УДК 351.746.1

ДЕРЕКО Владислав Наільович

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ КЛАСИФІКАЦІЇ ЗАГРОЗ ОБ'ЄКТАМ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Постановка проблеми. В умовах сьогодення володіння інформацією визначеному суб'єкту дозволяє контролювати вирішення багатьох проблем світової спільноти. Інформація стала, з одного боку, негативним чинником, здатним спричинити надзвичайні ситуації, великомасштабні аварії, військові конфлікти та навіть дезорганізувати державне управління в цілому, а з іншого боку, ефективне використання інформації сприяє розвитку всіх сфер діяльності держави та окремо взятого об'єкта й у кінцевому підсумку може привести до значних позитивних моментів в його діяльності.

Володіння цінною інформацією покладає на суб'єкти, що мають на це право, високу відповідальність за її збереження та захист від можливого зовнішнього впливу, а саме різного роду факторів, подій та сучасних технологій, які в свою чергу можуть носити як навмисний, так і випадковий характер.

Треба зауважити, що стрімкий розвиток інформаційних технологій підносить на новий рівень практичне значення інформаційної безпеки, разом з тим все більше применшує розуміння сутності самої інформації, її форм і способів та методів впливу на розвиток суспільства, держави й об'єкт інформаційної безпеки в цілому.

Аналіз останніх досліджень і публікацій. Інформаційна безпека протягом двох останніх десятиліть є об'єктом актуальних наукових досліджень у різних сферах знань. Аналіз досліджень і публікацій свідчить, що загальнотеоретичні та окремі аспекти забезпечення інформаційної безпеки висвітлені у значній кількості наукових праць. Це роботи вітчизняних та зарубіжних авторів В. М. Богуша, О. М. Горбатюка, О. Г. Данільяна, В. М. Желіковського, В. А. Ліпкана, С. В. Ленкова, Ю. Є. Максименка, Д. А. Перегудова, В. А. Хорошко, Л. Дж. Хоффмана та інших.

Водночас слід зазначити, що залишаються недостатньо розкритими питання особливостей забезпечення інформаційної безпеки, зокрема класифікація загроз об'єктам інформаційної безпеки.

Отже недостатня увага до цієї проблеми визначила **мету** статті та спонукала розглянути деякі аспекти забезпечення інформаційної безпеки об'єкта.

Численні дослідники пропонують наступні точки зору щодо терміна «інформаційна безпека»:

- Так, за словами В. М. Богуша, інформаційна безпека – це стан захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави;
- На думку О. М. Горбатюка, інформаційна безпека являє собою стан захищеності потреб в інформації особистості, суспільства і держави, при якому забезпечується їх існування та прогресивний розвиток незалежно від наявності внутрішніх та зовнішніх інформаційних загроз;
- О. Г. Данільян додає у визначення технічну складову та описує інформаційну безпеку як безпеку об'єкта від інформаційних загроз або негативних впливів, пов'язаних з інформацією та нерозголошенням даних про той чи інший об'єкт, що є державною таємницею [1; 2; 3].

Виклад основного матеріалу. Треба зазначити, що поняття **«забезпечення інформаційної безпеки»** включає в себе: об'єкти інформаційної безпеки, загрози об'єктам інформаційної безпеки та діяльність із захисту цих об'єктів, засновану на сукупності сил, засобів, способів і методів забезпечення інформаційної безпеки.

Головними цілями діяльності відповідних суб'єктів щодо забезпечення інформаційної безпеки є ліквідація загроз об'єктам інформаційної безпеки та мінімізація можливих збитків, завданих внаслідок реалізації певних загроз.

Розглядаючи термін «загроза», треба зауважити, що це одне з ключових понять у сфері забезпечення інформаційної безпеки.

Загроза об'єкту інформаційної безпеки – сукупність факторів і умов, що можуть виникнути у процесі взаємодії різних об'єктів (їх елементів) та спроможні чинити негативний вплив на конкретно визначений об'єкт інформаційної безпеки. Сам негативний вплив можна розрізнити за характером шкоди, що може завдатися: по-перше, за ступенем зміни властивостей об'єкта безпеки, по-друге, за ступенем зміни можливостей ліквідації наслідків прояву загроз.

До найбільш важливих властивостей загрози треба віднести вибірковість, передбачуваність та шкідливість.

