та засобів;
- розрахувати й економічно обґрунтувати розмір необхідних вкладень у забезпечення безпеки на основі технологій аналізу ризиків, співвіднести витрати на забезпечення безпеки з потенційним збитком та імовірністю його виникнення;
- виявити і провести першочергове блокування найбільш небезпечних вразливостей до здійснення атак на вразливі ресурси;
- визначити функціональні відносини і зони відповідальності при взаємодії підрозділів і осіб по забезпеченню інформаційної безпеки, створити необхідний пакет організаційно-розпорядницької документації;
- забезпечити підтримку впровадженого комплексу захисту відповідно до умов роботи об'єкта, що змінюються, регулярними доробками організаційно-розпорядницької документації, модифікацією технологічних процесів і модифікацією технічних засобів захисту.

Різновид аналітичних і консалтингових робіт в області інформаційної безпеки об'єкта може бути наступним:

1. Комплексний аналіз інформаційної системи (ІС) на об'єкті і підсистеми інформаційної безпеки на методологічному, організаційно-управлінському, технологічному і технічному рівнях.

1.1 Дослідження й оцінка стану інформаційної безпеки нормативної ІС і підсистеми інформаційної безпеки об'єкта.

1.2 Роботи на основі аналізу ризиків.

Аналіз ризиків на рівні керування ризиками на основі якісних оцінок ризиків і на основі кількісних оцінок ризиків.

1.3 Інструментальні дослідження.

Інструментальне дослідження елементів інфраструктури комп'ютерної мережі і корпоративної ІС на наявність вразливостей.

Інструментальне дослідження захищеності точок доступу в Internet.

1.4 Аналіз документообігу об'єкта.

2. Розробка комплексних рекомендацій з методологічного, організаційно-управлінського, технологічного, загально технічного і програмно-апаратного забезпечення режиму інформаційної безпеки об'єкта.

2.1 Розробка концепції забезпечення інформаційної безпеки об'єкта.

2.2 Розробка нормативної політики забезпечення інформаційної безпеки об'єкта на організаційно-управлінському, правовому, технологічному та технічному рівнях.

2.3 Розробка плану захисту об'єкта.

2.4 Додаткові роботи з аналізу й створення методологічного, організаційно-управлінського, технологічного, інфраструктурного і технічного забезпечення режиму інформаційної безпеки об'єкта.

3. Організаційно-технологічний аналіз ІС об'єкта.

Оцінка відповідальності системи інформаційної безпеки об'єкта типовим вимогам нормативних документів в області організаційно-технологічних норм.

Додаткові роботи з дослідження й оцінки інформаційної безпеки об'єкта.

3.1 Розробка рекомендацій з організаційно-управлінського, технологічного, загально технічного забезпечення режиму інформаційної безпеки об'єкта.

Розробка елементів корпоративної політики забезпечення інформативної безпеки об'єкта на організаційно-управлінському, правовому, і технологічному рівні.

4. Експертиза рішень і проектів

4.1 Експертиза рішень і проектів автоматизації на відповідність вимогам по забезпеченню інформаційної безпеки експертно-документальним методом.

4.2 Експертиза проектів підсистем інформаційної безпеки на відповідність вимогам по безпеці експертно-документальним методом.

5. Роботи з аналізу документообігу й постачанню типових комплектів організаційно-розпорядницької документації.

5.1 Аналіз документообігу об'єкта категорії "конфіденційно" на відповідність вимогам концепції інформаційної безпеки, положенню про комерційну таємницю, іншим внутрішнім вимогам об'єкта по забезпеченню конфіденційності інформації.

5.2 Постачання комплекту типової організаційно-розпорядницької документації відповідно до рекомендацій корпоративної політики інформаційної безпеки об'єкта на організаційно-управлінському і правовому рівнях.

6. Роботи, що підтримують практичну реалізацію плану захисту і підготовку об'єкта до атестації. Розробка організаційно-розпорядницької і технологічної документації.

7. Підвищення кваліфікації і перепідготовка фахівців. Тренінги в області організаційно-правової складової захисту інформації в області технології захисту інформації. Навчання основам економічної безпеки, роботі з іншими технічними засобами захисту інформації, а також діям при спробі несанкціонованого отримання інформації або при спробі злому інформаційної системи.

Основна частина.

