Кириленко А. І.
Бабинюк О. І.
к.е.н., доцент
ДВНЗ «Київський національний економічнийуніверситет імені Вадима Гетьмана», м. Київ

КІБЕРБЕЗПЕКА НА ЗАХИСТІ БІЗНЕСУ

Успішний бізнес – мета будь-якого підприємця. Проте майже завжди є ще хтось, хто вже надаю таку послугу, що призводить до інцидентів інформаційної безпеки задля зупинення росту розвитку конкурента. Так безліч компаній як мінімум один раз на рік зазнавали зовнішньої атаки або зіштовхувалися з внутрішніми інцидентами інформаційної безпеки (рис. 1) [1].

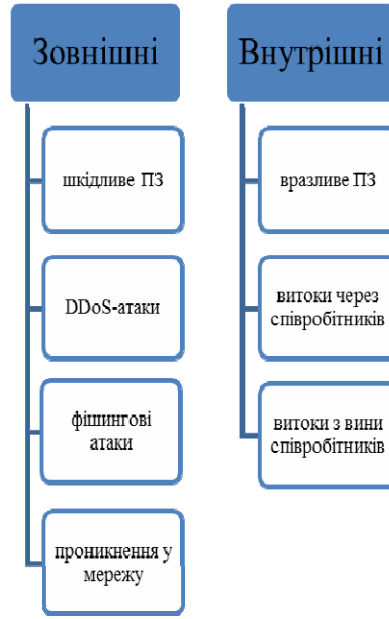

Рисунок 1. Схема видів інцидентів інформаційної безпеки

Сьогодні вкрай критичною є проблема розкрадання інформації через збільшення вагомості даних клієнтської бази і цінності інтелектуальної власності в успішності проду-

кції, яка виробляється, або надаваної послуги. Метою конкуруючих компаній можуть стати фінансова інформація та інформація про внутрішні процеси у компанії, інтелектуальна власність.

Проблема кібербезпеки полягає у тому, що бізнес рідко використовує надійне антивірусне ПЗ чи спеціалізовані рішення щодо захисту від DDoS-атак, вживає дій для захисту інформації та фінансових транзакцій. Заголовки новин містять безліч повідомлень про зломи комерційних структур, витік даних, електронне шахрайство тощо. Так в 2014 році компанія «Лабораторія Касперського» спільно з Європолом та Інтерполом розкрила групу Carbanak, яка успішно протягом багатьох років виводила кошти з банків через банкомати або онлайн-банкінг. Діяла група досить просто, через електронну пошту заражалися комп'ютери рядових співробітників і збиралися з них дані про те, яким чином влаштована робота в цьому банку і хто за що відповідає, а у подальшому це допомагало сформувати шляхи викрадання коштів [2]. Українські ЗМІ протягом останніх років розповідали про кібератаки на енергетичні компанії України, розсилку вірусів через пошту від імені податкової та майнінг криптовалюти через розміщення скриптів на сайтах державних установ [3].

Система захисту складається з багатьох взаємопов'язаних частин: організаційних, правових, інженерно-технічних заходів, а також заходів криптографічного та технічного захисту інформації, спрямованих на запобігання кіберінцидентам, виявлення та захист від кібератак, ліквідацію їх наслідків, відновлення сталості і надійності функціонування комунікаційних, технологічних систем [4]. Далі розглянемо юридичну складову, яка є основою для надійної системи захисту інформації.

Питання кібербезпеки наразі є досить гострим для усіх країн світу. Так до прийняття Закону України «Про основні засади здійснення кібербезпеки України» [5], національне регулювання обмежувалося нормами загального характеру, прийнятими на

галузевому рівні міністерств та відомств та деякою кількістю Указів Президента України. Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу зафіксовані Департаментом спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України ще в документі НД ТЗІ 2.5-004-99 [6].

Спеціалізований структурний підрозділ Державного центру кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв'язку та захисту інформації України (CERT-UA) періодично публікує рекомендації, які стосуються безпеки поштового сервісу, з протидії загрозі інсайдера, усунення вразливостей, пов'язаних з некоректним налаштуванням DNS-серверів тощо.

Рисунок 2. Заходи безпеки інформаційних систем

Для компанії досить важливо підготувати ефективне підґрунтя для впровадження технічної складової, переглянути і оптимі-

зувати минулі і поточні процедури та організувати на належному рівні ризик-менеджмент. Такі заходи забезпечать рівень безпеки інформаційних систем, та врахують її елементи (рис. 2).

Кібербезпека потребує постійної підтримки та аналізу її ефективності. Слід узгоджувати бізнес-ініціативи з питаннями безпеки. Важливою складовою захисту є постійне оновлення засобів забезпечення безпеки та підняття рівня захисту.

Заходи щодо протидії кіберзлочинності є і будуть залишатися актуальними для будь-якої компанії. Для цього обов'язково потрібно визначити ризики інформаційної структури, щоб забезпечити стабільний розвиток та успішність компанії, адже кібербезпека - це не разова акція.

Список використаних джерел

1. Раєцький А. Кібербезпека бізнесу це не лише технічні заходи URL: https://legalitgroup.com/kiberbezpeka-biznesu-tse-ne-lishe-tehnichni-zahodi/

2. Большое банковское ограбление: APT-кампания Carbanak URL: https://securelist.ru/bolshoe-bankovskoe-ograblenie-apt-kampaniya-carbanak/25106/

3. Україна стала плацдармом для кібератак URL: https: //dt.ua/business/ukrayina-stala-placdarmom-dlya-kiberatak-292894_.html

4. What is a security system and how does it work? URL: https://www.safewise.com/home-security-faq/how-do-security-systems-work/

5. Закону України «Про основні засади здійснення кібербезпеки України» URL: https://zakon.rada.gov.ua/laws/show/2163-19

6. НД ТЗІ 2.5-004-99 URL: https://tzi.ua/assets/files/%D0%9D%D0%94%D0%A2%D0%97%D0%86-2.5-004-99.pdf

Кмитюк Т.Л.
к.е.н.
ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана», Київ

ОСНОВНІ АСПЕКТИ МОДЕЛЮВАННЯ ЕКОНОМІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ЕКОНОМІКИ

Глобалізація, інтенсивний розвиток міжнародних економічних відносин, розвиток інформаційного суспільства призводить