УДК 65.012.45:658.114

Твердохліб І.С., студент гр. 125м-16-1,
Ковальова Ю.В., асистент кафедри безпеки інформації та телекомунікацій
(Державний ВНЗ «Національний гірничий університет», м. Дніпро, Україна)

УПРАВЛІННЯ ІНЦИДЕНТАМИ КІБЕРБЕЗПЕКИ НА МАЛИХ КОМЕРЦІЙНИХ ПІДПРИЄМСТВАХ

Питання забезпечення інформаційної безпеки на малих комерційних підприємствах актуальне в наш час, як ніколи раніше. Відповідно, і питання запобігання появи небажаних або несподіваних подій ІБ, інцидентів, з якими пов'язана значна вірогідність компрометації бізнес-операцій та створення загроз ІБ, теж актуальні. А виходячи з того, що значна частина існуючих організацій та підприємств складають малі приватні підприємства, даний питання стає особливо гострим і важливим, якому необхідно приділити належну увагу.

Малі комерційні підприємства є невід'ємною частиною соціально-економічної країни. По-перше, вони сприяють підтримці стабільності ринкових відносин, оскільки значна частина населення втягується в цю систему відносин

По-друге, вони забезпечують необхідну мобільність виробництва в умовах ринку, поглиблення спеціалізації та широке розвиток кооперації виробництва, без яких немислима його висока ефективність. В підсумку це веде до динамічності господарського розвитку та зростання національній економіки.

По-третє, роль малих підприємств у діяльності крупних та середніх підприємств постійно зростає. Велика значення має здатність малих підприємств розширювати сфери доповнення трудової діяльності, створювати нові можливості не тільки для працевлаштування, а перш за все для підприємницької діяльності населення та використання вільних виробничих можливостей.

Інцидент інформаційної безпеки - один або кілька небажаних або несподіваних подій інформаційної безпеки, які з значною ступенем ймовірності піддають небезпеки ділову діяльність та загрожують інформаційної безпеки

В даній таблиці представлені завдання та засоби їх реалізації, безпосередньо пов'язані з управлінням інцидентами інформаційної безпеки. Основна інформаційна частина взята з міжнародного стандарту ІБ 27001. [таб.1]

Управління ризиками інформаційної безпеки вимагає відповідають оцінки ризиків і методу обробки ризиків, які можуть включати оцінку втрат і вигод, законодавчі вимоги, питання, що викликають заклопотаність зацікавлених осіб та інші відповідні вихідні дані. Оцінка ризиків повинна виявляти, кількісно оцінювати і пріоритезувати ризики відповідно до критеріїв прийнятності ризиків і цілями, істотними для організації.

Ці результати повинні служити орієнтиром і визначати відповідні дії і пріоритети для управління ризиками інформаційної без-пеки і впровадження засобів управління, обраних для захисту від цих ризиків. Оцінка ризиків повинна включати систематичний підхід до оцінки величини ризику (аналіз ризику) і процес порівняння прогнозної оцінки ризику з критеріями для визначення значущості ризиків (визначення ступеня ризику). Оцінка ризиків повинна виконуватися періодично для урахування змін у вимогах інформаційної безпеки і ситуації з ризиками, наприклад, для активів, погроз, вразливостей, впливів, оцінки ступеня ризику, а також коли відбуваються істотні зміни.

В першу чергу, компанія повинна мати чітко визначену політику безпеки, адже без документованих принципів, правил, процедур і багато чого іншого неможливо регулювати інформаційні потоки.

Якщо прислухатися до рекомендацій і порад міжнародних стандартів ІБ, можна значно поліпшити безпеку системи в області управлінні інцидентами інформаційної безпеки.

Таблиця 1.

Завдання	**Засоби реалізації**
Обов'язки та процедури	Повинні бути встановлені обов'язки керівництва та процедури, щоб гарантувати швидкий, результативний і належну відповідь на інциденти інформаційної безпеки.
Оповіщення про події, пов'язані з інформаційною безпекою	Оповіщення про події інформаційної безпеки повинно доводитися по відповідних каналах управління якомога швидше.
Оповіщення про уразливість в інформаційній безпеці	Від співробітників і працюють за контрактом, що використовують інформаційні системи і сервіси організації, необхідно вимагати фіксувати і повідомляти про будь-які виявлені або передбачуваних вразливості в інформаційній безпеці систем і сервісів
Оцінка і рішення щодо подій інформаційної безпеки	Події інформаційної безпеки повинні оцінюватися і потім прийматися рішення, чи слід їх класифікувати як інцидент інформаційної безпеки.
Відповідні заходи на інциденти інформаційної безпеки	Реагування на інциденти інформаційної безпеки має здійснюватися відповідно до документально оформленими методиками.
Лікування уроків з інцидентів інформаційної безпеки	Знання, отримані з аналізу та дозволу інцидентів інформаційної безпеки, повинні використовуватися для зменшення ймовірності інцидентів в майбутньому або їх впливу.
Збір свідчень	Організація повинна визначити і застосовувати процедури для ідентифікації, збору, комплектування і збереження інформації, яка може служити в якості свідчень

Основою для цих рекомендацій служив міжнародний, які більш детально описує не тільки питання в області УІІБ, а й основні правила менеджменту ІБ. Резюмуючи, хочеться сказати про те, що якщо керівництво комерційних підприємств буде приділяти належну увагу питанням УІІБ, то воно може заощадити фінанси, які були б витрачені на виправлення наслідків інцидентів і зберегти чисту репутацію своєї фірми.

ПЕРЕЛІК ПОСИЛАНЬ

1. ISO/IEC 27002:2013. Information technology - Security techniques - Code of practice for information security controls.