УДК 339.9
DOI: https://doi.org/10.26642/jen-2020-1(91)-38-42

І.Ю. Маковський, аспірант
Державний університет «Житомирська політехніка»

Аналіз вихідних даних для формування політики інформаційної безпеки на підприємстві

(Представлено: д.е.н., проф. Валінкевич Н.В.)

В статті розглянуто фактори, що підлягають аналізу в процесі формування політики інформаційної безпеки на підприємстві в цілому та в кожному з його бізнес-процесів також запропоновано класифікацію загроз інформаційній безпеці (за аспектом інформаційної безпеки, на який спрямовані загрози, за розташуванням джерела загроз, за розмірами завданих збитків, за ступенем впливу на інформаційну систему, за природою виникнення) та їх потенційних носіїв – порушників безпеки (за місцем дії, за мотивом порушення, за рівнем знань про інформаційну систему, за рівнем можливостей, за часом дії). На підставі вимог чинного законодавства автор пропонує формувати відповідні моделі загроз і порушників, виходячи з потреб підприємства, а також з урахуванням важливості інформації, що підлягає захисту. Аналіз загроз і порушників інформаційної безпеки дозволяє керівнику підприємства сформувати оптимальну політику безпеки, застосувавши конкретний набір заходів, спрямованих на її реалізацію. Водночас особлива увага зосереджується на співвідношенні можливих втрат до видатків, спрямованих на унеможливлення реалізації конкретних загроз. Закладено підґрунтя для подальших досліджень щодо формування політики інформаційної безпеки на підприємстві з визначенням критичних даних, втрата яких може значною мірою вплинути на економічні показники підприємства; формування функціональних профілів захищеності з урахуванням потреби в максимальному захисті за мінімальних видатків.

Ключові слова: *інформаційна безпека; модель загроз; модель порушника; конфіденційна інформація.*

Постановка проблеми. В сучасному світі, де дуже швидко розвиваються інформаційні технології, гостро стоїть проблема забезпечення захисту інформації від витоку та несанкціонованого доступу. На сьогодні питання інформаційної безпеки дедалі більше стосується саме суб'єктів підприємницької діяльності, яким потрібно захищатися від витоку інформації. Ми вважаємо, що для формування якісної політики безпеки на підприємстві необхідно чітко визначити, що загрожує тій чи іншій інформації, а також хто може бути потенційним носієм таких загроз. Від аналізу загроз та можливих порушників інформаційної безпеки залежить подальший розрахунок співвідношення можливих втрат до видатків, необхідних для унеможливлення реалізації цих загроз.

Аналіз останніх досліджень і публікацій. У наукових працях, національних та міжнародних стандартах приділяється значна увага проблемам інформаційної безпеки діяльності підприємств. Проблематику аналізу загроз та носіїв загроз інформаційній безпеці у своїх працях розглядали: М.Ю. Танцюра [2], О.М. Блінов [7], Ю.М. Щебланін, Д.І. Рабчун [8], А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк [9] та багато інших українських і зарубіжних науковців. Однак, незважаючи на вагомий внесок зазначених дослідників, існує необхідність удосконалення алгоритмів аналізу загроз інформаційній безпеці під час формування політики безпеки на підприємстві, що дозволить більш якісно та з мінімальними затратами захистити конфіденційну інформацію.

Метою статті є аналіз і структурування вихідних даних, необхідних для формування політики інформаційної безпеки на підприємстві.

Викладення основного матеріалу дослідження. Поняття «інформаційна безпека» з'явилось із появою засобів інформаційної комунікації між окремими людьми чи цілими соціумами. Це пов'язано з обміном тією інформацією, заволодіння якою може завдати збитків особі чи суспільству, яких стосується та чи інша інформація.

Єдиного визначення поняття «інформаційна безпека» не існує, втім деякі дослідники подають такі визначення:

Кіссель Р.Л. визначає «інформаційну безпеку» як практику попередження несанкціонованого доступу, використання, розкриття, перекручення, зміни, дослідження, запису чи знищення інформації [1]. Таке універсальне визначення застосовується незалежно від форми, яку можуть набувати дані (електронна чи, наприклад, фізична).

