ІНФОРМАЦІЙНА БЕЗПЕКА БІЗНЕСУ: СИСТЕМНИЙ ПІДХІД

Радіонов В. С., *аспірант Навчально-наукового Інституту економіки і менеджменту, Харківський національний університет міського господарства імені О. М. Бекетова*

Протягом кількох років ми спостерігаємо, що в нашому суспільстві серед фахівців, які так чи інакше стосуються питань безпеки взагалі та питань інформаційної безпеки зокрема, не знижується інтерес до питань забезпечення інформаційної безпеки бізнесу. Існує значна кількість публікацій з різних аспектів безпеки, кожна з яких більшою чи меншою мірою претендує на певну точку зору чи інтерпретацію цього складного питання стосовно бізнесу. Слід зазначити, що загальних, системних підходів до проблеми, зазвичай, не формулюються, кожен аналізований і аналізований аспект відбиває лише професійні переваги фахівців.

Загалом для ситуації характерний вузькоспеціалізований підхід, погляд на проблему крізь призму професійних прихильностей, що ніколи й ніде не сприяло розумінню питання і, зрештою, справі.

У цьому багатоголоссі практичному фахівцю, який реально займається питаннями забезпечення безпеки власної організації, досить складно орієнтуватися, знайти відповіді на питання, що виникають, виробити правильний шлях діяльності. Це підтверджують гострота і розпал дискусій, що спалахують практично з будь-якого питання, як зараз, наприклад, з проблеми персональних даних.

Слід сказати, що наша країна загалом орієнтується на економічну відкритість, взаємодію із західним бізнесом, тому потрібна платформа для такої взаємодії. Один із практичних кроків на цьому шляху – широке використання зарубіжних стандартів та кращих практик там, де досі не вдалося створити сучасних вітчизняних регламентів, стандартів та правил. Гостро постало питання транскордонної взаємодії економічних суб'єктів, а також інститутів держав. Для такої взаємодії також потрібні універсальні правила, зрозумілі, прийнятні та однаково застосовні у країнах, де знаходяться суб'єкти цих відносин.

На цьому фоні безпека як специфічна галузь знань переживає виключно динамічний етап розвитку. Протягом тисяч років під забезпеченням безпеки інформації розумілось виключно завдання забезпечення її конфіденційності. Були випробувані різні способи забезпечення конфіденційності – від таємнопису та використання незнайомої іноземної мови для приховання інформації від недруга до відрізання мови носієві інформації, що було, мабуть, ефективно в умовах, коли писемністю володіли одиниці людей і онімілий носій не міг передати нікому знання секрету. У результаті конкуренції методів забезпечення конфіденційності розвинулося і перемогло новий науковий напрямок – криптографія, у якому працювали та працюють видатні математики як минулого, так і сучасності.

Цей напрямок отримав два поштовхи в XX столітті – радіо представило нову можливість передачі інформації по «ефіру», і відразу виникла необхідність передавати по відкритих «ефірних» каналах великі обсяги конфіденційної інформації, а пізніше з'явилися обчислювальні машини, спочатку аналогові, трохи пізніше електронні, які одночасно були використані на вирішення двох завдань: створення ефективних шифрів і алгоритмів та його «злом».

І нарешті, у 1980-ті роки все суттєво змінилося у зв'язку з появою персональних ЕОМ та трохи пізніше – виникненням мережі інтернет. У зв'язку зі створенням великих баз даних та переведенням все більших обсягів інформаційних ресурсів у цифрову форму, у проблемі захисту інформації намітилося зрушення від інженерного підходу до питань інформатики в область управління доступом до обчислювальних та інформаційних ресурсів.

Міжнародними експертами в галузі безпеки приблизно в один час було сформовано два напрямки розвитку – створення технічних стандартів із забезпечення безпеки продуктів інформаційних технологій під загальною назвою «Загальні критерії» та створення сімейства стандартів якості, а останнім часом – управління, під загальною назвою «Стандарти аудиту безпеки» [1].

Стало очевидно, що «Загальні критерії» не набули широкого поширення через ряд причин (обмеженість сфери застосування, складність і обмеженість використовуваних механізмів оцінок), тому почалося їх активне доопрацювання у напрямку другої групи стандартів, а сама група стандартів аудиту збагатилася концепцією «ризик-орієнтованого підходу» [2], що означало фундаментальні зміни в концептуальних поглядах на проблему безпеки в цілому та зсув проблеми захисту інформації, а якщо точніше – інформаційної безпеки у сферу управління складними технічними системами та колективами як експлуатаційного персоналу, так і користувачів.

Останнім часом у теорії та практиці управління виник ще один напрямок – створення стандартів управління організаціями, що має на меті оптимізацію внутрішньої структури організації для отримання максимального результату від їх діяльності (реінжиниринг) [3].

Об'єкт захисту, тобто те, до чого прикладаються сервіси безпеки з метою надати цьому об'єкту важливу додаткову, спочатку відсутню властивість – захищеність (надійність, стійкість), є в абсолютній кількості випадків складною системою.

При цьому в практичному житті ми зазвичай маємо справу зі складними системами, складеними у свою чергу не з простих елементів, а складних систем. Таким чином, ми маємо справу зі складними системами складних систем.

Стосовно питань безпеки слід враховувати такі характеристики складних систем:

– найімовірніший відгук складної системи на одиничний вплив – хаотичний;

– складна система має нові інші властивості, ніж сукупність властивостей елементів, що становлять цю систему;

– відгук складної системи на вплив є нелінійним і змінюється в залежності від сили цього впливу. Нові властивості системи при слабких впливах можуть виявлятися, тому не можна з упевненістю сказати, що властивості конкретної складної системи повністю вивчені і її поведінка під впливом потужного впливу передбачувано.

