СИСТЕМИ УПРАВЛІННЯ БЕЗПЕКОЮ ЛАНЦЮГА ПОСТАЧАННЯ ЗА ISO 28000. ПРАКТИЧНІ АСПЕКТИ

В. Ситніченко, кандидат технічних наук, директор,
Г. Кісельова, завідувач сектору,
Є. Стоякін, завідувач сектору,
НТЦ «Станкосерт», м. Одеса

СИСТЕМЫ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ ЦЕПИ ПОСТАВОК ПО ISO 28000. ПРАКТИЧЕСКИЕ АСПЕКТЫ

В. Ситниченко, кандидат технических наук, директор,
А. Киселева, заведующий сектором,
Е. Стоякин, заведующий сектором,
НТЦ «Станкосерт», г. Одеса

SAFETY MANAGEMENT SYSTEMS OF DELIVERY CHAIN IN ACCORDANCE WITH ISO 28000. PRACTICAL ASPECTS

V. Sytnichenko, Candidate of Technical Sciences, Director,
H. Kiseliova, Section Chief,
Ye. Stoiakin, Section Chief,
Scientific and Technical Centre «Stankocert», Odesa

У статті розглянуто принципи побудови та процеси системи управління безпекою ланцюгів постачання (СУБ), наведено вигоди від її упровадження.

Вступ України до Світової організації торгівлі корисний для вітчизняних підприємців з точки зору просування своїх товарів на світові ринки та участі в міжнародному розподілі праці. Але можливостями єдиного торгового простору користуються і злочинні організації, що призводить до збільшення нелегального обігу наркотиків, зброї, контрафактної продукції, нелегальної міграції, зростання обсягів крадіжок і псування перевезених товарів, сировини та комплектуючих при транспортуванні.

В. Ситніченко

Г. Кісельова

Є. Стоякін

Таким чином, ланцюг постачання (починаючи від виробника продукції й закінчуючи споживачем, включаючи транспортні компанії, дистриб'юторів, склади, оптових і роздрібних продавців) як особливо складний об'єкт управління є досить вразливим, і збій на одній ділянці може призвести до тяжких наслідків для всіх учасників процесу.

Серія стандартів ISO 28000 (2007 року) спрямована на допомогу підприємцям у зменшенні ризиків для людей і товарів у ланцюзі постачання. Загальні вимоги щодо безпеки викладено у стандартах [1, 2], загальні керівні настанови — [3, 4].

Об'єктами сертифікації в [1—4] може бути безпосередньо СУБ, що відповідає вимогам [1], та організація процесу убезпечення міжнародних ланцюгів постачання відповідно до [3].

Враховуючи, що базовим стандартом серії є [1], у процесі розробляння та упровадження СУБ доцільно залучити суттєві елементи з [3].

Стандарт [1] досить органічно вписується в інтегровану систему менеджменту організації, бо заснований на підході [5], що базується на аналізі ризиків та методології Демінга-Шухарта: «плануй — виконуй — перевіряй — дій».

У [1] передбачено п'ять ключових елементів СУБ:

- Політика управління безпекою ланцюга постачання;
- Планування убезпечення ланцюга постачання;
- Упровадження та функціонування системи управління;
- Перевірка і коригувальні дії;
- Аналіз та постійне удосконалення.

Реалізуючи ці елементи, треба визначити сферу поширення СУБ системи з урахуванням залучених сторонніх організацій. Вимоги щодо формулювання Політики СУБ містять стандартний набір вимог: узгодженість з політикою організації в інших сферах; узгодженість із загальною організаційною структурою управління загрозами та ризиками; зобов'язання відповідності чинному законодавству і постійному вдосконаленню, документальне оформлення; доведення до співробітників і всіх зацікавлених сторін, доступності, можливості перегляду. Але у [1] є примітки, що організації можуть обрати детальну політику для внутрішнього користування з конфіденційною частиною і мати зведений неконфіденційний варіант для розповсюдження серед зацікавлених сторін.

Розробивши Політику, потрібно планувати дії щодо реалізації. На першому етапі потрібно вивчити ділове середовище, визначити законодавчі, нормативні та інші обов'язкові вимоги. За аналізом ділового середовища ідентифікуються загрози безпеки ланцюга постачання, оцінюються ризики їхньої реалізації. Для цього, маючи визначену сферу розповсюдження СУБ, необхідно в ланцюгах постачань конкретної організації виділити типові сегменти вірогідного виникнення та реалізації загрози, наприклад, місця виготовлення, обробляння або перероблення продукції перед завантаженням; зберігання; транспортування; завантаження, перевантаження, відвантаження; передача контролю за продукцією від однієї організації до іншої; формування, обробляння і доступ до документації та інформації стосовно перевезення продукції; транспортні маршрути; засоби перевезення та перевізники.

