О. І. Богдан
здобувач кафедри
адміністративного та фінансового права
Національного університету природокористування
і біоресурсів України (м. Київ)

УДК 34:65.012.45

ПЛАНУВАННЯ В СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

У статті розглядаються правові питання планування у сфері технічного захисту інформації, що є важливою складовою ефективної системи управління у досліджуваній царині правовідносин.

В статье рассматриваются вопросы планирования в сфере технической защиты информации, что является важной составной эффективной системы управления в исследуемой области правоотношений.

In the article in the field of technical protection planning issues are discussed. That is vital constituent of effective control system in the analyzed field of legal relation.

Технічний захист інформації (ТЗІ) — це діяльність, спрямована на забезпечення інженерно—технічними заходами порядку доступу, цілісності та доступності (унеможливлення блокування) інформації, яка становить державну та іншу передбачену законом таємницю, конфіденційної інформації, а також цілісності та доступності відкритої інформації, важливої для особи, суспільства і держави.

У державному стандарті ДСТУ 3396.0-96 [1] визначено основні цілі технічного захисту інформації. Відповідно до даного документу такими є: запобігання витоку чи порушенню цілісності інформації з обмеженим доступом [1, с. 3]. Згідно того ж документу, досягнення цілей ТЗІ може бути реалізовано шляхом побудови системи захисту інформації (СЗІ) яка являє собою організовану сукупність методів і засобів забезпечення ТЗІ [1, с. 3].

Таким чином, система захисту інформації є утворенням, призначеним для досягнення цілей захисту інформації, а методи забезпечення ТЗІ — однією з центральних категорій у галузі технічного захисту інформації. Разом із цим, проведений нами аналіз більше, ніж 30 наукових досліджень та публікацій (зокрема, робіт Ю. Я. Самохвалова, В. О. Темнікова, В. О. Дорошко [2], Л. І. Северина, С. Л. Северина, А. В. Дудатьєва [3], В. В. Домарева [4], В. І. Ярочкіна [5]) дозволяє стверджувати, що на сьогодні питання визначення методологічної бази у сфері захисту інформації залишається відкритим. Зокрема, явно недостатня увага приділяється питанням підвищення ефективності управлінської діяльності в сфері технічного захисту інформації шляхом застосування науково визначених методів управління.

На перший погляд здається, що така ситуація обумовлена детальною регламентацією управлінської діяльності діючою нормативною базою (зокрема, державними стандартами України ДСТУ 3396.0-96 1], ДСТУ 3396.1-96 [6], нормативними документами системи технічного захисту інформації НД ТЗІ 1.4-001-2000 [7], НД ТЗІ 2.1-001-2001 [8] тощо) — відповідно, необхідність визначення методів управління в сфері ТЗІ не виглядає аж надто актуальною.

Разом із цим ми приєднуємося до думки відомого фахівця в галузі управління В. Д. Сущенка, який у монографічному дослідженні [9] слушно зазначає: "Дії виконавця і керівника визначаються тим, наскільки він володіє науковим апаратом, сучасними методами управління, розуміє тенденції розвитку системи управління" [9, с. 7]. Більше того, актуальність такої позиції по відношенню до сфери управління технічним захистом інформації підтверджується досвідом практичної діяльності автора.

Відсутність чітко сформованого управлінського підходу до процесів побудови та функціонування системи захисту інформації призводить до цілого ряду негативних

www.univer.km.ua Університетські наукові записки, 2009, № 2(30), с. 212-215.

наслідків. Застосування нами методології системного підходу дозволило розподілити їх на дві групи: негативні наслідки на рівні окремо взятої системи захисту інформації підприємства, установи, організації та негативні наслідки на державному рівні.

До першої групи ми віднесли:

1. Підміну в процесі проведення робіт з технічного захисту інформації основних цілей ТЗІ, зазначених вище, на одну — побудову системи захисту інформації. Це призводить до недооцінки важливості управлінської діяльності, яка, після завершення створення СЗІ, часто зводиться виключно до контрольних функцій.

