Посилання на статтю

Велігура А.В. Оцінювання стану інформаційної безпеки підприємства / А.В. Велігура // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2014 - №4(52). - С. 28-39.

УДК 621.396.2

А.В. Велігура

ОЦІНЮВАННЯ СТАНУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПІДПРИЄМСТВА

Розроблено методику комплексного оцінювання стану інформаційної безпеки підприємства, запропонований комплекс показників, визначено порогові значення показників, які забезпечують достатній рівень інформаційної безпеки. Рис. 2, дж. 16.

Ключові слова: інформаційна безпека, суб'єкти господарювання, система менеджменту, комплексне оцінювання.

А. В. Велигура

ОЦЕНИВАНИЕ СОСТОЯНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Разработана методика комплексного оценивания состояния информационной безопасности предприятия, предложен комплекс показателей, определены пороговые значения показателей, обеспечивающие достаточный уровень информационной безопасности. Рис. 2, ист. 16.

A.V. Veligura

EVALUATION OF THE ENTERPRISE INFORMATION SECURITY

The technique of integrated state estimation information security, a set of indicators defined threshold levels to ensure an adequate level of information security.

G32

ВСТУП

Інформаційна безпека (ІБ) - комплекс заходів та засобів щодо забезпечення збереження інформації, що знаходиться в системі інформаційного забезпечення діяльності підприємства, переданої, оброблюваної, а також тієї, що зберігається та надається системою.

Призначення системи інформаційної безпеки полягає в організації безпечних і надійних: заходів з доступу до інформації, способів передачі та зберігання інформації, методів обробки інформації, правил управління доступом до інформації, способів відновлення інформації, методів резервування інформації тощо.

Завдання системи інформаційної безпеки обумовлюються її призначенням і полягають у: забезпеченні безпечного, надійного зберігання і передачі інформації в електронному вигляді, розташованої на різних носіях; організації надійного доступу до електронної інформації; обмеження і контроль доступу до інформації,

з якою працюють співробітники; створенні правил безпечної роботи з інформацією; проведенні заходів щодо резервування інформації; забезпеченні відновлення інформації в аварійних ситуаціях; підтримці інформаційної безпеки на заданому рівні.

Забезпечення інформаційної безпеки в епоху постіндустріальної економіки стає життєво важливим для успішного існуванні підприємства. З іншого боку, постає питання належного визначення стану інформаційної безпеки підприємства, показників, що його характеризують, а також значень цих показників, які б забезпечували належний рівень інформаційної безпеки підприємства.

Також важливим є питання оцінювання значень цих показників в умовах невизначеності, яка притаманна сфері безпеки.

Постановка проблеми у загальному вигляді. В нинішній час для забезпечення належного стану інформаційної безпеки потрібна не просто розробка окремих механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування підприємства, запобігання загроз його безпеки, захист законних інтересів підприємства від протиправних посягань, недопущення розкрадання фінансових засобів, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках виробничої діяльності всіх підрозділів підприємства.

Аналіз останніх досліджень і публікацій, в яких започатковано розв'язання даної проблеми і виділення невирішених раніше частин. Питанням побудови та аналізу системи інформаційної безпеки присвячено роботи таких провідних світових та українських науковців, як Домарев В.В., Зефіров С.Л., Голованов М.Б., С. Норкатт, Рамазанов С.К., Рач В.А., Ляшенко О.М. та інші. В роботах одних з вищеназваних авторів наведено велику кількість показників, які характеризують стан інформаційної безпеки [1, 2, 3, 4], інших – заходи щодо підвищення рівня захищеності інформації підприємства [5, 6, 7], третіх - комплексні методики, які, нажаль по-перше, дуже важко впроваджувати через велику кількість віжко оцінюваних показників, а з іншого боку – нелегко узгодити із існуючим законодавством та міжнародними і національними стандартами, що регламентують діяльність, пов'язану із інформаційною безпекою [5, 3, 4].

