Тема 10. Складові інформаційної безпеки держави

План лекції

1. Передумови та виклики цифрової трансформації в Україні та світі
2. Елементи та рівні інформаційної безпеки
3. Загрози інформаційній безпеці держави

- Захист інформаційного суверенітету держави тісно пов'язаний із поняттям інформаційної безпеки, якщо вести мову про інформаційну безпеку, деякі вчені сприймають її досить вузько, як набір апаратних і програмних засобів для забезпечення схоронності даних в комп'ютерних мережах.

- Відповідно до Концепції інформаційної безпеки України, інформаційна безпека – це стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій

Суб'єкти забезпечення інформаційної безпеки є:

- громадяни України, об'єднання громадян, громадські організації та інші інститути громадянського суспільства;
- Президент України, Верховна Рада України, Кабінет Міністрів України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;
- засоби масової інформації та комунікації різних форм власності, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність;
- наукові установи, освітні і навчальні заклади України, які, зокрема, здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності, в галузі інформаційної безпеки.

Загрози інформаційній безпеці.

За джерелами походження:

- природного походження – це небезпечні геологічні, метеорологічні, гідрологічні явища, деградацію ґрунтів чи надр, природні пожежі, масове руйнування (через природні катаклізми) каналів зв'язку, зміна стану водних ресурсів та біосфери тощо;
- техногенного походження – транспортні аварії (катастрофи), пожежі, неспровоковані вибухи чи їх загроза, раптове руйнування каналів зв'язку, аварії на інженерних мережах і спорудах життєзабезпечення, аварії головних серверів системи управління національною безпекою тощо;
- антропогенного походження-вчинення людиною різноманітних дій з руйнування інформаційних систем, ресурсів, програмного забезпечення тощо. До цієї групи за змістом дій належать: ненавмисні, викликані помилковими чи ненавмисними діями людини (наприклад, помилковий запуск програми, ненавмисне допущення через недотримання правил безпеки роботи в Інтернеті інсталяції закладок тощо); навмисні (інспіровані), результат навмисних дій людей (наприклад, навмисна інсталяція програм, які передають інформацію на інші комп'ютери, навмисне зараження вірусами, навмисна дезінформація тощо).

За ступенем гіпотетичної шкоди:

- загроза – явні чи потенційні дії, які ускладнюють або унеможливлюють реалізацію національних інтересів у інформаційній сфері і створюють небезпеку для системи управління національною безпекою, життєзабезпечення її системостворюючих елементів;
- небезпека – безпосередня дестабілізація функціонування системи управління національною безпекою.

За повторюваністю вчинення:

- повторювані – такі загрози, які мали місце раніше;
- продовжувані – неодноразове здійснення загроз, що складається з ряду тотожних загроз, які мають спільну мету.

За сферами походження:

- екзогенні – джерело дестабілізації системи лежить поза її межами;
- ендогенні – алгоритм дестабілізації системи перебуває у самій системі.

За ймовірністю реалізації:

- вірогідні – такі загрози, які за виконання певного комплексу умов обов'язково настануть. Прикладом може слугувати оголошення атаки інформаційних ресурсів системи управління НБ, яке передує власне атаці;
- неможливі – такі загрози, які за виконання певного комплексу умов ніколи не настануть. Такі загрози зазвичай мають більш декларативний характер, не підкріплений реальною і навіть потенційною можливістю здійснити проголошені наміри, вони здебільшого мають залякуючий характер;
- випадкові – такі загрози, які за виконання певного комплексу умов кожного разу протікають по-різному. Загрози даного рівня доцільно аналізувати за допомогою методів дослідження операцій, зокрема теорії ймовірностей і теорії ігор, які вивчають закономірності у випадкових явищах.

За рівнем детермінізму:

- закономірні – такі загрози, які носять стійкий, повторюваний характер, що зумовлені об'єктивними умовами існування та розвитку системи інформаційної безпеки. Так, наприклад, будь-який суб'єкт системи забезпечення національної безпеки піддаватиметься інформаційним атакам, якщо в ньому не функціонує, або функціонує не на належному рівні система забезпечення інформаційної безпеки. Прикладом тому слугують численні атаки хакерів на офіційні сайти ФБР, ЦРУ, ДВБ США;
- випадкові – такі загрози, які можуть або трапитися або не трапитися. До таких загроз належать загрози хакерів дестабілізувати інформаційній системи органів державного управління.

За значенням:

- допустимі – такі загрози, які не можуть призвести до колапсу системи. Прикладом можуть слугувати віруси, які не пошкоджують програми шляхом їх знищення;
- неприпустимі – такі загрози, які:

  1) можуть у разі їх реалізації призвести до колапсу і системної дестабілізації системи;

  2) можуть призвести до змін, не сумісних із подальшим існуванням СНБ. Так, наприклад, вірус «i love you», спричинив пошкодження комп'ютерних систем у багатьох містах світу і завдав загального збитку майже 100 мільйонів доларів США.

За структурою впливу:

- системні – загрози, що впливають одразу на усі складові елементи системи управління національною безпекою;
- структурні – загрози, що впливають на окремі структури системи;
- елементні – загрози, що впливають на окремі елементи структури системи. Дані загрози мають постійний характер і можуть бути небезпечними лише за умови неефективності або непроведення їх моніторингу.

