КІБЕРБЕЗПЕКА ЯК ЗАПОРУКА КОРПОРАТИВНОЇ СТІЙКОСТІ

Іваненко В. С.,
здобувач вищої освіти спеціальності 015 «Професійна освіта»
(Технологія виробництва та переробки продукції сільського господарства)»
Курепін В.М.,
канд.екон.наук, старший викладач
Миколаївський національний аграрний університет

Питання захисту конфіденційної інформації є актуальними для кожного сучасного підприємства. Конфіденційні дані компанії повинні бути захищені від витоку, втрати, інших шахрайських дій, оскільки це може призвести до критичних наслідків для бізнесу. Важливо розуміти, які дані потребують захисту, визначити способи та методи організації інформаційної безпеки.

Сховати дані від сторонніх можна у різний спосіб. Наприклад, програмними засобами побудувати бар'єр на шляху потенційного викрадача інформації. Або криптографічного способу змінити їх до невпізнанності. Але розкрадання – це не єдина небезпека, яка загрожує конфіденційній інформації. Також уважно їх слід захищати від пошкодження або втрати у разі пошкодження обладнання, недбалості або злого наміру працівників [1]. Тут допоможуть такі рішення, як резервне копіювання, дублювання, розподілене та віддалене зберігання тощо.

Підходити до питання захисту даних потрібно як до цілісного завдання - оцінити зовнішні та внутрішні ризики, особливості бізнес-процесів, у яких ці дані беруть участь [2], забезпечити захист каналів зв'язку та шифрування трафіку.

Надзвичайно важлива для ведення бізнесу інформація повинна мати обмежений доступ для підприємства, її використання підлягає чіткій регламентації [3]. До даних, які потрібно ретельно захистити, належать:

- комерційна таємниця;
- виробнича документація секретного характеру;
- ноу-хау компанії;
- клієнтська база;
- персональні дані працівників;
- інші дані, які компанія вважає за потрібне захистити від витоку.

Конфіденційність інформації часто порушується внаслідок шахрайських дій співробітників, запровадження шкідливого вірусу, шахрайських операцій зовнішніх зловмисників [4]. Неважливо, з якого боку виходить загроза, убезпечити конфіденційні дані потрібно в комплексі, що складається з кількох окремих блоків:

- визначення переліку активів, що підлягають захисту;
- розробка документації, що регламентує та обмежує доступ до даних компанії;
- визначення кола осіб, яким буде доступна конфіденційна інформація;
- визначення процедур реагування;
- оцінка ризиків;

- використання технічних засобів захисту конфіденційної інформації.

Державні закони встановлюють вимоги до обмеження доступу до інформації, що є конфіденційною. Ці вимоги повинні виконуватись особами, які отримують доступ до таких даних. Вони не мають права передавати ці дані третім особам, якщо їх власник не дає на це своєї згоди.

Державні закони вимагають захистити основи конституційного ладу, права, інтереси, здоров'я людей, моральні принципи, забезпечити безпеку держави та обороноздатність країни. У зв'язку з цим необхідно обов'язково дотримуватися конфіденційної інформації, до якої доступ обмежується законами. Ці нормативні акти визначають:

- за яких умов інформація відноситься до службової, комерційної, іншої таємниці;

- обов'язковість дотримання умов конфіденційності;

- відповідальність за розголошення конфіденційної інформації.

Інформація, яку отримують співробітники компаній та організації, що здійснюють певні види діяльності, має бути захищена відповідно до вимог закону щодо захисту конфіденційної інформації, якщо відповідно до законів на них покладено такі обов'язки [5]. Дані, що належать до професійної таємниці, можуть бути надані третім особам, якщо це прописано тими же законами.

При здійсненні службових обов’язків роботодавець і співробітники здійснюють обмін великою кількістю інформації, що носить різний характер, включаючи конфіденційне листування, роботу з внутрішніми документами (персональні дані працівника, розробки підприємства). Ступінь надійності захисту інформації має пряму залежність від того, наскільки цінною вона є для компанії.

Комплекс правових та організаційних заходів, передбачених для цих цілей, складається з різних засобів, методів та заходів [3]. Вони дозволяють істотно знизити вразливість інформації, що захищається, і перешкоджають несанкціонованому доступу до неї, фіксують і запобігають її витоку або розголошенню.

Правові методи повинні застосовуватися всіма компаніями, незалежно від простоти використовуваної системи захисту. Якщо ця складова відсутня або дотримується не повною мірою, компанія не зможе забезпечити захист корисної інформації, не зможе на законній підставі притягнути до відповідальності винних у її втраті або розголошенні.

Люди є основою системи захисту цінної конфіденційної інформації. Необхідно підібрати ефективні методи роботи з персоналом підприємства [1]. А заходи щодо забезпечення безпеки конфіденційної інформації повинні бути серед пріоритетних.

Важливе місце у захисті конфіденційної інформації має бути забезпечення технічних заходів, оскільки у високотехнологічному інформаційному світі корпоративне шпигунство, несанкціонований доступом до інформації, ризики втрати даних у результаті вірусних кібератак є досить поширеним явищем. Сьогодні не лише великі компанії стикаються з

проблемою витоку інформації, а й середній, а також малий бізнес відчуває потребу у захисті конфіденційних даних.

Хакерство, інтернет-зломи, крадіжка конфіденційної інформації, яка сьогодні стає дорожчою за золото, вимагають від власників компаній надійно її захищати та запобігати спробам викрадень та пошкоджень цих даних. Від цього залежить успіх бізнесу.

