Автор:
Конофольська Вікторія Вадимівна,
студентка 21І групи
Науковий керівник:
Франчук Василь Михайлович,
кандидат педагогічних наук,
доцент кафедри комп'ютерної інженерії

ІНФОРМАТИЗАЦІЯ СУСПІЛЬСТВА ТА ЇЇ ВПЛИВ НА ІНФОРМАЦІЙНУ БЕЗПЕКУ

Анотація. Метою даного дослідження є висвітлення питання впливу інформатизації суспільства та проблем інформаційної безпеки, що виникли в наслідок цього процесу. Окреслено основні прорахунки та недоліки захисту даних під час інформаційних війн. Акцентовано увагу на трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів і відповідні наслідки таких способів захисту. Зазначено позитивні і негативні наслідки інформатизації суспільства в аспекті інформаційної безпеки, основні категорії інформаційної зброї та найяскравіші її приклади.

Ключові слова: інформатизація, інформаційна безпека, інформаційна війна, загроза, несанкціонований доступ, ресурси.

Вступ. На сучасному етапі розвитку суспільства особливо важливим є процес інформатизації, впровадження інформаційних технологій у різноманітні сфери людської діяльності. Належне інформаційне забезпечення стає нагальною вимогою часу, адже саме інформаційні ресурси у поєднанні з наукою та інтелектом людини, продукують нові знання, починають поступово змінювати тенденції сучасного суспільства, змінюючи його тип на зовсім новий − інформаційний.

Основна частина. Інформатизація суспільства − це глобальний соціальний процес, особливість якого полягає в тому, що домінуючим видом діяльності в сфері суспільного виробництва є збір, накопичення, продукування, зберігання, передача та використання даних, які здійснюються на основі сучасних засобів обчислювальної техніки, а також на базі різноманітних засобів інформаційного обміну [1, с.7].

Загрози інформаційної безпеки − це зворотний бік використання інформаційних технологій. Із цього означення випливає два важливі твердження:

1. Трактування проблем, пов'язаних з інформаційною безпекою, для різних категорій суб'єктів може істотно розрізнятися. Для ілюстрації досить зіставити режимні державні організації й навчальні інститути. У першому випадку "нехай краще все зламається, ніж ворог довідається хоч один секретний біт", у другому − "так немає в нас ніяких секретів, аби тільки все працювало".
2. Інформаційна безпека не зводиться винятково до захисту від несанкціонованого доступу до даних, це принципово більш широке поняття. Суб'єкт інформаційних відносин може постраждати (зазнати збитків й/або одержати моральний збиток) не тільки від несанкціонованого доступу, але й від поломки системи, що викликала перерву в роботі. Більше того, для багатьох відкритих організацій (наприклад, навчальних) власне захист від несанкціонованого доступу до даних стоїть за важливістю аж ніяк не на першому місці.

Останнім часом у пресі все частіше згадуються такі поняття, як "інформаційна війна" та "інформаційна боротьба". Інтерес викликають взаємозв'язки цих понять із поняттям "інформаційна безпека".

Існує багато визначень "інформаційної війни", в яких вона тлумачиться як комплекс заходів і операцій, здійснюваних у конфліктних ситуаціях, коли дані є водночас зброєю, ресурсом і ціллю. Тобто це, війна за знання, пошук відповідей на питання: що, де, коли, чому і наскільки надійними окремо узяте суспільство або армія вважають свої знання про себе і своїх супротивників. Інформаційна війна може вестися як у воєнний, так і в мирний час [2,

с.1]. "Інформаційна війна є електронним конфліктом, де дані є стратегічним здобутком, який варто захопити чи знищити. І комп'ютери, й інформаційні системи стають привабливим напрямком першого удару" [3, с.49].

Можна у такий спосіб згрупувати види інформаційної зброї, використовуваної в інформаційній війні:

- засоби пропагандистсько-психологічного впливу (через пресу, телебачення, радіо, Інтернет, інші канали);
- засоби програмно-математичного впливу (комп'ютерні віруси, логічні "бомби", засоби придушення комп'ютерних мереж тощо);
- засоби психологічного впливу (голографічні зображення, синтезатори голосів відомих лідерів) ;
- психотронна зброя (зомбування, гіпноз).

