Директор НТЦ «СТАНКОСЕРТ», м.Одеса,
к.т.н. Ситніченко В.М.
Зав.сектором НТЦ «СТАНКОСЕРТ»
Кісельова Г.Б.
Зав.сектором НТЦ «СТАНКОСЕРТ»
Стоякин Є.А.

Безпека ланцюга постачання за стандартом ISO 28000 – основа міжнародного розподілу праці. Практичні аспекти впровадження

Вступ України до Всесвітньої торгівельної організації безумовно буде корисним для вітчизняних підприємців з погляду просування своїх товарів на світові ринки і участі в міжнародному розподілі праці.

Однак, слід відзначити, що перевагами єдиного торгівельного простору в такому ж ступені користуються злочинні і терористичні організації, що привело до збільшення нелегального обороту наркотиків, зброї, мігрантів, контрафактної продукції, а також зростанню об'ємів крадіжок і псування товарів, сировини і комплектуючих, які перевозять,

Згідно опублікованих статистичних даних по регіону Європа, Близький Схід, Африка (EMEA) у 2008 році було 3756 інцидентів, пов'язаних з розкраданнями вантажів при загальних втратах 214,58 млн.дол. США.

При цьому в 2008 році в порівнянні з попереднім роком число крадіжок і шахрайств зросло.

Дослідження компанії Aberdeen Group проведені серед 138 компаній США показали, що 58% компаній понесли збитки в наслідок збоїв у ланцюгу постачання.

Таким чином, ланцюг постачання (починаючи від виробника продукції і закінчуючи споживачем, включаючи транспортні компанії дистриб'юторів, склади, морські термінали, оптових і роздрібних продавців) як особливо складний об'єкт управління, через взаємозалежність між її складовими, є достатньо вразливим і збій на будь якій одній дільниці ланцюгу може привести до тяжких наслідків для всіх учасників процесу.

Порівняно нова (2007 рік) серія стандартів ISO 28000 якраз і спрямована на допомогу підприємцям в скороченні ризиків для людей і товарів в ланцюгу постачання.

Стандарти серії ISO 28000 розроблені Технічним комітетом ISO/TC8 «Судна і морські технології» і спрямовані на захист людей, забезпечення збереження вантажів, інфраструктури, устаткування, включаючи транспорт, захист від нещасних випадків і попередження негативних наслідків.

Загальні вимоги щодо безпеки ланцюгу постачання, викладені в двох стандартах:

ISO 28000:2007 (ДСТУ ISO 28000:2008) «Технічні умови на системи управління безпекою ланцюга постачання»;

ISO 28003:2007 «Система менеджменту безпеки ланцюга постачання. Вимоги до органів аудиту і сертифікації систем менеджменту безпеки ланцюга постачання».

Загальні керівні вказівки також викладені в двох стандартах:

ISO 28001:2007 «Система менеджменту безпеки ланцюга постачання. Найкращі методи забезпечення безпеки оцінок і планів у ланцюгу постачання. Вимоги і керівні вказівки»;

ISO 28004:2007 «Система менеджменту безпеки ланцюга постачання. Настанова з впровадження ISO 28000».

У стадії розробки знаходиться стандарт ISO 28005 «Судна і морські технології. Комп'ютерні програми. Електронна митниця суднів».

Об'єктами сертифікації в даній серії стандартів може бути безпосередньо система менеджменту безпеки ланцюга постачання, відповідна вимогам, викладеним в ISO 28000, а також організація процесу забезпечення безпеки в міжнародних ланцюгах постачання відповідно до вимог, викладених в ISO 28001.

Внаслідок того, що базовим стандартом даної серії є ISO 28000, то, на наш погляд, при розробці і впровадженні системи менеджменту безпеки ланцюга постачання по ISO 28000 доцільно також включити суттєві елементи з ISO 28001, про які буде сказано нижче і проходити сертифікацію на відповідність вимогам стандарту ISO 28000.

Стандарт ISO 28000 достатньо органічно вписується в інтегровану систему менеджменту організації, тому що він заснований на форматі ISO, прийнятом стандартом ISO 14001 із-за його підходу до системи менеджменту, заснованого на аналізі ризиків і методології Демінга-Шухарта: «Плануй – Здійснюй – Перевіряй - Дій».

Природно, що в даній серії акцент робиться на забезпечення безпеки ланцюга постачання.

