Н.Ф. Васильєва,
А.С. Гінкул,
В.Л. Кавура

ОРГАНІЗАЦІЯ БЕЗПЕКИ ОНЛАЙНОВОГО ЕЛЕКТРОННОГО БІЗНЕСУ

На сьогодні економічний розвиток країни, зростання обсягу товарообігу у внутрішніх і зовнішніх угодах, кількості учасників економічної діяльності у країні і на світовому ринку, діяльність органів державної влади з управління і регулювання економічних і фінансових потоків, упровадження нової форми ведення бізнесу, тобто онлайнового електронного бізнесу (далі – ОЕБ), неможливі без широкого застосування інформаційно-телекомунікаційних технологій (далі – ІТТ).

З огляду на забезпечення економічної безпеки суб'єктів господарювання, це породжує дослідження з вирішення проблем безпеки застосування ІТТ (В. Воронов, Ж. Дебре, С. Злобін, С. Кавун, В. Носов, О. Манжай, Ф. Модельяні, О. Тякін, Б. Хант, У. Швартау та інші), але ще недостатньо розглянуто проблеми безпеки онлайнового електронного бізнесу.

Мета статті – визначити поняття організації безпеки ОЕБ, завдання та стратегію (відповідно до основних напрямів захисту бізнес-процесів) суб'єктів господарювання, які мають намір застосування нових форм ведення бізнесу, що буде сприяти укріпленню їх економічної безпеки.

Поняття *«безпека»* можна трактувати як стан, за яким відсутня небезпека, є захист від неї, або як стан, за яким відсутня можливість заподіяння збитку потребам і інтересам суб'єкта відносин [3].

Організація безпеки – це особливим чином організована діяльність, яку спрямовано на збереження внутрішньої стійкості суб'єкта господарювання, його здатності протистояти руйнівному агресивному впливу різних чинників, а також активна протидія існуючим видам загроз.

Щодо до ОЕБ визначення його безпеки можна сформулювати таким чином: *це стан захищеності інтересів суб'єктів господарювання і їх відносин, що здійснюють комерційні операції (угоди) за допомогою технологій ОЕБ, від загроз матеріальних і інших втрат.*

Організація безпеки ОЕБ необхідна для будь-яких суб'єктів господарювання й установ незалежно від форми власності. Розходження полягають лише в тому, які засоби і методи, у якому обсязі потрібні. Від стану організації безпеки ОЕБ значно залежить його економічна безпека.

Організація безпеки ОЕБ – це сукупність заходів, спрямованих на збереження фінансово-економічної безпеки суб'єкта господарювання, який працює у режимі ОЕБ.

Загрози безпеки ОЕБ можуть бути пов'язані з діями чинників, значення і вплив яких практично не завжди відомі. Присутність такої невизначеності й обмеженість доступних ресурсів і засобів не дозволяють створити абсолютно безпечну систему. Тому при створенні системи безпеки ОЕБ необхідно мінімізувати ступінь ризику виникнення збитку, виходячи з особливостей загроз безпеки і конкретних умов суб'єкта господарювання, що займається ОЕБ.

Організацію безпеки ОЕБ можна розглядати за такими напрямами її захисту:

техніко-технологічний, тобто використання технічних та програмних засобів, що перешкоджають завданню збитків суб'єкту господарювання при здійсненні ним бізнес-операцій у режимі ОЕБ;

нормативно-правовий, що забезпечує наявність відповідних нормативно-правових елементів: таких як патенти, авторські права, у тому числі на інтелектуальну власність,

© Васильєва Наталія Федорівна – кандидат економічних наук;
Гінкул Антоніна Степанівна;
Кавура Віктор Леонідович.
Інститут економіки промисловості НАН України.

ISSN 1562-109X

ліцензії, закони, положення, накази, стандарти та інше, що надає правові гарантії безпеки ОЕБ;

організаційний, тобто регламентація виробничої діяльності та взаємовідносин суб'єктів господарювання як партнерів при укладанні й реалізації електронної угоди, що виключає завдання збитків.

Розглянемо організацію безпеки ОЕБ за наведеними вище напрямами захисту.

