УДК 004.9

АНАЛІЗ ВИЗНАЧЕННЯ ОЦІНОК РІВНЯ БЕЗПЕКИ ІНФОРМАЦІЙНИХ СИСТЕМ

Б. В. Дурняк, Т. М. Майба

Українська академія друкарства,
вул. Підголоско, 19, Львів, 79020, Україна

Проаналізовано способи оцінювання рівня безпеки та методи оцінювання захисту інформаційних систем управління технологічним процесом. Висвітлено процеси прогнозування різних типів атак.

Ключові слова: *оцінка рівня безпеки, інформаційна система, засоби захисту, атаки, прогнозування.*

Постановка проблеми. У завданнях захисту інформаційних технологій (*IT*) важливим аспектом є можливість оцінювання захищеності *IT*. Переважно така оцінка має інтегральний характер, і тому вона в багатьох випадках є неоднозначною, оскільки на безпеку може впливати низка факторів різної природи. Крім того, уявлення про безпеку функціонування деякої *IT* може допускати ряд неоднозначностей, які залежать від того, що називати безпекою функціонування інформаційної системи. Якщо критерієм безпечного функціонування вважати гарантію того, що кінцевий продукт, який виготовляється відповідною *IT*, буде виготовлений відповідно до визначених вимог, то коло факторів, що впливають на оцінки безпеки, розширюється технологічними аспектами процесу виробництва [1]. Якщо встановити вимоги тільки до інформаційної системи управління деяким процесом, то до факторів, що впливають на безпеку *IT*, будуть належати помилки, що могли виникнути на етапі проектування чи на етапі технологічної підготовки системи управління до конкретного процесу функціонування.

Мета статті — узгодити рівні безпеки всіх компонент *IT*: інформаційна система управління (*IS*); технологічний процес *TP*, яким повинна управляти система *IS*; система обслуговування окремого *TP* і *IS*, яку будемо позначати *SO*.

Виклад основного матеріалу дослідження. Доцільно розглядати інформаційну систему управління деяким технологічним процесом та сам технологічний процес у контексті дослідження проблем, пов’язаних з рівнем безпеки функціонування, оскільки природа факторів, які можуть приводити до зниження рівня безпеки, є цілком різною. Такий розподіл дасть змогу коректно формувати завдання захисту відповідних систем і, що найголовніше, при такому розподілі можливе розв’язання багатьох задач, що виникають у процесі дослідження проблеми безпеки *IT*.

При цьому узгодженість повинна допускати можливість порівняння їх числових значень, або оцінок. В ідеальному випадку такі оцінки повинні бути рівними. Це означає, що немає сенсу одну з виділених систем забезпечувати більшим рівнем безпеки, ніж приймаючий рівень безпеки іншої системи, що функціонує в комплексі з усіма необхідними компонентами. Це зумовлює

доцільність не тільки оцінювання рівня безпеки окремої системи, а й управління цим рівнем, оскільки загальновідомо, що підвищення рівня безпеки приводить до її подорожчання, підвищення її складності, яка є не тільки структурною, а й функціональною. Необхідність в управлінні рівнем безпеки зумовлює потребу розв'язання задач з розробки управління безпосередньо засобами, які забезпечують різні типи захисту. Всі задачі забезпечення необхідного рівня безпеки *IT* розв'язуються в рамках системи безпеки *SB*, засоби захисту Zg_i входять до складу *SB* [2, 3].

До відомих інтегральних оцінок можна віднести:

– величину гарантованої безпеки процесу функціонування *IS*;
– величину ризику, що може виникнути при функціонуванні *IS* та інших компонент;
– міру захищеності системи.