Як завжди, передбачено п'ять елементів системи менеджменту безпеки ланцюга постачання, що мають вирішальне значення:

- політика менеджменту безпеки ланцюга постачання;
- планування забезпечення безпеки ланцюга постачання;
- впровадження і функціонування системи менеджменту;
- перевірка і коригувальні дії,;
- аналіз менеджменту і постійне вдосконалення.

Приступаючи до реалізації вище перелічених елементів, треба чітко визначити область розповсюдження системи з урахуванням сторонніх організацій-субпідрядників.

Вимоги відносно формулювання Політики менеджменту безпеки ланцюга постачання містять стандартний набір вимог про узгодження з політикою організації в інших галузях, узгодженості із загальною організаційною структурою менеджменту погроз і ризиків безпеки,

зобов'язань по забезпеченню відповідності чинному законодавству і по постійному вдосконаленню, документальному оформленню, доведені до співробітників і всіх зацікавлених сторін, доступності, можливості перегляду. Але крім того, в стандарті є примітки, що організації можуть вибрати детальну політику для внутрішнього користування з конфіденційною частиною і мати звідний не конфіденційний варіант, що містить основні цілі, для розповсюдження серед зацікавлених осіб і організацій.

Розробивши «Політику», необхідно приступити до етапу планування дій з її реалізації.

На першому етапі слід вивчити навколишнє ділове середовище, в якому веде свій бізнес організація і визначити всі законодавчі, нормативні і інші обов'язкові вимоги, що відносяться до діяльності даної організації.

На основі аналізу ділового середовища здійснюється ідентифікація погроз безпеці ланцюга постачання і оцінка ризиків реалізації цих погроз.

Для цього, маючи сформульовану галузь розповсюдження системи безпеки ланцюга постачання, необхідно в ланцюгах постачання конкретній організації виділити типові сегменти, де найімовірніше можуть виникнути і реалізуватися погрози безпеці, наприклад:

- місця виготовлення, обробки або переробки продукції перед відвантаженням;
- місця зберігання продукції;
- місця, в яких продукція транспортується;
- місця завантаження, перевантаження і вивантаження продукції;
- місця передачі контролю за продукцією від однієї організації до іншої;
- місця формування, обробки і доступу до документації і інформації про продукцію, що перевозиться;
- транспортні маршрути;
- засоби перевезення і перевізники.

Для ідентифікації погроз і оцінки ризиків безпеки ланцюга постачання використовуються дані, отримані з різних джерел інформації, зокрема:

- правові та інші вимоги до безпеки;
- політика в галузі безпеки;
- записи подій;
- невідповідності;
- результати перевірок системи менеджменту безпеки;
- передача інформації від співробітників і інших зацікавлених сторін;
- інформація, що отримується в результаті консультацій співробітників по питаннях безпеки, перегляду і вдосконаленню діяльності на робочих місцях (ці дії по своєму характеру можуть бути або відповідними, або попереджувальними);

- інформація по кращій практиці, типовим ризикам організацій, пов'язаним з безпекою, подіям і надзвичайним ситуаціям, що мають місце в аналогічних організаціях;
- промислові стандарти;
- застереження уряду;
- інформація по технічних засобах, процесах і діяльності організації, включаючи наступне:
  - детальний опис процедур управління змінами;
  - ситуаційні плани;
  - інструкції по процесах і робочі процедури;
  - дані по безпеці;
  - дані моніторингу.

Оцінка повинна розглядати правдоподібність подій і всі їх наслідки, перераховані нижче:

- загрози та ризики фізичної відмови, такі як функційна відмова, випадкове пошкодження, навмисне пошкодження або терористичні чи кримінальні дії;
- загрози та ризики поточного виробництва, зокрема контроль за безпекою, людські чинники та інші види робіт, які впливають на результативність, стан чи безпечність діяльності організації;
- події у природному середовищі (буревії, повені тощо), які можуть призвести до неефективності заходів та устаткування у сфері безпеки;
- чинники неконтрольовані організацією, такі як відмови в устаткованні та послугах сторонніх постачальників;
- загрози та ризики зацікавлених сторін, такі як недотримання нормативних вимог або заподіяння шкоди репутації чи бренду;
- проектування та встановлення устаткування, пов’язаного з безпекою, зокрема його заміну, технічне обслуговування тощо;
- управління інформацією та даними та їх оприлюднення;
- загрозу для безперервності робіт.