Таким чином, виникла необхідність розробки комплексного показника стану інформаційної безпеки підприємства, методики його розрахунку та визначення екстремальних значень окремих показників, які забезпечують достатній рівень інформаційної безпеки.

Мета статті є узагальнення дослідження провідних вчених у галузі інформаційної безпеки та запропонувати керівникам підприємств комплекс показників із методикою їх оцінювання, а також перелік заходів щодо забезпечення належного рівня інформаційної безпеки підприємства.

ОСНОВНІ РЕЗУЛЬТАТИ

Інформаційна безпека підприємства відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління на підприємстві [1-5].

Процес забезпечення інформаційної безпеки підприємства можна представити як взаємодію трьох підсистем:підсистема інформаційного забезпечення процесу управління на підприємстві;підсистема захисту

інформаційного середовища підприємства;підсистема діагностики рівня інформаційної безпеки.

Ключовими задачами підсистеми інформаційного забезпечення процесу управління на підприємстві є: збирання необхідної інформації;обробка і систематизація інформації;оцінка й аналіз інформації;прогнозування всіх аспектів діяльності підприємства;надання необхідної інформації особам, що приймають рішення.

Безперервне виконання всіх цих задач необхідне для ефективного функціонування зазначеної підсистеми. Захист інформаційного середовища підприємства включає захист від зловмисних дій як конкурентів, так і власних співробітників, а також захист від незловмисних внутрішніх негативних впливів.

Методи та методики дослідження. Для забезпечення захисту інформаційного середовища підприємства необхідне систематичне виконання наступних етапів (рис. 1.):

- аналіз загроз інформаційній безпеці;
- планування та розробка заходів щодо забезпечення інформаційної безпеки;
- оперативна реалізація запланованих дій.

Діагностику рівня інформаційної безпеки підприємства пропонується проводити за трьома ключовими напрямками (рис. 2): оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається особам, що приймають рішення, інформаційною службою підприємства [8-12].

Для оцінки інформаційної надійності персоналу пропонується розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства та коефіцієнт підготовленості персоналу до розпізнавання погроз [13-15].

Оцінку інформації, що надається особам, що приймають рішення, інформаційною службою підприємства пропонується проводити за допомогою трьох показників: коефіцієнт повноти інформації, коефіцієнт точності інформації та коефіцієнт суперечливості інформації, які варто доповнити коефіцієнтом своєчасності надання інформації та коефіцієнтом надійності інформації.