Для ідентифікації загроз та оцінювання ризиків безпеки ланцюга постачання використовуються дані, отримані з різних джерел: правові та інші вимоги до безпеки; політика в галузі безпеки; записи пригод; невідповідності; результати перевірок СУБ; передання інформації від співробітників та інших зацікавлених сторін; інформація, надана співробітниками з питань безпеки, перегляду та вдосконалення діяльності на робочих місцях (ці дії за своїм характером можуть бути як наслідковими, так і попереджувальними); інформація щодо кращої практики, типових ризиків, пов'язаних з безпекою, пригодами і надзвичайними ситуаціями, що мають місце в аналогічних організаціях; промислові стандарти; застереження уряду; інформація стосовно технічних засобів, процесів і діяльності організації (зокрема: докладний опис процедур управління змінами; ситуаційні плани; інструкції з процесів і робочі процедури; дані з безпеки; дані моніторингу).

Оцінюючи ризики, потрібно розглядати правдоподібність подій та їхні наслідки:

- фізичні загрози та ризики виходу з ладу, наприклад, функціональні відмови, випадкові збитки, зловмисне заподіяння шкоди, кримінальні дії;
- загрози та ризики, що виникають в процесі діяльності, враховуючи управління убезпеченням, людський фактор та дії, що впливають на роботу, стан і безпеку організації;
- природні явища (шторм, повінь тощо), які можуть призвести до того, що заходи із убезпечення і зберігання устаткування виявляться неефективними;
- фактори, неконтрольовані організацією, наприклад, дефекти устаткування і недоліки сервісу;
- загрози та ризики з боку зацікавлених сторін, наприклад, невиконання обов'язкових вимог або нанесення збитку репутації;
- конструкцію та розміщення обладнання з убезпечення, включаючи заміну, технічне обслуговування тощо;
- управління інформацією та даними, а також систему зв'язку;
- загрози безперервності операцій.

Приклади загроз безпеки і можливі наслідки наведено у таблиці.

Після визначення переліку загроз, притаманних даному виду діяльності в ланцюзі постачання, оцінюються наслідки для конкретного бізнесу, визначається ймовірність їх реалізації, визначається рівень ризику. Таку відповідальну роботу повинна ви-

Приклади загроз безпеки і можливі наслідки

Загрози безпеки	Можливі наслідки від реалізації загроз
1. Вторгнення в активи та / або взяття їх під контроль (включаючи транспортні засоби) у ланцюзі поставок	Завдання збитку / ліквідація активів. Нанесення збитку / ліквідація зовнішнього ланцюга з використанням активів або товарів. Ініціювання громадянських заворушень чи нанесення економічних втрат. Взяття заручників / позбавлення життя людей
2. Використання ланцюга поставок як засіб контрабанди	Незаконне ввезення зброї в країну / економічну зону або вивезення зброї з країни / економічної зони. Сприяння терористам в країні / економічній зоні
3. Фальсифікація інформації	Локальне або дистанційне отримання доступу до систем інформації / документації ланцюга постачання з метою порушення операцій або полегшення незаконної діяльності
4. Цілісність вантажів	Фальсифікація, саботаж і / або крадіжка з метою тероризму
5. Несанкціоноване використання	Проведення операцій у міжнародному ланцюзі постачання для полегшення виконання терористичних актів, включаючи використання різних видів транспортних засобів як зброю
6. Витік конфіденційної інформації щодо вантажу або клієнтів	Економічні втрати, зниження кількості клієнтів
7. Пошкодження продукції або втрата вантажу	
8. Зрив термінів доставки, недоставляння вантажу	
9. Втрата особистих речей або документів клієнтів	
10. Травми і каліцтва при транспортуванні людей	Економічні втрати, зниження кількості клієнтів, загроза здоров'ю

конувати група фахівців, задокументувати підсумки аналізу та оцінювання ризиків, наприклад, у формі бланка або звіту з оцінювання ризиків [6].

Для кожного сегмента ланцюга постачання, в якому бере участь організація, визначаються загрози, наслідки, ймовірність і рівень ризику — високий, середній, низький. За високого потрібно негайно прийняти контрзаходи:

- перегляд організаційної структури, обов'язків і відповідальності;
- перегляд політики, цілей, планів або програм з управління безпекою;
- перегляд процесів і процедур;
- упровадження нової інфраструктури, обладнання чи технологій, пов'язаних із убезпеченням, які можуть містити апаратні засоби та / або програмне забезпечення;
- залучення нових підрядників, постачальників або персоналу;
- перенесення ризику шляхом страхування, залучення субпідряду, фізичного перенесення в інші місця, на інший час, зміни маршруту постачання тощо.

За неможливості знизити високий рівень ризику, необхідно розглянути доцільність дій у цьому сегменті ланцюга постачання. За середнього рівня ризику розглядаються шляхи його зниження до низького або формуються цілі, завдання і програма для його подальшого зниження.

Усі ризики записуються у бланк [6] і перебувають під управлінням задля недопущення зростання їх рівня. У процесі ідентифікації загроз та оцінювання ризиків розглядаються нормальні, періодично або рідко виконувані операції та процедури всередині організації та, крім того, можливі надзвичайні ситуації.

Здійснюючи моніторинг процесу ланцюга постачання, фахівці постійно тримають у полі зору ризики за бланком [6], їхні оцінки, щоб не допустити зростання їх рівня, і ведуть роботу з додаткового виявлення загроз.

