УДК 330.658.005.5

Сотниченко В.М., к.пед.н., доцент,
Державний університет
телекомунікацій

ІНФОРМАЦІЙНА БЕЗПЕКА ЯК БАЗОВА СКЛАДОВА ЕКОНОМІЧНОЇ БЕЗПЕКИ ТЕЛЕКОМУНІКАЦІЙНОГО ПІДПРИЄМСТВА

В статті розглянуто основні аспекти залежності стану економічної безпеки підприємства від безпеки інформаційної, від ступеню надійності зберігання інформації тадоступу до неї. Висвітлено окремі причини недостатньої захищеності інформації та шляхи покращення ситуації.

Ключові слова: *інформаційна безпека, економічна безпека, інформаційно-телекомунікаційні системи, інформаційний ресурс, цифровий простір, конкурентоздатність.*

Постановка проблеми. Економічна сфера діяльності – це сфера завжди актуальна, завжди була і є полем протистояння, боротьби інтересів між людьми, суспільствами і державами. Але і не тільки боротьби, а й співробітництва. Арсенал співробітництва і, одночасно, боротьбі (чесної і нечесної конкуренції) є надзвичайно різноманітним і різноплановим, але більша його частина – це технології, методи, способи та прийоми оволодіння інформацією конкурента.

Є багато самих різних визначення змісту поняття «інформація», але в контексті даної статті найбільш підходить таке: інформація – це дані, доступні індивідам, фірмам або урядам під час прийняття економічних рішень. В принципі існує нескінченно великий обсяг інформації; на практиці навіть такі найбільші і досвідчені організації, як центральні банки і багатонаціональні компанії, володіють лише невеликою її часткою. Інформація може стосуватися загального стану справ, інтелектуально-кадрового потенціалу, технологій, рішень інших економічних агентів і своїх власних переваг і планів, системи доступу до інформації [7, с. 97-99]. Ніщо з цього не відомо з повною визначеністю.

У сучасних умовах розвитку світових ринків ключовим фактором, який визначає конкурентоспроможність підприємства, виступає наявність у нього унікального інформаційного ресурсу. Унікальність його полягає в тому, що він відображає специфіку саме цього конкретного підприємства. Інформаційний ресурс існував завжди, але не розглядався як окрема категорія. Його спеціально не вивчали, не виділяли в окрему тему. Вважалося, що конкурентоздатність підприємству забезпечить висока якість його продукції, реклама і короткий часовий проміжок між виникненням потреби та її задоволенням [4, с. 7-9]. Хоча з політичної і військової точок зору значимість національних інформаційних ресурсів усвідомлювалася вже багато століть, а економічний аспект став досліджуватися лише в останній чверті XX століття.

З розвитком суспільства і подальшою його трансформацією в суспільство інформаційне, із переходом від національних економік в економіки цифрові і, зрештою, з їх інтеграцією, інформаційний ресурс стає самим головним фактором впливу на соціально-економічний і політичний розвиток суспільства. Боротьба за володіння інформацією конкурента стає пріоритетною. Для забезпечення успіху в цій війні розробляються спеціальні інформаційно-комунікаційні технології, які нерідко, використовуються як зброя.

Аналіз останніх досліджень і публікацій. Впровадження системи інформаційної безпеки – одне з головних завдань, яке слід вирішувати вже на стадії відкриття компанії. Інформаційна безпека – це захищеність інформації від навмисного або випадкового

втручання, яке може завдати шкоди власнику інформації – як окремої людини, так і компанії, підприємству. Слід зазначити, що інформаційна безпека не зводиться лише до її захисту від несанкціонованого втручання, а може постраждати і від пошкодження всієї системи або їїчастини, точніше, з технічних і технологічних причин. Крім цього, інформація може зчитуватися і без прямого втручання в систему, а з електромагнітного випромінювання каналів і пристроїв при передачі її від одного об'єкту до іншого [8, с. 8-13].

Інформаційною безпекою сьогодні все більше цікавляться як фахівці в галузі телекомунікацій,так і науковці, для яких зрозуміло, що стан економічної безпеки треба розглядати, у першу чергу, через захищеність інформаційного ресурсу підприємства.

