УДК 336.72

ПОБУДОВА КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ МАЛОГО ПІДПРИЄМСТВА

Мартинюк О.О.
Національний технічний університет України
«Національний технічний університет України імені Ігоря Сікорського»

Розглянуто проблему побудови цілісної та якісної системи захисту інформації з обмеженим доступом для малого підприємства. Сформульовано основні етапи планування та моделювання комплексної системи захисту інформації. Проаналізовано негативні чинники, що можуть завадити проведенню якісної її побудови та налаштування.

Ключові слова: моделювання, система захисту інформації, стандартизація, керування ризиками, малі підприємства.

Постановка проблеми. У провідних країнах світу, зокрема США та країнах Євросоюзу, малий бізнес займає значну частину ринку. Це пов'язано з тим, що такий вид підприємництва передбачає стабільну інноваційну складову, виходячи зі значної конкуренції. Саме тому у багатьох країнах існує спрощена система реєстрації малого підприємства та передбачені різного роду допоміжні державні дотації для підприємців, що вирішили почати власну справу.

Згідно із законодавством України, малими підприємствами вважаються юридичні особи, що є суб'єктами будь-якого виду підприємницької діяльності, для яких кількість працюючих протягом календарного року не перевищує 50 осіб, а загально річний дохід не перевищує 500000 євро (ст. 1 Закону України «Про державну підтримку малого підприємництва» від 19.10.2000 р. № 2063-III) [1]. Таким чином малий бізнес може бути способом зменшення безробіття, засобом для розвитку здорової економіки, яка позбавлена монополізації багатьох галузей підприємницької діяльності, і, що найголовніше, джерелом доходів для держави.

Варто враховувати, що сучасний бізнес – як малий, так і середній та великий, використовує у своїй діяльності інформаційні технології для спрощення керування грошовими активами, для мобілізації діяльності та поширення власної продукції. Виходячи з цього, безпека інформації є одним із пріоритетів підприємства, стоячи поруч із отриманням доходу. Адже захищеність персональних даних працівників та клієнтів, інформації про економічні операції та стратегії розвитку є ключовим аспектом якісної і стабільної діяльності підприємства. Проте, якщо для середнього та великого бізнесу використання сучасних технологій, послуг провідних спеціалістів у сфері інформаційної безпеки та впровадження комплексних систем захисту не є проблемою у економічному плані, то для малого підприємництва бюджет, який можна використати для убезпечення інформації з обмеженим доступом від несанкціонованого використання, є порівняно малим. Саме тому питання моделювання та планування системи безпеки інформації є надзвичайно актуальним для малого бізнесу.

Аналіз попередніх досліджень і публікацій показав, що основною проблемою на шляху побудови цілісної та якісної системи захисту інформації з обмеженим доступом є невеликий бюджет та відсутність у штаті відповідних спеціалістів [8]. Виходячи з цього, стає неможливим наступне:

– використання дорогих сучасних систем технічного захисту інформації;

– залучення до побудови комплексної системи захисту інформації провідних спеціалістів із компаній, що спеціалізують на впровадженні систем захисту інформації;

– наймання кваліфікованих працівників для створення якісного відділу захисту інформації в штаті підприємства;

– повна відповідність системи захисту нормативним документам та міжнародним стандартам у галузі інформаційної безпеки та подальше проведення експертних оцінок роботоздатності даної системи.

Проте, виходячи із положень стандартів ISO/IEC серії 27000 [2], можна скласти модель проектування та створення комплексної системи захисту інформації для малого підприємства з урахуванням обмеження кількості персоналу та грошових засобів, порівняно із великими та середніми підприємствами. За основу будуть взяті положення стандарту ISO/IEC 27001 [3].

До невирішених частин загальної проблеми входять: врахувати обмеження малого бізнесу при побудові системи захисту інформації, визначити методику оцінки ризиків та сформувати ключові етапи побудови цієї системи.