Техніко-технологічний захист. На рисунку відображено еволюцію технологій забезпечення безпеки при інтеграційних процесах ОЕБ. На сьогодні є актуальними проблеми безпеки ОЕБ у зв'язку із глобалізацією бізнес-процесів і інформаційного простору. Розглянемо деякі із цих проблем. Так, наприклад, питання захисту угод ОЕБ постає найбільш гостро у США, де спостерігалося найшвидше зростання числа користувачів глобальної мережі. У 2001-2003 рр. за участю ФБР було організовано Національний центр із боротьби з високотехнологічними злочинами, а незабаром – центр зі збору відомостей про шахрайство з використанням глобальної мережі. Ці центри регулярно проводять моніторинг глобальної мережі і видають бюлетень і звіти про види і факти шахрайства. Наприклад, за даними цих центрів, протягом 2007 р. у США було виявлено 103959 фактів шахрайства того або іншого роду з використанням глобальної мережі. Сумарні втрати від шахрайських угод склали 68,2 млн. дол., з медійним значенням – 219,6 дол. на одну угоду. При цьому, за даними центрів, обсяг угод ОЕБ у США у 2007 р. досяг 98516 млн. дол., а втрати внаслідок тих або інших видів шахрайства – 0,15% [4].

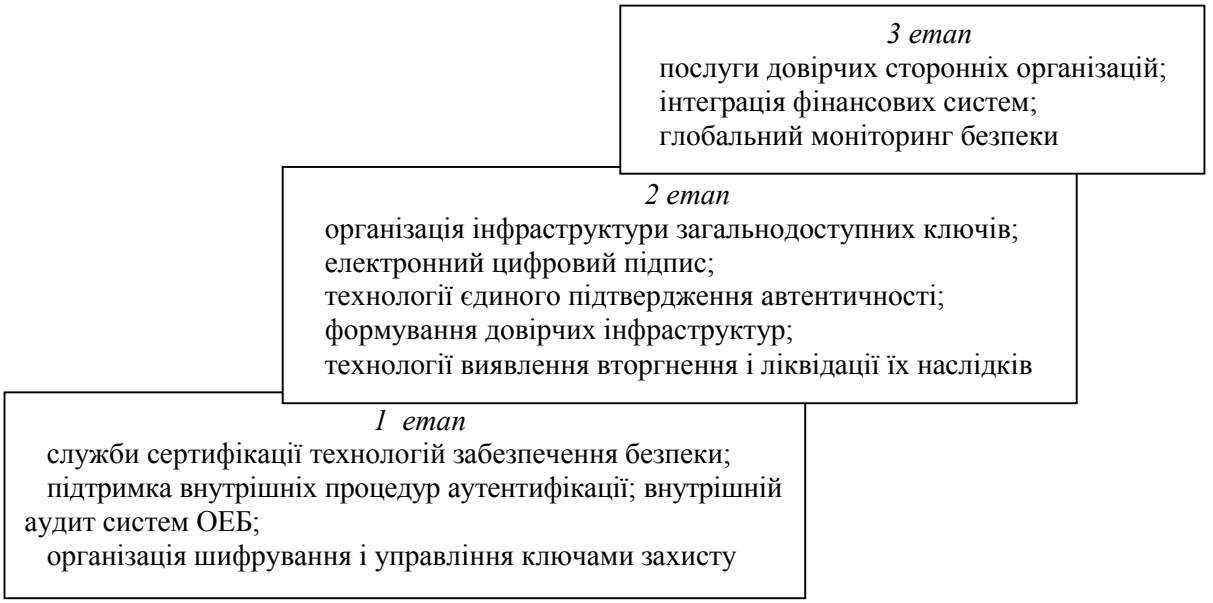

Рисунок. Еволюція технологій забезпечення безпеки при інтеграційних процесах ОЕБ

Слід зазначити, що серед учасників ОЕБ угодами з найбільшим захистом від зовнішньої загрози шахрайства володіють кредитно-фінансові установи, оскільки банки обов'язково мають відповідну професійну службу безпеки й у більшості випадків вони мають домовленість з іншими учасниками фінансового ринку про спільні активні протидії різним можливим формам фінансової злочинності.