Різні аспекти інформаційної безпеки на підприємствах в своїх працях розглядають такі дослідники як Альшанская Т.В., Ястремская Н.Ю., Фролова Л.А. вони виділять рівні інформаційної безпеки, основні види носіїв інформації, її класифікацію.

Питання методологічного забезпечення інформаційної безпеки суб'єктів інформаційних відносин досліджує Атаманов Г.А. Новикова І.В. вивчає питання управління конкурентоспроможністю телекомунікаційних підприємств значною мірою через інформаційну безпеку. Гранатуров В.М., Литовченко І.В., працюючи над питання управління послугами звязку, методами оцінки, підтримки та підвищення конкурентоспроможності послуг зв'язку, значну вагу приділяють захисту інформаційного ресурсу.

Проблема інформаційної безпеки внесла новизну і у відповідну термінологію. З'явилися такі поняття як кіберпростір, комп'ютерна безпека, інформаційна війна та інформаційна зброя, війська інформаційних операцій [7, с. 97]. Проблема інформаційної безпеки має для України глобальне значення. Особливо сьогодні, в надзвичайно скрутний для держави час і на фоні тих економічних завдань, які Україна повинна вирішувати. А успішно їх вирішити можна тільки через підключення до світового інформаційного простору. Без вирішення цього глобального завдання економіка України приречена на занепад. Це сьогодні сама велика загроза економічній безпеці підприємств і національній безпеці держави.

Присутність України в міжнародному цифровому просторі, як обов'язкова умова успішного економічного розвитку, буде можливою лише тоді, коли буде вирішено питання інформаційної безпеки. Сьогодні Україна посідає серединні позиції в світі по основним показникам розвитку Інтернету і має оперативний доступ до інформаційного та обчислювального ресурсу [2, с. 167]. Це позитивне досягнення. Однак, треба пам'ятати, що Інтернет – це не тільки благо, а й джерело небезпеки.

Невирішена раніше частина загальної проблеми. Інтернет сьогодні може слугувати засобом вирішення певних завдань із застосуванням інформаційної зброї. Це пов'язано, в основному, з вирішенням проблем захисту інформаційного ресурсу, телекомунікаційних систем, мереж і технологій, запобіганням комп'ютерних злочинів. Для України вирішення цієї проблеми є першочерговим завданням. Особливо це усугубляється тим, що процес розбудови власної інфраструктури ще далеко не завершено. А це фундамент, на якому вже поетапно будуть вирішуватися завдання зі створення цифрової країни.

Мета статті. Інформаційний ресурс будь-якої компанії, а телекомунікаційної особливо, є предметом посиленої уваги з боку конкуруючих фірм. Конкурентна боротьба в ідеалі представляє собою чесне змагання за лідерство на ринку товарів і послуг, однак прикладів нечесної конкуренції більш ніж достатньо. І основним методом боротьби в нечесній конкуренції є доступ у будь-який спосіб до інформаційного ресурсу конкурента.

Виклад основного матеріалу. Інформаційний ресурс має відповідну ієрархічну структуру за ступенем конфіденційності інформації. Інформація про підприємство може бути у відкритому доступі і обмеженому. Інформація вільного, відкритого доступу використовується з метою презентації самого підприємства, в рекламі його продукції, при роботі з клієнтами тощо.

Інформація для службового користування – це інформація обмеженого доступу. Це стосується, в основному, режиму на підприємстві, порядку доступу до об'єктів, місця їх розташування, зберігання та транспортування продукції, порядок її реалізації, розподіл кадрового потенціалу за функціональним призначенням. До такої інформації доступ має обмежене коло співробітників самого підприємства і представники контролюючих органів: податкова служба, контрольно-ревізійне управління, спецслужби.

Конфіденційна інформація.Це інформація особливої важливості і, в першу чергу,вона стосується технологій виробництва, порядку доступу до управління основними ресурсами підприємства. До такої інформації доступ мають одиниці спеціально підготовлених працівників, діяльність яких також знаходиться під контролем спеціальних органів. Рівень контролю залежить від місця підприємства на ринку, виду продукції, що випускається та форми власності.

