З іншого боку, дуже важливо, щоб кожен член суспільства, навіть якщо він не є експертом у певній сфері, був підкріплений такими знаннями, які допоможуть виявити фейкову інформацію та протидіяти її впливу на свідомість.

**Список використаних джерел:**

1. Головко Б. Інформаційна соціологія: тематична диспозиція / Борис Головко // Соціологія: теорія, методи, маркетинг. – 2004. – № 2.

2. Вплив ЗМІ на свідомість людини [Електронний ресурс] / Володарська дер- жавна районна рада – 2015. – 18 лютого. – Режим доступу: http://volodarka-rda.gov.-ua/index.php?option=com_content&view

3. Малюк А. Глобалізація як процес виникнення інформаційного суспільства / Андрій Малюк // Соціологія: теорія, методи, маркетинг. – 2015. – № 4. – С. 20–39.

4. Мінченко О. Страх і ненависть в мережі: огляд сайтів, що поширюють фейки та чутки [Електронний ресурс] / Ольга Мінченко // watcher: – Режим доступу: http://watcher.com.ua/2014/09/26/ strah-i-nenavyst-v-merezhi-ohlyad-saytiv-scho-poshyryuyut-feyky-ta-chutky

4. Прокопенко М. Фейк як інструмент війни [Електронний ресурс] / Марія Прокопенко // День. – Режим доступу: http://m.day.kiev.ua/uk/ article/media/feyk-yak-instrument-viyni

**Харламов Б.С.**

*студент,*

*Навчально-науковий інститут інформаційної безпеки*

*Національної академії Служби безпеки України*

## ПОНЯТТЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ ІНФОРМАЦІЇ

Роботи із захисту інформації у нас в країні ведуться досить інтенсивно і вже тривалий час. Накопичено значний досвід. Зараз вже ніхто не думає, що достатньо провести на підприємстві ряд організаційних заходів, включити до складу автоматизованих систем деякі технічні і програмні засоби – і цього буде достатньо для забезпечення безпеки.

Головний напрямок пошуку нових шляхів захисту інформації полягає не просто в створенні відповідних механізмів, а являє собою реалізацію регулярного процесу, здійснюваного на всіх етапах життєвого циклу систем обробки інформації при комплексному використанні всіх наявних засобів захисту. При цьому всі засоби, методи і заходи, що використовуються для ЗІ, найбільш раціональним чином об’єднуються в єдиний цілісний механізм – причому не тільки від зловмисників, але і від некомпетентних або недостатньо підготовлених користувачів і персоналу, а також позаштатних ситуацій технічного характеру.

Основною проблемою реалізації систем захисту є:

– З одного боку, забезпечення надійного захисту, що знаходиться в системі інформації: виключення випадкового і навмисного отримання інформації

сторонніми особами, розмежування доступу до пристроїв і ресурсів системи всіх користувачів, адміністрації і про обслуговуючого персоналу;

З іншого боку, системи захисту не повинні створювати помітних незручностей користувачам в ході їх роботи з ресурсами системи.

Проблема забезпечення бажаного рівня захисту інформації дуже складна, що вимагає для свого рішення не просто здійснення деякою сукупності наукових, науково-технічних і організаційних заходів та застосування спеціальних засобів і методів, а створення цілісної системи організаційно-технологічних заходів та застосування комплексу спеціальних засобів і методів по ЗІ [1].

Під системністю як основною частиною системно-концептуального походу розуміється:

– Системність цільова, тобто захищеність інформації розглядається як основна частина загального поняття якості інформації;

– Системність просторова, що пропонує взаємопов'язане вирішення всіх питань захисту на всіх компонентах підприємства;

– Системність тимчасова, що означає безперервність робіт з ЗІ, що здійснюються відповідно до планів;

– Системність організаційна, що означає єдність організації всіх робіт по ЗІ та управління ними.

Концептуальність підходу передбачає розробку єдиної концепції як повної сукупності науково обґрунтованих поглядів, положень і рішень, необхідних і достатніх для оптимальної організації та забезпечення надійності захисту інформації, а також цілеспрямованої організації всіх робіт по ЗІ.

Комплексний (системний) підхід до побудови будь-якої системи включає в себе: перш за все, вивчення об'єкта впроваджуваної системи; оцінку загроз безпеці об'єкта; аналіз засобів, якими будемо оперувати при побудові системи; оцінку економічної доцільності; вивчення самої системи, її властивостей, принципів роботи та можливість збільшення її ефективності; співвідношення всіх внутрішніх і зовнішніх факторів; можливість додаткових змін в процесі побудови системи і повну організацію всього процесу від початку до кінця [2].