2. "Випадання" системи захисту інформації з кола об'єктів управлінської діяльності підприємства, відповідно — зниження ефективності її функціонування.

3. Як один із можливих наслідків попереднього пункту — ускладнення, а іноді і неможливість урахування економічних показників ефективності при створенні та функціонуванні СЗІ, коли заходи щодо забезпечення безпеки інформації не лише не окуповуються, а й шкодять нормальному розвиткові та функціонуванню підприємства в цілому, або ж навпаки, ужиті заходи не дозволяють забезпечити ефективний розвиток через низький рівень фінансування і, як наслідок, недостатній рівень інформаційної безпеки.

До другої групи ми віднесли:

1. Відсутність серйозних наукових досліджень процесів управління системою захисту інформації.

2. Диспропорційність нормативно—правової бази у галузі ТЗІ, коли питанням управлінської діяльності приділяється незаслужено мала увага.

3. Дисонанс між системами захисту інформації та іншими суміжними системами, що забезпечують безпеку інформації (наприклад системою охорони державної таємниці). Така неузгодженість виникає на рівні держави і, як наслідок, на рівні окремого підприємства.

4. Загальне відставання від світового рівня безпеки інформації, коли Україна вимушена орієнтуватись на показники захищеності, розроблені у інших державах, замість стати розповсюджувачем передового досвіду у даній галузі.

5. Суттєве ускладнення формування загальнодержавної системи захисту інформації, яка включає в себе всі існуючі локальні СЗІ (як такі, що створюються у державному секторі, так і приватні). Це відбувається внаслідок різних управлінських підходів, що застосовуються керівниками окремих підприємств, установ, організацій. Відсутність єдиного підходу на найнижчих рівнях не дозволяє застосувати єдиний підхід і на рівні держави.

Подальше нівелювання значення методології управлінського підходу для галузі технічного захисту інформації може призвести до ситуації, коли протягом найближчих двох-трьох років відставання рівня розробленості сфери управління системами захисту інформації від передових управлінських наукових тенденцій набуде катастрофічних масштабів, а як наслідок — відбудеться зниження рівня захищеності інформації в усіх життєво важливих сферах діяльності в Україні.

Очевидна необхідність вирішення окресленого кола проблем обумовила актуальність обраної нами теми, визначила предмет, мету і задачі даної роботи. У статті, відповідно до предмету дослідження, ми спробували обґрунтовано довести необхідність застосуванням методології управління при створенні та забезпеченні функціонування систем захисту інформації. При чому ми не обмежуємося вивченням питань сфери ТЗІ, що вже досліджувалися раніше, а демонструємо власні теоретичні погляди на систему захисту інформації як об'єкт управління.

Головною метою нашого дослідження є привернути увагу фахівців із захисту інформації та управлінської сфери до методологічних проблем управління системами захисту інформації.

Обсяги статті не дозволяють нам провести повний аналіз системи технічного захисту інформації України на предмет відповідності методів управління, властивих даній системі, останнім науковим доробкам. Тому нами прийнято рішення застосувати метод екстраполяції, відповідно до якого, дослідивши процеси, що відбуваються при створенні системи захисту інформації окремо взятого підприємства, ми отримаємо уявлення і про стан проблеми для системи ТЗІ України взагалі. Враховуючи, що вивчення методів управління не є предметом даного дослідження, ми використали перелік власне управлінських методів, запропонований у монографічному дослідженні [9]. До окремонаукових методів сфери управління у даній статті віднесено методи: системного

Університетські наукові записки, 2009, № 2 (30), с. 212-215. www.univer.km.ua

аналізу, дослідження операцій, моделювання, організаційного проектування, сітьового планування.

Згідно з положеннями монографії [9] системний аналіз є окремим випадком системного дослідження, який має своїм об'єктом системи, що створені людиною, а предметом — проблеми управління цими системами [9, с. 118]. Враховуючи, що системи захисту інформації створюється людьми і є керованими (більше того, управління такими системами є одним із важливих напрямів діяльності в сфері ТЗІ), ми можемо зробити висновок про можливість використання даного методу для дослідження систем захисту інформації.