Існує ще й таке поняття як «асиметрична інформація». Це коли не всі учасники ринку володіють однаковою інформацією. До цього є багато причин. Наприклад, найбільш характерна з них – це коли інформація, яка існує в думках, не перенесена на інші носії, не озвучена і формується оперативно, в процесі ринкових взаємовідносин. Учасники ринку не володіють інформацією про те, якою інформацією володіють їхні партнери, конкуренти.

На кожному рівні ієрархії інформаційного ресурсу формуються загрози відповідного типу і характеру і з відповідними наслідками. Але особливий інтересдля конкурентів представляє собою конфіденційна, закрита інформація, яка ретельно охороняється.

За джерелом походження загрози для інформаційної безпеки телекомунікаційного підприємства поділяються на внутрішні і зовнішні. Найбільш небезпечними на думку багатьох фахівців є загрози внутрішні. Носієм і джерелом інформації, що може зацікавити недобросовісного конкурента, є працівник підприємства. Як правило, проблеми інформаційної безпеки підприємства зводиться до фінансових ризиків і можливих послідуючих втрат [6, с. 241-243]. Але не тільки матеріальні, а й моральні втрати є важливими і не менш значущими для репутації підприємства. Підприємства-партнери вибудовують модель співробітництва на засадах довіри, яка формується роками. І якщо в одному з них виявляються навмисні «зливи» інформації, то це дуже неприємне явище для репутації цієї компанії. Методи розкриття інформації можуть бути різними. По-перше, навмисними і ненавмисними. До останніх відноситься розміщеннянебажаної інформації в соціальних мережах, в блогах, в особистих розмовах між співробітниками підприємства у присутності сторонніх осіб, які випадково можуть бути зацікавленими в отриманні такої інформації [6]. Мова йде про те, що співробітники не мали намірів завдати шкоди своєму підприємству. Тобто, це є безадресною дією.

А от що стосується навмисного розкриття інформації, то ця дія вже орієнтована на конкретного адресата. У цьому випадку сам процес вже є більш структурованим і організованим: носій інформації – зміст інформації – канал передачі інформації – спосіб передачі – отримувач інформації. Наприклад, інформація про укладання важливих угод. Зазвичай, досвідчені керівники не поширюють таку інформацію, щоб передчасно не зашкодили конкуренти і не зірвали підписання угоди. Загроза посилюється, якщо до змісту самої викраденої інформації про важливу подію інсайдер додає час, місце та учасників. Знаючи час і місце, можна створити несприятливі умови для укладання угоди. Знаючи учасників, можна теж зашкодити. Методів багато. Наприклад, самий гуманний – оприлюднення компромату на укладачів угоди, або на одного з них.Тому, доступ до інформації будь-якого рівня повинен бути закритий і захищений. Але, якщо вже не вдалося уникнути витоку інформації, то до справи мають долучатися фахівці зі зв'язків з громадськістю.

Спеціалісти з цього напряму діяльності допоможуть мінімізувати наслідки кризової ситуації. Бажано заздалегідь виробити стратегію поведінки за більш типових ситуацій, узгодити з керівництвом, з представниками громадськості. При цьому, чим більше у PR-фахівця буде позитивних контактів за межами підприємства, тим сильніша буде його

позиція, а результати його роботи більш ефективними і переконливими. Від цього заложитиме репутація підприємства.

PR-фахівці служать захистом інтересів бізнесу від негативної громадської думки, втілюють в життя політику підтримки позитивного ставлення громадськості до діяльності підприємства і до його продукції. Саме вони безпосередньо спілкуються із засобами масової інформації і доводять до них інформацію, що сприяє іміджу підприємства в широких масах населення. Позитивний імідж підприємства – це его антикризовий ресурс. Саме цей ресурс дозволяє підприємствам тривалий час утримувати на позитивному рівні ставлення до нього громадських і ділових кіл [1, с. 7-9]. І поки не втрачено довіри до себе, керівництво повинно забезпечити успіх підприємству, а PR-фахівці вже на професійному рівні знають, що з цим робити.