Мета статті. Головною метою статті є формування порядку та рекомендацій для побудови комплексної системи захисту інформації для малого підприємства.

Виклад основного матеріалу. Перед початком моделювання системи захисту інформації проводиться аналіз ризиків та кількісно оцінюються втрати при реалізації передбачених загроз.

Виходячи з означення ризику, можна кількісно його оцінити як

$$R = p * q, \quad (1)$$

де p – вірогідність певної загрози, а q – можливі матеріальні в трати у випадку реалізації її негативного впливу на організацію. Для визначення ризиків можна керуватись певною послідовністю: джерело загрози – фактор – загроза – результат [7].

Схема на рис. 1 показує, що ідучи від більш загального (джерела) до більш конкретного (результат) стає можливим якісно оцінити найбільш явні ризики інформаційної безпеки малого під-

приємства. В цьому представленні джерелами загроз можуть бути антропогенні, природні та техногенні носії. Фактором, інакшими словами вразливістю, є така характеристика або властивість об'єкта інформації, що може привести до порушення цілісності, доступності чи конфіденційності інформації. Загроза – це можлива небезпека виконання певних несанкціонованих дій над об'єктом інформації, використовуючи певні його вразливості. Результат – можливий наслідок реалізації загрози при взаємодії джерела загрози з вразливостями.

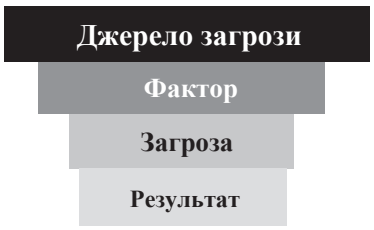

Рис. 1. Послідовність переходу від джерела загроз до її реалізації в процесі визначення ризиків

Для визначення вірогідності кожної загрози доволі важко оперувати конкретними числами, оскільки їхнє знаходження потребує значних обчислювальних ресурсів та врахування великої кількості факторів. В умовах малого бізнесу, де ресурси є строго обмеженими, стає неможливим обрахування точної імовірності загроз. Тому є раціональним розмістити загрози за певною шкалою імовірності – від найімовірніших для даної інформаційної системи до найменш імовірних. Зрозуміло, що така оцінка не є точною і може нести людський фактор, проте вона дає зрозуміти, які загрози є потенційно найнебезпечнішими.

Матеріальні втрати знаходяться як сума витрат від зниження продуктивності атакованого сегмента чи вузла, вартості повторного введення інформації, вартості відновлення вузла, вартості упущеної вигоди від виведення з ладу сегмента чи вузла. Отримана сума матеріальної шкоди буде фігурувати при оцінці затрат на побудову комплексної системи захисту інформації. Якщо в результаті оцінки витрат на систему захисту після її планування витрати при реалізації атаки на сегмент системи виявляться меншими, аніж витрати на саму систему захисту інформації, тоді впровадження такої системи захисту не є раціональним. Втрати також можна поділити на категорії (наприклад, недопустимі, високі, середні, низькі, допустимі). Таким чином створюється матриця загроз, як представлено на рисунку 2.

	Втрати			
Імовірність		Високі	Середні	Низькі
	Висока	Високий	Високий	Середній
	Середня	Високий	Середній	Низький
	Низька	Середній	Низький	Низький

Рис. 2. Проста матриця визначення ризику

Для кожної загрози за цією матрицею визначається її ризик. В результаті оцінки ризиків таким чином виділяються ключові загрози для інформаційної системи.

Планування та розробка системи захисту інформації для малого підприємства відповідає блок-схемі, зображеній на рисунку 3.

Рис. 3. Послідовність розробки системи захисту

1) Провести аналіз ризиків на базі моделі порушника та загроз або ж на базі потоків інформації. Для цього визначають основні напрями роботи підприємства, потім для кожного з них визначають можливі загрози захисту інформації та оцінюють вірогідність реалізації цих загроз [4]. Визначити ступінь ризику для кожної загрози та відібрати ті, що не можуть бути проігноровані.

