ється технічний комітет ISO, що розробляє стандарти на соціальну безпеку. Ці стандарти допоможуть організаціям підготуватись до інцидентів і створити можливість їхнього функціонування під час кризи, що приведе до підвищення довіри у ділових колах та суспільстві, забезпечить наплив клієнтів і полегшить взаємодію між організаціями.

Більшість із нас усвідомлюють серйозні ризики безпеки, що трапляються через крадіжку ідентифікаційних даних та шахрайств. Технічний комітет ISO/TC 68 розробляє стандарти на фінансову безпеку, що мають вирішальне значення для забезпечення майже миттєвого виконання мільярдів операцій, які у вигляді платежів щорічно становлять трильйони доларів. Це допоможе вирішувати проблеми у сфері безпеки.

Біометрію все частіше використовують для убезпечення себе. Міжнародні стандарти сприяють підвищенню рівня розвитку та ефективності цієї технології.

Телебіометрія набула визнання близько 10 років тому, коли ідентифікація та автентифікація були центральними питаннями у боротьбі з тероризмом. ISO, Міжнародна електротехнічна комісія (IEC) та Міжнародний союз електрозв'язку (ITU) спільно розробляють стандарти на пристрої безпечного передавання унікальних ідентифікаторів об'єкта у величинах, що належать до його галузі вимірювань.

Кібернебезпека є однією з найбільш серйозних проблем нашого цифрового століття. Стандарти ISO у цій сфері можуть допомогти запобігти атакам, вірусам і крадіжкам особистої інформації.

Бути готовими. Убезпечення та стабільність всього ланцюга постачання

Чарльз Пірсол[3]

Від сировинної бази до виробництва, обслуговування або зберігання, під час перетинання кордону всіма видами транспорту, на етапі виробництва або під час поставки кінцевому споживачеві ланцюги постачання піддаються різним загрозам безпеки, як навмисним, так і через довкілля.

ISO пропонує вирішити ці проблеми за допомогою стандартів серії ISO 28000 на убезпечення ланцюга постачання, які вже досягнули значних успіхів. Багато підприємств та організацій у різних галузях (наприклад, логістика, експедиторські послуги, програмне забезпечення, фармацевтика, електроніка, IT тощо) вже сертифіковані або проходять сертифікацію на відповідність вимогам стандартів серії ISO 28000 незалежними третіми сторонами. Нижче наведено огляд цих стандартів, приклади їх упровадження та оновлена інформація щодо останніх розроблень.

Визначення термінології

Обговорення тем безпеки, управління безпекою та безпеки постачання іноді пронизані термінологією з джерел, що не мають практичного досвіду та достатнього розуміння предмета, а також вимог до осіб, на яких покладено прийняття рішень. Тому необхідно розпочати огляд стандартів серії ISO 28000 з визначення поняття «ланцюг постачання». Це не звичайне поєднання декількох елементів в одному ланцюзі. Це «пов'язаний набір ресурсів та процесів, який починається з пошуку сировини і закінчується постачанням товарів та послуг кінцевому користувачеві всіма видами транспорту». Таким чином, це складна мережа, яка охоплює багато ланок і вузлів, призначених для задоволення потреб

[3] Чарльз Пірсол протягом 16 років був головою технічного комітету ISO/TC 8 «Судна та морські технології». Він відставний капітан ВМС США з-понад 54-річним досвідом роботи спочатку в званні старшого морського офіцера, а потім у сфері виконавчої влади. Він визнаний лідер у сфері управління безпекою міжнародних морських ланцюгів постачань по всьому світові. Під його керівництвом в 2005 році технічний комітет ISO/TC 8 отримав вищу нагороду ISO.

конкретної організації, промисловості та нормативних вимог уряду.

Поряд із цим є спроби створити додатковий ряд стандартів на системи управління, переглянути режими безпеки та ввести додаткові вимоги до сертифікації. Такий підхід не лише додає плутанини, а й створює необґрунтовані витрати для промисловості.