Неправильна позиція керівництва підприємства, у випадку втрати інформації – це вдавати, що нічого не відбулося, все нормально. У більшості випадків і колектив підприємства і, як наслідок, громадськість з часом дізнаються про це. Замовчування призводить до того, що втрачається тим самим позитивний людський ресурс колективу, який зацікавлений в успішній роботі підприємства і готовий спільно з керівництвом і громадськістю виправити ситуацію, так – втрачається довіра, виникають невдоволення. Можуть бути хворобливі наслідки. Наприклад, у 2014 році компанії Yahoo! стався масштабний витік персональних даних 500 млн користувачів. Протягом двох років компанія приховувала інформацію про цей інцидент. Але, абсолютно повно цього не вдалося зробити і проти компанії розпочала слідчі дії Комісія з цінних паперів і бірж США, стверджуючи, що Yahoo! повинна була попередити користувачів і інвесторів вчасно.

Переконливий приклад, який наштовхує на висновок, про те, що головним питанням, що стоїть перед компанією, - як не допустити витоку даних. Очевидно, що хакерська загроза і недосконала система кіберзахисту в Україні призведуть до втрати інформації, але здебільшого, найбільш цінну, важливу інформацію компрометують самі ж працівники підприємства. Захист від діяльності інсайдерів представляє надзвичайно важливий фронт роботи із захисту інформації [5]. А інсайдер на телекомунікаційному підприємстві представляє для нього особливу небезпеку, оскільки він є професіоналом в галузі і може відкрити канали витоку інформації так, що й не відразу вони можуть бути виявлені.

Зрозуміло, в державі, з метою захисту інформації налагоджено систему відповідних заходів. Наприклад, що безпосередньо стосується телекомунікаційних підприємств, то з метою захисту інформації в інформаційно-телекомунікаційних системах Адміністрацією Держспецзв'язку надається консультативно-методична допомога органам державної влади, підприємствам, організаціям, установам з питань застосування нормативних документів з захисту інформації. Не виключається і можливість створення відомчої нормативної бази, комплексних систем захисту інформації тощо [2, с. 164-165]. В той же час збільшення кількості документів в нормативній базі збільшує і кількість заходів контролю за їх дотриманням та виконанням. А це створює додаткове навантаження на співробітників, яке нерідко, коли систему контролю побудовано непрофесійно, відволікає персонал від виконання своїх функціональних обов'язків і негативно позначається на результатах роботи компанії. На превеликий жаль, така система «стимулювання» працівників з метою покращення основних показників діяльності продовжує функціонувати ще з часів радянської бюрократичної системи.

В комплексі заходів «на покращення» й дотепер домінують вказівки та рекомендації. А насправді необхідні структурні і технологічні зміни та модернізації здебільшого залишаються без належної уваги.

На сьогодні найбільш відомими є дві системи покращення основних показників: комбінаторна і настановча (рекомендувальна). І перша і друга мають єдину мету, але реалізуються різними шляхами і методами.

Рекомендувальна – на рівні збільшення настанов і посилення відповідальності за їх неналежне невиконання. Цим, в тому числі, пояснюються недоліки і невисокі результати роботи. А в галузі інформаційних систем і мереж недоліки призводять до масштабних втрат, які миттєво негативно позначаються на роботі телекомунікаційного підприємства, на стані його економічної безпеки.

Комбінаторна працює на рівні структурної перебудови, пошуку найбільш ефективної комбінації її складових. Очевидно, виходячи зі світового та європейського досвіду, така система є більш сучасною і результативною.

В Україні кожного року, до 31 березня до Кабінету Міністрів установленим порядком подаються результати аналізу стану захисту інформації на всіх рівнях в масштабі держави: від інформаційно-телекомунікаційних систем органів виконавчої влади до підприємств, установ та організацій. В державі існує Реєстр інформаційно-телекомунікаційних систем (ІТС). Так от, останні відомості про стан захисту інформації, подані до Реєстру свідчать про те, що оброблення інформаційних ресурсів в державі здійснюється із порушенням чинного законодавства [2, с. 164]. А це створює сприятливі умови для несанкціонованого доступу до інформації, її подальшого незаконного використання. Це загроза не лише для окремого телекомунікаційного підприємства, а й для інформаційної безпеки України.