Для запобігання та захисту витоку інформації багато компаній користуються сучасними високоефективними системами кіберзахисту, які виконують складні завдання щодо виявлення загроз. Якісні сучасні та надійні вузли захисту здатні швидко реагувати на повідомлення системи захисту інформаційних блоків про загрозу.

Для виявлення, зберігання, ідентифікації джерел, адресатів, способів витоку інформації використовуються різні IT-технології, серед яких варто виділити DLP та SIEM-системи, що працюють комплексно та всеосяжне. Вони захищають інформацію одночасно по кількох каналах, які можуть виявитися вразливими до атак: USB-роз'єми; локально функціонуючі та підключені до мережі принтери; зовнішні диски; мережа Інтернет; поштові послуги; акаунти тощо.

Отже, сьогодні будь-яка компанія, якщо їй важливо зберегти свою інформаційну безпеку, потребує захист від кібернебезпек, за допомогою систем захисту конфіденційної інформації. IT-технології допомагають уникнути витоку та дозволяють ідентифікувати того, хто намагається нашкодити роботодавцю шляхом розкрадання, знищення або пошкодження інформації.

Бібліографічний список

1. В. М. Курепін. Кадрова безпека як складова частина економічної безпеки підприємств аграрного профілю // Modern Economics. 2020. № 24. С. 94-99. URL:http://dspace.mnau.edu.ua/jspui/handle/123456789/8276.

2. Вишневська О. М. Конкурентні переваги держав у глобальному світі / О. М. Вишневська, Т. О. Христенко // Обліково-аналітичне і фінансове забезпечення діяльності суб'єктів господарювання: національні, глобалізаційні, євроінтеграційні аспекти : матеріали IV Міжнародної науково-практичної інтернет-конференції., 20-21 листопада 2019 р., м. Миколаїв. – Миколаїв : МНАУ, 2019. – С. 146-151. URL:http://dspace.mnau.edu.ua/jspui/handle/123456789/7159.

3. Курепін В. М. Механізм управління безпекою вітчизняних підприємств на засадах маркетингу // Сучасний маркетинг: стратегічне управління та інноваційний розвиток : матеріали II Міжнародної науково-практичної конференції присвяченої до 90-ча заснування Харківського національного технічного університету сільського господарства ім. П. Василенка, 17-18 жовтня 2020 року. Харків : Харківський національний технічний університет сільського господарства імені Петра Василенка, 2020. С. 154-158. URL:http://dspace.mnau.edu.ua/jspui/handle/123456789/8183.

4. Полторак А. С., Паламарчук В. С. Особливості гарантування безпеки об’єднаного світового фінансового простору. Modern Economics. 2020. № 20(2020). С. 215-225. DOI: https://doi.org/10.31521/modecon.V20(2020)-34.

5. Кібернетична безпека банківського сектора в системі фінансової безпеки держави / А. С. Полторак, І. В. Баришевська, О. І. Мельник, О. А. Боднар // Сучасні тенденції розвитку фінансово-кредитної системи: теорія та практика : колективна монографія. – К. : Центр фінансово-економічних наукових досліджень, 2019. - С. 79-83.

Науковий керівник: Курепін В.М., кандидат економічних наук,
старший викладач кафедри методики професійного навчання
Миколаївський національний аграрний університет.

ЗМІНА КЛІМАТУ: ПРИЧИНИ ТА НАСЛІДКИ

Іваненко В. С.,
здобувач вищої освіти спеціальності 015 «Професійна освіта»
(Технологія виробництва та переробки продукції сільського господарства)»
Миколаївський національний аграрний університет

Кліматична криза разом із зниженням біорізноманіття, це найсерйозніший виклик, який постає перед людством. На даний момент зростання середньої температури дуже впливає на наш клімат, і ці наслідки з роками стануть ще більш суттєвими.

Зараз у нас все ще є шанс змінити ситуацію, що склалася, і запобігти згубним наслідкам зміни клімату. Міжурядова група експертів зі зміни клімату наголошує, якщо ми плануємо скоротити зростання температури від 1^0С до $1,5^0$С порівняно з до індустріальним рівнем, викиди парникового газу, виробленого людиною, повинні скоротитися на 50% до 2025 року [1].

Незважаючи на кліматичні зміни, такі як зміна сезонів, зміна океанічних потоків, вулканічної діяльності, сонячного випромінювання, тощо, клімат за природою досить стабільний, тобто дані зміни відбуваються з певною регулярністю, зима завжди змінюється навесні, а мусони наступають у певний сезон.

Таким чином, зміна клімату - це значна і тривала зміна статистичного розподілу погодних умов, яка може відбуватися в період від десятиліть до мільйонів років [2]. Це може бути зміна звичайних погодних умов, наприклад, зміна дат сезону дощів у тропіках, або зміна частоти екстремальних погодних явищ, таких як повені, посухи та шторми.

Коливання кількості сонячного світла та радіації є найбільш значущим драйвером зміни клімату за останні тисячі років. Вони також були головною причиною останніх чотирьох циклів епох зледеніння та потепління. Проте, за останні 150 років клімат Землі суттєво змінився, і дуже важливо розуміти, що спричинило такі кардинальні зміни за такий короткий термін.

Багато досліджень науковців говорять про зростання середньої світової температури, починаючи з середини 1900-х. Цей процес прийнято називати глобальним потеплінням, причиною якого вважають людську активність, зокрема, викиди CO_2 в атмосферу [3].