Пітел Н.С., к.е.н., доц.
Набок І.Г., здобувач групи УФЕБ-21М
Центральноукраїнський національний технічний університет
м. Кропивницький, Україна

ВПРОВАДЖЕННЯ КІБЕРАУДИТУ В ДІЯЛЬНІСТЬ ОРГАНІЗАЦІЇ ЯК СКЛАДОВОЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ

Під час швидкого розвитку інфраструктури та розширення процесів інформатизації діяльності компаній, все більшої ролі набувають інформаційні технології, які застосовують в системах менеджменту. Сьогодення характеризується тим, що середовище інформаційних технологій являє собою структурний елемент підприємства, який є досить складним за своєю природою, позаяк об'єднує програмні, інформаційні, апаратні засоби, а також людську складову, які дозволяють забезпечити ефективну роботу компаній. Відповідно, постає потреба у нарощені економічності та результативності використання ІТ, забезпечені переваг в боротьбі із недоліками, які можуть бути виділені під час їх застосування та обґрунтування витрат, які виникають під час функціонування інформаційних технологій. Зауважимо, що діяльність телекомунікаційного підприємства напряму залежить від якості тих ІТ-технологій, які застосовуються. Зокрема, для забезпечення ефективної їх діяльності, особливої важливості набуває використання в системі менеджменту такого явища, як аудит інформаційних технологій.

Під аудитом інформаційних технологій варто розуміти основний елемент, який дозволяє забезпечити якість інформаційних систем, а також ефективне використання пакетів прикладних програм. Для забезпечення безпеки економічної діяльності ІТ-аудит відіграє важливу роль, оскільки без надійних заходів контролю компанія не матиме змоги ефективно здійснювати транзакції та операції, формувати надійну фінансову звітність та не зможе досягти запланованого рівня розвитку [2].

Однією із причин успішних кібератак виступає застосування компанією застарілого комп'ютерного обладнання, а також старих інформаційних систем, зниження рівня фінансування, яке необхідно використовувати на оновлення комп'ютерних систем, серверів операційного обладнання, відсутність новітніх систем аналізу, які дозволяють виявити шкідливе програмне забезпечення, застарілі системи управління інформаційною безпекою, тощо.

Відповідно забезпечення економічної безпеки досліджуваного підприємства, насамперед, залежить від того, наскільки ефективним буде захист від потенційних кібератак, які в найближчому майбутньому обов'язково будуть здійснюватися ворогом, а також недобросовісними конкурентами.

Тобто, робимо висновок, що питання інформаційної безпеки повинно носити постійний та системний характер і повинно здійснюватися, впливаючи на великі обсяги даних, які є різними за природою та цілями досягнення та можуть призводити до різних наслідків.

Для попередження кіберзагроз, а також мінімізації їх активного впливу, компанії необхідно створити системи захисту, яка дозволить їм протидіяти. Насамперед, це передбачає формування професійної команди, яка буде протидіяти загрозам в цій системі [2].

Доречним буде залучення до фахівців з ІТ-сфери також аудиторів, які будуть здійснювати моніторингові процедури та аудит, заснований на управлінні ризиками, що збільшить ефективність існуючої системи.

Залучені спеціалісти, які будуть вести боротьбу з можливими кіберзагрозами повинні бути достатньо обізнаними стосовно новинок та ризиків в сфері ІТ, які можуть настати, за умови несанкціонованого вторгнення в ІТ-систему. Спеціалістам, які будуть здійснювати ІТ-

аудит, а також аудит безпеки інформаційних систем, мають бути здатними визначати та оцінювати ризики настання кризових ситуацій, які будуть найбільш властиві організації, а також здійснювати допомогу для досягнення тих цілей господарської діяльності, які заплановані компанією, шляхом розробки моніторингових та контролінгових процедур ІТ-систем, що базуватимуться на оцінці ризиків.

Загалом, основним завданням здійснення ІТ-аудиту полягає в координації дій менеджменту та персоналу компанії під час вторгнення до комп'ютерних систем, а також мінімізація тих наслідків, які сталися після інциденту, застосування заходів щодо стримування порушників та їх витіснення із інформаційних систем компанії.

Для цього, на нашу думку, ефективним стане впровадження в діяльність організації ISO / IEC 27001:2013, за допомогою якої можна удосконалити менеджмент інформаційної безпеки компанії. Насамперед, мова йде про пошук факторів, які можуть призвести до ризику та застосування ефективних методів контролю щодо процесу менеджменту інформаційних загроз. Варто додати, що зазначений стандарт дає змогу гнучко адаптувати процес менеджменту компанії до особливостей її діяльності на ринку, а також тримати зацікавленість споживачів і дати їм розуміння захищеності їх особистих даних. Зауважимо, що в умовах сьогодення задовольнити такі потреби є актуальним на телекомунікаційному ринку [1].

Зазначена система менеджменту інформаційної безпеки дає змогу запровадити найкращий світовий досвід, який дає змогу удосконалити захист даних організації та мінімізувати загрозу щодо порушення безпечності його інформаційної системи. Зауважимо, що ефективний безпекоорієнтований менеджмент інформаційних систем, в даному випадку, базується на проведенні регулярних моніторингових та аудиторських процедур. Для поглиблення якості забезпечення інформаційної безпеки необхідно давати доступ до діяльності компанії і третій стороні, тобто органу який здійснюватиме оцінювання відповідності та надаватиме додаткові гарантії стосовно управління ризиками в інформаційних системах. Це передбачене означеною системою управління і підтверджено тим, що для покращення результативності бізнесової діяльності в усьому світі саме в сфері інформаційної безпеки компанією кожного року витрачається понад 1 млн годин [1].

Загалом кібераудит має важливе значення під час перманентного вдосконалення системи менеджменту безпеки в сфері ІТ за допомогою протокола ISO / IEC 27001. Передбачено, що із розвитком відповідних технологій також буде підвищено і захист даних, який залишається у ключових компетентностях ISO / IEC 27001. Таким чином, експертам організації надається інформація від сторонніх аудиторів, які прораховують рівень захисту інформації в ІТ-системах компанії, дають висновок стосовно ризику, який може настати для даної організації, тим самим, вдосконалюючи менеджмент їх інформаційних систем [2.

Знання протоколів ISO / IEC 27001 дасть змогу сформувати бачення ситуації з точки зору аудитора. А відповідно, досить важливим є планування формування звітності про діяльність компанії, здійснюючи його із перманентним вдосконаленням методів збору інформації, переглядаючи вузькі місця та потенційні загрози, які можуть вплинути на безпеку діяльності компанії, а також визначати вірні структурні елементи, які допоможуть ефективно управляти ІТ-системами.

Список використаної літератури:

1. Коваленко С. В., Смолєв Є. С., Баргилевич О. А. Технологія аудиту кібербезпеки корпоративної інформаційної системи за методикою ISO/IES: 27001. *Сучасний захист інформації*. 2021. № 3. С. 29-35.

2. Козлова О. Ю., Кононович В. Г., Кононович І. В., Романюков М. Г., Тимошенко Л. М. Динамічні властивості процесів забезпечення кібербезпеки на прикладі аудиту кібербезпеки. *Інформатика та математичні методи в моделюванні.* 2017. Т. 7, № 3. С. 205-212.