Більш практичне визначення можна знайти у М.Ю. Танцюри, який трактує його як відношення рівня інформаційного захисту до рівня інформаційних загроз [2]. Застосування такого визначення дає змогу обчислити ефективність вжитих заходів щодо забезпечення інформаційної безпеки в окремо взятій організації або на підприємстві.

© І.Ю. Маковський, 2020

Основним завданням інформаційної безпеки є збалансований захист конфіденційності, цілісності й доступності даних.

Як зазначає професор Г.Я. Аніловська, на сучасному етапі, з бурхливим розвитком інформаційних технологій і їх широким впровадженням в облікові процеси, виникає проблема взаємодії цих облікових систем з іншими системами та між собою, а також проблема конфіденційності. До того ж ці проблеми існують на технічному, програмному та інформаційному рівнях. Вирішити їх можна шляхом розроблення і впровадження єдиних, загальних і обов'язкових правил побудови та використання облікових інформаційних систем [3]. У світлі розвитку нових ІТ-технологій, поняття «інформаційної безпеки» значно розширилося. Сьогодні від захисту процесів, інформації та діяльності в кіберпросторі залежить значно більше, ніж просто втрата інформації. Тобто втрата інформації призводить до низки інших комплексних ускладнень. Нині комплекс заходів із захисту інформації повинен враховувати, зокрема, антивірусний захист, захист від хакерських атак, підробки даних тощо. Наприклад, враження комп'ютерними вірусами може не лише видалити чи викрасти дані, але й вплинути на роботу та продуктивність співробітників чи навіть зупинити виробництво.

Розглянемо види інформації, що підлягає захисту [4]. Сьогодні держава передбачає захист інформації з обмеженим доступом, в тому числі секретної інформації [5], службової інформації, конфіденційної інформації (в тому числі персональних даних); а також захисту в інформаційно-телекомунікаційних системах має бути відкрита інформація, яка належить до державних інформаційних ресурсів і належить до статистичної, правової, соціологічної інформації, інформації довідково-енциклопедичного характеру та використовується для забезпечення діяльності державних органів або органів місцевого самоврядування, а також інформація про діяльність зазначених органів, яка оприлюднюється в Інтернеті, інших глобальних інформаційних мережах і системах або передається телекомунікаційними мережами [6].

Відповідно до Закону України «Про інформацію», конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація може поширюватися за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом. Іншими словами, кожне підприємство може визначати, яка інформація належить до конфіденційної та щодо якої, відповідно, реалізовувати засоби захисту. Єдиним застереженням є те, що до інформації з обмеженим доступом не можуть належати такі відомості:

1) про стан довкілля, якість харчових продуктів і предметів побуту;

2) про аварії, катастрофи, небезпечні природні явища та інші надзвичайні ситуації, що сталися або можуть статися і загрожують безпеці людей;

3) про стан здоров'я населення, його життєвий рівень, враховуючи харчування, одяг, житло, медичне обслуговування та соціальне забезпечення, а також про соціально-демографічні показники, стан правопорядку, освіти і культури населення;

4) про факти порушення прав і свобод людини, враховуючи інформацію, що міститься в архівних документах колишніх радянських органів державної безпеки, пов'язаних з політичними репресіями, Голодомором 1932–1933 років в Україні та іншими злочинами, вчиненими представниками комуністичного та/або націонал-соціалістичного (нацистського) тоталітарних режимів;

5) про незаконні дії органів державної влади, органів місцевого самоврядування, їх посадових та службових осіб;

6) щодо діяльності державних та комунальних унітарних підприємств, господарських товариств, у статутному капіталі яких більше 50 відсотків акцій (часток) належать державі або територіальній громаді, а також господарських товариств, 50 і більше відсотків акцій (часток) яких належать господарському товариству, частка держави або територіальної громади в якому становить 100 відсотків, що підлягають обов'язковому оприлюдненню відповідно до закону;

7) інші відомості, доступ до яких не може бути обмежено відповідно до законів та міжнародних договорів України, згода на обов'язковість яких надана Верховною Радою України.

