Богдан О. І., Національний університет природокористування і біоресурсів

ПЛАНУВАННЯ В СФЕРІ ТЕХНІЧНОГО ЗАХИСТУ ІНФОРМАЦІЇ

В статье автор раскрывает понятие технической защиты информации, ее планирование, и основные цели.

In the article the author opens concept of technical protection of the information, its planning, and main objectives.

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 з цим, проведений нами аналіз більше ніж 30 наукових досліджень та публікацій (зокрема робіт Самохвалова Ю. Я., Темнікова В. О., Хорошко В. О. [2], Северина Л. І., Северина С. Л., Дудатьєва А. В. [3], Домарева В. В. [4], Ярочкіна В. І. [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 з 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 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 невіліювання 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 аналізу*, *дослідження операцій*, *моделювання*, *організаційного проектування*, *сітьового планування*.

Згідно положень 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.

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.

Важливе місце в ряду методів управління, застосування яких, дозволить значно підвищити ефективність захисту інформації, займає метод *моделювання*. Згідно положень 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].

Суть *організаційного проектування*, на думку авторів [9], полягає у корекції структури та кількості працівників підприємства його керівником відповідно до особливостей зовнішнього середови-

ща, 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. Проте у будь-якому випадку, застосування методології організаційного проектування є обов'язковим на етапі створення служби захисту інформації.

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.

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.

Література:

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., Темніков В. О., Хорошко В. О. Організаційно-технічне забезпечення захисту інформації. Навчальний посібник / За ред. проф. В. О. Хорошка – К.: НАУ, 2002. – 207 с.

3. Северин Л. І., Северин С. Л., Дудатьєв А. В. Правове забезпечення захисту інформації. Навчальний посібник. – Вінниця: ВНТУ, 2004. – 145 с.
4. Домарев В. В. Безопасность информационных технологий. Системный подход. – К.: ООО «ТИД «ДС», 2004. – 992 с.
5. Ярочкин В. И. Предприниматель и безопасность. Часть І. – 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., Смирнов А. М., Коваленко О. І., Смирнов А. А. Організація управління персоналом в органах внутрішніх справ. Монографічне дослідження. – Київ: Національна академія внутрішніх справ України, 1999. – 352 с.

Осін В. В., Академія митної служби України

ЩЕ РАЗ ДО ПИТАННЯ ПРО ІГРОВУ ОСНОВУ ПОЛІТИЧНОЇ НАУКИ

В статье предпринимается попытка выявить объяснительный потенциал интерпретации политической науки как игры, для чего используется концепция Й. Хёйзинги. Многие факты институциональной жизни политологии оказываются рассмотренными в качестве естественных последствий игровой сущности политической науки.

The attempt to reveal the explaining potential for interpretation the political science as a play is made in the article. J. Huizinga's theory is used. Many facts of the institutional life of this kind are considered as an integral part of political science's play nature.

Опитування, проведене серед членів *Американської асоціації політологів* в 1961 році, тобто в період їхнього найбільшого – принаймні, з ретроспективної точки зору – оптимізму, зокрема показав,