2) Визначити необхідні заходи для захисту інформації. В залежності від конкретних загроз, визначених у попередньому пункті, визначаються основні заходи захисту. Вони можуть відрізнятись також в залежності від матеріальних можливостей підприємства. Серед таких заходив можуть бути:

– Використання ліцензійних програмних засобів при роботі, зокрема офісних програм (Libre Office, Microsoft Office).

– Використання якісного мережевого екрану.

Особливу увагу потрібно звернути на можливість використання мережевих екранів нового покоління. Перевага їх цих пристроїв полягає у поєднанні функцій різних систем захисту. Зазвичай в них включені функціонал звичного мережевого екрану, URL-фільтрація, система попередження вторгнень (IPS), інспекція зашифрованого трафіку, синхронізація з контролером домену, налаштування VPN, антивірусний і анти-бот захист [5, 6]. В залежності від економічних можливостей компанії можна обирати між різними виробниками і підключати різний функціонал. Зазвичай підключення функціоналу забезпечується підключенням різних ліцензій. Це дозволяє зменшити витрати на використання того функціоналу, що є зайвим для організації.

– Антивірусний захист.

В залежності від того, чи буде антивірусний захист встановлений на кожну окрему обчислювальну станцію, чи буде частиною іншої підсистеми захисту, скажімо, мережевого екрану нового покоління, варіюватиметься його ціна і якість роботи. Поєднання кількох антивірусів на одній обчислювальній станції та використання базових антивірусних засобів операційних систем є поганою практикою і приводить до зниження якості роботи антивірусного захисту.

– Налаштування користувацьких облікові записи в домені. Всі легітимні користувачі корпо-

ративної мережі повинні бути ідентифіковані в домені. Доступи до спільних даних повинні розмежовуватись правами доступу для відповідних користувачів.

– Створити резервні копії всіх ключових ресурсів. Ті системи, які є ключовими для роботи підприємства, зокрема, доменний контролер, поштовий сервер, файлові сервери, мережеві пристрої (мережеві екрани, комутатори, роутери), потрібно дублювати, щоб попередити можливість їхньої недоступності в разі збою.

– Шифрувати дані. Всі дані на обчислювальних машинах користувачів повинні бути зашифровані або базовими засобами операційної системи (BitLocker у Windows), або спеціалізованими програмними засобами (наприклад, Symantec PGP). Встановлення клієнтів повинне виконуватись з допомогою групових політик у час, коли комп'ютер входить у домен компанії.

3) Визначення відповідальних осіб за забезпечення захищеності інформації. Оскільки в малих підприємствах штат працівників обмежується 50 особами, то відповідального за інформаційну безпеку можна призначити серед уже набраних працівників, наприклад, адміністратора мережі.

4) Довести до відома працівників компанії вимоги щодо затвердженої політики безпеки, використаних засобів захисту інформації та зіставити їх із загальними правилами роботи підприємства. Всі працівники повинні мати доступ лише до тих даних, з якими вони мають право працювати і бути достатньо кваліфікованими для якісної роботи із ними, щоб попередити ризики, що пов'язані із людською необережністю чи некомпетентністю.

5) Визначити міри покарання за порушення політики безпеки підприємства та довести це до відома працівників. Оскільки не тільки зовнішні зловмисники можуть бути загрозою для захисту інформації. Причиною компрометації системи захисту можуть стати також інсайдери. Тому обов'язково в підприємстві повинні бути визначені міри покарання за такі дії, як зловмисні, так і через необачність.

6) Задокументувати всі дані щодо системи захисту інформації. Документацію потрібно вести згідно із заданими правилами та нормами, що описані у нормативних документах чи статуті підприємства.

7) Проводити регулярні перевірки та документувати всі спроби компрометування системи захисту інформації для унеможливлення реалізації відомих загроз захисту інформації.

