ЗАХИСТ ІНФОРМАЦІЇ В ДЕРЖАВНИХ СТРУКТУРАХ УКРАЇНИ

Сулятицький П. Р., курсант; Грицюк Ю. І., д.т.н., проф.
Львівський ДУ БЖД, м. Львів, Україна

За останні декілька років почала приділятися особлива увага захисту конфіденційної інформації в різних державних структурах [2], в т.ч. і структурних підрозділах Державної служби України з надзвичайних ситуацій (ДСНС України). Проте, за відсутності належного фінансування, здебільшого використовується принцип максимальної заборони, який міцно укорінився й у підходах до побудови систем захисту інформації (СЗІ) [1]. Водночас, використання такого підходу не завжди сприяє успішній взаємодії та обміну інформацією не тільки між різними державними відомствами, але й в середині самої структури.

Спробуємо розглянути деякі проблеми, з якими стикаються структурні підрозділи ДСНС України при побудові СЗІ з використанням часто застарілих принципів, і тих позитивних тенденцій, які закладено в Указі Президент України «Про Положення про технічний захист інформації в Україні», тобто дають надію на значне поліпшення ситуації в майбутньому, що й становить основну мету цієї роботи.

Основною особливістю підходу до побудови СЗІ в структурних підрозділах ДСНС України є обов'язкове використання сертифікованих засобів – ліцензіатів державних органів влади. Їх використання у СЗІ забезпечує конфіденційність переданої інформації та дотримання законодавства — що, поза всяким сумнівом, важливо для державних установ. Водночас, розробники таких засобів часто дотримуються вимог, які пред'являє сертифікаційний орган [2], забуваючи при цьому про їх функціональність. Окрім цього, час, витрачений розробником на сертифікацію засобів СЗІ, також впливає не на користь їх функціональності. Відомо, що програмний продукт чи апаратний засіб, який отримав сертифікат, через різні затримки в часі може стати застарілим з точки зору підтримуваних ним різних платформ чи інших нововведень.

В Україні так склалося, що СЗІ різних відомств розроблялися відособлено одна від інших, внаслідок чого уніфікованих і стандартизованих правил взаємодії між ними не було вироблено [1]. Розроблення схеми взаємодії між різними державними структурами та відомствами — надзвичайно дорогий процес, а його ефективність залежить від чинників, на які можна вплинути тільки опосередковано або не впливати взагалі.

Сьогодні в структурних підрозділах ДСНС України актуальною залишається проблема недостатнього фінансування, в т.ч. призначеного для забезпечення інформаційної безпеки. Але ситуація поступово міняється, тобто в багатьох головних і територіальних управліннях, ця проблема ус-

пішно вирішується. Однак існує ще немало районних підрозділів, яких вона ще навіть не торкнулася. Внаслідок цього головні чи територіальні управління з надзвичайних ситуацій намагаються «заощадити» на впровадженні СЗІ, і наслідки такої «вигоди» очевидні. Здебільшого в районах відсутні не тільки СЗІ, але й фахівці з інформаційної безпеки.

Часто проектування СЗІ навіть в головних управліннях проводиться власними силами без залучення сторонніх фахівців. Це призводить до того, що прийняті рішення щодо захисту комп'ютерного обладнання та мережевого устаткування здебільшого копіюється з інших управлінь, а при виборі архітектури СЗІ керуються не реальними завданнями, а дотриманням формальних вимог. Окрім цього, фахові знання кадрових працівників, які відповідають за інформаційну безпеку, далекі від нормативних. Як правило, такі співробітники переважно мають знання з області обов'язкових вимог до технічних засобів захисту інформації. Внаслідок цього інформаційна безпека зводиться до формального дотримання законодавства і регламентів її забезпечення, тоді як реальна її складова — набагато ширша проблема.

Однією з проблем структурних підрозділів ДСНС України є вибір пріоритетів – куди саме мають бути направлені зусилля щодо забезпечення інформаційної безпеки і наскільки важливо дотримуватись протоколу, аби забезпечити необхідний рівень захищеності інформаційної системи. Сьогодні в ЗМІ багато говориться про проблему внутрішньої інформаційної безпеки, про значні витоки інформації за халатності чи низької кваліфікації працівників. Значна кількість статистичних даних свідчить про те, що в цьому напрямі є великі прогалини в роботі насамперед працівників служби інформаційної безпеки. Якщо на шкідливі програми і хакерські атаки вони завжди реагують як на загрозу, від якої необхідно захищатися, то внутрішні вороги (тобто інсайдери) хоча і сприймаються такими ж небезпечними, проте заходи захисту від них застосовуються не завжди, не скрізь і в недостатньому обсязі.

Доводиться констатувати, що інформаційну безпеку в структурних підрозділах ДСНС України ще й до цього часу не вдалося повністю позбавити від перерахованих вище проблем. Проте існують резервні можливості, використовуючи які головні, територіальні та районні управління пожежно-рятувальних служб в змозі вивести захищеність своїх інформаційних систем на значно вищий і прогресивніший рівень, який би відповідав хоча б нормативних показникам їх експлуатації.

Література

1. Грайворонський М. В. Безпека інформаційно-комунікаційних систем / М. В. Грайворонський, О. М. Новіков — К. : Вид. група BHV, 2009. — 608 с.

2. Макаренко Є. А. Міжнародна інформаційна безпека: сучасні виклики та загрози / Є. А. Макаренко, М. А. Ожеван, М. М. Рижков та ін. — К. : Центр Вільної преси, 2006. — 916 с.