Вибірковість характеризує націленість загрози на заподіяння шкоди тим чи іншим конкретним властивостям об'єкта безпеки.

Передбачуваність характеризує наявність ознак виникнення загрози, що дозволяють заздалегідь прогнозувати можливість появи загрози та визначати конкретні об'єкти, на які вона буде спрямована.

Шкідливість характеризує можливість завдати об'єкту безпеки шкоди різної тяжкості. Шкода, як правило, може бути оцінена вартістю витрат на ліквідацію наслідків виявлення загрози або на запобігання її появи [6].

Виділяють такі типи загроз:

1. Намір завдати шкоди, що з'являється у вигляді оголошеного мотиву діяльності окремого суб'єкта.

2. Можливість заподіяння шкоди, коли існують достатні для цього умови та фактори.

Особливість першого типу загроз полягає в невизначеності можливих наслідків, неясності питань щодо наявності у окремого суб'єкта, що здійснює загрозу, сил і засобів, достатніх для здійснення наміру.

А можливість завдати шкоди полягає в існуванні саме достатніх для цього умов і факторів. Особливість загроз другого типу зводиться до того, що оцінка потенціалу сукупності факторів, які можуть послужити перетворенню цих можливостей і умов на шкоду, може бути здійснена тільки, власне, визначеним суб'єктом загрози.

Між загрозою та небезпекою завдання шкоди завжди існує стійкий причиново-наслідковий зв'язок.

Загроза завжди породжує небезпеку. А саму небезпеку можна уявити як стан, в якому знаходиться об'єкт безпеки внаслідок виникнення загрози цьому об'єкту. Головна відмінність між ними полягає в тому, що небезпека є властивістю об'єкта інформаційної безпеки й характеризує його здатність протистояти проявам загроз, а загроза є властивістю об'єкта взаємодії або знаходиться у взаємодії елементів об'єкта безпеки, що виступають джерелами загроз. Поняття загрози має причиново-наслідковий зв'язок не тільки з поняттям небезпеки, а й з можливою шкодою як наслідком негативних змін в умовах існування об'єкта інформаційної безпеки та визначає величину небезпеки.

Перелік загроз, оцінка їх ймовірності та реалізації, а також модель суб'єкта загроз є основою для аналізу ризику реалізації загроз і формулювання вимог до системи захисту об'єкта інформаційної безпеки. Крім виявлення можливих загроз доцільно здійснювати додатковий аналіз цих загроз на основі їх класифікації за низкою ознак. Кожна з ознак класифікації відбиває одну з узагальнених вимог до системи захисту об'єкта. Загрози, що відповідають певній ознаці класифікації, дозволяють деталізувати відображену за цією ознакою вимогу.

Існує певна класифікація загроз інформаційної безпеки об'єкта:

– *за джерелом (його місцезнаходженням):*
  - внутрішні (виникають безпосередньо на об'єкті та зумовлюють взаємодією між його елементами або суб'єктами);
  - зовнішні (виникають внаслідок його взаємодії із зовнішніми об'єктами);

– *за ймовірністю реалізації: потенційні та реальні;*

– *за розмірами завдання шкоди:*
  - загальні (спричиняє об'єкту безпеки негативний вплив на умови його діяльності);

- локальні (зачіпають умови існування окремих елементів об'єкта безпеки);
- приватні (завдають шкоди окремим властивостями елементів об'єкта або окремим напрямам його діяльності);

– *за природою походження:*

- випадкові (не пов'язані з діями персоналу, станом і функціонуванням об'єкта інформаційної безпеки; такі, як відмови, збої та помилки в роботі засобів автоматизації; стихійні лиха та інші надзвичайні обставини);
- навмисні (зумовлені зловмисними діями людей);

– *за передумовами виникнення:*

- об'єктивні (викликані недоліками системи інформаційної безпеки об'єкта, наприклад, недосконалістю розроблених нормативно-методичних та організаційно-планових документів, відсутністю підготовлених фахівців із захисту інформації тощо);
- суб'єктивні (зумовлені діяльністю персоналу об'єкта безпеки, наприклад, помилками в роботі, низьким рівнем підготовки з питань захисту інформації, зловмисними діями або намірами сторонніх осіб);

– *за видами об'єктів безпеки:*

- загрози інформації (зумовлені спробами отримання захищеної інформації різними способами і методами незалежно від її місцезнаходження);
- загрози персоналу об'єкта (пов'язані зі зменшенням впливу персоналу на ситуацію у сфері забезпечення інформаційної безпеки, зі спробами отримання конфіденційної інформації від допущеного до неї персоналу);
- загрози діяльності із забезпечення інформаційної безпеки (спрямовані на зниження ефективності або нейтралізацію зусиль, що здійснюються керівництвом і персоналом об'єкта безпеки для унеможливлення витоку відомостей з обмеженим доступом, втрати або розкрадання носіїв, ослаблення системи захисту інформації тощо).