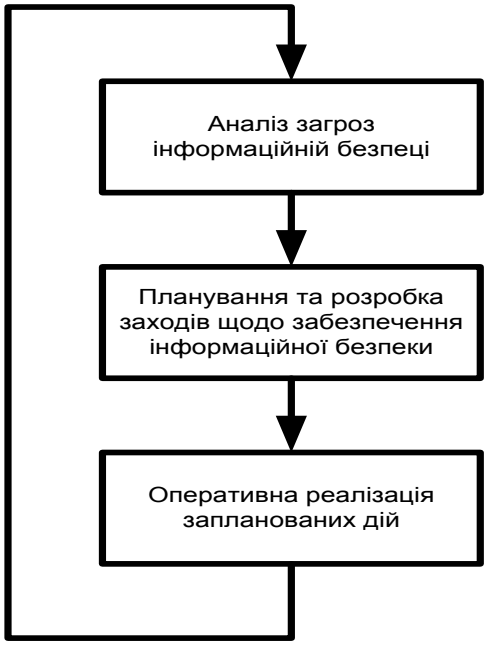

Рисунок 1. Схема функціонування системи інформаційної безпеки підприємства

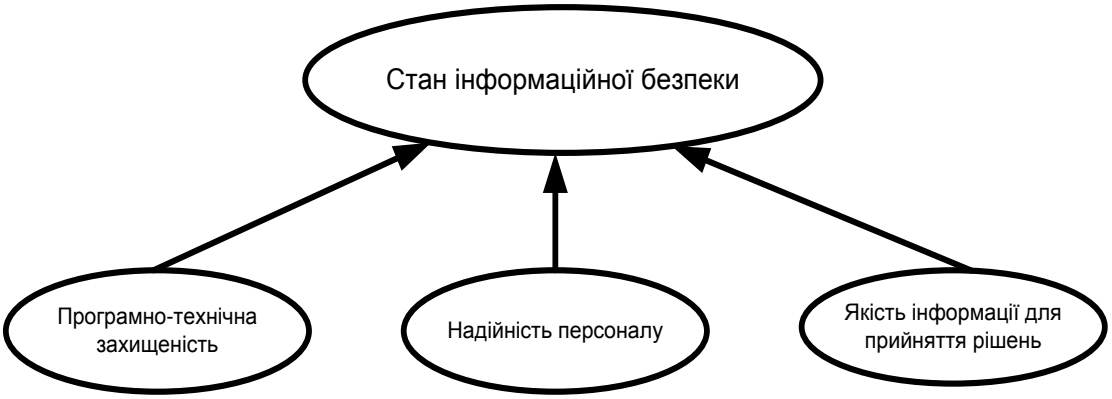

Рисунок. 2. Визначення стану інформаційної безпеки підприємства

Варто зазначити, що для отримання інформації, необхідної для розрахунку наведених показників, обов'язковою умовою є наявність системи моніторингу діяльності інформаційної служби підприємства [16].

Кількісний аналіз та моделювання є тими інструментальними засобами, які дають змогу оцінити, виокремити, нехай і наближено, суттєві ризики з несуттєвих (надуманих).Однак у більшості випадків одного лише якісного аналізу недостатньо для ідентифікації та виокремлення суттєвих чинників ризику й нехтування несуттєвими (надуманими). З цією метою необхідно здійснювати кількісний аналіз небезпеки. А це потребує здобуття відповідної інформації.

Методи експертних оцінки включають комплекс логічних і математико-статистичних методів і процедур, пов'язаних з діяльністю експерта по переробці

необхідної для аналізу і прийняття рішень інформації. Центральною «фігурою» експертної процедури є сам експерт - це фахівець, який використовує свої здібності (знання, вміння, досвід, інтуїцію і т.п.) для знаходження найбільш ефективного рішення.

Експерти, що залучаються для оцінки небезпеки, в тому числі і інформаційної, повинні: мати доступ до всієї наявної в розпорядженні розробника інформації; володіти достатнім рівнем креативності мислення та необхідними знаннями у відповідній предметній області; бути вільним від особистих переваг щодо проекту (не лобіювати його).

Можна виділити наступні основні методи експертних оцінок, що застосовуються для аналізу небезпеки: запитальники; SWOT-аналіз; роза і спіраль ризиків; оцінка ризику стадії проекту; метод Дельфі.

Інформація може існувати в самих різних формах. Її можна друкувати або писати на папері, зберігати на електронних носіях, пересилати за традиційною або електронною поштою, показувати у фільмах або передавати в усній розмові. Яку б форму не приймала інформація і які б кошти не використовувалися для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень її захисту.

Інформаційна безпека досягається шляхом впровадження сукупності необхідних засобів захисту, до числа яких можуть входити політики, рекомендації, інструкції,організаційні структури і програмні функції. Ці засоби необхідно реалізувати для того, щоб гарантувати виконання вимог до безпеки в конкретній організації.

Виклад основного матеріалу дослідження. Система показників оцінки рівня інформаційної безпеки підприємства за кожним з запропонованих напрямків з розрахунковими формулами та гранічні значеннями наведена нижче:

Оцінка програмно-технічної захищеності інформації

Коефіцієнт технічного захисту інформації $K_{T.З.}$

$$K_{T.З.} = IA_{H.B.} \tag{1}$$

де $IA_{H.B.}$ – кількість не відвернутих інформаційних атак.