За характером реалізації:

- реальні -активізація алгоритмів дестабілізації є неминучою і не обмежена часовим інтервалом і просторовою дією;
- потенційні – активізація алгоритмів дестабілізації можлива за певних умов середовища функціонування органу державного управління;
- здійснені -такі загрози, які втілені у життя;
- Уявні – псевдоактивізація алгоритмів дестабілізації, або ж активізація таких алгоритмів, що за деякими ознаками схожі з алгоритмами дестабілізації, але такими не є.

За ставленням до них:

- об'єктивні – такі загрози, які підтверджуються сукупністю обставин і фактів, що об'єктивно характеризують навколишнє середовище. При цьому ставлення до них суб'єкта управління не відіграє вирішальної ролі через те, що об'єктивні загрози існують незалежно від волі та свідомості суб'єкта. Відтак об'єктивні загрози, не відображені в офіційних документах, ми назвали ненормативні загрози;
- суб'єктивні – така сукупність чинників об'єктивної дійсності, яка вважається суб'єктом управління системою безпеки загрозою. За даного випадку визначальну роль у ідентифікації тих чи інших обставин і чинників відіграє воля суб'єкта управління, який і приймає безпосереднє рішення про надання статусу або ідентифікації тих чи інших подій в якості загроз безпеці.

За об'єктом впливу:

- особа;
- суспільство;
- держава.

Головним призначенням класифікації загроз є демонстрації багатошаровості їх видової картини. Безперечно, що загрози інформаційній безпеці постійно змінюються. Відтак, головна мета теорії інформаційної безпеки розробити критерії моніторингу причин та умов, детермінант активізації алгоритмів дестабілізації національної безпеки в інформаційній сфері. Класифікація допомагає усвідомити не лише розмаїття загроз, а й наблизитися до розуміння витоків їх формування, а отже і розробляти управлінські моделі впливу на них.

Логічним продовженням аналізу загроз інформаційній безпеці є розгляд теоретичних проблем формування та функціонування системи забезпечення інформаційної безпеки України.

Рівні інформаційної безпеки:

- нормативно-правововий — закони, нормативно-правові акти тощо;
- адміністративний — дії загального характеру, які вживаються органами державного управління;
- процедурний — конкретні процедури забезпечення інформаційної безпеки;
- програмно-технічний — конкретні технічні заходи забезпечення інформаційної безпеки.

Характеристика українського інформаційного простору:

- 1) український інформаційний простір є незахищеним від зовнішніх негативних пропагандистсько-маніпулятивних впливів і стає об'єктом інформаційної експансії;
- 2) у світовому медіапросторі відсутній український національний інформаційний продукт, що поширював би об'єктивну, неупереджену та актуальну інформацію про події в Україні.
- 3) діяльність вітчизняних ЗМІ щодо систематичного, об'єктивного висвітлення фактів, подій та явищ є недостатньою та позбавлена стратегічного планування;
- 4) інформаційно-комунікативна політика України у сфері національної безпеки потребує невідкладного перегляду та удосконалення

Пріоритетні напрями державної інформаційної політики та важливі кроки з боку владних органів України:

- 1) інтеграція України до світового та регіонального європейського інформаційного просторів;
- 2) інтеграція у міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації;
- 3) створення власної національної моделі інформаційного простору та забезпечення розвитку інформаційного суспільства;
- 4) модернізації усієї системи інформаційної безпеки держави та формування й реалізація ефективної інформаційної політики;
- 5) удосконалення законодавства з питань інформаційної безпеки, узгодження національного законодавства з міжнародними стандартами та дієве правове регулювання інформаційних процесів;
- 6) розвиток національної інформаційної інфраструктури;
- 7) підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг;
- 8) впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління;
- 9) ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації та коригуванні державної політики в інформаційній сфері.

З метою недопущення інформаційної експансії, діяльність держави в інформаційному просторі має здійснюватись за такими напрямами:

- 1) реалізація упереджувальної стратегії та тактики (превентивні заходи);
- 2) здійснення реагувальної стратегії (оперативне реагування на інформаційні атаки супротивника та активний наступ);
- 3) захист національного інформаційного простору.
- 4) контроль за інформаційними потоками;
- 5) надання об'єктивної, вичерпної інформації, представлення фахових коментарів та пояснень щодо подій;
- 6) систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів

Загрози національним інтересам і національній безпеці в інформаційній сфері було віднесено наступні:

- прояви обмеження свободи слова та доступу громадян до інформації;
- поширення засобами масової інформації культу насильства, жорстокості, порнографії;
- комп'ютерна злочинність та комп'ютерний тероризм;
- розголошення інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави;
- намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної, неповної або упередженої інформації

Актуальні загрози національним інтересам та національній безпеці України в інформаційній сфері:

- здійснення спеціальних інформаційних операцій, спрямованих на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів,
- підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;
- проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;
- інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;
- інформаційне домінування держави-агресора на тимчасово окупованих територіях;
- недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та проактивно діяти в інформаційній сфері для реалізації національних інтересів України;
- неефективність державної інформаційної політики, недосконалість законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства;
- поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні

Інформаційна експансія – це діяльність із досягнення національних інтересів методом безконфліктного проникнення в інформаційну сферу а метою:

- поступової, плавної, непомітної для суспільства зміни системи соціальних відносин за зразком системи джерела експансії;
- витіснення положень національної ідеології і національної системи цінностей і заміщення їх власними цінностями й ідеологічними установками;
- збільшення ступеня свого впливу та присутності, встановлення контролю над стратегічними інформаційними ресурсами, інформаційно-телекомунікаційною структурою і національними ЗМІ;
- нарощування присутності власних ЗМІ в інформаційній сфері об'єкта проникнення і тому подібне