Застосування системного аналізу у сфері управління СЗІ підприємства дасть можливість:

а) з урахуванням усієї сукупності економічних та соціально-політичних умов чітко сформулювати цілі захисту інформації на підприємстві і з'ясувати їхню ієрархію до початку робіт зі створення системи захисту інформації;

б) встановити конкретні взаємопов'язані завдання для кожного рівня та ланки управління системою захисту інформації (зокрема, для керівництва підприємства, керівника служби захисту інформації тощо) виходячи з його внеску в досягнення цілей захисту інформації з узгодженням строків, потрібних та наявних ресурсів на єдиній інформаційній, методичній та процедурній основі;

в) підготувати та всебічно оцінити альтернативні варіанти управлінських рішень за критерієм досягнення оптимального рівня захищеності інформації підприємства;

г) здійснити виділення та розподіл матеріальних, фінансових і людських ресурсів з урахуванням пріоритетності цілей та напрямів діяльності щодо створення та забезпечення функціонування СЗІ, їх взаємозв'язку та фактора часу;

д) оцінити управлінський потенціал системи захисту інформації, з'ясувати необхідність та можливості делегування відповідальності і повноважень по рівнях ієрархії управління.

Дослідження операцій, на думку авторів [9], являє собою комплекс заснованих на системному аналізі логічних дій та методів прикладної математики, що використовуються для вироблення логічних та кількісних основ управлінських рішень [9, с. 129]. Можливість застосування зазначених методів у сфері захисту інформації не викликає сумніву. За аналогією із висновками авторів монографії, ми можемо виділити чотири великих блоки, де комплексне застосування сучасних методів дослідження операцій може сприяти здобуттю найкращих кінцевих результатів:

а) підвищення мобільності та швидкості реагування служби захисту інформації підприємства на порушення встановленого порядку поводження з інформацією;

б) підвищення ефективності взаємодії структурних підрозділів підприємства в процесі створення та забезпечення функціонування системи захисту інформації;

в) інтенсифікація процесів управління системою захисту інформації підприємства;

г) підвищення ефективності розслідувань випадків порушень встановленого порядку поводження з інформацією.

Важливе місце в ряду методів управління, застосування яких, дозволить значно підвищити ефективність захисту інформації, займає метод моделювання. Згідно з положеннями монографії [9] моделювання — це метод теоретичного та практичного опосередкованого пізнання, коли суб'єкт замість безпосереднього об'єкта пізнання обирає чи створює схожий із ним допоміжний об'єкт—замісник (модель), досліджує його, а здобуту інформацію переносить на реальний предмет вивчення [9, с. 122].

Застосування даного методу у сфері управління СЗІ підприємства дозволяє:

а) використовувати у процесі створення та забезпечення функціонування СЗІ електронно—обчислювальну техніку для автоматизації окремих робіт;

б) розрахувати ефективність створюваної СЗІ на етапі розробки такої системи;

в) спроектувати організаційну структуру служби захисту інформації, з урахуванням особливостей функціонування підприємства;

г) створити модель потенційного порушника СЗІ, з метою виявлення найбільш слабких місць створеної системи захисту інформації;

д) розробити плани першочергових дій на випадок атак на систему захисту інформації підприємства;

е) прогнозувати збитки підприємства у разі скоєння порушень встановленого порядку поводження з інформацією.

Суть організаційного проектування, на думку авторів [9], полягає у корекції

www.univer.km.ua Університетські наукові записки, 2009, № 2 (30), с. 212-215.