За даними Реєстру ІТС критична ситуація зі станом захищеності інформації на сьогодні склалася в Міністерстві інфраструктури України, в Міністерстві юстиції, в Міністерстві охорони здоров'я, в Міністерстві екології та природних ресурсів, в Міністерстві науки і освіти, в Державній службі України з питань безпечності харчових продуктів та захисту споживачів і, відповідно, в структурах цих органів виконавчої влади [2, с. 165]. Масштаби вражаючі.

Серед основних причин такого стану справ в системі захисту інформації, як зазначалося на парламентських слуханнях Верховної Ради України [1, с. 163-172], названі такі, як:

- відсутність сталого фінансування заходів із захисту інформації з боку Міністерства фінансів України;
- низький рівень професійної підготовки співробітників, що відповідають за стан інформаційної безпеки на підприємствах, організаціях, установах [3]. Пояснюється це, в першу чергу, нерозумінням керівництва значення питання забезпечення захисту інформації для економічної безпеки підприємства. Це з одного боку, а з іншого – небажання витрачати кошти на якісну підготовку та перепідготовку відповідних фахівців;
- керівники підприємств мало приділяють уваги аналізу стану справ із захистом інформації, вважають це неважливим, другорядним завданням, до того ж цим питанням нерідко займаються некваліфіковані спеціалісти.

Ще одним з найбільш важливих моментів є дисонанс, що утворився в контексті розгляду трьох базових складових вітчизняного цифрового світу в нашому суспільстві: рівень проникнення Інтернету, рівень технологічної готовності та рівень конкурентоспроможності. А дані показники, у співвідношенні своєї значущості для розвитку національної економіки дають підстави зробити висновки про те, що, чим вище буде технологічний рівень в галузі інформаційно-комунікаційних технологій, тим більше загроз буде для економічної безпеки інформаційно-телекомунікаційних систем. Порівняємо. За рівнем проникнення Інтернету Україна посіла 46 місце з 86 країн світу. Цей показник є комплексним і говорить про ступінь впливу Інтернету на населення у всіх сферах суспільного життя.

За рівнем конкурентоспроможності – 76 місце з 144 країн, а за рівнем розвитку інформаційно-комунікаційних технологій – 79 місце з 166 країн світу [2, с. 166-167]. З логіки порівняння наведених показників слідує, що всі три позиції знаходяться пропорційно на одному рівні, а рівень розвитку ІКТ навіть трохи поступається. Крім того, користувачі Інтернету явно потребують підвищення рівня інформаційної грамотності. Особливо це актуально там, де вони мають справу із вирішення питань економічної безпеки підприємства.

Це треба враховувати ще й тому, що починаючи з 2015 року серед українських телекомунікаційних підприємств, ІТ-компаній явно простежується тенденція підвищення рівня складності створюваних ними проектів. Це є, безумовно, шляхом підвищення рентабельності телекомунікаційних підприємств, зростання рівня їх економічної безпеки. Але, в той же час вимагає високого рівня професійної підготовки фахівців галузі. Своєчасного і систематичного підвищення кваліфікації.

Процес захисту інформації на телекомунікаційному підприємстві як основи його економічної безпеки вимагає впорядкованого та структурно організованого підходу до інформації. Епізодичність і безсистемність сприяють створенню загроз, які відносяться до загроз внутрішнього характеру. Тобто створюються відповідними працівниками компанії. В силу недостатнього професійного рівня або ж особистої безвідповідальності.

Система захисту інформації буде надійною, якщо вона побудована на основі таких складових:

- законодавча – на рівні законів, норм, актів;
- адміністративна – на рівні адміністрації підприємства;
- апаратно-програмна – на рівні спеціальних програм і пристроїв;
- фізична – на рівні електронно-механічних перешкод для проникнення порушників;
- морально-етична – на рівні норм поведінки, престижу як однієї людину, так і цілого підприємства.