Коефіцієнт програмної захищеності інформації $\mathrm{К}_{\mathrm{П.З.}}$

$$K_{П.З.} = \frac{Ч_{б.ф.}}{Ч_{н.ф.}} \tag{2}$$

де $Ч_{б.ф.}$ – час безперебійного функціонування корпоративної інформаційної системі, год.

$Ч_{н.ф.}$ – нормативний час функціонування корпоративної інформаційної системи, год.

Коефіцієнт фінансового захисту інформації $\mathrm{К}_{\mathrm{ф.з.}}$

$$\mathrm{К}_{\mathrm{ф.з.}} = \frac{\mathrm{В}_{\mathrm{з.ін.}}}{\mathrm{В}_{\mathrm{пр.ін.}}}, \text{ 0,15, зростання} \tag{3}$$

де $В_{з.ін.}$ – витрати на захист інформаційних ресурсів, грн.;

$В_{пр.ін.}$ – витрати на придбання інформаційних ресурсів,грн.

Коефіцієнт фінансування інформаційних служб підприємства $К_{фін.}$

$$К_{фін} = \frac{В_{фін}}{В_з}, \quad 0{,}5\text{-}0{,}15, \text{ зростання} \qquad (4)$$

де $В_{фін.}$ – витрати на фінансування інформаційних служб підприємства, грн.;

$В_з$ – загальні витрати підприємства.

Оцінка інформаційної надійності персоналу

Коефіцієнт правової захищеності інформації $К_{пр.з.}$

$$К_{пр.з.} = \frac{I}{I_{юр.з.}}, \quad 1, \text{ зменшення} \qquad (5)$$

де I – обсяг інформації, розголошення якої може спричинити негативні наслідки для підприємства, %

$I_{юр.з.}$ – загальний обсяг юридично захищеної інформації, %

Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку підприємства $К_{д.р.}$

$$К_{д.р.} = \frac{ЧП_1}{ЧП_з}, \quad 1, \text{ зростання} \qquad (6)$$

де $ЧП_1$ – чисельність працівників, які мають доступ до комерційної таємниці, що працюють на підприємстві більше одного року, ос.;

$ЧП_з$ – загальна чисельність працівників, що мають доступ до комерційної таємниці, ос.

Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку підприємства $К_{н.п.}$

$$К_{н.п.} = \frac{ЧП_{з.зв.} - Ч_{вип}}{ЧП_{з.зв.}}, \quad 1, \text{ зростання} \qquad (7)$$

де $ЧП_{вип}$ – чисельність працівників, звільнених за причиною витоку інформації, ос.;

$ЧП_{з.зв.}$ – загальна чисельність звільнених працівників, ос.

Коефіцієнт підготовленості персоналу до розпізнавання погроз $К_{п.п.}$

$$К_{н.п.} = \frac{ЧП_з - ЧП_п}{ЧП_з}, \quad 1, \text{ зростання} \qquad (8)$$

де $ЧП_п$ – чисельність працівників, ненавмисні дії яких призвели до витоку інформації завдяки низькому рівню підготовки персоналу до розпізнавання загроз безпеки, ос.;

$ЧП_з$ – загальна чисельність працівників, що мають доступ до закритої інформації, ос.

Оцінка інформації, що надається особам, що приймають рішення (ОПР), інформаційною службою підприємства

Коефіцієнт повноти інформації $К_{п.ін.}$

$$К_{п.ін.} = \frac{I_н}{I_{необ.}}, \text{ 1, зменшення} \qquad (9)$$

де $I_н$ – обсяг інформації, що є в розпорядженні ОПР, %;

$I_{необ.}$ – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %

Коефіцієнт точності інформації $К_{т.ін.}$

$$К_{т.ін.} = \frac{I_р}{I_н}, \quad 1, \text{ зростання} \qquad (10)$$

де $I_р$ – обсяг релевантної інформації, %

$I_н$ – загальний обсяг наявної в розпорядженні ОПР інформації, %

Коефіцієнт суперечливості інформації $К_{с.ін.}$

$$К_{с.ін.} = \frac{I_{ухв}}{I_з}, \quad 1, \text{ зростання} \qquad (11)$$

де $I_{ухв}$ – кількість незалежних свідчень на користь ухвалення рішення, %;

$I_з$ – загальна кількість незалежних свідчень у сумарному обсязі релевантної інформації, %.