Рішення

Стандарти серії ISO 28000 допомагають організаціям успішно планувати та відновлюватись після будь-яких руйнівних дій. Основний стандарт ISO 28000:2007 *«Система управління безпекою ланцюга постачання. Технічні умови»* є стандартом на систему управління, завдяки якому підвищується загальна продуктивність і безпека з одночасним зниженням фінансового тягаря.

Структура системи управління, встановлена стандартом ISO 28000, охоплює всі аспекти безпеки: оцінення ризику, готовність до надзвичайних ситуацій, забезпечення безперервності бізнесу, сталість, відновлення, стійкість до стихійних лих, пов'язаних з тероризмом, піратством, крадіжками вантажів, шахрайством і багатьма іншими порушеннями безпеки.

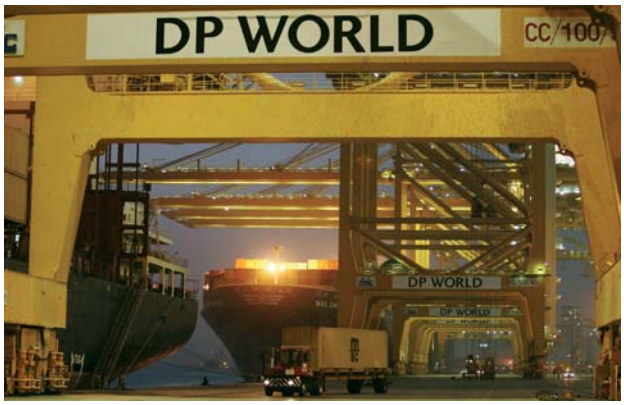
Організації можуть створювати власний підхід, сумісний з існуючою системою, а впроваджена на підприємстві система управління якістю може бути використана як основа для впровадження майбутньої системи управління безпекою відповідно до вимог стандарту ISO 28000.

Крім того, стандарт ISO 28000 — це єдиний опублікований міжнародний стандарт, на відповідність вимогам якого проводять сертифікацію і який встановлює цілісний, заснований на оціненні ризику підхід до управління ризиком, пов'язаним з будь-якими руйнівними інцидентами в ланцюзі постачання «до, під час і після». Стандарт встановлює, як підвищити сталість та готовність підприємства до діяльності економічно ефективним способом на основі моделі системи управління: «Плануй — Роби — Перевіряй — Дій» (PDCA).

Як зазначено в стандарті ISO 28000: *«Оцінення ризику розглядає ймовірність події та всі її наслідки, які охоплюють фізичні загрози і ризики; оперативні загрози і ризики; вплив довкілля; чинники, що перебувають поза контролем організації; ризики зацікавлених сторін, наприклад, недотримання нормативних вимог, зниження репутації чи торгової марки; будь-які загрози безперервності операцій»*.

Хто використовує ISO 28000?

Не дивно, що все більше і більше галузей використовують стандарт ISO 28000. Нижче наведено де-



кілька прикладів різних галузей промисловості щодо упровадження стандарту ISO 28000 та сертифікації відповідності його вимогам:

DP World — перше підприємство, яке сертифікувало морський термінал, планувало до 2012 року завершити сертифікацію на відповідність вимогами стандарту ISO 28000 всієї своєї мережі, що складається з 48 терміналів у 31 країні по всьому світові, а також C-TPAT[4] членство. Його європейські термінали також було сертифіковано як уповноважені економічні оператори (AEO) Європейського Союзу.

Port of Houston Autority, один з найбільших у світі портів, був також першим у світі портом, який пройшов сертифікацію на відповідність вимогам стандарту ISO 28000.

YCH Grap, Сінгапур, є першою компанією з питань управління ланцюгами постачання та логістикою, яка сертифікована на відповідність вимогам стандарту ISO 28000. YCH Grup — провідна інтегрована компанія і є діловим партнером відомих по всьому світові виробників електроніки, хімії, медичної техніки, таких яких Canon, Dell, Moet-Hennessy, ExxonMobil, B. Braun, LVMH, Royal Friesland Campina і Motorola.

TNT Express Asia, компанія з регіональним офісом в Сінгапурі, першою пройшла сертифікацію на відповідність вимогам стандарту ISO 28000.