структури та кількості працівників підприємства його керівником відповідно до особливостей зовнішнього середовища, обсягів робіт, що виконуються, навантаження на персонал. Враховуючи, що об'єктам нашого дослідження обрано окреме підприємство, можливості по застосуванню методології організаційного проектування у першу чергу залежать від повноважень керівника відповідного рівня. Наприклад, якщо підприємство очолює його власник — він самостійно визначає структуру всього підприємства в цілому та служби захисту інформації зокрема, або ж може делегувати частину своїх повноважень керівникам нижчого рівня. Для підприємства державної форми власності, у більшості випадків можливості керівника по корекції структури обмежені.

Сітьове планування, відповідно до монографії [9] входить до великої групи методів оптимізації планових рішень. Враховуючи, що дослідження процесів планування являє собою окрему, досить значну, сферу управлінської діяльності ми обмежимося лише констатацією фактів: діючою нормативною базою передбачено використання планів у процесі створення та забезпечення функціонування системи захисту інформації, однак вивчення ефективності процесів планування в даній сфері має стати предметом окремого дослідження.

Відтак є достатні підстави стверджувати про необхідність розгляду процесів створення та функціонування системи захисту інформації крізь призму управлінської діяльності. Застосування найновіших методологічних розробок сфери управління дозволить підвищити ефективність функціонування системи технічного захисту інформації України.

Отримані нами результати можуть стати основою для нових наукових розробок теорії управлінської діяльності у галузі ТЗІ, а також можуть бути використані у процесі створення та забезпечення діяльності системи захисту інформації окремого підприємства, установи, організації.

Перспективними напрямами подальших наукових досліджень є:

а) вивчення можливості впровадження у сферу ТЗІ інших найсучасніших методів управлінської діяльності;

б) адаптація методів управлінської діяльності до вирішення специфічних завдань по захисту інформації;

в) розробка практичних рекомендацій по застосуванню методології управління при створенні та забезпеченні функціонування систем захисту інформації;

г) вироблення спеціальнонаукових методів досліджень в галузі ТЗІ.

Список використаних джерел

1. ДСТУ 3396.0-96. Технічний захист інформації. Основні положення. — Введено вперше; Чинний від 1997-01-01. — К. : Держстандарт України, 1997. — 15 с.
2. *Самохвалов Ю. Я.* Організаційно-технічне забезпечення захисту інформації : Навч. посіб. [Ю. Я. Самохвалов, В. О. Темніков, В. О. Хорошко] / За ред. В. О. Хорошка. — К. : НАУ, 2002.
3. *Северин Л. І.* Правове забезпечення захисту інформації. Навч. посіб. / Л. І. Северин, С. Л. Северин, А. В. Дудатьєв. — Вінниця : ВНТУ, 2004. — 145 с.
4. *Домарев В. В.* Безопасность информационных технологий. Системный подход. / В. В. Домарев. — К. : ООО "ТИД "ДС", 2004. — 992 с.
5. *Ярочкин В. И.* Предприниматель и безопасность. Часть I. / В. И Ярочкин. — М. : "Экспертное бюро", 1994. — 64 с.
6. ДСТУ 3396.1-96. Технічний захист інформації. Порядок проведення робіт. — Введено вперше; Чинний від 1997-07-01. — К. : Держстандарт України, 1997. — 11 с.
7. Типове положення про службу захисту інформації в автоматизованій системі. НД ТЗІ 1.4-001-2000 / Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. — К. : ДСТСЗІ СБ України, 2000. — 54 с.
8. Створення комплексів технічного захисту інформації. Атестація комплексів. Загальні положення. НД ТЗІ 2.1-001-2001 / Департамент спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України. — К. : ДСТСЗІ СБ України, 2001. — 7 с.
9. *Сущенко В. Д.* Організація управління персоналом в органах внутрішніх справ : Монографічне дослідження / В. Д. Сущенко, А. М. Смирнов, О. І. Коваленко, А. А. Смирнов. — К. : Національна академія внутрішніх справ України, 1999. — 352 с.

Надійшла до редакції 11.06.2009
Рекомендована до друку 19.06.2009

У університетські наукові записки, 2009, № 2 (30), с. 212-215. www.univer.km.ua