Коефіцієнт своєчасності надання інформації $К_{с.н.ін.}$

$$К_{с.н.ін.} = \frac{I_{с.н.}}{I_{необ.}}, \quad 1, \text{ зростання} \qquad (12)$$

де $I_{с.н.}$ – обсяг своєчасно наданої ОПР інформації, %;

$I_{необ.}$ – обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %

Коефіцієнт надійності інформації $К_{н.ін.}$

$$К_{н.ін.} = \frac{I_{н.д.}}{I_{з.н.}}, \quad 1, \text{ зростання} \qquad (13)$$

де $I_{н.д.}$ – обсяг інформації, наданої ОПР з надійних джерел, %;

$I_{з.н.}$ – загальний обсяг наданої ОПР інформації, %

Будь-яка організація повинна визначити свої вимоги до безпеки. При оцінці вимог використовуються три основні показники.

Першим показником служить оцінка небезпек, з якими стикається організація. Шляхом оцінки небезпек визначаються загрози для інформації, її вразливість та ймовірність виникнення загроз, а також можливий збиток.

Другий показник - це законодавчі, нормативні та договірні вимоги, які повинна дотримуватися організація, її партнери по бізнесу, підрядники та постачальники послуг.

Третій показник - це певний набір принципів, цілей і вимог до обробки інформації, розроблених організацією для підтримки своєї діяльності.

Визначення вимог до безпеки проводиться шляхом методичної оцінки ризиків. Витрати на підтримку безпеки необхідно збалансувати з шкодою для бізнесу,який може виникнути при порушенні безпеки. Методи оцінки небезпек можуть застосовуватися до всієї організації або лише до її частин, а також до окремих інформаційним системам, системним компонентів і сервісів, в залежності від того, що виявиться найбільш практичним, реалістичним і корисним.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи опису і класифікації. Для здійснення ефективного захисту системи управління інформаційною безпекою слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження причинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних зв'язків можна назвати наступні: метод схожості, метод розбіжності, метод сполучення схожості і розбіжності, метод супроводжувальних змін, метод залишків.

ОБГОВОРЕННЯ

При забезпеченні режиму ІБ досить важливе місце відводиться завданням аналізу інформаційних небезпек компанії та управління ними.

Незалежно від розмірів організації і специфіки її інформаційної системи роботи щодо забезпечення режиму ІБ зазвичай складаються з наступних етапів:вироблення політики безпеки;визначення сфери (меж) системи управління інформаційною безпекою та конкретизація цілей її створення;оцінка небезпек;вибір контрзаходів, які забезпечують режим ІБ;управління ризиками;аудит системи управління ІБ.

Для управління інформаційною безпекою підприємства розробляється деяка стратегія управління небезпеками. Наприклад, тут можливі такі підходи до управління інформаційними ризиками компанії:зменшення ризику;ухилення від ризику;зміна характеру ризику;прийняття ризику.

Виділяють декілька типів методів управління інформаційною безпекою: однорівневі методи будуються на підставі одного принципу управління інформаційною безпекою;багаторівневі методи будуються на основі декількох принципів управління інформаційною безпекою, кожний з яких слугує вирішення власного завдання. При цьому приватні методи не пов'язані між собою і спрямовані лише на конкретні чинники інформаційних загроз;комплексні методи — багаторівневі методи, які об'єднані у єдину систему координуючих функцій на організаційному рівні з метою забезпечення інформаційної безпеки, виходячи з аналізу сукупності чинників небезпеки, які мають семантичний зв'язок або генеруються з єдиного інформаційного центру інформаційного впливу;інтегровані високоінтелектуальні методи — багаторівневі, багатокомпонентні технології, які побудовані на підставі могутніх автоматизованих інтелектуальних засобів з організаційним управлінням.