Безпека як самостійний об'єкт дослідження також має деякі фундаментальні властивості:

– безпека ніколи не буває абсолютною – завжди є певний ризик її порушення, таким чином, зусилля щодо забезпечення безпеки реально зводяться до завдання зниження рівня ризику до прийнятного рівня, не більше;

– виміряти рівень безпеки неможливо, можна лише побічно його оцінити, вимірявши відповідні показники, що характеризують стан безпеки системи; у зв'язку з цим можна говорити лише про ймовірність настання тієї чи іншої події та ступеня її наслідків, тобто використовуватиме для оцінок рівня безпеки ризиковий підхід;

– настання ризикової події в загальному випадку запобігти неможливо, можна лише знизити ймовірність його наступу, тобто домогтися того, що такі події наступатимуть рідше;

– можна також знизити ступінь шкоди від настання такої події, але при цьому чим рідше настає ризикова подія, тим сильніша шкода від них;

– за будь-якого втручання в систему в першу чергу страждає її безпека.

Виявилося, що для аналізу властивостей безпеки складних систем, що складаються з технічних компонентів людей, що взаємодіють один з одним, повною мірою можуть бути застосовані деякі соціологічні та психологічні правила, виведені на основі спостереження за розвитком процесів та подій:

– Закон Парето (універсальний закон нерівності), сформульований італійським економістом і соціологом Вільфредо Парето в 1897 р., відоміший як жартівливий вислів «20 % німців випиває 80 % пива», відповідно до яких перші 20 % зусиль дають 80 % результатів [4], або 8 всіх проблем породжуються людиною (персоналом) і лише 20% посідає частку технічного устаткування.

Методологічний принцип, який отримав назву на ім'я англійського філософа-номіналіста Вільяма Оккама, що говорить: «Те, що можна пояснити за допомогою меншого, не слід висловлювати за допомогою більшого» [5]. Відповідно до нього за рівної ймовірності подій із різним ступенем тяжкості наслідків, зазвичай, першим трапляється подія, ступінь тяжкості наслідків якого менше.

З цього також випливає, що зловмисник, плануючи атаку на ресурс, з усіх можливих буде вибирати найпростіший спосіб здійснення своїх цілей, а віруси потраплятимуть у систему найпростішим способом.

Як зазначалося, аспектів забезпечення інформаційної безпеки бізнесу досить багато, але загалом є й низка загальних моментів, у яких слід коротко зупинитися.

Ведення бізнесу завжди передбачає наявність когось первинного капіталу, активу, який вкладається в якусь «справу» з метою отримання прибутку. Решта, що не має активу, до бізнесу не відноситься і не розглядається.

Ефективність бізнесу тим вища, що вищий прибуток – це аксіома. На величину прибутку впливає кілька факторів, серед них виділяються найістотніші:

– величина внутрішніх витрат, зокрема утримання колективу та витрат за забезпечення безпеки у тому числе;

– якість управління власним активом. Якщо крім власника активу або його представника активом може керувати ще хтось у власних інтересах, то актив може розкрадатись, а бізнес – суттєво погіршуватись. Приклад перед очима – розкрадання коштів у карткових платіжних системах та системах дистанційного банківського обслуговування;

– якість роботи колективу, що забезпечує бізнес;

– швидкість реакції колективу на зовнішні чинники, які впливають бізнес, чи управляючі впливу;

– стратегія та якість ведення самого бізнесу;

– обрана стратегія управління ризиками, зокрема економічними ризиками та ризиками інформаційної безпеки.

Слід зазначити, що бізнес ведеться, зазвичай, у ворожому середовищі, за умов конкурентної боротьби, несприятливого законодавства, ризику рейдерства, часто нескоординованої діяльності різних наглядових органів. Особливе місце у цьому списку займає кримінал, який прагне відібрати або поставити під контроль прибуток від вкладення активів.

Також слід зазначити, що серед всього набору загроз та ризиків існує певна ієрархія, за силою впливу та рівнем катастрофічності для бізнесу загрози серйозно різняться. Так, політичні ризики або ризики невідповідності законодавству є для бізнесу визначальними, оскільки здатні незалежно від того, наскільки якісно здійснюється робота з мінімізації ризиків інформаційної безпеки фізично знищити бізнес.

Список використаних джерел:

1. Цвілій О.О. Системи управління інформаційною безпекою: гармонізація з міжнародними стандартами, правилами та процедурами. / Перша всеукраїнська науково-практична конференція «Перспективні напрями захисту інформації». Збірник тез. – 2015. – с. 107-11.

2. Керівництво із застосування ризик-орієнтованого нагляду, FATF, Париж. 2021 URL: www.fatf-gafi.org/publications/documents/Guidance-RBA-Supervision.html

3. Орлов П.І., Духов В.Є. Основи економічної безпеки фірми: Навчальний посібник. - Х.: ТОВ «Прометей-Прес», 2004. – 284 с.

4. Закон Парето URL: https://www.forbes.ru/forbeslife/489362-zakon-pareto-ili-pravilo-80-20-kak-dostigat-bol-sego-pri-minimal-nyh-usiliah

5. Бритва Оккама. URL: http://ni.biz.ua/1/1_11/1_11410_spisok-hudozhestvennih-tekstov-dlya-obyazatelnogo-chteniya-po-kursu.html