При використанні пластикових карток як платіжного засобу до проведення операцій ОЕБ включається платіжна банківська система, яка представляє асоціацію фінансово-кредитних і сервісних організацій. Крім того, якщо внаслідок шахрайства покупець або продавець може втратити до 100% своїх активів, то для банку втрата в результаті шахрайської угоди навіть дуже великої суми означає втрату в розмірі не більш 1% активів, які будуть компенсовані страховими виплатами. Проте, на жаль, донедавна кредитні установи не були готові взяти на себе основну частку ризику за фінансовий супровід угод ОЕБ.

Результати дослідження дозволяють сформулювати такі основні вимоги до організації безпеки платіжних систем, а саме забезпечення:

неможливості списання коштів з аккаунта платника третьою особою;

легітимного підтвердження платником перед третіми особами (наприклад, судом) факту здійснення платежу, його отримання одержувачем і призначення даного платежу (наприклад, отримання товару належної якості);

можливості легітимного підтвердження одержувачем перед третіми особами факту отримання платежу та його призначення;

легітимного підтвердження емітентом факту проведення всіх авторизованих трансакцій по даному аккаунту істинним власником даного аккаунту;

запоруки, що суму, яку переміщено з аккаунта, не буде вкрадено у момент передачі і вона попаде точно і виключно за призначенням;

неможливості підробки квитанцій емітента користувачем;

вирішення всіх спірних питань між емітентом та користувачем виключно електронним чином за допомогою повідомлень з електронним цифровим підписом;

можливості вирішення спірних питань поміж користувачем поза участю емітента;

базування електронної платіжної системи на добре перевіреній і надійній технології.

Нормативно-правовий захист. Проведений аналіз можливостей ефективного функціонування ОЕБ у контексті проблем безпеки його розвитку в Україні дозволив визначити такі основні положення з формування правового і нормативного забезпечення процесів ОЕБ.

Процес розподілу ролей і відповідальності при реалізації різних бізнес-процесів ОЕБ має підтримуватися необхідними нормативними актами, що є запорукою безпеки його функціонування. Певна частина діяльності у сфері ОЕБ регулюється використанням інформації, яка міститься всередині суб’єкта господарювання і має бути визначена відповідними рішеннями керівництва. Відзначимо, що відсутність чіткого визначення прав та обов’язків учасників бізнес-процесів часто є причиною глухих ситуацій при розслідуванні інцидентів, пов'язаних із порушеннями у сфері безпеки ОЕБ.

Розвиток нормативно-правового регулювання безпеки українського ОЕБ має здійснюватися з урахуванням регулярної оцінки результативності застосування існуючих нормативно-правових актів у контексті реалізації національної стратегії та галузевих програм соціально-економічного розвитку, що випливають із неї.

Нормативно-правове забезпечення безпеки процесів ОЕБ має будуватися на принципах досяжності електронних інформаційних ресурсів (далі – ЕІР) про законодавчу діяльність державних органів, інтеграції державних інформаційних ресурсів, гармонізації їх із міжнародним європейським правом.

Першочерговим завданням нормативно-правового забезпечення безпеки ОЕБ є завершення роботи над комплексом нормативних актів, що забезпечують права громадян на ЕІР про діяльність органів державної влади і порядок використання інформаційних технологій у взаєминах між державою, суспільством і громадянами.

ІТТ змінюють традиційний підхід до регулювання відносин між захистом прав виробників ЕІР і захистом прав споживачів цих ресурсів. Інформаційні технології дозволяють із первинних ЕІР створити нові продукти і послуги, що використовуються багаторазово. З одного боку, нові ІТТ дозволяють копіювати ЕІР при низьких витратах для широкого кола споживачів, з іншого – створюється конфліктна ситуація, за якою для творців ЕІР існує високий ризик утрати прибутку, який вони можуть отримати.

Для сприяння забезпеченню безпеки ОЕБ у системі захисту інтелектуальної власності щодо

EIP та ITT доцільно акцентувати увагу на двох основних аспектах:

удосконаленні процесів запобігання використанню інформаційних технологій, які не мають ліцензійного супроводу, для охорони авторських прав;

прикладному використанні питань захисту інтелектуальної власності, що має переважно обов'язковий і немайновий характер.