Розглядаючи загрози інформаційної безпеки об'єкта, особливу увагу необхідно приділити класифікації компонентів об'єкта інформаційної безпеки, які також повинні підлягати надійному захисту.

Відповідно до наведеної вище класифікації загроз за видом об'єкта впливу підкреслимо, що вони поділяються на загрози інформації, загрози персоналу об'єкта та загрози діяльності щодо забезпечення інформаційної безпеки об'єкта. При більш детальному розгляді загроз, власне, самої інформації можна розширити класифікацію та вказати на загрози носіям конфіденційної інформації (автоматизованим системам), місцям їх розміщення (розташування), каналам передачі (системам інформаційного обміну), а

також інформації, що зберігається в документованому (електронному) вигляді на різних носіях.

Для забезпечення конфіденційності, цілісності та доступності інформації необхідно захищати інформацію не тільки від витоку технічними каналами та несанкціонованого доступу, але й виключати можливість негативного впливу на інформацію, втручання в процес її обробки та порушення працездатності самої системи.

Тому забезпечення безпеки автоматизованих систем (АС) – є однією з найважливіших та складних проблем в сфері обробки та захисту інформації, оскільки компонентами АС є апаратні засоби, програмне забезпечення, інформація, що обробляється, лінії зв'язку, персонал та документація. При цьому заподіяною шкодою буде вважатися не тільки явне пошкодження якогось окремого компонента системи, але й різного роду витоки інформації, зміни окремих фізичних та логічних характеристик АС тощо [4].

Визначення ймовірної шкоди АС є важким завданням для суб'єктів безпеки, які залежать від багатьох умов, тому буде правильним питання безпеки АС поділити на три групи.

Перша група захисту включає в себе питання забезпечення фізичної безпеки компонентів АС. До цієї групи можна віднести питання захисту АС від пожежі, затоплення та інших стихійних лих, перебоїв з живленням, крадіжки, пошкодження тощо.

До другої групи захисту належать питання логічної безпеки компонентів АС. До неї відносяться питання захисту АС від несанкціонованого доступу, від навмисних або ненавмисних помилок в діях людей та програм, що можуть завдати шкоди, тощо.

Третя група охоплює питання забезпечення соціальної безпеки АС. Це питання розробки законодавства, що регулює застосування АС та визначає порядок розслідування і покарання при порушеннях безпеки АС для її користувачів.

Процес виявлення можливих загроз інформації та вплив їх на саму інформацію, що знаходиться в АС певного об'єкта, вимагає надання додаткової класифікації загроз для АС за наступними критеріями:

1. За місцем розміщення джерела загроз стосовно АС:

- дистанційні – поза контрольованою зоною АС (перехоплення даних, переданих каналами зв'язку, перехоплення побічних електромагнітних, акустичних та інших випромінювань від технічних пристроїв);
- контактні – у межах контрольованої зони АС (проникнення в приміщення, де розташовані засоби обробки та зберігання інформації з метою застосування спеціалізованих пристроїв, а також викрадання та копіювання носіїв інформації тощо);
- безпосередні – в самих АС (некоректне використання ресурсів АС).

2. За ступенем залежності від активності АС:

- незалежні від активності АС (злам шифрів криптозахисту інформації);
- активні в процесі обробки даних (загрози впровадження та поширення програмних вірусів).

3. За ступенем впливу на АС:

- пасивні загрози, які при роботі нічого не змінюють у структурі та змісті АС (загроза копіювання секретних даних);
- активні загрози, які при впливі вносять зміни в структуру та зміст АС (впровадження «троянських коней» і вірусів).

