УДК 351:007+519.87
DOI https://doi.org/10.32838/2663-5941/2019.3-1/17

Дудатьєв А.В.
Вінницький національний технічний університет

Войтович О.П.
Вінницький національний технічний університет

Миронюк В.В.
Вінницький національний технічний університет

МОДЕЛЬ ЗАГРОЗ СОЦІОТЕХНІЧНОЇ СИСТЕМИ: СОЦІАЛЬНИЙ АСПЕКТ

У представленій статті запропонована модель загроз для соціальної частини соціотехнічної системи, яка враховує спеціально створену інформацію – меми та можливі джерела впливу: внутрішні і зовнішні. Представлена модель взаємодії різнорідних складників соціотехнічної системи, яка демонструє можливі деструктивні впливи соціуму на технічну частину системи. У статті також представлена ситуаційна модель взаємодії складників соціотехнічної системи, яка демонструє можливість реалізації прямого й опосередкованого впливу людини на технічну частину системи. Запропоновані моделі пропонується використовувати під час побудови комплексних систем захисту інформації.

Ключові слова: *інформаційна безпека держави, модель загроз, ситуаційна модель взаємодії складників соціотехнічної системи.*

Постановка проблеми. Інформаційна безпека держави як соціотехнічної системи (СТС) залежить від стану її складників – технічного і соціального. Стан інформаційної захищеності соціального складника СТС відіграє значущу роль для визначення стану всієї системи, оскільки соціум перебуває під дією спеціальних кібернетичних операцій, зокрема інформаційно-психологічних операцій (ІПО). Наслідком проведення таких операцій стає зміна свідомості елементів соціального складника СТС і, як наслідок, можливість проведення деструктивних інформаційних впливів на технічний складник системи. Для технічного складника, з точки зору забезпечення комплексної інформаційної безпеки, найбільш важливими є різноманітні автоматизовані системи (АС) обробки інформації, інформаційно-телекомунікаційні системи (ІТС), що забезпечують роботу різноманітних промислових підприємств, об'єктів фінансової інфраструктури і насамперед об'єктів критичної інфраструктури. До таких об'єктів належать насамперед підприємства енергетичної та хімічної галузей, транспортні системи, системи зв'язку, військові системи тощо. Таким чином, порушення інформаційної безпеки окремого об'єкта захисту, наприклад енергогенеруючого об'єкта, може привести до зміни режимів управління цим об'єктом, а також до негативних екологічних, техногенних, соціальних наслідків. Тому від рівня інформаційного захисту окремого підприємства (групи підприємств) залежить загальний стан безпеки регіону (групи регіонів) і, як наслідок, держави в цілому. У роботі [1] наведена статистика інцидентів на різних підприємствах за участю персоналу, а у роботі [2] наведено дані щодо порушень інформаційної безпеки у інформаційних системах, при цьому зауважено, що людина за певних умов стає джерелом загроз.

Аналіз досліджень. Модель загроз є одним з базових понять для формулювання загальних вимог до створення комплексних систем захисту інформації (КСЗІ). Зокрема, у НД ТЗІ 1.4-001-2000 визначається, що у процесі упорядкування матриці загрози/компоненти може уточнюватися список загроз і об'єктів захисту, внаслідок чого коригуватись модель загроз. Фактично для створення моделі загроз необхідно: скласти перелік суттєвих загроз, описати методи і способи їх здійснення, визначити, якими з можливих способів можуть здійснюватися загрози в АС, визначити основні види загроз для безпеки інформації, які можуть бути реалізовані стосовно АС, визначити перелік можливих загроз і класифікувати їх за результатом впливу на інформацію.

У роботі [3] запропонована модель загроз, що враховує зовнішні дестабілізуючі фактори, зокрема загрозу – інформаційно-психологічну операцію, що спрямовується на персонал АС. Запро-

понована у наведеній статті модель є фактичним розвитком моделі, наведеної у роботі [3], яка враховує можливі канали і механізми реалізації ІПО.

Постановка завдання. Для забезпечення заданого рівня інформаційної безпеки СТС шляхом побудови ефективного захисту потрібно вирішити низку складних і важливих задач, однією з яких є побудова узагальненої моделі загроз. Тому рішення вищенаведеної задачі є актуальним завданням. Метою роботи є розробка моделі загроз, яка формалізує ймовірні впливи на соціальний складник СТС, що дасть можливість підвищити ефективність захисту інформаційного простору.

Нехай маємо множину загроз R_z, яка відображає реалізацію загрози – появу зовнішніх мемів, множину R_t, яка відображає реалізацію загрози опосередкованого впливу на технічний складник, та множину загроз R_v, яка відображає реалізацію загрози – появу внутрішніх мемів.