Перший аспект. Використання неліцензійних інформаційних технологій знижує якість обслуговування, рівень надійності й безпеки інформаційних систем, зокрема безпеки ОЕБ. Запобігти цьому можуть такі заходи:

формування іміджу достоїнства, респектабельності придбання і використання ліцензійних інформаційних технологій;

вільне поширення серед учасників ОЕБ ліцензованих ITT, розроблених за кошти державного бюджету;

придбання переважно готового програмного забезпечення зарубіжного виробництва з відкритим кодом;

підвищення якості вітчизняних інформаційних систем, технологій і ресурсів;

створення системи інвентаризації, каталогізації та маркетингового використання інформаційних технологій.

Другий аспект. Доцільно використовувати державне сприяння організації науково-практичних досліджень загальнозначущих форм і процесів раціонального мислення і способів фіксації EIP. У рамках цих робіт можуть бути поставлені питання створення умов і розробки регламентів для включення програмного забезпечення до складу матеріальних активів, прискорення стратегічної ідентифікації людини, колективу, підприємства, організації та галузі в цілому в контексті використання інформаційних технологій і вирішення питань інформаційно-телекомунікаційної безпеки, у тому числі й ОЕБ [1, 5].

Обов'язкові стандарти і вимоги в сфері захисту EIP мають вводитися тільки для державних органів і бюджетних організацій. В інших випадках питання сертифікації з метою захисту EIP мають вирішуватися за розсудом користувачів цих засобів, що самостійно несуть ризик із використання. У контексті вирішення питань національної безпеки доцільно створити інформаційно-аналітичний центр стандартизації, підпорядкований органам державної влади, рішення якого будуть обов'язкові для виконання.

Прихильність до міжнародних стандартів – найбільш важливий елемент розвитку суб'єктів господарювання. Він є найважливішим критерієм оцінки їх діяльності в міжнародному ОЕБ, забезпеченні безпеки ОЕБ. Розвиток українського ОЕБ буде все більшою мірою залежати від застосування стандартів, особливо їх домінування в сфері надання EIP. Тому є доцільним створення і введення національного стандарту у сфері ОЕБ на базі міжнародних стандартів.

Задля поліпшення безпеки спільного використання інформаційних технологій усіма учасниками ОЕБ у рамках міжнародних систем стандартизації мають бути сформульовані національні стандарти: метаописання інформаційних технологій, інформаційно-технологічних стандартів, стандартів де-факто і де-юре, надання універсальних державних інформаційно-телекомунікаційних послуг, регламентів, надання інформаційно-телекомунікаційних послуг (сервісів) та інформаційно-телекомунікаційного забезпечення мережної взаємодії [2].

Організаційний захист. Для завоювання довіри до ефективності використання ОЕБ усе більшого значення набуває вирішення проблем організації безпеки його функціонування. Це означає в першу чергу наведення порядку в управлінні суб'єктами господарювання, організаціями, банками. Зараз сотні українських суб'єктів господарювання виходять на світовий ринок, що потребує якості планування виробництва, застосування ефективних технологій для прийняття управлінських рішень як по вертикалі, так і по горизонталі, правильної організації роботи з EIP, участі в ОЕБ та організації системи його безпеки.

Процес організації безпеки систем ОЕБ в Україні розвивається вкрай нерівномірно. Позитивні зміни проходять дуже в'яло. Водночас при правильній організації справи стан, пов'язаний із безпекою ОЕБ, можна кардинально змінити. Для цього необхідна не тільки державна програма з інформатизації, яка вже існує, але і відповідне фінансування перебігу інформатизаційних робіт, у тому числі і з питань безпеки ОЕБ.

Таким чином, можна окреслити такі основні завдання, що стоять перед суб'єктом господарювання, який виходить на рівень ОЕБ, що потребує організації його безпеки:

підвищення ефективності організаційної структури;

підтримка впровадження інформаційних технологій у всі сфери бізнес-діяльності;

удосконалення технологій управління, які базуються на електронному документообігу.