Виходячи з рівня втілення інформаційних технологій сучасності та розглядаючи інформацію, як об'єкт діяльності, слід відмітити, що в залежності від її важливості та значення для користування нею витрачаються відповідні ресурси. Але важливість та значення інформації для тих чи інших суб'єктів інформаційних відносин в умовах

комерційного, відомчого та державного інтересу визначити складно. Тому зрозуміло, що задоволення інформаційних потреб знаходиться в пропорційній залежності від умов та методів (засобів) практичної діяльності відповідних суб'єктів, а високий рівень автоматизації, до якого прагне людство, ставить його в залежність від рівня безпеки інформаційних технологій, що використовуються ними. В зв'язку з цим інформаційні ресурси потребують розмежування доступу, відповідно до цього інформацію за рангом доступу та правовим режимом.

Сучасні інформаційні технології сублімують у собі якості усіх форм, різні поточні форми можуть трансформуватися між собою.

Умовно, всі трансформації даних в ІС визначено як трансформації інформаційних потоків, модифікація яких викликає питання порушення цілісності та достовірності даних (властивості інформації, яка полягає в тому, що інформація не може бути модифікована неавторизованим користувачем і/або процесом).

Головною метою будь-якої системи інформаційної безпеки є забезпечення стійкого функціонування об'єкта, запобігання загроз його безпеці, захист законних інтересів користувача ІС від протиправних зазіхань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, перекручування і знищення інформації, забезпечення нормальної виробничої діяльності всіх підрозділів об'єкта. Іншою метою системи інформаційної безпеки є підвищення якості наданих послуг і гарантій безпеки прав й інтересів клієнтів. Досягнення заданих цілей можливо в ході рішення наступних основних задач:

- віднесення інформації до категорії обмеженого доступу (службової таємниці);
- прогнозування і своєчасне виявлення загроз безпеки інформаційним ресурсам, причин і умов, що сприяють нанесенню матеріального і морального збитку, порушенню цього нормального функціонування та розвитку;
- створення умов функціонування з найменшою ймовірністю реалізації загроз безпеки інформаційним ресурсам і нанесення різних видів збитків;
- створення механізму й умов оперативного реагування на загрози інформаційній безпеці і прояву негативних тенденцій у функціонуванні, ефективне припинення зазіхань на ресурси на основі правових, організаційних і технічних мір та засобів забезпечення безпеки;
- створення умов для максимально можливого відшкодування і локалізації збитку, який може бути нанесений неправомірними діями фізичних і юридичних осіб, послаблення негативного впливу наслідків порушення безпеки ІС на досягнення стратегічних цілей.

Стосовно інформації юридичні особи, організації (відомства, установи) виступають її джерелом, споживачем або порушником прав доступу (несанкціонованим користувачем).

Орієнтуючись на захист відомчих, комерційних, державних інтересів слід зауважити, що на всіх етапах трансформації інформації витрачається даний проміжок часу, тобто інформація має свій життєвий цикл (див. рис.1).

Життєвий цикл інформації на об'єкті залежить від оцінки її цінності, а також відповідно від спроможності санкціонованих користувачів забезпечити її надійний захист, і, таким чином, не допустити "знецінення" інформації. Він передбачає, що інформація здобувається, обробляється (аналізується), зберігається, охороняється, використовується, транслюється, розкрадається та знищується. Тому розглянемо етапи життєвого циклу інформації з позиції цільової ознаки ІС детальніше, щоб відокремити вразливі ланки трансформації, котрі потребують розгляду (захисту). Підкреслимо, що процес модифікації інформації охоплює всі етапи життєвого циклу. Під терміном "модифікація" будемо розуміти будь-яку зміну попереднього змісту виключно етапу створення об'єкту (рис.1).

