Паливода Т. В.
головний спеціаліст – юрисконсульт
відділу правової роботи управління правового забезпечення,
Міністерство культури України

СТРАТЕГІЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ПІДПРИЄМСТВІ

В умовах глобалізації та євроінтеграції України у світовий бізнес-простір важливим питанням постає інформаційна безпека інноваційно-інтелектуальної ідентифікації вітчизняного підприємства. З метою збереження науково-практичної спадщини та безперервного розвитку вітчизняного підприємства пропонуємо узагальнену стратегію безпеки на підприємстві, яка складається із таких етапів.

Етап 1. Аналізування безпеки зовнішніх і внутрішніх ризиків інформаційних потоків.

Так, до зовнішніх ризиків інформаційної безпеки підприємства можна віднести такі:

− психологічна війна;

− електронна війна;

− радіоелектронний вплив;

− кібератаки;

− хакінг;

− промисловий шпіонаж;

− та інші інформаційні методи вторгнення в роботу підприємства.

До внутрішніх ризиків інформаційної безпеки підприємства варто зазначити:

− низький рівень правової культури працівників;

− низький рівень постійного оновлення інформаційного захисту на підприємстві;

− низький рівень оплати праці працівників на підприємстві;

− та інші форс-мажорні обставини.

Варто зазначити про важливість проведення постійного аналізування і оцінювання ступенів ризиків впливу на інформаційну безпеку підприємства. Методику аналізування і оцінювання можна обрати з існуючих, розроблених вітчизняними та іноземними фахівцями, чи адаптувати відповідно до підприємства.

Етап 2. Організування інформаційної безпеки на підприємстві.

Важливим аспектом організування інформаційної безпеки є наявність чіткого розподілу прав і обов'язків кожного працівника підприємства та відповідальності за нерозповсюдження будь-якої інформації, що стосується роботи підприємства.

Етап 3. Мотивування та стимулювання працівників підприємства з метою забезпечення інформаційної безпеки.

Так, мотивування і стимулювання працівників з боку керівництва має бути постійно діючим та для всіх без винятку, не залежно від посади та професійного вкладу на підприємстві. Крім ефективних і дієвих методів стимулювання працівників у вигляді премії, надбавок, варто також врахувати такі нематеріальні методи стимулювання як: розвиток правової культури на основі загальнолюдських цінностей (віра, надія, любов та ін.) сприяння для працівників навчання та самовдосконалення; надання відпочинку тощо.

Етап 4. Контролювання інформаційної безпеки.

Процес контролювання інформаційної безпеки є одним з важливих чинників успіху підприємства в цілому. Зокрема, можна виділити деякі важливі способи контролю:

− антивірусний контроль;

− парольний контроль;

− захист інформаційної мережі на підприємстві;

− інформаційний захист кожного робочого місця працівника;

− та інші.

Варто зазначити, що питаннями контролю мають займатись професійні ІТ-спеціалісти, психологи, менеджери, юристи, економісти. Це має бути командна робота щодо ефективної і непроникної інформаційної безпеки підприємства.

Етап 5. Регулювання системи управління інформаційною безпекою на підприємстві.

Даний етап є одночасно і завершальним і новим витком для збереження та розвитку підприємства. Так, необхідно періодично проводити внутрішній та зовнішній аудит для діагностування і вирішення проблемних ділянок роботи з інформаційного забезпечення.

Варто зазначити, що питання інформаційної безпеки на підприємстві є актуальним і потребує вивчення юристами, економістами, молодими науковцями, державними службовцями. Адже, основна інформаційна загроза як безпеки підприємства так і безпеки держави є загроза руйнівного впливу через інформаційні ресурси на свідомість, підсвідомість особистостей.