За умови незалежності і несумісності загроз та наявності сприятливих умов Q_k для реалізації загроз задача розробки моделі загроз соціальній компоненті СТС буде полягати у побудові інтегрованої моделі загроз, яка об'єднує всі можливі типи загроз.

Модель загроз. Загрози з боку соціального складника СТС можуть виникнути внаслідок проведення спеціальних інформаційно-психологічних операцій. Метою проведення таких операцій є загострення всіляких проблем і потреб працівників, ініціації міжособистісних конфліктів тощо. Проведення ІПО, використовуючи соціальний аспект, може бути реалізовано через поширення спеціально створених мемів – умовних одиниць інформації, які призначені для так званої культурної еволюції, зміну культурного наслідування або зміну культурного коду. За аналогією із теорією генного наслідування головною задачею мему є забезпечення процесів наслідування та змін інформаційного простору, в якому відбувається життєдіяльність соціального складника СТС. Таким чином, соціокультурний аспект відіграє суттєву роль у забезпеченні комплексної інформаційної безпеки СТС [4; 5].

Соціотехнічну систему можна представити виразом:

$$STS = \{SuBSTS_t, SuBSTS_s\},$$

де $SuBSTS_t$ – підсистема СТС, яка представляє технічний складник системи, $SuBSTS_s$ – підсистема СТС, яка представляє соціальний складник системи. Свою чергою $SuBSTS_t$ може бути представлена такими ознаками, як: критичність об'єкта, специфіка системи управління, характеристика інформаційно-телекомунікаційної системи, ознаки автоматизованої системи, технології, що використовують на об'єкті захисту, обладнання, яке розташовано на об'єкті.

Підсистема $SuBSTS_s$ може бути представлена такими ознаками, як: мета впливу, розташування суб'єкта впливу, кваліфікація, доступ до спеціальних технологій, обладнання тощо.

Сучасні СТС функціонують в умовах критичних глобальних змін, основними ознаками яких є:

– різного роду аварії і катастрофи;

– збільшення використання енергії різного походження;

– погіршення стану екології навколишнього середовища;

– терористичні акти.

При цьому життєдіяльність СТС характеризується невизначеністю, яка може бути викликана невчасно отриманою, неповною або навмисно перекрученою інформацією. Варто також відзначити можливість використання конфіденційної інформації потенційними конкурентами у власних цілях, що вже є ознакою інформаційного протиборства.

Для подальшої формалізації моделі загроз, пов'язаних саме із соціальним складником СТС, представимо модель взаємодії різнорідних систем (соціальної і технічної), а також їх імовірний взаємний вплив.

Функціонування різнорідних частин СТС пропонується представити як взаємодію детермінованого автомата (ДА), який формалізує технічну частину СТС та недетермінованого автомата (НДА), який представляє соціальний складник. Схема причинно-наслідкового комплексу, який представляє взаємодію двох різнорідних частин, наведена на рис.1.

Недетермінований автомат може бути представлений як абстрактна система:

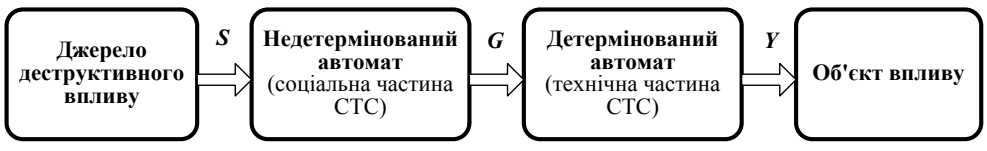

Рис. 1. Схема причинно-наслідкової взаємодії частин СТС

$$N = (S,Q,G,f,\mu),$$

де S – множина вхідних сигналів, $Q=\{Q_c,Q_н\}$ – множина внутрішніх станів, де Q_c – стійкий внутрішній стан, $Q_н$ – нестійкий внутрішній стан, $G=\{G_c,G_н\}$ – множина вихідних станів, де Gc – стійкий вихідний стан, $G_н$ – нестійкий вихідний стан, f – функція переходів, μ – функція виходів. Стан НДА (соціальної частини СТС) формує вхідний сигнал для ДА або технічного складника СТС, що може бути описаний як система:

$$A= (Z,X,Y,\delta,\lambda),$$

де Z – множина станів, $X=G$ – множини вхідних сигналів, Y – множина вихідних сигналів, δ – функція переходів, λ – функція виходів.

На запропонованій схемі на вхід НДА надходить множина вхідних сигналів S яка впливає на соціальну частину СТС. Під вхідними сигналами ми сприймаємо меми. Під їхньою дією НДА може перейти у так званий нестійкий стан $Q_н$, або залишитись у стійкому стані Q_c. Нестійкий внутрішній стан $Q_н$ формує вихідний сигнал $G_н$, який є несприятливим для технічної частини СТС. Такий стан призведе до деструктивного впливу соціальної частини СТС на техніко-технологічну частину СТС або інші ресурси об'єкта захисту, що своєю чергою у разі незадовільного комплексного захисту призведе до нестійкого стану всієї системи, але бажаного стану для суб'єкта, який проводив ІПО, з метою виведення з ладу всієї системи.