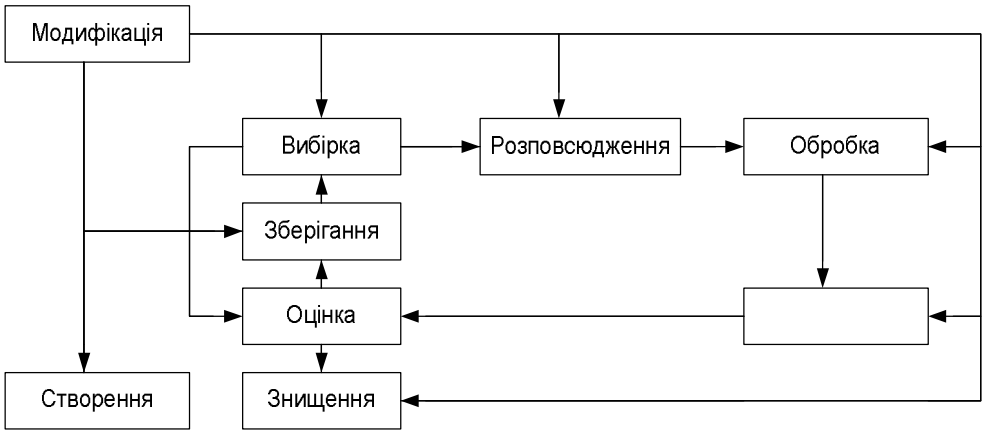

Рис.1. Життєвий цикл інформації

Процеси створення та знищення інформації, тобто відображення або стирання на деякому матеріальному носії, папері, або електронній копії накопичених даних з врахуванням визначених завдань до розробки документів здійснюються авторизованими користувачами (у випадку знищення це не має значення). Після створення документу призводиться його оцінка на предмет відповідності абстрактним і конкретним вимогам для подальшого спрямування та використання у визначених та дозволених межах. Процес зберігання включає як розробку порядку та правил підготовки до зберігання, так і саме зберігання інформації на різних носіях з послідуючою технологією (обмеження) доступу. Вибірка об'єкту та послідуюча оцінка вибору обумовлена конкретністю поставленої задачі. Критичність по відношенню до даних наступає з моменту вибірки та подальшого їх опрацювання.

Обробка та використання інформаційного об'єкту суб'єктами розподіленої системи, які обумовлюють практичне використання інформації при прийнятті рішень та реалізації тих чи інших життєвих процесів, дозволяє виділити найбільш уразливу ланку захищеної системи – етап її передачі, де має місце можливість несанкціонованих дій з боку неавторизованих користувачів.

При виконанні робіт на об'єкті можна використовувати різні моделі побудови системи інформаційної безпеки (рис. 2), засновані на адаптації нормативних документів і проведенні аналізу ризику.

Розроблена модель інформаційної безпеки – це сукупність об'єктивних зовнішніх і внутрішніх факторів та їх вплив на стан інформаційної безпеки на об'єкті і на збереження матеріальних чи інформаційних ресурсів.

Розглядаються наступні об'єктивні фактори:

- загрози інформаційній безпеці, що характеризуються ймовірністю виникнення та ймовірністю реалізації;
- вразливості ІС чи системи контрзаходів (системи інформаційної безпеки), що впливають на ймовірність реалізації загрози;
- ризик-фактор, що відображує можливий збиток організації в результаті реалізації загрози інформаційній безпеці: витоку інформації й її неправомірного використання (ризик в остаточному підсумку відображає ймовірні фінансові втрати – прямі чи непрямі).

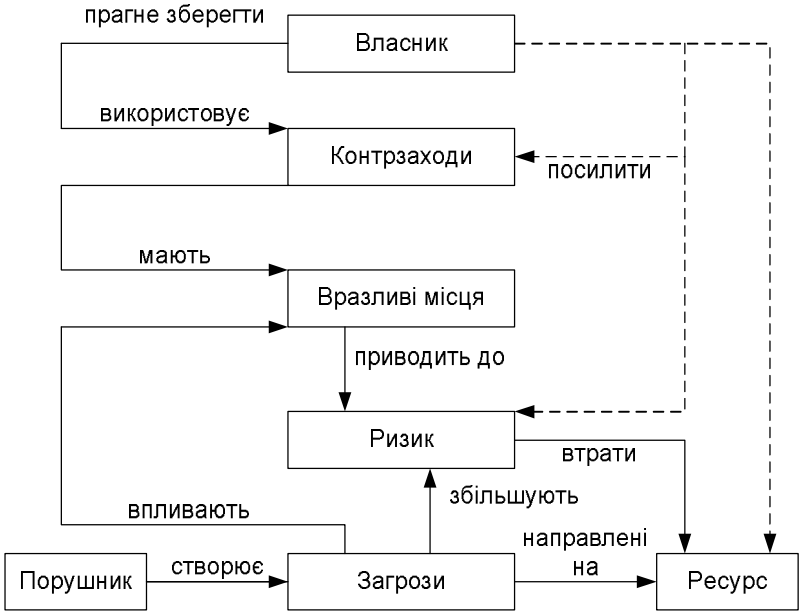

Рис.2. Модель побудови системи інформаційної безпеки об'єкта

Для побудови збалансованої системи інформаційної безпеки передбачається спочатку провести аналіз ризиків в області інформаційної безпеки. Потім визначити оптимальний рівень ризику для організації на основі заданого критерію. Систему інформаційної безпеки має бути побудовано таким чином, щоб досягти заданого рівня ризику.