[4] Митно-торговельне партнерство проти тероризму (C-TPAT) — добровільна ініціатива уряду США та ділової спільноти щодо побудови співробітництва, спрямованого на зміцнення і підвищення безпеки загального міжнародного ланцюга постачання та безпеки кордонів.

YCH India сертифікована Асоціацією захисту транспортованих цінностей (TAPA[5]) в А-класі, при цьому стандарт ISO 28000 виявився сумісним з її системою безпеки. YCH India розробляє індивідуальні ланцюги постачання електроніки, товарів загального вжитку, хімічних речовин, а також товарів медичної та автомобільної індустрій в Індії. Серед його клієнтури — DELL, ACER, TPV, General Mills, HCL тощо.

DB Schenker — другий за величиною у світі експедитор, що отримав сертифікат відповідності стандарту ISO 28000 для свого регіонального офісу в Азіатсько-Тихоокеанському секторі в Сінгапурі, а також для свого місцевого офісу, розташованого в аеропорту Changi у Сінгапурі. Клаус Еберлін, головний виконавчий директор Азіатсько-Тихоокеанського регіону, бачить стандарт ISO 28000 як *«певного виду парасольку, стандарт, що містить елементи, такі як програми TAPA. Стандарт ISO 28000 виходить за фізичні аспекти безпеки, оскільки охоплює такі елементи, як інформаційний потік і фінансові дані»*.

Asian Terminals, портове підприємство, розробник та інвестор у Філіппінах і перший морський термінал, що пройшов сертифікацію на відповідність вимогам стандарту ISO 28000 у цій країні.

CTS Logistics-Chin займається логістикою та виробництвом, здійснює комплектацію і збирання систем для управління споживчою електронікою, інформаційними технологіями й телекомунікаційною продукцією, компанія успішно впровадила систему управління відповідно до вимог стандарту ISO 28000.

Banner Plasticard, Філіппіни, надає послуги з дизайну та друку карток, персоналізації, тиснення, кодування, термального друку, пакування і пакетування, сертифікована на відповідність вимогам стандарту ISO 28000.

Для інших підприємців та митників проводять підготовку та професійне навчання з питань убезпечення на основі стандарту ISO 28000.

Дорога в майбутнє

Крім згаданих вище прикладів, існують й інші транспортні та фармацевтичні організації, організації охорони здоров'я та інформаційних технологій, державні установи, що перебувають у процесі впровадження стандарту ISO 28000 та сертифікації відповідно до його вимог.

З часу першої публікації стандарту в 2007 році він стрімко набуває популярності. Причина цього проста: існує необхідність у чітких, однозначних міжнародних рекомендаціях, які допоможуть вирішувати проблеми ланцюга постачання і світової торгівлі в усіх галузях. Стандарт ISO 28000 є тим самим інструментом, який здатний допомогти в цьому.

Стандарти серії ISO 28000

Стандарт ISO 28000:2007 *«Системи управління безпекою ланцюга постачання. Технічні умови»* — загальна «парасолька» — стандарт на систему управління для убезпечення ланцюга постачання, на відповідність вимогам якого проводять сертифікацію.

Стандарт ISO 28001:2007 *«Системи управління безпекою ланцюга постачання. Найкращі методи забезпечення безпеки в ланцюзі постачання, оцінювання та плани. Вимоги та настанови»* призначений сприяти промисловості в задоволенні вимог програми уповноваженого економічного оператора (AEO).

Стандарт ISO/PAS 28002:2010 *«Системи управління безпекою ланцюга постачання. Розвиток стабільності в ланцюзі постачання. Вимоги та настанови щодо застосовування»* робить додатковий акцент на стабільність. Відповідає на потребу підприємств забезпечувати своїх постачальників, розширювати ланцюги постачання і вживати заходи для запобігання та зменшення загроз і небезпек, яким вони піддаються. У рамках системи управління, відповідно до вимог стандарту ISO 28000, стандарт ISO/PAS 28002 підкреслює необхідність тривалої роботи, інтерактивного процесу для запобігання, реагування та забезпечення безперервної роботи основних процесів організації в разі руйнівних подій.