4. За етапами доступу користувачів або програм до ресурсів АС:

- загрози, які виявляються на етапі доступу до ресурсів АС (загрози несанкціонованого доступу в АС);
- загрози, які виявляються після надання дозволу на доступ до ресурсів АС (загрози несанкціонованого або некоректного використання ресурсів АС).

5. За способом доступу до ресурсів АС:

- загрози, що здійснюються з використанням стандартного шляху доступу до ресурсів АС (незаконне отримання паролів та інших реквізитів розмежування доступу з подальшим маскуванням під зареєстрованого користувача);
- загрози, що здійснюються з використанням прихованого нестандартного шляху доступу до ресурсів АС (несанкціонований доступ до ресурсів АС шляхом використання недокументованих можливостей АС).

6. За місцем розташування інформації, що зберігається та обробляється в АС:

- загроза доступу до інформації, що знаходиться на зовнішніх запам'ятовуючих пристроях (несанкціоноване копіювання секретної інформації з жорсткого диска, флеш-носія);
- загроза доступу до інформації, що знаходиться в оперативній пам'яті (читання залишкової інформації з оперативної пам'яті, доступ до системної області оперативної пам'яті за допомогою прикладних програм);
- загроза доступу до інформації, що циркулює по лініях зв'язку (незаконне підключення до ліній зв'язку з подальшим уведенням помилкових повідомлень або модифікацією переданих повідомлень, незаконне підключення до ліній зв'язку з метою прямої підміни законного користувача з подальшим уведенням дезінформації та нав'язуванням помилкових повідомлень);
- загроза доступу до інформації, яка відображається на екрані, або до тієї, що друкується на принтері (запис інформації на приховану відеокамеру) [5].

Таким чином, можна зробити **висновок** про те, що дії загроз, що можуть спричинити інформаційну небезпеку об'єкту, спрямовані на створення можливих каналів витоку захищеної інформації (передумов до її витоку) та безпосередньо на сам витік інформації. Ключовий аспект, на який в першу чергу потрібно постійно звертати увагу при оцінці ефективності виявлення загроз об'єкту інформаційної безпеки, – це збитки, що можуть бути завдані цьому об'єкту в результаті впливу різного роду загроз.

Список використаних джерел

1. Богуш В. Інформаційна безпека держави / В. Богуш, О. Юдін ; [гол. ред. Ю. О. Шпак]. – К. : МК-Прес, 2005. – 432 с.

2. Горбатюк О. М. Сучасний стан та проблеми інформаційної безпеки України на рубежі століть / О. М. Горбатюк // Вісник Київського університету імені Т. Шевченка. – 1999. – Вип. 14: Міжнародні відносини. – С. 46–48.

3. Данільян О. Г. Національна безпека України: сутність, структура та напрямки реалізації / О. Г. Данільян, О. П. Дзьобань, М. І. Панов. – Х. : ФОЛІО, 2002. – 296 с.

4. Ленков С. В. Методы и средства защиты информации : в 2-х т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко ; под ред. В. А. Хорошко. – К. : Арий, 2008. – Т. 1. Несанкционированное получение информации. – 464 с.

5. Ленков С. В. Методы и средства защиты информации : в 2-х т. / С. В. Ленков, Д. А. Перегудов, В. А. Хорошко, под ред. В. А. Хорошко. – К. : Арий, 2008. – Т. 2. Информационная безопасность. – 344 с.

6. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський : [навч. посіб.]. – К. : КНТ, 2006. – 280 с.

7. Про основи національної безпеки України : [закон України: офіц. текст: за станом на 19 червня 2003 р., із змінами, внесеними Законом України від 13 жовтня 2012 р.] // Відомості Верховної Ради України. – 2012. – № 7. – Ст. 53.

Рецензенти:
кандидат технічних наук, старший науковий співробітник В. Міхалко,
кандидат юридичних наук В. Григор'єв

Аннотация: В статье исследуются вопросы сущности информационной безопасности. Рассматриваются основные свойства угроз. Анализируются источники угроз информационной безопасности и приводится их классификация.

Ключевые слова: автоматизированные системы, информация, информационная безопасность, обеспечение информационной безопасности, угроза.

Abstract: The article deals with the essence of the issue of information security. The basic features of threats are considered. The sources of threats to information security are analyzed and their classification is provided .

Key words: automatic systems, the information, the information security, the implementation of information security, the threat.