При цьому методика проведення аналітичних робіт дозволяє:

- цілком проаналізувати і документально оформити вимоги, пов'язані з забезпеченням інформаційної безпеки;
- уникнути витрат на зайві заходи безпеки, можливі при суб'єктивній оцінці ризиків;
- надавати допомогу в плануванні і здійсненні захисту на всіх стадіях життєвого циклу інформаційних систем;
- забезпечити проведення робіт у стислий термін;
- представити обґрунтування для вибору мір протидії;
- оцінити ефективність контрзаходів, порівняти різні варіанти контрзаходів.

У ході робіт повинні бути встановлені границі дослідження. Для цього необхідно виділити ресурси ІС, для яких надалі будуть отримані оцінки ризиків. При цьому потрібно розділити розглянуті ресурси і зовнішні елементи, з якими здійснюється взаємодія. Ресурсами можуть бути засоби обчислювальної техніки, програмне забезпечення, дані. Прикладами зовнішніх елементів є мережі зв'язку і т.п.

При побудові моделі будуть враховуватися взаємодії між ресурсами. Наприклад, вихід з ладу якого-небудь устаткування може привести до втрати інформації чи виходу з ладу іншого критично важливого елемента системи. Подібні взаємозв’язки визначають основу побудови моделі організації з погляду інформаційної безпеки.

Ця модель, у відповідності із пропонованою методикою, будується в такий спосіб: для виділених ресурсів визначається їхня цінність, як з погляду асоційованих з ними можливих фінансових утрат, так і з погляду збитку репутації організації, дезорганізації її діяльності, нематеріального збитку від розголошення конфіденційної інформації тощо. Потім описуються взаємозв’язки ресурсів, визначаються загрози безпеки й оцінюються ймовірності їх реалізації.

На базі запропонованої моделі можна обґрунтовано вибрати та обґрунтувати систему контрзаходів, що знижує ризики до припустимих рівнів, які мають найбільшу цінову

ефективність. Частиною системи контрзаходів будуть рекомендації з проведення регулярних перевірок ефективності системи захисту. Керування ризиками – забезпечення підвищених вимог до інформаційної безпеки припускає відповідні заходи на всіх етапах життєвого циклу інформації та інформаційних технологій. Планування цих заходів здійснюється по завершенні етапу аналізу ризиків і вибору контрзаходів. Обов'язковою складовою частиною цих планів є періодична перевірка відповідності існуючого режиму інформаційної безпеки, політики безпеки, сертифікація ІС (технології) на відповідність вимогам визначеного стандарту безпеки.

На завершенні робіт, можна буде визначити міру гарантії безпеки інформаційно-обчислювального середовища, засновану на оцінці, з якою можна довіряти інформаційно-обчислювальному середовищу об'єкта.

Висновки.

Таким чином, життєвий цикл інформації на об'єкті залежить від оцінки її цінності, а також від спроможності санкціонованих користувачів забезпечити її надійний захист, і, таким чином, не допустити "знецінення" інформації. Він передбачає, що інформація здобувається, обробляється (аналізується), зберігається, охороняється, використовується, транслюється, розкрадається та знищується. Тому було доцільним розглянути етапи життєвого циклу інформації з позиції цільової ознаки ІС детальніше, щоб відокремити вразливі ланки трансформації, котрі потребують захисту.

Розроблена модель інформаційної безпеки представляє сукупність об'єктивних зовнішніх і внутрішніх факторів та їх вплив на стан інформаційної безпеки на об'єкті і на збереження матеріальних чи інформаційних ресурсів. На базі запропонованої моделі можна обґрунтовано вибрати та обґрунтувати систему контрзаходів, що знижує ризики до припустимих рівнів, які мають найбільшу цінову ефективність. На завершенні робіт, можна буде визначити міру гарантії безпеки інформаційно-обчислювального середовища, засновану на оцінці, з якою можна довіряти інформаційно-обчислювальному середовищу об'єкта.

Надійшла: 06.06.2012

Рецензент: д.т.н., проф. Дудикевич В.Б.