Загальні методи забезпечення інформаційної безпеки активно використовуються на будь-якій стадії управління загрозами. До таких стадій належать: прийняття рішення по визначенню області та контексту інформаційної загрози і складу учасників процесу протидії; ухвалення загальної стратегії і схеми дій в політичній, економічній, соціальній та інших сферах життєдіяльності; забезпечення адекватного сприйняття загрози та небезпеки у нижчих організаційних ланках системи управління інформаційною безпекою; виділення необхідних політичних, економічних, соціальних, адміністративних і організаційних ресурсів, достатніх для реалізації програми відбиття інформаційної загрози і збереження сталого розвитку інформаційних ресурсів системи управління: трансформації результатів оцінки ризиків у відповідну політику безпеки, включаючи національну.

Специфіка методів, що використовуються, значно залежить від суб'єкта діяльності, об'єкта впливу, а також переслідуваних цілей. Так, методи діяльності індивіда у зв'язку із його обмеженою можливістю по забезпеченню інформаційної безпеки здебільшого зводяться до джерела загрози, апелювання до суспільної думки, а також до держави, яка має вживати рішучих заходів по нейтралізації інформаційних загроз. Саме суспільство використовує у своїй діяльності методи соціального регулювання, надання допомоги окремим індивідам і суспільним організаціям, яким спричинена шкода внаслідок виявлення загрози.

Іншим завданням захисту є забезпечення незмінності інформації під час її зберігання або передачі, тобто забезпечення її цілісності. Таким чином конфіденційність інформації, яка забезпечується за допомогою криптографічних методів не є головною вимогою при управлінні інформаційною безпекою. Виконання процедур криптокодування і декодування може уповільнити передачу даних та зменшити доступ до них через те, що користувач буде позбавлений можливості своєчасного і швидкого доступу до цих даних та інформації. Саме тому забезпечення конфіденційності інформації має відповідати можливості доступу до неї. Таким чином, управління в сфері інформаційної безпеки має

здійснюватися на підставі принципу доступності та безпеки. Система забезпечення інформаційної безпеки в першу чергу має гарантувати доступність і цілісність інформації, та її конфіденційність у випадку необхідності.

Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. Їх варіативність занадто лабільна і залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторах загрози, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє достатньо точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Важливим методом забезпечення інформаційної безпеки є метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів.

Існують методи, які можна вважати основоположними, що дозволяють створити надійну основу для реалізації інформаційної безпеки. Ці методи або базуються на важливих законодавчих вимогах, або відносяться до загальновизнаних методів роботи в області управління інформаційною безпекою.

З законодавчої точки зору найважливішими для організації вважаються наступні заходи:захист даних і нерозголошення особистої інформації;захист організаційних записів;захист прав на інтелектуальну власність.

До загальновизнаних методів забезпечення інформаційної безпеки відносяться наступні:створення документа, що визначає політику інформаційної безпеки;розподіл відповідальності за інформаційну безпеку;навчання і підготовка в галузі інформаційної безпеки;створення звітів про інциденти;підтримка безперервності бізнесу.

Ці методи можуть застосовуватися в більшості організацій і в більшості середовищ. Слід зауважити,що незважаючи на те, що всі описані методи є важливими,значимість кожного методу слід визначати у світлі конкретних ризиків, з якими стикається організація.

Обґрунтування отриманих результатів. Основним чинником, від якого залежить ставлення організації до питань інформаційної безпеки, є ступінь її зрілості. Так, наприклад, відома аналітична компанія GartnerGroup і університет CarnegieMellon запропонували свої моделі визначення зрілості компанії та стану інформаційної безпеки. Різним рівням зрілості відповідають різні потреби в області інформаційної безпеки.

GartnerGroup виділяє чотири рівня зрілості компанії - починаючи з нульового і закінчує третім.