В недержавному секторі ми можемо вирізнити захист конфіденційної та окремих видів відкритої інформації. За формою представлення інформація, що підлягає захисту, може бути на матеріальних носіях (паперових, машинних тощо), у вигляді сигналу чи повідомлення, а також інформація, що озвучується.

Далі варто класифікувати загрози інформаційній безпеці. За основу можна взяти класифікацію, яку пропонує О.М. Блінов [7]. Загрози інформаційній безпеці можуть бути класифіковані за різними ознаками (рис. 1):

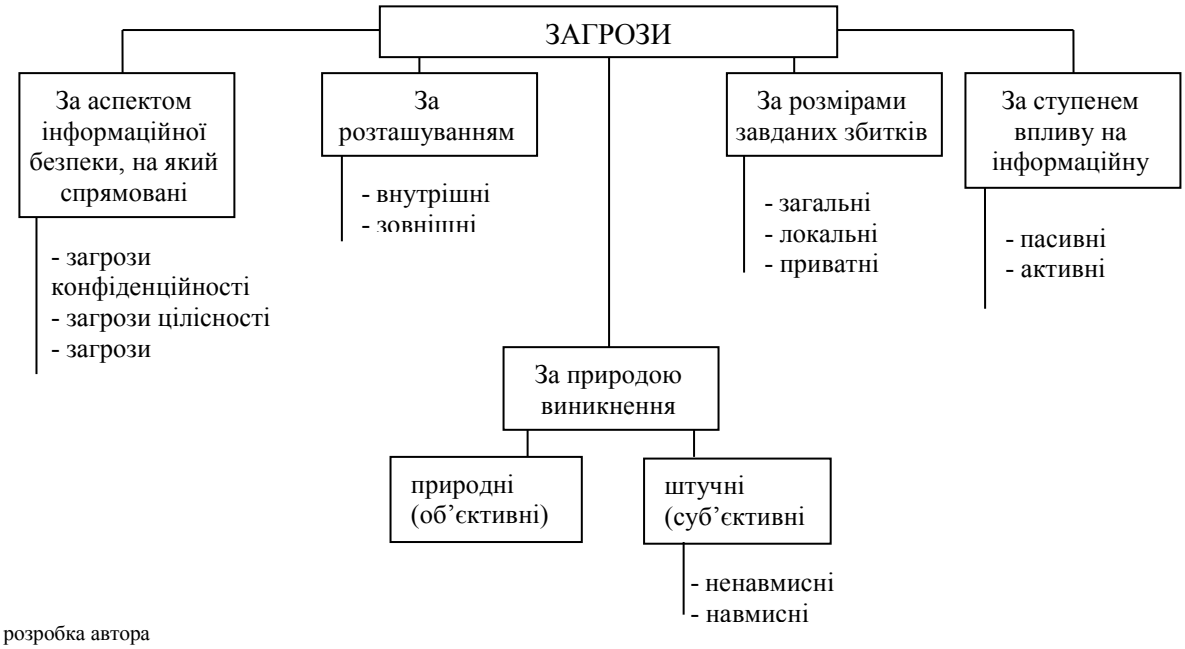
- За аспектом інформаційної безпеки, на який спрямовані загрози:

– загрози конфіденційності (несанкціонований доступ до інформації). Такі загрози полягають у тому, що інформація стає відомою тому, хто не має повноважень доступу до неї. Виникнення подібних загроз може бути зумовлене людським фактором або ж збоями в роботі програмних чи апаратних засобів;

– загрози цілісності (неправомірна зміна даних). Подібні загрози пов'язані з імовірним впливом на дані з метою їх знищення чи перекручення. Причинами порушення цілісності інформації можуть бути як вихід з ладу програмного забезпечення, так і навмисні дії персоналу чи сторонній вплив (наприклад, вірусні атаки);

– загрози доступності (здійснення дій, які унеможливлюють чи ускладнюють доступ до ресурсів інформаційної системи). Задля реалізації таких загроз створюються такі умови, за яких доступ до інформації або блокується, або ж обмежується на час, що унеможливить виконання тих чи інших бізнес-цілей.