В комплексі ці складові спрямовуються на усунення загрози безпеки, утворюють систему захисту інформації.

Системний підхід передбачає побудову такої моделі захисту інформаційної та економічної безпеки, яка б повністю відповідала специфіці діяльності підприємства, працювала б гармонічно з основними процесами і реагувала на всі сигнали, що від них надходять. Функціонування телекомунікаційного підприємства, у даному випадку, розглядається через систему соціально-економічних та політичних (у випадках проявів агресії) викликів. Ця система зумовлює режим роботи підприємства, сегмент ринку, потребу в кінцевому продукті.

Не вдаючись у деталі, умовно можна визначити три фази функціонування підприємства: прийом замовлення – виготовлення затребуваного продукту – поставка замовнику.Так само працює і система захисту економічної безпеки підприємства. Одночасно, паралельно, трьохфазно. Очевидно, що кожна фаза є потенційним носієм загроз для економічної безпеки підприємства. Система захисту інформації повинна, у звязку з цим, мати в своїй структурі сигнальну систему, адаптовану під кожну фазу. І відповідні механізми нейтралізації (знищення) загроз. Щоб загрози не переходили далі.

Всі процеси, що відбуваються у процесі функціонування підприємства, зведені в систему, яка захищається цілим комплексом як технічних, так і організаційних заходів. В їх складі антивірусна система, міжмережеве екранування, електромагнітне випромінювання. Крім того, така система повинна захищати інформацію на електронних носіях. Важливим прийомом в плані забезпечення інформації повинно бути впорядкування інформації і розмежування її по каналам доступу, систематизація різнопланових документів. Обов’язковим є створеннярезервних копій.

Повноцінне забезпечення економічної безпеки шляхом надійного захисту інформаційного ресурсу телекомунікаційного підприємства повинно бути стандартизовано, перебувати під надійним контролем в чітко означеному часі і просторі. Система захисту економічної безпеки підприємства повинна враховувати повний життєвий цикл інформаційного ресурсу – від зародження інформації і до її знищення або ж втрати нею актуальності.

Система повинна враховувати безліч чинників: об’єкти загроз, їх джерела, цілі зловмисників, способи оволодіння інформацією, технології і засоби захисту. У такому

випадку, коли буде максимально повно враховано всі фактори і деталі, система буде здатною забезпечити збереження інформаційного ресурсу та економічної безпеки підприємства.

Важливо розуміти, що характер загроз може бути різний. Різної природи, різних джерел походження, інтенсивності прояву, тривалості дій. Вони (загрози) інтегруються в тіло продукту, що виробляється на замовлення. І мало того, що вони будуть присутніми у готовому продукті, який до того ж стає їх носієм, вони ще й можуть залишатися у виробничій системі підприємства. Потім, з наступним циклом, об'єднаються з новими загрозами і, зрештою, створять власну систему в системі – антисистему.

Логіка функціонування систем інформаційної безпеки, побудована за такими принципами й підходами, припускає наступні дії:

- прогнозування і швидке розпізнавання загроз для інформаційного ресурсу та економічної безпеки підприємства, мотивів і умов, що сприяли нанесенню шкоди підприємству і зумовили збої в його функціонуванні і розвитку;
- створення таких умов роботи, за яких рівень небезпеки і ймовірність нанесення шкоди підприємству зведені до мінімуму;
- відшкодування збитків та мінімізація впливу виявлених спроб нанесення збитку.

Цей алгоритм представляє собою концептуальну основу, на якій вибудовується система захисту інформації підприємства і, як логічний результат – його економічна безпека.

Висновки. Захист інформації та створення надійної системи економічної безпеки є однією з найбільш важливих завдань як для невеликих компаній, так і для великих корпорацій. Віруси і троянські програми, спам, недосконаліть та уразливість певних комп'ютерних програм, неакуратне поводження співробітників з конфіденційної інформацією – все це представляє собою лише невелику частину потенційних проблем, з якими регулярно стикаються IT-фахівці компаній. За прогнозами провідних фахівців в галузі цифрової економіки у майбутньому очікується підвищення інтенсивності цільових атак на бізнес. Це потребує спеціальних знань, вмінь та навичок.