Значно розширену модель визначення рівня зрілості компанії з точки зору інформаційної безпеки запропонував університет CarnegieMellon.

Відповідно до цієї моделі виділяється п'ять рівнів зрілості компанії, яким можна поставити у відповідність різне розуміння проблем інформаційної безпеки організації.

Проблема забезпечення режиму інформаційної безпеки буде формулюватися (хоча б у неявному вигляді) і вирішуватися по-різному для організацій, що знаходяться на різних рівнях розвитку.

На першому рівні ця проблема, як правило, керівництвом формально не висувається. Але це не означає, що вона не вирішується співробітниками з власної ініціативи - і, можливо, ефективно. Тим не менш, з точки зору керівництва організації, що знаходиться на першому рівні зрілості, завдання

забезпечення режиму інформаційної безпеки, як правило, неактуальні. І все ж такі організації можуть бути цілком життєздатними.

На другому рівні проблема забезпечення інформаційної безпеки вирішується неформально, на основі поступово сформованої практики. Комплекс заходів (організаційних і програмно-технічних) дозволяє захиститися від найбільш ймовірних загроз, як потенційно можливих, так і тих, що мали місце раніше. Питання щодо ефективності захисту не піднімається. Таким чином, поступово складається неформальний список актуальних для організації класів ризиків, який поступово поповнюється. Якщо серйозних інцидентів не відбувалося, керівництво організації, як правило, не вважає питання інформаційної безпеки пріоритетним. У випадку серйозного інциденту сформована система забезпечення безпеки коригується, а необхідність пошуку інших можливих слабких місць в захисті іноді усвідомлюється керівництвом.

Для даного рівня зрілості організації типовою є локальна (не пов'язана з іншими етапами життєвого циклу технології) постановка завдання аналізу ризиків: вважається достатнім перерахувати актуальні для конкретної інформаційної системи класи ризиків і, можливо, описати модель порушника, а завдання аналізу варіантів контрзаходів, їх ефективності, управління ризиками, як правило, не розглядається в якості актуальних.

На третьому рівні в організації прийнято слідувати в тій чи іншій мірі (можливо, частково) стандартам і рекомендаціям, що забезпечує базовий рівень інформаційної безпеки (наприклад, ISO 17799). Питанням документування приділяється належна увага. Завдання аналізу ризиків не є, на думку керівництва, своєчасною. Аналіз ризиків розглядається як один з елементів технології управління режимом інформаційної безпеки на всіх стадіях життєвого циклу. Поняття ризику включає кілька аспектів: вірогідність, загрозу, уразливість, іноді вартість. Один з варіантів оцінки ризику (певного класу) в цьому випадку: ймовірність виникнення інциденту в результаті того, що наявна вразливість сприятиме реалізації загрози.

Технологія управління режимом інформаційної безпеки в повному варіанті містить такі елементи:документування інформаційної системи організації з позиції інформаційної безпеки; категоріювання інформаційних ресурсів з позиції керівництва організації;визначення можливого впливу різного роду подій в галузі безпеки на інформаційну технологію; аналіз ризиків;технологія управління ризиками на всіх етапах життєвого циклу;аудит в області інформаційної безпеки.

На даному рівні зрілості організації аналіз ризиків пов'язаний з іншими компонентами технології управління режимом інформаційної безпеки.

На четвертому рівні для керівництва організації актуальні питання вимірювання параметрів, що характеризують режим інформаційної безпеки. На цьому рівні керівництво відповідає за вибір певних величин залишкових ризиків (які залишаються завжди). Ризики, як правило, оцінюються за кількома критеріями (не тільки вартісним).

Технологія управління режимом інформаційної безпеки залишається колишньою, але на етапі аналізу ризиків застосовуються кількісні методи, що дозволяють оцінити параметри залишкових ризиків та ефективність різних варіантів контрзаходів при управлінні ризиками.