- За розташуванням джерела загрози можна розділити на внутрішні – передусім це персонал і програмне забезпечення, що використовуються на підприємстві; та зовнішні – будь-які впливи сторонніх осіб, апаратних засобів, програмного забезпечення тощо.
- За розмірами завданих збитків загрози поділяються на загальні – такі, що можуть завдати значних збитків об'єктові захисту в цілому або ж заподіяти критичної шкоди; локальні – такі, що можуть завдати збитків окремим частинам об'єкта безпеки; приватні – такі, що можуть заподіяти шкоди окремим властивостям елементів об'єкта безпеки.
- За ступенем впливу на інформаційну систему виокремлюють пасивні, за яких структура та зміст системи не змінюються; й активні загрози, вплив яких змінює структуру чи зміст системи в цілому чи окремих її елементів.
- За природою виникнення загрози можна поділити на природні, або об'єктивні – загрози, спричинені впливом на систему природних явищ чи стихії та не залежать від волі людини; та штучні, або суб'єктивні – загрози, спричинені так званим людським фактором, тобто впливом людини на інформаційну систему. Серед штучних загроз у свою чергу вирізняють: ненавмисні (випадкові) загрози, помилки програмного забезпечення, персоналу, збої в роботі систем, відмови апаратних засобів обробки чи передачі інформації; навмисні загрози – умисні дії персоналу чи сторонніх осіб, спрямовані на порушення конфіденційності, цілісності або доступності інформації. Основні проблеми в реалізації політики безпеки будь-якого підприємства пов'язані саме з навмисними загрозами.



Довідка: розробка автора

Рис. 1. Класифікація загроз інформаційній безпеці

Окрім класифікації загроз, потрібно чітко розуміти й те, ким є порушник інформаційної безпеки. Модель порушника у своїх працях розглядали: Ю.М. Щебланін, Д.І. Рабчун [8], А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк [9] та багато інших.

Для того щоб деталізувати можливого порушника інформаційної безпеки, потрібно розробити конкретну для кожного підприємства модель такого порушника. При цьому варто визначитися, що має відображати ця модель. Виходячи з потреб, модель порушника може бути:

– змістовною – відображає цілі порушника, його мотивацію, а також загальний характер його дій під час підготовки та реалізації порушень інформаційної безпеки;

– математичною – визначає послідовність дій порушника, застосовуючи кількісні показники, що характеризують результати й наслідки порушень, а також функціональні зв'язки порушника з елементами об'єкта захисту;

– сценарієм впливу порушника – визначає типи порушень та конкретний алгоритм дій порушника на кожному етапі.

Разом з тим, для найкращої характеристики порушника та його дій необхідно розробляти комплексну модель з урахуванням усіх ступенів деталізації. Для якісного аналізу можливих дій порушника його потрібно класифікувати (рис. 2). Наприклад:

- за місцем дії порушники можуть бути внутрішніми – всі користувачі системи (співробітники підприємства), які мають відповідний рівень доступу до інформації та можуть тією чи іншою мірою впливати на систему (в тому числі, мають права адміністратора й адміністратора безпеки, мають доступ до конфігурування системи тощо); або ж зовнішніми – суб'єкти несанкціонованого доступу до системи чи її елементів (сторонні особи);
- за мотивом порушення носіїв загроз можуть спонукати недбалість або безвідповідальність, тобто, порушник вчиняє дії, спрямовані на порушення безпеки, ненавмисно або ж через власні низькі морально-ділові якості («Недбалий»); самоствердження або помста, тобто, порушник свідомо йде на порушення з метою завдання шкоди підприємству чи його керівництву. Як правило, такий порушник не має високого рівня технічних навичок («Месник»); корисливий інтерес, тобто втручання в роботу системи з метою отримання вигоди. Такий порушник, як правило, має високий рівень технічних навичок («Вигода»);
- за рівнем знань про інформаційну систему порушник може знати структуру й функціональні особливості системи, принципи її функціонування та безпеки, вміє користуватися технічними засобами, що входять до складу системи («Адміністратор»); мати знання та досвід роботи з технічними засобами (елементами системи), їх обслуговування («Технік»); в цілому мати високу кваліфікацію в програмуванні й архітектурі інформаційних систем, але не мати знань щодо конкретної системи («Хакер»); мати високі знання та навички щодо принципів роботи, будови та експлуатації засобів захисту інформації («Налаштувальник»);
- за рівнем можливостей порушники можуть поділятися на таких, що використовують персонал підприємства (штатних користувачів системи) для отримання доступу до інформації чи елементів інформаційної системи («Агент»); застосовують технічні засоби зняття та перехоплення інформації без впливу на інформаційну систему («Розвідник»); використовують штатні технічні засоби та недоліки в їх роботі для обходу засобів захисту, а також портативні машинні носії інформації для проходження постів охорони («Кріт»); застосовують методи й засоби активного впливу на інформаційні ресурси, їх зміни, використовуючи спеціальні апаратно-програмні засоби, технічні пристрої, що мають підключення до каналів передачі даних, впровадження програмних закладок, використання спеціального програмного забезпечення («Програміст»);
- за часом дії порушники можуть реалізовувати загрози інформаційній безпеці безпосередньо під час функціонування системи чи її окремих складових («Робочий час»); у періоди неактивності системи чи її елементів, в тому числі в неробочий час, під час перерв на регламентні роботи тощо («Неробочий час»); як під час функціонування системи, так і під час перерв у їх роботі («Постійно»).

Довідка: розробка автора

Рис. 2. Класифікація порушника інформаційної безпеки

Аналіз і запропонована класифікація загроз інформаційній безпеці, а також потенційних носіїв цих загроз є необхідними умовами для проведення подальших робіт з формування політики інформаційної безпеки на підприємстві. Проведений аналіз вихідних даних, на нашу думку, дозволить продовжити роботу з формування політики безпеки на підприємстві.

Висновки та перспективи подальших досліджень. Ми вважаємо, що визначивши всі можливі загрози, які можуть завдати шкоди інформації на підприємстві, й тим самим завдати певних збитків, передусім фінансових,

а також провівши аналіз потенційних носіїв цих загроз, керівник підприємства отримає набір факторів, на основі яких можна формувати політику інформаційної безпеки. Таким чином, викладена у статті класифікація покликана спростити роботу з формування чітких моделей загроз і порушників, що дозволяє відкинути зайві фактори та зосередитись на тих, що несуть реальну загрозу. Водночас необхідно враховувати й потенційно небезпечні впливи, тобто припускати ймовірність різноманітних загроз. Як зазначав М.Ю. Танцюра [2], важливо визначити, чи не перевищать витрати на реалізацію політики безпеки можливі фінансові втрати від реалізації тих чи інших загроз.

Виходячи з викладеного вище, ми пропонуємо детально розглянути проблему формування функціональних профілів захищеності інформації, що буде напрямом подальших досліджень. Наступними ми проаналізуємо критерії захищеності інформації на підприємстві, на базі яких і формуватиметься відповідний функціональний профіль захищеності з урахуванням конкретних потреб підприємства та видатків, необхідних для реалізації послуг функціонального профілю.