З урахуванням представленої моделі взаємодії складників СТС важливим моментом є врахування загроз і відповідних вразливостей, які впливають на людину або персонал.

На соціальний складник СТС можуть впливати такі спеціально створені меми:

– зовнішні, які створюються і поширюються ймовірними конкурентами;

– внутрішні, які створюються і поширюються спеціально підготовленими особами-агентами;

– внутрішньо-технічні, які опосередковано створюються за рахунок впливу технічного складника на соціальний (рефлексивне управління).

Можливі різні комбінації взаємодії технічного і соціального складників системи і, як наслідок, різні ризики потенційних деструктивних інформаційних впливів.

Ситуаційна модель взаємодії складників СТС, яка демонструє комбінації ймовірних впливів соціального складника на технічний, представлена на рис. 2.

Наведена ситуаційна модель взаємодії різнорідних частин СТС демонструє реалізацію деструктивного впливу, який може бути реалізований такими шляхами:

– безпосередній вплив соціального складника на технічний;

– опосередкований вплив, реалізований через рефлекторний вплив технічного складника на соціальний.

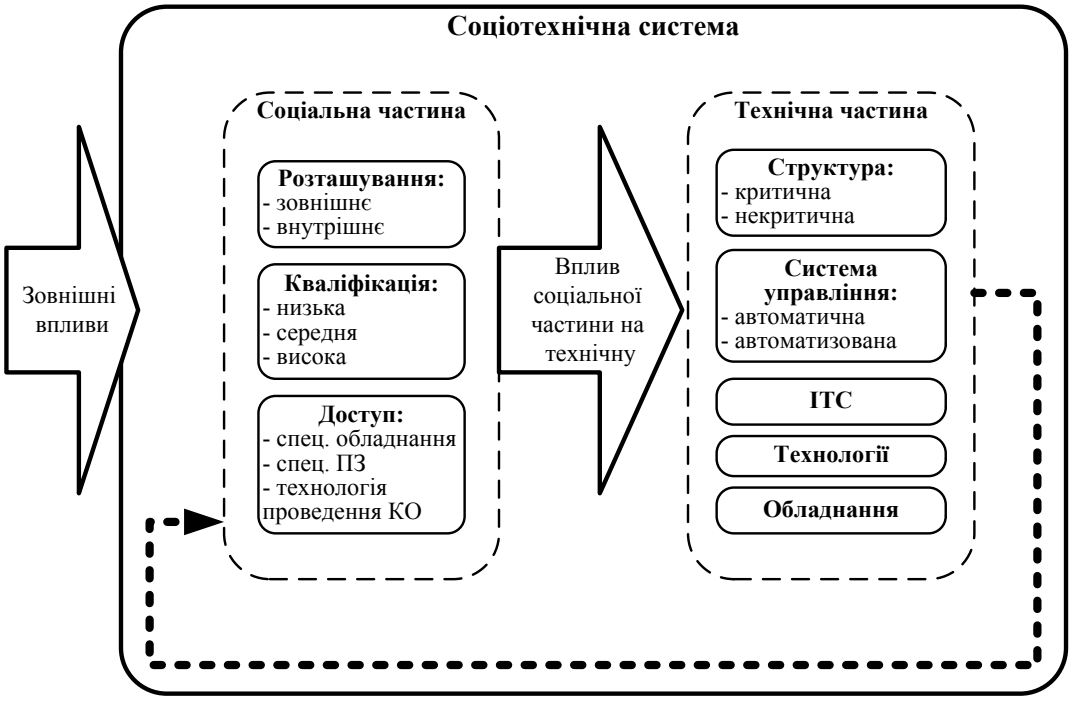

Рис. 2. Ситуаційна модель взаємодії частин СТС

З урахуванням типів мемів, які можуть впливати на соціальний складник СТС, узагальнена модель загроз соціального складника СТС представлена у вигляді виразу:

$$R = F(R_z, R_t, R_y).$$

Необхідно зазначити, що кінцева мета деструктивного впливу на соціум (персонал) з боку конкурента полягає здебільшого у впливі на технічний складник СТС, якщо це стосується впливу, наприклад, на локальний промисловий об'єкт, і навпаки, кінцевою метою може бути соціум, якщо це стосується масштабів держави.