На п'ятому рівні ставляться і вирішуються різні варіанти оптимізаційних завдань у галузі забезпечення режиму інформаційної безпеки. Приклади постановки завдань:вибрати варіант підсистеми інформаційної безпеки, оптимізованої за критерієм «вартість-ефективність» при заданому рівні залишкових ризиків;вибрати варіант підсистеми інформаційної безпеки, при якому мінімізуються залишкові ризики при фіксованій вартості підсистеми

безпеки;вибрати архітектуру підсистеми інформаційної безпеки з мінімальною вартістю володіння протягом життєвого циклу при встановленому рівні залишкових ризиків.

Висновки. Запропонований підхід було випробувано на підприємствах Луганської області. Використання пропонованого підходу до оцінювання стану і управління інформаційною безпекою підприємства дозволило суттєво підвищити якість управлінських рішень, забезпечити ефективне використання інформаційних ресурсів підприємства, скоротити витрати на забезпечення інформаційної безпеки.

Перспективи подальших досліджень у даному напрямку. Наступним кроком повинна стати розробка автоматизованої системи моніторингу стану інформаційної безпеки, яка б накопичувала відомості про стан інформаційної безпеки, обчислювала значення показників та надавала рекомендації щодо управління станом інформаційної безпеки підприємства.

ЛІТЕРАТУРА

1. Інноваційні технології антикризового управління економічними системами [Текст] : монографія / С.К. Рамазанов, Г.О. Надьон, Н.І. Кришталь, О.П. Степаненко, Л.А. Тимашова; під ред.. проф. С. К. Рамазанова. – Луганськ-Київ: вид-во СНУ ім. В. Даля, 2009. – 584 с.
2. Безбожний В.Л. Передумови забезпечення соціально-економічної безпеки великих промислових підприємств [Текст] / В.Л. Безбожний // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В. Даля, 2013. – №1(45). С. 10-15.
3. Россошанская О.В. Метод оценки экономической безопасности инновационных проектно-ориентированых предприятий с позиции метрики внутренней среды деятельности [Текст] / О.В. Россошанская // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В. Даля, 2013 – No 1(45). -С. 33-44.
4. Єрмолаєв П.В. Функціональний профіль економічної безпеки підприємства: методичні та прикладні аспекти [Текст] / П. В. Єрмолаєв // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2013. – № 1(45). С. 26-33.
5. Рач В.А. Проблеми захисту інформації в управлінні проектами в епоху економіки знань [Текст] / В.А. Рач // Управління проектами та розвиток виробництва: Зб.наук.пр. - Луганськ: вид-во СНУ ім. В.Даля, 2009. – № 2 (30). – С. 156-160.
6. Рач В.А. «Небезпека/ризик/криза» як тріадна сутність процесів розвитку в сучасній економіці [Текст] / В.А. Рач // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В. Даля, 2013. – № 1 (45). – С. 155-160.
7. Ляшенко О. М. Логіка керованості економічної безпеки підприємства / О.М. Ляшенко [Текст] // Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В.Даля, 2013. – №1(45). – С. 5-10.
8. ISO/TC 176/SC 2/N 544R2, ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems, 13 May 2004.
9. ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements.
10. ISO/IEC 38500:2008, Corporate governance of information technology.
11. ISO GUIDE 72:2001, Guidelines for the justification and development of management system standards.
12. ISO/IEC 27003, Information technology – Security techniques – Information security management system implementation guidance.
13. Technical Report ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management.
14. Deming W. Edward. Out of the Crisis: Quality, Productivity, and Competitive Position. – Cambridge (Mass.) Mass. Inst. of Technology, Center for Advanced Engineering Study: Cambridge University Press, 1982.
15. NIST Special Publication 800-61, Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, January 2004.

16. Курило А.П. Аудит информационной безопасности. [Текст] / Курило А. П., Зефиров С.Л., Голованов В.Б. и др. Аудит информационной безопасности. – М.: Издательская группа «БДЦ-пресс», 2006. – 420 с.

Рецензент статті
д.е.н., проф.Даніч В.М.

Стаття надійшла до редакції
19.05.2014