Концептуальні основи категорії «Інформаційна безпека» у сучасному просторі

***Карпушенко М.Ю.**, к. е. н., доц., **Чередниченко О.Ю.**, **Чередниченко А.О.**, асп.,*
Харківський національний університет міського господарства

Інформація стала першоосновою життя сучасного суспільства, предметом та продуктом його діяльності, а процеси її створення, накопичення, збереження, передачі та обробки, в свою чергу, стимулювали виробництво відповідних пристроїв, які б забезпечували таку трансформацію.

В період загострення конкурентної боротьби, намагань збереження позицій на будівельному ринку, отримання нових замовлень, насамперед в період світової фінансової кризи, набуває важливого значення захист ділової, фінансової, технологічної та іншої інформації від крадіжок, несанкціонованого використання, її зміни чи знищення взагалі. Успішне вирішення вказаних питань потребує комплексного, наукового та системного підходу.

Суб'єкти господарювання, зацікавлені у своїй конкурентоспроможності, вживають відповідні заходи щодо захисту такої інформації, спираючись на відповідні норми чинного законодавства, норми міжнародного права та власну нормативно-правову основу.

Режим доступу до інформації - це передбачений правовими нормами порядок одержання, використання, поширення і зберігання інформації. За режимом доступу інформація поділяється на відкриту інформацію та інформацію з обмеженим доступом. Доступ до відкритої інформації забезпечується шляхом:

— систематичної публікації її в офіційних друкованих виданнях (бюлетенях, збірниках);

— поширення її засобами масової комунікації;

— безпосереднього її надання заінтересованим громадянам, державним органам та юридичним особам.

Захист інформації з обмеженим доступом є одним з першочергових завдань забезпечення інформаційної безпеки в системі корпоративного управління будівельних підприємств.

З погляду інформаційної безпеки для інформації можна виділити наступні категорії:

— конфіденційність - гарантія того, що конкретна інформація доступна тільки тому колу осіб, для кого вона призначена; порушення цієї категорії називається розкраданням або розкриттям інформації;

— цілісність - гарантія того, що інформація зараз існує в її початковому вигляді, тобто при її зберіганні або передачі не було проведено несанкціонованих змін; порушення цієї категорії називається фальсифікацією повідомлення;

— автентичність - гарантія того, що джерелом інформації є саме та особа, яка заявлено як її автор; порушення цієї категорії також називається фальсифікацією, але лжеавтора повідомлення.

У відношенні інформаційних систем слід застосовувати наступні категорії:

— надійність - гарантія того, що система поводиться в нормальному і позаштатного режимах так, як заплановано;

— точність - гарантія точного і повного виконання всіх команд;

— контроль доступу - гарантія того, що різні групи осіб мають різний доступ до інформаційних об'єктів, і ці обмеження доступу постійно виконуються;

— контрольованість - гарантія того, що в будь-який момент може бути проведена повноцінна перевірка будь-якого компонента програмного комплексу;

— контроль ідентифікації - гарантія того, що клієнт, підключений у даний момент до системи, є саме тим, за кого себе видає;

— стійкість до умисних збоїв - гарантія того, що при умисному внесенні помилок у межах заздалегідь обговорених норм система буде вести себе так, як обумовлено заздалегідь.

Таким чином, з урахуванням визначених категорій інформаційна безпека організаціїце цілеспрямована діяльність її органів та посадових осіб з використанням дозволених сил і засобів по досягненню стану захищеності інформаційного середовища організації, що забезпечує її нормальне функціонування і динамічний розвиток.

Для реалізації захищеності інформаційного середовища організації підприємства чи установи необхідно функціонування саме комплексної системи захисту, яка включатиме механізми фізичної охорони, технічний, інтелектуальний, правовий захист відомостей, матеріальних носіїв,об’єктів підприємств та установ тощо. Але ж у сучасних умовах в будівельній галузі України така цілісна система щодо комплексного захисту інформаційного середовища фактично не функціонує з ряду об’єктивних та суб’єктивних причин, до яких слід віднести ліквідацію потужних державних будівельних спеціалізованих підприємств, де вона діяла, втрата кадрового потенціалу, фахівців з охорони й захисту, зміни в законодавчо-нормативній базі, політики оптимізації та скорочення непрофільних напрямків діяльності тощо. Саме для реалізації захищеності інформаційного середовища організації підприємства чи установи в системі корпоративного управління будівельними підприємствами необхідно створити або відновити окремі самостійні підрозділи з захисту інформаційних ресурсів, які будуть проводити аналітичну роботу, надавати керівництву установи прогнози і пропозиції щодо підвищення рівня захисту інсайдерської інформації .