Приклади погроз безпеці і можливі наслідки наведені в таблиці

Погрози безпеці	Можливі наслідки від реалізації погроз
1. Вторгнення в активи і/або узяття їх під контроль (включаючи транспортні засоби) в ланцюгу постачання	Нанесення збитку/ліквідація активів. Нанесення збитку/ліквідація зовнішнього ланцюга з використанням активів або товарів. Ініціація громадянських безладів або нанесення економічної втрати. Узяття заручників/позбавлення життя людей.
2. Використання ланцюга постачання як засіб контрабанди	Незаконне ввезення зброї в країну/економічну зону або вивіз зброї із 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 незаконній діяльності.
4. Цілісність вантажів	Фальсифікація, саботаж і/або крадіжка з метою тероризму.
5. Несанкціоноване використання	Проведення операцій в міжнародному ланцюгу постачання для полегшення виконання терористичних актів, включаючи використання різних видів транспортних засобів як зброю.
6. Втрата конфіденційної інформації про вантажі 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, шкода здоров'ю

Після визначення конкретного переліку погроз властивих даному виду діяльності в ланцюгу постачання, проводиться оцінка наслідків для конкретного бізнесу при реалізації виділених погроз і визначається вірогідність реалізації цих погроз. На підставі отриманих даних, визначається рівень ризиків.

Таку відповідальну роботу повинна виконувати команда фахівців, яка має задокументувати підсумки аналізу і оцінки ризиків, наприклад, у формі Бланка або звіту з оцінки ризиків [1].

Тобто, для кожного сегменту ланцюга постачання, в якому бере участь організація, визначаються погрози, наслідки, вірогідність і рівень ризиків «високий», «середній» або «низький».

При високому рівні ризику потрібне негайне прийняття контрзаходів, наприклад:

- перегляд організаційної структури, обов'язку і відповідальності;
- перегляд політики, цілей, планів або програм в галузі менеджменту безпеки;
- перегляд процесів і процедур;
- впровадження нової інфраструктури, устаткування або технологій, пов'язаних із забезпеченням безпеки, які можуть включати апаратні засоби і/або програмне забезпечення;
- залучення нових субпідрядників, постачальників або персоналу, якщо це необхідно;
- перенесення ризику шляхом страхування, залучення субпідряду, фізичного перенесення в інші місця, на інший час, зміни маршруту постачання і таке інше.

При неможливості знизити високий рівень ризику, необхідно розглянути доцільність дій в цьому сегменті ланцюга постачання.

При середньому рівні ризику розглядаються шляхи його зниження до низького рівня або формуються цілі, завдання і програма по його зниженню надалі.

Всі ризики записуються в Бланку і знаходяться під управлінням з метою недопущення зростання їх рівня.

В процесі ідентифікації погроз і оцінки ризиків розглядаються нормальні, а також періодичні або рідко виконувані операції або процедури всередині організації і можливі надзвичайні ситуації.

Здійснюючи моніторинг процесу ланцюга постачання фахівці постійно тримають в полі зору ризики по Бланку оцінки ризиків, з тим щоб не допустити зростання їх рівня і ведуть роботу по додатковому виявленню погроз і ризиків.

Підсумовуючи, можна виділити дев'ять кроків в процесі оцінки ризиків і розробці контрзаходів:

1. Розгляд сценаріїв погроз;
2. Класифікація наслідків;
3. Класифікація вірогідності подій;
4. Градація подій, пов'язаних з недостатнім забезпеченням безпеки;
5. Розробка контрзаходів;
6. Здійснення контрзаходів;
7. Оцінка контрзаходів;
8. Повторення процесу для наступного сценарію погроз;

9. Продовження процесу оцінювання на регулярній основі і коли відбуваються значні зміни в операційному середовищі організації.

Такий підхід допомагає створити розумний рівень безпеки і ухвалювати якнайкращі ризик-обгрунтовані рішення по захисту ланцюга постачання тому, що оцінивши і виділивши ризики, ми можемо дійсно сформулювати вимірні цілі, конкретні завдання в розвиток цих цілей і оформити Програму менеджменту безпеки для досягнення своїх цілей і вирішення завдань.

У Програму записуються цілі, завдання, терміни виконання, відповідальні ресурси, що виділяються, відмітки про виконання.