Список використаної літератури:

1. NIST Interagency or Internal Report 7298 : Glossary of Key Information Security Terms / editor *Richard L.* Kissel. – Revision 2. – Gaithersburg. – USA : National Institute of Standards and Technology, 2013. – 222 s.
2. *Танцюра М.Ю.* Забезпечення ефективності системи інформаційного забезпечення підприємства (на прикладі туристичних підприємств АР Крим) : автореф. дис. на здобуття наук. ступеня канд. екон. наук : 08.00.04 / *М.Ю. Танцюра*. – Сімферополь, 2012. – 21 с.
3. *Аніловська Г.Я.* Інформаційна безпека підприємства в умовах використання сучасних інформаційних технологій / *Г.Я. Аніловська* // Науковий вісник ЛНТУ України. – 2008. – Вип. 18 (9). – 270 с.
4. Про інформацію : Закон України від 13.01.2011 № 2938-VI // Відомості Верховної Ради України. – 1992. – № 48. – 650 с.
5. Про державну таємницю : Закон України від 21.09.99 № 1079-XIV // Відомості Верховної Ради України. – 1994. – № 16. – 93 с.
6. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах, затверджені постановою КМУ від 29.03.2006 № 373.
7. *Блинов А.М.* Информационная безопасность : учеб. пособие. Ч. 1 / *А.М. Блинов.* – СПб. : СПБГУЭФ, 2010. – 96 с.
8. *Щебланін Ю.М.* Математична модель порушника інформаційної безпеки / *Ю.М. Щебланін, Д.І. Рабчун* // Кібербезпека: освіта, наука, техніка. – 2018. – № 1 (1). – С. 63–72.
9. Основні параметри для ідентифікації порушника інформаційної безпеки / *А.І. Гізун, В.В. Волянська, В.О. Риндюк, С.О. Гнатюк* // Захист інформації. – 2013. – Вип. 15 (1). – С. 66–74.

References:

1. Richard L. Kissel (ed.) (2013), Interagency or Internal Report 7298, Glossary of Key Information Security Terms, National Institute of Standards and Technology NIST, Revision 2, USA, Gaithersburg, 222 p.
2. Tancjur, M.Ju. (2012), *Zabezpechennja efektyvnosti systemy informacijnogo zabezpechennja pidpryjemstva (na prykladi turystychnyh pidpryjemstv AR Krym*), Abstract of Diss. of. k.e.n., spec. 08.00.04, Simferopol', 21 p.
3. Anilovs'ka, G.Ja. (2008), «Informacijna bezpeka pidpryjemstva v umovah vykorystannja suchasnyh informacijnyh tehnologij», *Naukovyj visnyk LNTU Ukrai'ny*, Issue 18 (9), 270 p.
4. Verhovna Rada Ukrai'ny (1992), Pro informaciju, Zakon Ukrai'ny vid 13.01.2011 No. 2938-VI, *Vidomosti Verhovnoi' Rady Ukrai'ny*, No. 48, 650 p.
5. Verhovna Rada Ukrai'ny (1994), Pro derzhavnu tajemnycju, Zakon Ukrai'ny vid 21.09.99 No. 1079-XIV, *Vidomosti Verhovnoi' Rady Ukrai'ny*, No. 16. 93 p.
6. KMU (2006), Pravyla zabezpechennja zahystu informacii' v informacijnyh, telekomunikacijnyh ta informacijno-telekomunikacijnyh systemah, zatverdzheni postanovoju KMU, vid 29.03, No. 373.
7. Blinov, A.M. (2010), *Informacionnaja bezopasnost'*, ucheb. posobie, Ch. 1, SPBGUJeF, SPb, 96 p.
8. Shheblanin, Ju.M. and Rabchun, D.I. (2018), «Matematychna model' porushnyka informacijnoi' bezpeky», *Kiberbezpeka: osvita, nauka, tehnika*, No. 1 (1), pp. 63–72.
9. Gizun, A.I., Voljans'ka, V.V., Ryndjuk, V.O. and Gnatjuk, S.O. (2013), «Osnovni parametry dlja identyfikacii' porushnyka informacijnoi' bezpeky», *Zahyst informacii'*, Issue 15 (1), pp. 66–74.

Маковський Ігор Юрійович – аспірант кафедри менеджменту і підприємництва Державного університету «Житомирська політехніка».

Наукові інтереси:

– організація та забезпечення захисту інформації;
– інформаційна безпека підприємницької діяльності.

Стаття надійшла до редакції 27.01.2020.