Головна інформаційна загроза національній безпеці – це загроза впливу іншої сторони на інформаційну інфраструктуру країни, її інформаційні ресурси, на суспільство, свідомість, підсвідомість особистості, з метою нав’язати державі бажану систему цінностей, поглядів, інтересів і рішень в суспільній і державній діяльності, спрямовувати їх поведінку і розвиток у бажаному для іншої сторони руслі.

Щодо цілей атак в інформаційній війні, то чим більш залежний супротивник від інформаційних систем при ухваленні рішення, тим більше він уразливий до ворожого маніпулювання.

Чим сучасніше суспільство, тим більше воно покладається на дані та засоби її доставки. Сюди відноситься і мережа Інтернет − але це лише вершина системи. Будь-яка розвинена країна має телефонну, банківську та безліч інших мереж, що управління якими здійснюється за допомогою комп'ютерів, а отже мають властиві для них вразливі сторони.

Для запобігання та ліквідації загроз інформаційної війни використовують правові, програмно-технічні і організаційно-економічні методи. Правові методи − передбачають розробку комплексу нормативно-правових актів і положень, регламентуючих інформаційні відносини в суспільстві. Програмно-технічні методи − це сукупність засобів:

- запобігання витоку даних;
- виключення можливості несанкціонованого доступу до даних;
- запобігання впливам, які призводять до знищення, руйнування, спотворення повідомлень, або збоям чи відмовам у функціонуванні мереж або систем;
- виключення перехоплення даних технічними засобами;
- використання криптографічних засобів захисту даних при передачі каналами зв’язку.

Організаційно-економічні методи передбачають формування і забезпечення функціонування систем захисту секретних і конфіденційних даних, сертифікацію цих систем згідно до вимог інформаційної безпеки, ліцензування діяльності в сфері інформаційної безпеки, стандартизацію способів і засобів захисту, контроль за діями персоналу в захищених інформаційних системах.

На сьогодні саме інформаційні війни становлять найбільшу небезпеку нормальному функціонуванню системи національної безпеки. Події січня 2006 року з постачанням газу в Україну супроводжувалися застосуванням прийомів та засобів інформаційної війни Росією, про що було офіційно заявлено посадовими особами. Проте спостерігаючи перебіг подій кількох останніх місяців, можна із впевненістю сказати, що ця війна продовжується. Дискредитування уряду та політики держави, інверсія справжніх подій, викривлення фактів – ось головна зброя сьогодення. І вона стає дедалі небезпечнішою, призводячи до конфліктів, сутичок між мирним населенням. Саме це й обумовлює детальний розгляд питань щодо визначення поняття та встановлення сутнісних ознак інформаційної війни.

Висновок. З огляду на стрімкий розвиток віддаленого користування послугами, захист конфіденційних даних людини − це, безумовно, головне в інформаційній безпеці. Структурувати цю складну різноманітну проблему можна технологічно. Будь-яка інформаційна технологія складається з трьох аспектів: створення повідомлення, його

зберігання та використання. З огляду на безпеку необхідно забезпечити надійність роботи всіх трьох елементів системи.

Отже підсумовуючи усе вище сказане, інформатизація несе як позитивні, так і негативні процеси за собою.

Серед основних позитивних можна виокремити: розширення комунікативних зв'язків між людьми, широкий спектр інформації доступний майже в будь-якому куточку світу, швидкість і зручність послуг, спілкування з людьми, що знаходяться за сотні кілометрів в режимі реального часу, поліпшення обороноздатності країни.

Щодо негативних, то можна віднести наступні процеси: ненадійність багатьох Інтернет ресурсів в плані конфіденційності, як варіант, ізоляція індивіда від інших членів суспільства, зниження культури населення і кожної особи окремо, залежність від певних держав.

Список використаних джерел

1. Биков В.Ю. Моделі організаційних систем відкритої освіти : монографія / В.Ю. Биков. – К.: Атіка, 2009. – 684 с.

2. Михальчук В.Ф. Спеціальні інформаційні операції в контексті інформаційних війн/ В.Ф. Михальчук. –К.: Національний університет «Острозька академія», 2004. - 3с.

3. Schwartau W. An introduction to information warfare // War in the information age: new challenges for U.S. security policy. – Washington etc., 1997. – P. 49.