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

Аналогічно ISO 14001, необхідне призначення представника вищого керівництва, і проведення всіх дій з підтримки компетентності, навчання і обізнаності персоналу.

У частині передачі необхідній інформації відповідним співробітникам, підрядчикам і іншим зацікавленим сторонам і отримання інформації від них, необхідно враховувати ступінь секретності інформації, що надається.

Також потрібно робити необхідні кроки по запобіганню несанкціонованому доступу до секретної інформації, що відноситься до безпеки ланцюга постачання.

За наявності в організації системи менеджменту по ISO 9001 і ISO 14001, OHSAS 18001 завдання впровадження елементів «Впровадження і функціонування», «Перевірка і коригувальні дії», «Аналіз менеджменту і постійне вдосконалення» в основному, зводиться до додавання в наявні процедури специфіки безпеки ланцюга постачання на основі проведеного аналізу і оцінки ризиків.

З нових документів, якщо враховувати вимоги ISO 28001, можна згадати :

- заяву про застосування вимог стандарту до тієї частини (сегменту) ланцюга постачання, в якому бере участь організація;
- декларацію про безпеку учасника ланцюга постачання, який заповнюють партнери по бізнесу;
- лист оцінки ефективності безпеки ланцюга постачання;
- план забезпечення безпеки ланцюга постачання.

На закінчення, перерахуємо можливі комерційні вигоди від впровадження системи менеджменту безпеки ланцюга постачання:

1. Відповідність стандарту ISO 28000 однозначно демонструє, що підприємство піклується не тільки про свою безпеку, але і забезпечує безпеку і збереження товарів своїх клієнтів.

2. Стандарт ISO 28000 стає міжнародним орієнтиром для підприємств-учасників ланцюга постачання, позитивно впливаючи на формування бренду підприємства, що піклується про безпеку товарів.

3. Система, що ефективно діє, по ISO 28000 дозволяє утримати клієнтів і збільшує частку підприємства на ринку послуг.

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

5. Підвищується організаційна стійкість підприємства, тобто знижується ризик того, що підприємству буде завданий непоправний збиток від інцидентів, що впливають на діяльність підприємства, його фінансове здоров'я і репутацію.

6. Чітке розділення відповідальності і підзвітності дозволяє раціонально управляти наявними ресурсами.

7. Захист активів підприємства і клієнтів служить доказом ефективного корпоративного управління, що підвищує ринкову вартість підприємства.

8. Впровадження ISO 28000 в рамках організації має прямий вплив на рівень безпеки і захисту персоналу, що позитивно впливає на задоволеність співробітників і через їх діяльність на задоволеність клієнтів.

9. Будучи по своїй структурі ідентичної ISO 14001, система менеджменту по ISO 28000 цілком органічно вписується в інтегровану систему менеджменту підприємства на основі ISO 9001, ISO 14001, OHSAS 18001.

10. Стандарт ISO 28000 визнаний Європейським співтовариством і може служити базою для реєстрації підприємства в ЄС як «Уповноважений економічний оператор».

11. Впровадження ISO 28000 сприяє мінімізації страхових внесків і робить позитивний вплив на кредитний рейтинг підприємства.

Згідно даних досліджень Стендфордського університету (США) на прикладі одинадцяти найбільших виробників і постачальників, опублікованих в 2006 році, підвищена увага і інвестиції в безпеку ланцюга постачання дозволяють:

- скоротити масштаби митних перевірок на 48%;
- збільшити автоматизацію обробки імпорту на 43%;
- скоротити час транзиту на 29%;
- поліпшити спостереження за активами в ланцюгу постачання на 50%;
- поліпшити час морських перевезень на 30%;
- скоротити час, необхідний для виявлення проблем на 21%;
- скоротити крадіжки при управлінні запасами на 38%;
- скоротити зайві запаси на 14%;
- скоротити спад клієнтів на 26%.

Таким чином на додаток до меншого ризику і вищого рівня безпеки, інвестиції в безпеку ланцюга постачання можуть дати значні переваги для організації, допомагаючи їм удосконалювати внутрішні операції, зміцнити стосунки зі своїми клієнтами і добитися загального збільшення прибутковості.

Література

1. Ситніченко В.М., Ю.Г.Паленний, В.Д.Погасій «Оцінка ризиків для виходу на ринок ЄС»

Інформаційний бюлетень Мінпромполітики України № 3 (17), 2008, стор. 40-44