Секція 6
КОМП'ЮТЕРНА ІНЖЕНЕРІЯ ТА КІБЕРБЕЗПЕКА ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМ І ТЕХНОЛОГІЙ

ЗНАЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА КІБЕРБЕЗПЕКА

Гончаренко П.О., здоб. ОС «бакалавр»
Науковий керівник – канд. екон. наук, доц. **Р.М. Остапенко**
Державний біотехнологічний університет

Стрімкий розвиток і широке застосування інформаційних технологій, як у повсякденному житті, так і в управлінні державою являється основним фактором оригінальності сучасного етапу економічного та нуково – технічного прогресу. Інформація та інформаційні технології все більш становляться частиною суспільства і визначають його розвиток.

Взагалі, можна виділити наступні основні завдання інформатизації:

- створення глобального інформаційного простору, що забезпечує інформаційну безпеку;
- створення, вміщення та експлуатація інформаційних систем, інформаційних технологій і інформаційних продуктів загального значення;
- багатогранне забезпечення інформаційних потреб суб'єктів інформаційних відношень;
- підготовка персоналу і проведення організаційних заходів у сфері підвищення їх інформатизованої кваліфікації.

Взагалі, інформаційна безпека складається з цілого комплексу різноманітних дій. Це, насамперед, контроль дій різноманітних суб'єктів бізнес – процесів – рядових співпрацівників підприємств, привілегійованих користувачів, IT – аутсорсерів, контрагентів. Окрім цього, це чітке розмежування прав доступу всередині компанії, використання резервного копіювання даних, а також наявність простої, зрозумілої і доведеної до розуміння працівників політики безпеки.

Інформаційна безпека являється одним із важливих аспектів інтегральної безпеки, на якому б рівні не розглядалася безпека.

Багато хто вважає, що кібербезпека являється синонімом до терміну «інформаційна безпека», але насправді це помилка, адже кібербезпека являється лише складовою частиною процесу

забезпечення інформаційної безпеки, і вона пов'язана виключно з інформаційними системами.

Взагалі, кібербезпека – це процес, який забезпечує усім властивості конфіденційності, цілісності, доступності, але тільки в деяких абстрактних рамках – на кіберпросторі.

Як зазначає Б.А. Кормич: «кібербезпека — це захищеність встановлених законом правил, за якими відбуваються інформаційні процеси в державі, що забезпечують гарантовані Конституцією умови існування і розвитку людини, всього суспільства та держави»[77].

А ось, наприклад, дослідники під керівництвом В.В. Остроухова визначають кібербезпеку, як: «стан захищеності особи, держави і суспільства, при якому досягається інформаційний розвиток (технічний, інтелектуальний, соціально-політичний, морально-етичний), за якого сторонні інформаційні впливи не завдають їм суттєвої шкоди»[60].

А якщо взяти значення у зарубіжних країнах, то Оксфордський університет дає поняття "cybersecurity" як: "Стан захищеності від кримінального або несанкціонованого використання електронних даних, або заходів, вжитих для досягнення цього"[21].

Як відомо, в умовах глобалізації та стрімкого розвитку інформаційно – комп'ютерних технологій ні одна держава світу не може самотужки забезпечити надійний захист свого цифрового простору. Проте, процес формування міжнародної системи кібербезпеки далекий від завершення і має доволі суперечливий і непередбачений характер, що підвищує значення розвитку двосторонніх відносин в плані передбачення загроз, що породжуються інформаційно – комп'ютерними технологіями.

Проблеми кібербезпеки, особливо у розрізі нещодавних масштабних атак на комп'ютери підприємств, банків та державних закладів, набули надзвичайну актуальність

Спектр інтересів суб'єктів, що пов'язані з використанням інформаційних систем, можна розділити на наступні категорії:

- забезпечення доступності;
- забезпечення цілісності;
- забезпечення конфіденційності інформаційних ресурсів і підтримуючої інфраструктури.

Крім того, кібербезпека — це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через:

- неповноту, невчасність та невірогідність інформації, що використовується;

- негативний інформаційний вплив;
- негативні наслідки застосування інформаційних технологій;
- несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [146].

Організаційні заходи безпеки інформаційних систем прямо чи опосередковано пов'язані з адміністративним управлінням і відносяться до рішень і дій, які застосовуються керівництвом для створення таких умов експлуатації, які зведуть до мінімуму слабкість захисту. Дії адміністрації можна регламентувати по наступних напрямках:

- заходи фізичного захисту комп'ютерних систем;
- регламентація технологічних процесів;
- регламентація роботи з конфіденційною інформацією;
- регламентація процедур резервування;
- регламентація внесення змін;
- регламентація роботи персоналу і користувачів;
- підбір та підготовка кадрів;
- заходи контролю і спостереження[4].

Взагалі, мати уявлення про можливі загрози, а також про уразливі місця, які ці загрози зазвичай експлуатують, необхідно для того, аби обирати найбільш економічні засоби забезпечення безпеки. Варто зазначити, що в галузі кібербезпеки важлиоо розробити механізми генерації нових рішень, що дозволять адекватно реагувати на погрози кібербезпеки або передбачати нові погрози та вміти їм протистояти.

Інформаційні джерела

1. Корупційні ризики в діяльності державних службовців: роз'яснення міністерства юстиції України від 12.04.2011 р URL: http://zakon5.rada.gov.ua/laws/show/n0026323-11
2. Калюжний Р.А. Інформаційне забезпечення управлінської діяльності в умовах інформатизації : організаційно-правові питання теорії і практики. К. : Академія державно-податкової служби України, 2002. — 296 с.
3. Oxford Dictionaries. URL: https://en.oxforddictionaries.com/definition/us/cybersecurity
4. Проект Національної стратегії у сфері прав людини станом на 25 березня 2015 року (українською мовою) http://old.minjust.gov.ua/file/44709
5. Безпека інформаційних систем та технологій URL: https://refdb.ru/look/1515966.html