Величина ризику пов'язана насамперед з уявленнями про можливі втрати, що детальніше повинно розглядатися окремо. Оцінками, тісніше пов'язаними безпосередньо зі структурою *IS* та її функціональними можливостями, є уявлення про рівень безпеки та міру захищеності системи. Рівень захищеності здебільшого пов'язується з відомими факторами негативного впливу на об'єкт захисту. Це означає, що параметр, або оцінка захищеності, пов'язаний з окремими атаками, які можуть активізуватися відомими небезпеками. В цьому випадку рівень захищеності може оцінюватися кількістю небезпек, щодо яких в *SB* використовуються відповідні засоби захисту. В ідеальному випадку це означає, що система може бути повністю захищена від визначених небезпек, і така оцінка обчислюється таким співвідношенням:

$$CZ(IS) = \sum_{i=1}^{m} Nb_i ,$$

де Nb_i — окрема небезпека, *Cz* — оцінка захищеності *IS*.

Насправді кожна Nb_i відрізняється від інших Nb_i такими ознаками, пов'язаними з дією Nb_i на *IS*:

– величиною пошкоджень, до яких призводить Nb_i в середовищі відповідної;
– значущістю пошкоджень, що виникли в результаті дії атак, для процесу функціонування *IS,* (Zn_i);
– кількістю різних атак, які може активізувати Nb_i по відношенню до $IS(mn_i)$;
– загрозами, які використовує Nb_i для активізації атак Za_i.

Ці параметри ускладнюють наведений вираз визначення *Cz(IS)*. Таке ускладнення полягає у необхідності встановлення залежності

$$Nb_i = f(Vn_i, Zn_i, mn_i, Za_i, in_i).$$

Засоби захисту, що використовуються стосовно відомих Nb_i і, відповідно, до відомих атак At_i даної Nb_i, можуть модифікуватися залежно від зміни значень параметрів Nb_i. Для випадку використання оцінки типу *CZ* необхідно підтримувати її рівень у заданих границях, незалежно від модифікації Nb_i,

в проявах у вигляді атак $At_i \in Nb_i$, тому можна стверджувати, що міра захищеності, яку заперечує окремий Zg_i, залежить від параметрів, які в загальному характеризують Nb_i, але безпосередньо відносяться до атак $At_i \in Nb_i$. Оскільки кожна атака At_{ij} реалізується з використанням загроз Za_i, що існують в *IS*, то, визначаючи величину впливу на *CZ* окремої атаки, необхідно врахувати можливості відповідних загроз. Наведене вище доводить, що задача побудови явної форми залежності $Nb_i=f(x^i_j)$ є досить складною. Розв'язання цієї задачі дуже тісно пов'язане з реалізацією конкретної *SB* та заданою мірою захищеності. Складність побудови явного виразу $Nb_i=f(x^i_j)$, де $x^i_j=(Vn_l)\vee(Zn_l)\vee(mn_l)\vee(Za_l)\vee(n_l)$ збільшиться залежно від кількості факторів, що враховуються при визначенні величини *CZ*.

Розглянемо можливість інтерпретації величини рівня захищеності від однієї відомої небезпеки Nb_i. Вважатимемо, що кожна з окремих небезпек деякої *IS* активізує свої атаки на *IS* незалежно одна від одної. У цьому випадку можна прийняти, що коли відома деяка атака $At_{ij} \in Nb_i$ і потрібно від цієї атаки захищати *IS*, то можна говорити про створення засобу захисту Zg_i, який орієнтований на протидію вибраній атаці, або умовно можна записати, що $(Ag_i - Zg_l)=0$ чи $Zg_i=-At_i$, де знак мінус означає протидію. Цей факт можна описати у вигляді $(Zg_i \rightarrow At_l) \rightarrow 0$, де стрілка на загальному рівні описує протидію Zg_i відповідній атаці Ag_i. На підставі цього можна вважати, що міра захищеності є максимальною, якщо має місце співвідношення: $\sum_{i=1}^{n}(At_i - Zg_i) = 0$, або $\mu(IS)=\max$, коли $\mu=0$. Це означає, що максимальна міра захищеності дорівнює нулю, якщо її вимірювати наведеним співвідношенням. Якщо $\mu(IS)<0$, то міра захищеності є надмірною. Цей випадок детально розглядати не будемо, оскільки він означає, що в *SB* існують надмірні Zg_i. Очевидно, що на практиці величина μ може мати певне ціле значення. Це буде означати, що μ є неповне і може виникнути ситуація, коли функціонування *IS* буде порушене в результаті виникнення деякої атаки At_i. Така ситуація є натуральною, якщо прийняти, що *IS* може використовуватися для розв'язання різних задач. При цьому різні задачі потребують різної міри захищеності. Прикладом таких інформаційних продуктів можуть бути системні продукти або продукти, які використовуються для різних прикладних задач. У цьому випадку, як було зазначено, стосовно окремих атак використовуються коефіцієнти, які визначають міру небезпеки, що може походити від відповідної атаки. Таким чином, величина міри захищеності не буде приймати тільки цілі значення, а буде змінюватися більш рівномірно.