Зростаючою проблемою є також те, що багато працівників компаній мають доступ до IT-інфраструктури компанії з власних незахищених пристроїв. Використання особистих пристроїв створюють прецеденти витоків інформації і створення загрози для економічної безпеки підприємства.Співробітники компанії підключаються до корпоративних мереж і працюють з конфіденційною інформацією. Використання незахищених пристроїв при цьому може стати причиною втрати даних. На підприємстві, у зв'язку з цим, повинна бути спеціально розроблена і впроваджена політика безпеки, що враховує використання для роботи мобільних пристроїв – як особистих, так і корпоративних.

Потребує належної уваги рівень комп'ютерної грамотності персоналу, зокрема в плані захисту інформації. Особливо це важливо на рівні головних менеджерів компанії. Без цього неможливо забезпечити ефективну роботу і подальший розвиток IT-інфраструктури підприємства. У даний момент, в цілому по Україні менше половини фахівців вважають свою компанію готовою до боротьби з сучасними загрозами.

Менеджерам телекомунікаційних компаній і IT-інфраструктури підприємств треба звернути увагу на готовність до цільових атак.Хоча цільові атаки поки ще не так поширені, алев майбутньому очікується збільшення кількості цільових атак на інфраструктуру. При цьому, за прогнозами фахівців, на компанії чекають такі випробування, наслідки яких важко передбачити. У зв'язку з цим рекомендовано приділяти більше уваги превентивним методам захисту, що дозволить уникати загроз, а не усувати їх наслідки.

З огляду на вище сказане не можна залишати без належної уваги роботу з персоналом. Дослідження, проведені лабораторією Касперського, показали, що значна кількість IT-фахівців компаній нічого не знають про сучасні кіберзагрози, з якими вони повинні боротися. Крім того, низький рівень комп'ютерної грамотності персоналу є однією з причин зараження IT-інфраструктури компанії і втрати конфіденційної інформації. Тому навчання

всіх співробітників компанії основ інформаційної безпеки не менш важливо, ніж установка сучасного захисного програмного забезпечення.

Перспектива подальших наукових досліджень закладена практично в кожній позиції наведених вище висновків. Але найбільш цікавою представляється проблема, пов'язана з тенденцією зростання загрози за допомогою цільових атак на IT-інфраструктури підприємств.

Список використаної літератури

1. *Альшанская Т.В. Проблемы информационной безопасности на предприятиях / Т.В. Альшанская, Е.А. Гурьянова, Ю.В. Королькова / Развитие науки и образования в современном мире: сб. тр. Междунар. науч.-практ. конф. - Люберцы: АР-Консалт, 2014. - Ч. 3. - С. 97-99.*
2. *Новикова І.В. Управління конкурентоспроможністю телекомунікаційних підприємств: теорія, методологія, практика: монографія / И.В. Новикова. – Миколаїв: ФОП Швец В.Д., 2013. – 296 с.*
3. *Атаманов Г.А. Азбука безопасности. Методология обеспечения информационной безопасности субъектов информационных отношений / Г.А. Атаманов / Защита информации. - 2014. - № 5. - С. 8-13.*
4. *Реформи галузі інформаційно-комунікаційних технологій та розвиток інформаційного простору України: матеріали парламентських слухань у Верховній Раді України 3 лютого 2016 р. / Верховна Рада України, Комітет з питань інформатизації та звязку; ред. кол.: О.І. Данченко (голова), Г.О. Андрощук, О.Г. Старинець, О.А. Баранов [та ін.]. – К.: Парлам. вид-во, 2016. – 256 с.*
5. *Петрик В.М., Остроухов В.В., Штоквиш А.А. и др. Информационно-психологическая безопасность в эпоху глобализации: Учеб. Пособ. / Под ред. В.В. Остроухова. – К., 2008. – 544 с.*
6. *Гранатуров В.М. Управління послугам звязку: навч.посібник / В.М. Гранатуров, І.В. Литовченко. – К.: Освіта України, 2010, - 254 с.*
7. *Ястремская Н.Ю., Фролова Л.А. Развитие информационного рынка как условие и результат становления информационной экономики. [Електронний ресурс] //Инженерный вестник Дона. - №4 (27) / Том 27 / 2013. – Режим доступа: http://cyberleninka.ru/article/n/razvitie-informatsionnogo-rynka-kak-uslovie-i-rezultat-stanovleniya-informatsionnoy-ekonomiki*
8. *Янковский А. Проблемы в сфере кибербезопасности в Украине. [Електронний ресурс] // Украинская правда. – Режим доступа: http://www.pravda.com.ua/rus/columns/2017/02/15/7135442/*
9. *Ястремская Н.Ю., Фролова Л.А. Развитие информационного рынка как условие и результат становления информационной экономики. [Електронний ресурс] //Инженерный вестник Дона. - №4 (27) / Том 27 / 2013. – Режим доступа: http://cyberleninka.ru/article/n/razvitie-informatsionnogo-rynka-kak-uslovie-i-rezultat-stanovleniya-informatsionnoy-ekonomiki*
10. *Петрик В.М., Остроухов В.В., Штоквиш А.А. и др. Информационно-психологическая безопасность в эпоху глобализации: Учеб. Пособ. / Под ред. В.В. Остроухова. – К., 2008. – 544 с.*

