УДК 621.38:[621.38-025.53+621.38-022.532]

ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ЗАКОНОДАВСТВА ПРО ЗАХИСТ ІНФОРМАЦІЇ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ОСНОВНІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

Єсипенко В.Ю.
Науковий керівник – Чепела С.П.
Харківський національний університет радіоелектроніки, каф. філософії,
м. Харків, Україна
тел. (096) 084-20-39)

The abstract highlights the importance of information protection in today's digital world and the critical role of legislation in ensuring that organizations adhere to laws and regulations related to cybersecurity. It emphasizes the need for a comprehensive cybersecurity strategy, including risk management frameworks, security policies and procedures, and employee awareness training. Finally, it underscores the significance of effective cybersecurity measures such as continuous monitoring and rapid response to security incidents in ensuring cybersecurity in Ukraine.

Відповідальність за порушення законодавства про захист інформації у сфері інформаційних технологій:

Захист інформації є важливою проблемою в сучасному цифровому світі, і існують закони та нормативні акти, які забезпечують належне поводження з конфіденційною інформацією. Відповідальність за порушення законодавства про захист інформації у сфері інформаційних технологій несуть особи чи організації, які не дотримуються цього законодавства. Такі порушення можуть призвести до серйозних наслідків, таких як витік даних, крадіжка особистих даних і фінансові втрати. Тому для всіх організацій важливо розуміти та дотримуватися законів і правил, пов'язаних із захистом інформації.

Кібербезпека в Україні:

Кібербезпека викликає серйозне занепокоєння в Україні, де останнім часом кібератаки стають все більш поширеними. Для забезпечення кібербезпеки в Україні необхідно дотримуватися кількох принципів, зокрема проактивних заходів безпеки, постійного моніторингу та швидкого реагування на інциденти безпеки. Профілактичні заходи включають проведення регулярних оцінок ризиків, впровадження засобів контролю безпеки та навчання працівників з питань безпеки. Постійний моніторинг включає виявлення потенційних загроз і вразливостей, а також моніторинг незвичайної активності в системах і мережах. Швидке реагування на інциденти безпеки передбачає наявність плану швидкого та ефективного реагування на інциденти безпеки.

Важливість захисту інформації:

У сучасному цифровому світі інформація є цінним активом, і втрата або крадіжка конфіденційної інформації може мати серйозні наслідки. Тому дуже важливо захистити інформацію від несанкціонованого доступу, розголошення та зміни. Відсутність захисту інформації може призвести до значних фінансових втрат, шкоди репутації, а в деяких випадках навіть до втрати життя. Тому організації повинні серйозно ставитися до захисту інформації та вживати необхідних заходів для захисту конфіденційних даних.

Роль законодавства у захисті інформації:

Законодавство відіграє вирішальну роль у захисті інформації, забезпечуючи рамки, яких організації повинні дотримуватися під час захисту конфіденційної інформації. В Україні діє кілька законів і нормативних актів, пов'язаних із захистом інформації, зокрема Закон «Про захист персональних даних», який регулює обробку та захист персональних даних. Інші закони та нормативно-правові акти, пов'язані з кібербезпекою та захистом інформації, включають Стратегію кібербезпеки України та Закон «Про кібербезпеку». Ці закони містять вказівки для організацій, яких слід дотримуватися, і встановлюють покарання для тих, хто їх не дотримується.

Підсумовуючи, захист інформації в епоху цифрових технологій має вирішальне значення, і організації повинні ставитися до цього серйозно. Відповідальність за порушення законодавства про захист інформації у сфері інформаційних технологій несуть особи, які не дотримуються законів та нормативних актів. Ефективні заходи кібербезпеки, включаючи проактивні заходи безпеки, постійний моніторинг і швидке реагування на інциденти безпеки, є важливими для забезпечення кібербезпеки в Україні. Впроваджуючи комплексну стратегію кібербезпеки та дотримуючись відповідних законів і нормативних актів, організації можуть захистити свої конфіденційні дані та системи від кіберзагроз.

Список використаних джерел

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»

2. Скакун О. Ф. Теорія держави і права

3. Положення про державний контроль за станом технічного захисту інформації, затверджене наказом Адміністрації ДССЗЗІ України №87 від 16.05.2007 р.,

4. Курс інформатизації управління в ОВС / Під заг. ред. професора Я. Ю Кондратьєва.