Комплексний (системний) підхід – це принцип розгляду проекту, при якому аналізується система в цілому, а не її окремі частини. Його завданням є оптимізація всієї системи в сукупності, а не поліпшення ефективності окремих частин. Це пояснюється тим, що, як показує практика, поліпшення одних параметрів часто призводить до погіршення інших, тому необхідно намагатися забезпечити баланс суперечностей вимог і характеристик [3].

Комплексний (системний) підхід не рекомендує приступати до створення системи до тих пір, поки не визначені наступні її компоненти:

1. Вхідні елементи. Це ті елементи, для обробки яких створюється система. В якості вхідних елементів виступають види загроз безпеки, можливі на даному об'єкті;

2. Ресурси. Це кошти, які забезпечують створення та функціонування системи (наприклад, матеріальні витрати, енергоспоживання, допустимі розміри і т. д.). Зазвичай рекомендується чітко визначати види і допустиме споживання кожного виду ресурсу як в процесі створення системи, так і в ході її експлуатації;

3. Навколишнє середовище. Слід пам'ятати, що будь-яка реальна система завжди взаємодіє з іншими системами, кожен об'єкт пов'язаний з іншими об'єктами. Дуже важливо встановити межі області інших систем, не підкоряються керівнику даного підприємства і не належать до сфери його відповідальності.

Характерним прикладом важливості вирішення цього завдання є розподіл функцій щодо захисту інформації, переданої сигналами в кабельної лінії, що проходить по територіях різних об'єктів. Як би не встановлювалися кордону системи, не можна ігнорувати її взаємодія з навколишнім середовищем, бо в цьому випадку прийняті рішення можуть виявитися безглуздими. Це справедливо як для кордонів захищається, так і для кордонів системи захисту;

4. Призначення і функції. Для кожної системи повинна бути сформульована мета, до якої вона (система) прагне. Ця мета може бути описана як призначення системи, як її функція. Чим точніше і конкретніше вказано призначення або перераховані функції системи, тим швидше і правильніше можна вибрати найкращий варіант її побудови. Так, наприклад, мета, сформульована в самому загальному вигляді як забезпечення безпеки об'єкта, змусить розглядати варіанти створення глобальної системи захисту. Якщо уточнити її, визначивши, наприклад, як забезпечення безпеки інформації, що передається по каналах зв'язку всередині будівлі, то коло можливих рішень істотно звузиться. Слід мати на увазі, що, як правило, глобальна мета досягається через досягнення безлічі менш загальних локальних цілей (підцілей). Побудова такого «дерева цілей» значно полегшує, прискорює і здешевлює процес створення системи;

5. Критерій ефективності. Необхідно завжди розглядати кілька шляхів, що ведуть до мети, зокрема декількох варіантів побудови системи, що забезпечує задані цілі функціонування. Для того щоб оцінити, який із шляхів краще, необхідно мати інструмент порівняння – критерій ефективності. Він повинен: характеризувати якість реалізації заданих функцій; враховувати витрати ресурсів, необхідних для виконання функціонального призначення системи; мати ясний і однозначний фізичний зміст; бути пов'язаним з основними характеристиками системи і допускати кількісну оцінку на всіх етапах створення системи [4].

Таким чином, враховуючи різноманіття потенційних загроз інформації на підприємстві, складність його структури, а також участь людини в технологічному процесі обробки інформації, мети захисту інформації можуть бути досягнуті тільки шляхом створення СЗІ на основі комплексного підходу.

**Список використаних джерел:**

1. Герасименко В.А. Защитаинформации в автоматизированных системах обработкиданных. В 2-х томах / В.А. Герасименко – М.: Энергоатомиздат, 1994.

2. Горбатов В.С., Кондратьева Т.А. Информационнаябезопасность. Основыправовойзащиты / В.С. Горбатов, Т.А. Кондратьева. – М., 1993.

3. Гришина К.В., Мецатунян М.В., Морозова Е.В. Сущность и значение информационной безопасности ресурсов электронных библиотек. К.В. Гришина, М.В. Мецатунян, Е.В. Морозова // Безопасность информационных технологий. – № 2. – 1999.

4. Купріянов А.І. Основи захисту інформації: навч. Посібник для студ. вищ. навч. закладів / А.І. Купріянов, А.В. Сахаров, В.А. Шевцов – М.: Видавничий центр «Академія», 2006. – 256 с.