Негативними чинниками, що можуть завадити проведенню якісної побудови та налаштування системи захисту інформації можуть бути:

– небажання керівництва підприємства витрачати ресурси на створення системи захисту інформації;
– обмеження у людських ресурсах;
– обмеження у матеріальних ресурсах;
– некомпетентність персоналу.

Таким чином, побудова системи захисту інформації потребує якісного попереднього аналізу та скрупульозності при виконанні кожного етапу.

Висновки і пропозиції. Отже, малий бізнес є дуже важливою ланкою сучасної економіки. Особливо значущим є те, що юридичні особи-підприємці у своїй діяльності використовують сучасні інформаційні технології та керують потоками даних різного ступеню доступності. Тому побудова системи захисту інформації навіть для таких підприємств є дуже важливою. Більше того, вона ускладнюється обмеженнями у економічному плані та з точки зору нестачі кваліфікованих фахівців. Якщо для великих підприємств можна строго будувати систему захисту інформації відповідно до нормативних документів та стандартів ISO/IEC, то для малого бізнесу стає неможливим залучення до такої роботи експертів. Таким чином, відповідальність за якість побудови системи безпеки лежить безпосередньо на керівниках малого підприємства. Вирішення таких проблем можливе, якщо спростити аналіз чинників та побудувати систему захисту інформації за вище описаною моделлю.

Список літератури:

1. Закон України «Про державну підтримку малого підприємництва» [Електронний ресурс] – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2063-14
2. Матеріали щодо стандартизації та сертифікації [Електронний ресурс] – Режим доступу: http://intercert.com.ua/articles/regulatory-documents/210-iso-27000-seriya
3. Международный стандарт ISO-IEC 27001 [Електронний ресурс] – Режим доступу: http://etr-spektr.com.ua/standarts_download/ISO-IEC_27001-2005.pdf
4. Иванченко П.Ю., Кацуро Д.А., Медведев А.В., Трусов А.Н. Математическое моделирование информационной и экономической безопасности на предприятиях малого и среднего бизнеса [Електронний ресурс] – Режим доступу: http://rae.ru/fs/?section=content&op=show_ article&article_id=10002191
5. Анатолий Скородумов Почему все переходят на системы защиты нового поколения – Firewall: Next Generation [Електронний ресурс] – Режим доступу: http://www.itsec. ru/articles2/firewall/pochemu-vse-perehodyat-na-sistemy-zaschity-novogo-pokoleniya-firewall-next-generation
6. 700 Security Appliances [Електронний ресурс] – Режим доступу: https://www.checkpoint.com/products/700-security-appliances/
7. Риски информационной безопасности веб-приложений [Електронний ресурс] – Режим доступу: https://habrahabr.ru/company/pentestit/blog/279219/
8. Особенности обеспечения информационной безопасности малого и среднего бизнеса [Електронний ресурс] – Режим доступу: https://www.anti-malware.ru/Small_Business_Security

Мартынюк А.А.
Национальный технический университет Украины
«Киевский политехнический институт имени Игоря Сикорского»

ПОСТРОЕНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ МАЛОГО ПРЕДПРИЯТИЯ

Аннотация
Рассмотрена проблема построения целостной и качественной системы защиты информации с ограниченным доступом для малого предприятия. Сформулированы основные этапы планирования и моделирования комплексной системы защиты информации. Проанализированы негативные факторы, которые могут помешать проведению качественной ее построения и настройки.
Ключевые слова: моделирование, система защиты информации, стандартизация, управление рисками, малое предприятие.

Martyniuk O.O.
National Technical University of Ukraine
«Igor Sikorsky Polytechnic Institute»

BUILDING AN INFORMATION SECURITY SYSTEM FOR A SMALL BUSINESS WERE INVESTAGATED

Summary
The problem of constructing an integrated qualitative system protection of classified information for small business was reviewed. The basic stages of planning and modeling of information security system were formed. Negative factors that can prevent a quality of construction and customization of the security system were analyzed.
Keywords: modeling, information security system, standardization, risk management, small business.