Будь-який суб'єкт господарювання може домогтися успіхів у сучасному економічному середовищі тільки в тому випадку, якщо його система управління відповідає певним вимогам, найбільш важливими з яких є такі:

прозорість бізнесу і його «аналітичність», що дозволяють не тільки володіти ЕІР про поточну ситуацію, але й аналізувати можливі причини – слідчі зв'язки, робити висновки і приймати на їх основі економічно обґрунтовані управлінські рішення;

керованість і ефективний розподіл повноважень і відповідальності всередині суб'єкта господарювання, що забезпечує ефективне використання переваг централізації одних управлінських функцій і децентралізації інших;

забезпечення «інтервенції» інформаційно-телекомунікаційних технологій у діючу систему управління, що підсилює прозорість бізнесу, сприяє розвитку так званого третього сектору економіки, виникненню нових форм ведення бізнесу, принциповій зміні організації праці на користь децентралізації управління, тимчасового наймання працівників і створення віртуальних робочих місць, тобто появі ОЕБ, що поєднує різноманітні можливості взаємодії постачальників і споживачів. Крім того, він робить їх незалежними, не прив'язаними до стаціонарних пристроїв, надаючи можливість здійснити покупку, здійснити платежі, взяти участь в аукціоні при наявності всього лише мобільного телефону або кишенькового комп'ютера. Послугами ОЕБ можна скористатися завжди, незалежно від часу або місця перебування.

Стратегія організації безпеки ОЕБ повинна містити такі дії:

потрібно встановити правила організації безпеки;

необхідно вирішити, що і від чого захищатимемо, і обов’язково визначитися з розумним співвідношенням ризику і витрат;

дотримуватися балансу між процедурними і технічними засобами контролю безпеки;

визначитися з реалізацією установлених правил, тобто з тим, які і кому надавати права доступу, до яких ресурсів, що робити в нештатній ситуації і т.ін.;

розробити план освітніх заходів, щоб робітники розуміли, наскільки ризиковано працювати не віддаючи собі звіту у своїх

діях (це може бути відвідування якихось сумнівних вузлів в Інтернеті, натискання кнопки “завантажити”, не розуміючи, які ризики з цим пов’язані);

проект інформатизації суб’єкта господарювання або окремих бізнес-процесів має містити систему захисту як один із його компонентів;

визначитися із продуктами, які застосовуються для безпеки ОЕБ відповідно до розробленого проекту інформатизації. Вони повинні створювати деяку складну архітектуру і комплекс, які б забезпечили виконання бізнес-процесів і водночас реалізацію зведених правил політики безпеки таким чином, щоб люди утримувалися від необміркованих дій.

Оцінку ефективності системи безпеки ОЕБ, на наш погляд, доцільно здійснювати за допомогою узагальненого вірогідного показника, який відображає стан захищеності, характеризує ступінь ризику одержання суб'єктом господарювання матеріального або іншого збитку у грошовому вимірюванні не вище заданого рівня при здійсненні комерційної операції.

Таким чином, проблеми організації ефективної системи безпеки ОЕБ, що виникають як зі складності й різновиду сучасних ІТТ, зокрема електронних платіжних систем, так і з комплексного підходу до безпеки із залученням законодавчих, адміністративних, програмно-технічних заходів, потребують необхідності подальшого дослідження. Від своєчасного їх вирішення залежить економічна безпека суб’єкта господарювання.

Література

1. Злобін С.В. Теоретичні засади організації електронної комерції / С.В. Злобін // Науково-технічна інформація. – 2007. – № 4. – С. 16-22.

2. Иванов П. Электронные проекции бизнес-процессов / П. Иванов // Сети. – 2002. – № 3. – С. 122.

3. Кавун С.В. Інформаційна безпека / С.В. Кавун. – Харків: Вид. ХНЕУ, 2009. – 368 с.

4. US Census Bureau QUARTERI.Y RETAN.F.-COMMERCE SALES 4RD QUARTER 2004 [Электронный ресурс]. – Режим доступа: http://www.census.gov/mrts/www/data/html/04O4 html.