Стандарт ISO 28003:2007 *«Системи управління безпекою ланцюга постачання. Вимоги до органів аудиту та сертифікації систем управління безпекою ланцюга постачання»* надає настанови з акредитації та сертифікації.

Стандарт ISO 28004:2007 *«Системи управління безпекою ланцюга постачання. Настанови з упровадження стандарту ISO 28000»* допомагає користувачам упроваджувати системи управління відповідно до вимог стандарту ISO 28000.

[5] TAPA являє собою форум, який об'єднує світових виробників, логістичних провайдерів, вантажних перевізників, правоохоронні органи та інші зацікавлені сторони з загальною метою скорочення втрат вздовж міжнародних ланцюгів поставок.

Три додатки до стандарту ISO 28004 було розроблено після публікації стандарту з метою надання додаткових корисних рекомендацій:

Amd 1 призначений для виконання середніх та малих операцій підприємствами морського порту (на підтримку прохання Міжнародної морської організації (IMO)).

Amd 2 надає конкретні настанови малим і середнім підприємствам (SMEs) щодо впровадження стандарту ISO 28000.

Amd 3 надає конкретні настанови організаціям, які прагнуть виконувати вимоги стандарту ISO 28001. Настанови щодо убезпечення, вміщені до стандарту ISO 28001, детально розроблено у співпраці зі Світовою митною організацією (WCO). Опублікований як PAS у 2010 році.

Стандарт ISO 28005 *«Системи управління безпекою ланцюга постачання. Портові операції з використанням електронних систем (EPC)»*. Цей стандарт розроблений відповідно до вимог IMO та WCO. Для прискорення розроблення стандарт ISO 28005 було поділено на дві частини:

Стандарт ISO 28005-1 «*Повідомлення структур*»;

Стандарт ISO/FAS 28005-2:2009 *«Елементи основних даних»*.

Стандарт ISO 28006 *«Управління безпекою RO-RO пасажирських поромів. Найкраща практика застосування заходів безпеки»*.

Стандарт ISO 20858:2007 *«Судна і морські технології. Оцінювання безпеки споруд морських портів і розроблення планів безпеки»* забезпечує застосування Кодексу безпеки портів.

Діяльність з кібер-безпеки. Рішення для бізнесу

Едвард Хемфрі[6]

Існує багато різноманітних історій про кібер-загрози, з якими стикаються підприємства, уряди та громадяни. Це не просто чутки, такі загрози є реальними, а їхній вплив є досить значним.

Питання кібер-безпеки постало задовго до загальновідомого скандалу з WikiLeaks. Відомо багато повідомлень щодо випадків крадіжки особистої інформації та даних стосовно клієнтів, у тому числі сотні тисяч номерів соціального страхування. Інші кібер-загрози охоплюють поширені крадіжки особистих даних, інтернет-шахрайства та злочини проти дітей.

Однією з найтривожніших подій 2010 року стала поява комп'ютерного «хробака Stuxnet», який став загрозою для безпеки промислових систем, таких як АЕС-контролери, гідроелектростанції, електричні мережі та інші енергетичні об'єкти. Частота і складність цього виду шкідливих програм, а також питання стосовно можливої мотивації злочинців викликають стурбованість урядів та інших схильних до ризику інфраструктур.

«Хробак Stuxnet» виявив уразливі місця Інтернет-комунікацій, а також той факт, що деякі частини національної інфраструктури можна розглядати як «бомбу сповільненої дії». Але це не єдина галузь, що є вразливою для кібер-війни в багатьох країнах.

[6] Професор Едвард Хамфрі протягом 35 років працював у сфері інформаційної безпеки у великих міжнародних компаніях Європи, Північної Америки та Азії, а також у таких організаціях та установах, як Європейська Комісія, Рада Європи та Організація економічного співробітництва та розвитку (OECD). Він є керівником робочої групи ISO/IEC з питань розроблення стандартів на ISMS. Професор Едвард Хамфрі читає лекції в університетах по всьому світові і видав декілька видатних книг з питань упровадження стандартів ISMS.