Оцінивши та виділивши ризики, можна сформулювати вимірні цілі, конкретні завдання у розвиток цих цілей і оформити Програму СУБ. До Програми записуються цілі, завдання, терміни виконання, відповідні ресурси, що виділяються, відмітки про виконання.

Основа етапу впровадження СУБ — формування організаційної структури, розподіл ролей, відповідальності та повноважень відповідно до виробленої політики, цілей, завдань і програм у галузі безпеки ланцюга постачання, що спираються на фундамент виділених ризиків.

Аналогічно ISO 14001, необхідне призначення представника вищого керівництва, проведення всіх дій з підтримання компетентності, навчання та поінформованості персоналу. У частині передачі необхідної інформації відповідним працівникам, підрядникам та іншим зацікавленим сторонам і отримання інформації від них, слід враховувати рівень її секретності. Також потрібно вживати необхідні кроки для запобігання несанкціонованого доступу до секретної інформації, що належить до безпеки ланцюга постачання.

За наявності в організації системи управління відповідно до [5, 7, 8] завдання упровадження елементів «Упровадження та функціонування», «Перевірка і коригувальні дії», «Аналіз менеджменту та постійне удосконалення» в основному зводиться до додавання до наявних процедур специфіки безпеки ланцюга постачання на основі проведеного аналізу та оцінювання ризиків. Додаткові документи відповідно до [3]: заява щодо застосування вимог стандарту до частини ланцюга постачання, в якій бере участь організація; декларація щодо безпеки учасника ланцюга постачання, яку заповнюють партнери; лист оцінювання ефективності безпеки ланцюга постачання; план убезпечення ланцюга постачання.

Можливі вигоди від упровадження СУБ:

1. Відповідність стандарту [1] однозначно демонструє, що підприємство дбає не лише про свою безпеку, але й убезпечує збереження товарів своїх клієнтів.

2. Стандарт [1] стає міжнародним орієнтиром для підприємств-учасників ланцюга постачання, позитивно впливаючи на формування іміджу підприємства.

3. Ефективно діюча СУБ дозволяє утримати клієнтів і збільшує частку підприємства на ринку послуг.

4. Управління ризиками стає активним засобом ефективного управління, бо ключові рішення, пов'язані з виділенням ресурсів, приймаються на основі оцінки ризиків.

5. Підвищується організаційна стійкість підприємства, тобто знижується ризик, що йому буде завдано непоправної шкоди від інцидентів, що впливають на діяльність, його фінансове здоров'я і репутацію.

6. Чіткий розподіл відповідальності та підзвітності дозволяє раціонально управляти наявними ресурсами.

7. Захист активів підприємства та клієнтів є доказом ефективного корпоративного управління, що підвищує його ринкову вартість.

8. Упровадження [1] СУБ у рамках організації має прямий вплив на рівень безпеки та захисту персоналу, що позитивно впливає на задоволеність співробітників, а через їхню діяльність і на задоволеність клієнтів.

9. СУБ, за своєю структурою, ідентичною [1], цілком органічно вписується в інтегровану систему менеджменту підприємства на основі [5, 7, 8].

10. Стандарт [1] визнаний Європейським співтовариством і може бути базою для реєстрації підприємства в ЄС як «Уповноваженого економічного оператора».

11. Упровадження СУБ сприяє мінімізації страхових внесків і позитивно впливає на кредитний рейтинг підприємства. ■

ЛІТЕРАТУРА

1. ISO 28000:2007 (ДСТУ ISO 28000:2008). Технічні умови на системи менеджменту безпеки ланцюга постачання.
2. ISO 28003:2007. Security management systems for the supply chain — Requirements for bodies providing audit and certification of supply chain security management systems (Системи менеджменту безпеки ланцюга постачання. Вимоги до органів аудиту та сертифікації систем менеджменту безпеки ланцюга постачання).
3. ISO 28001:2007. Security management systems for the supply chain — Best practices for implementing supply chain security, assessments and plans — Requirements and guidance (Системи менеджменту безпеки ланцюга постачання. Найкращі методи забезпечення безпеки оцінок і планів в ланцюзі постачання. Вимоги та керівні вказівки).
4. ISO 28004:2007. Security management systems for the supply chain — Guidelines for the implementation of ISO 28000 (Системи менеджменту безпеки ланцюга постачання. Керівництво з впровадження ISO 28000).
5. ISO 14001:2004 (ДСТУ ISO 14001:2006). Системи екологічного керування. Вимоги та настанови щодо застосовування.
6. Ситніченко В., Козловський Я., Чеглатонєв І. Технологія виходу на ринок ЄС // Стандартизація, сертифікація, якість. — 2008. — № 5. — С. 57—61
7. ISO 9001:2008 (ДСТУ ISO 9001:2009) Системи управління якістю. Вимоги.
8. OHSAS 18001:2007 (ДСТУ-П OHSAS 18001:2006). Системи управління безпекою та гігієною праці. Вимоги.