Сотниченко Владимир Николаевич. Информационная безопасность как базовая составляющая экономической безопасности телекоммуникационного предприятия. *Защита информации и создание надежной системы экономической безопасности является одной из наиболее важных задач как для небольших компаний, так и для крупных корпораций. Вирусы и троянские программы, спам, несовершенство и уязвимость определенных компьютерных программ, неаккуратное обращение сотрудников с конфиденциальной информацией — все это представляет лишь небольшую часть потенциальных проблем, с которыми регулярно сталкиваются IT-специалисты.*

В цифровой экономике ожидается повышение интенсивности целевых атак на бизнес. Это требует специальных знаний, умений и навыков. Многие сотрудники имеют доступ к IT-инфраструктуре компании с собственных незащищенных устройств. Использование личных устройств создают прецеденты утечек информации и создание угрозы для экономической безопасности предприятия. Использование незащищенных устройств является одной из причин потери данных. На предприятии должна быть специально разработана и внедрена политика безопасности, учитывающая использование для работы мобильных устройств — как личных, так и корпоративных.

Требует должного внимания уровень компьютерной грамотности персонала в плане защиты информации. Менеджерам телекоммуникационных компаний и IT-инфраструктур предприятий надо обратить внимание на готовность к целевым атакам. Это представляет собой и научный интерес на перспективу.

***Ключевые слова**: информационная безопасность, экономическая безопасность, информационно-телекоммуникационные системы, информационный ресурс, цифровое пространство, конкурентоспособность.*

***Sotnychenko Volodymyr. Information security as a basic component of economic security of a telecommunications enterprise.** Protecting information and creating a reliable system of economic security is one of the most important tasks for small companies and large corporations. Viruses and Trojans, spam, imperfection and vulnerability of certain computer programs, inaccurate treatment of employees with confidential information - all this represents only a small part of potential problems that IT professionals regularly face.*

The digital economy is expected to increase the intensity of targeted attacks on business. This requires special knowledge, skills, and skills. Many employees have access to the company's IT infrastructure from their own unprotected devices. The use of personal devices creates precedents of information leaks and a threat to the economic security of the enterprise. Using unprotected devices is one of the causes of data loss. At the enterprise, a security policy should be developed and implemented, considering the use of mobile devices for work, both personal and corporate.

The level of computer literacy of personnel in terms of information protection requires due attention. Managers of telecommunications companies and IT infrastructure of enterprises should pay attention to the readiness for targeted attacks. This is a scientific interest in the future.

***Keywords:** information security, economic security, information and telecommunication systems, information resource, digital space, competitiveness.*