***

ВПЛИВ СУЧАСНИХ ТЕХНОЛОГІЙ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ ПІДПРИЄМСТВ УКРАЇНИ

Максимова Юлія Олександрівна[1], Іванов Олексій Олексійович[2],
[1]Одеський національний університет імені І. І. Мечникова, м. Одеса,
[2]Фаховий коледж ОНУ імені І.І. Мечникова, м. Одеса

Питання інформаційної безпеки можна назвати актуальним для України сьогодні, оскільки частина, а іноді і уся важлива інформація підприємства зберігається у електронному вигляді. Усі сучасні підприємства намагаються уберегти себе від крадіжки даних. Будь-який витік інформації може призвести до серйозних проблем для компанії — від значних фінансових збитків до повної ліквідації.

XXI століття можна назвати століттям науково-технічного прогресу, який змінив життя людей. Перехід економіки до нового рівня підвищив значення інноваційної діяльності, розвитку наукомістких виробництв, які забезпечують умови для розвитку усіх галузей економіки України.

Нові технології швидко розвиваються, і вони впроваджуються в сектор підприємницької діяльності. Сучасні інформаційні технології допомагають налагоджувати та захищати виробничі та бізнес-процеси на підприємствах, забезпечуючи грамотну та безперебійну роботу. Завдяки активному використанню інформаційних технологій Україна може покращити своє економічне становище.

Сучасні підприємства України стикаються з багатьма загрозами та атаками з боку зовнішнього середовища. У зв'язку з цим є нагальна потреба в забезпеченні безпеки, як підприємств, так і клієнтів. Визнання цієї проблеми стало ключовим фактором тісної співпраці та переплетення двох різних, але взаємодоповнюючих структур — інформаційної безпеки та підприємницької діяльності [1]. Одне з головних завдань підприємницького сектору спрогнозувати, які технології стануть ергономічним інструментом для вирішення існуючих проблем. Впровадження нових технологічних процесів, сприяє оптимізації роботи підприємств, позитивним фінансовим результатам, покращенню інформаційної безпеки , а також лояльності клієнтів.

Діяльність кожного підприємства тісно пов'язана з отриманням, накопиченням, зберіганням, обробкою і використанням різноманітної інформації. Сучасний розвиток інформаційних технологій вимагає від підприємств здійснювати розробку заходів щодо збереження даних, перекриття можливих каналів витоку інформації та забезпечення рівнозначного надійного захисту всіх носіїв.

Хоча існує багато різних підходів до захисту цифрових активів підприємства, є кілька найкращих практик, які кожна компанія повинна мати на увазі. Це особливо вірно при оцінці переваг одного рішення порівняно з іншим.

Для захисту даних як у стані спокою, так і під час передачі потрібно шифрування. Якщо можливо, шифрування слід застосовувати у всій мережі підприємства, це роблять тому, що важко визначити, де зловмисник намагатиметься підслухати передачу [2].

Необхідно також використовувати концепцію найменших привілеїв. З найменшими привілеями дозволено входити лише тим, кому абсолютно потрібен доступ до сектора мережі або важливої для бізнесу програми. Якщо хтось інший хоче увійти, навіть якщо він випереджає тих, хто має доступ, йому буде заборонено працювати з тими даними . Це захищає мережу навіть від випадкових подій, коли хтось із непотрібними привілеями помилково залишає облікові дані доступу, або його телефон чи інший особистий пристрій викрадають, відкриваючи сховища облікових даних для входу.

Також важливим є аварійне відновлення: у разі форсмажорних ситуацій дуже важливо, щоб необхідні системи створювали резервні копії та працювали якомога швидше. Це може досягти за допомогою резервування систем і компонентів, які можуть впоратися з робочим навантаженням, необхідним для

підтримки роботи бізнесу. Створити резервування в усій архітектурі дуже складно, критичні системи можна ідентифікувати та підтримувати резервними компонентами та процесами. У разі порушення роботи ці системи можна автоматично розгорнути, обмежуючи час простою роботи підприємства.

Навчання співробітників основам кібербезпеки дуже важлливо на сьогоднішньому етапі розвитку економіки та ІТ. Наприклад, працівників можна навчити розпізнавати фішингові атаки, які використовують електронні листи або текстові вкладення, щоб спонукати людей натискати та завантажувати зловмисне програмне забезпечення. Працівників також можна навчити, як найкраще захистити свої паролі та облікові дані для входу, а також як відстежувати будь-які пристрої, які використовуються для MFA.

Можна зробити висновок що забезпечення інформаційної безпеки на підприємствах України потребує постійного вдосконалення. Необхідний контроль за джерелам виникнення потенційних загроз інформаційній безпеці, та використання сучасних програмних засобів захисту.

Список використаних джерел:

1. ISO/IEC 17799:2005. *ISO*. URL: http://surl.li/cagte (date of access: 20.05.2022).

2. What Is Enterprise Security? | Fortinet. *Fortinet*. URL: http://surl.li/cagtc (date of access: 20.05.2022).