Реалізація зовнішньої загрози (зовнішнього мему) формалізується виразом:

$$P(R_z) = \sum_{k=1}^{k} P(R_z \mid Q_k) \cdot P(Q_k).$$

Реалізація внутрішньої загрози (внутрішнього мему) представлена виразом:

$$P(R_v) = \sum_{k=1}^{k} P(R_v \mid Q_k) \cdot P(Q_k).$$

Реалізація загрози через опосередкований вплив людини на техніку формалізується виразом:

$$P(R_t) = \sum_{k=1}^{k} P(R_t \mid Q_k) \cdot P(Q_k).$$

У представлених виразах: R_z – подія, яка відображає реалізацію загрози – появу зовнішніх мемів, R_v – подія, яка відображає реалізацію загрози – появу внутрішніх мемів, R_t – подія, яка відображає реалізацію загрози шляхом опосередкованого впливу на технічний складник, Q_k – подія, яка відображає сприятливі умови.

За умови незалежності і несумісності подій R_z, R_v та R_t ймовірність реалізації ІПО можна представити таким виразом:

$$P(R_v) = \sum_{k=1}^{k} P(R_v \mid Q_k) \cdot P(Q_k) +$$
$$+ \sum_{k=1}^{k} P(R_z \mid Q_k) \cdot P(Q_k) + \sum_{k=1}^{k} P(R_t \mid Q_k) \cdot P(Q_k).$$

Перелік загроз, оцінки їх реалізації та модель ситуаційної взаємодії складників СТС, яка фактично є моделлю ймовірного зловмисника, є основою для аналізу ризику реалізації загроз.

Висновки. Запропонована модель загроз дає змогу враховувати кількісні оцінки ймовірностей виникнення слабоформалізованих загроз – ІПО. З огляду на це, можна зробити висновок, що для забезпечення комплексної інформаційної безпеки необхідно приділяти значну увагу захищеності соціальної компоненти СТС. Фактично це може бути реалізовано у розробці спеціальних методів та методик щодо захисту соціального складника соціотехнічної системи і дасть змогу вирішити актуальну задачу щодо інформаційної підтримки управління комплексною інформаційною безпекою відповідно до ISO/IEC 27001:2013.

Список літератури:

1. Гончар С.Ф., Леоненко Г.П., Юдин А.Ю. Анализ угроз и уязвимостей индустриальных автоматизированных систем управления. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2013. Вип. 2(26). С. 9–14.

2. Анализ угроз сетевой безопасности. URL: http://ypn.ru/138/analysis-of-threats-to-network-security/6/.

3. Гончар С.Ф., Леоненко Г.П., Юдин А.Ю. Загальна модель загроз безпеці інформації АСУ ТП. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. 2015. Вип. 1(29). С. 78–82.

4. Артёмов А.А. Теоретические основы информационного управления. *Информационные войны*. 2015. № 3. С. 83–97.

5. Дудатьєв А.В. Комплексна інформаційна безпека СТС: моделі впливу та захисту : монографія. Вінниця : ВНТУ, 2017. 128 с.

МОДЕЛЬ УГРОЗ СОЦИОТЕХНИЧЕСКОЙ СИСТЕМЫ: СОЦИАЛЬНЫЙ АСПЕКТ

В представленной статье предложена модель угроз для социальной части социотехнической системы, которая учитывает специально созданную информацию – мемы и возможные источники влияния: внутренние и внешние. Представлена модель взаимодействия разнородных составляющих социотехнической системы, которая демонстрирует возможное деструктивное влияние социума на техническую часть системы. В статье также представлена ситуационная модель взаимодействия составляющих социотехнической системы, которая демонстрирует возможность реализации прямого и опосредованного воздействия человека на техническую часть системы. Предложенные модели предлагается использовать при создании комплексных систем защиты информации.

Ключевые слова: *информационная безопасность государства, модель угроз, ситуационная модель взаимодействия составляющих социотехнической системы.*

THE THREAT MODEL OF SOCIO-TECHNICAL SYSTEM: SOCIAL ASPECT

Information security of the state to a large extent depends on the level of security of the society, which is an integral part of the socio-technical system. Special destructive information-psychological operations conducted against the social component of the system pursue the main goal of the information war – reprogramming the consciousness of society. Achieving this goal will allow to make further "necessary" transformations over the entire system and eventually achieve controllability of the influence object or its destruction. This circumstance emphasizes the need to ensure comprehensive protection of information resources, the essence of which boils down to solving two tasks: protecting your own information resources and protecting against possible information-psychological operations of competitors. There is the threats model which takes into account possible sources of influence: internal and external for the social part of the socio-technical system is proposed in the article. The model of the interaction of socio-technical system heterogeneous components which demonstrates the possible destructive influence on the society technical part is presented. The article also presents the situational model of interaction between the socio-technical system components, which demonstrates the possibility of implementing direct and indirect human influence on the technical part of the system. The models can be used while designing complex information security system.

Key words: *information security of the State, threat model, situational model of interaction of the socio-technical system components.*