У цьому випадку максимальна міра незахищеності $n\mu$ буде визначатися співвідношенням:

$$n\mu(IS) = \sum_{i=1}^{m} \alpha_i At_i ,$$

де α_i — коефіцієнт негативного впливу атаки At_i на *IS*. Для введення однозначності в термінологію $\max n\mu(IS)$ будемо називати мінімальною захищеністю *IS*, або $n\mu(IS)=\min\mu(IS)$.

Для того щоб такий підхід був однозначно визначеним, необхідно міру $\mu(IS)$ розглядати для однотипних IS_i або IS_i одного класу, що визначає для таких IS_i однакову кількість небезпек та, відповідно, атак. Тому говорити про міру захищеності для довільних систем *IS* не коректно. Така міра повинна розглядатися для систем одного класу при умові, що для цього класу існують одинакові типи небезпек [4].

Ще одним поширеним способом оцінювання безпеки є спосіб, який використовує уявлення про гарантовану безпеку. У цьому випадку, на відміну від міри захищеності, йдеться про захист *IS* від довільних відомих та невідомих небезпек. Цей параметр позначатимемо символом C_B і розглядатимемо його як параметр, який охоплює міру захищеності C_Z та розширюється невідомими небезпеками і, відповідно, невідомими атаками. Як і у випадку співвідношення, всі появи невідомих небезпек будемо вважати подібними, випадковими та незалежними. В цьому випадку існує можливість розглядати складову оцінки C_B, якою є оцінка C_Z, як окрему складову загальної оцінки, якою є C_B. Тоді можна записати співвідношення:

$$C_B = C_Z + C_{NB},$$

де C_{NB} — оцінка небезпек, що є невідомими для *IS*. Слід відзначити, що уявлення про невідому небезпеку є досить широким. Це означає, що стосовно Nb_i^N, на відміну від Nb_i^V, про які йдеться в C_Z, по відношенню до Nb_i^N не відомо наступне:

– не відомі моменти появи Nb_i^N у вигляді активізовуваних останніми атаками At_i^N;
– не відомі типи атак, що активізуються Nb_i^N;
– не відомі загрози Za_i, що характеризують *IS*;
– не відомі можливі наслідки дії атак на систему *IS*.

У випадку використання уявлень про міру захищеності об'єкта атаки, невідомим є лише виникнення атаки. Це є єдиним фактором, який та чи інша небезпека Nb_i може використовувати для здійснення успішної атаки на *IS*. У випадку уявлень про безпеку *IS*, всі перераховані фактори можуть використовуватися Nb_i^n для забезпечення успішності атаки, яка ініціюється. Оскільки всі фактори стосуються тієї самої небезпеки, то вважатимемо, що між ними існують певні залежності.

Основним і найпоширенішим підходом до елімінації відповідних факторів, які вносять невизначеність у процес реалізації та функціонування атаки, є процедура прогнозування параметрів, які відповідні фактори характеризують. Для фактора, яким є момент виникнення атаки, основним параметром є момент часу, коли може виникнути відповідна атака. Цей параметр може являти собою інтервал часу Δt_i, через який може виникнути атака, починаючи від поточного моменту часу процесу функціонування *IS*. Параметр часу в задачах прогнозування є найпоширенішим.

Прогнозування типу атаки, яка може виникнути, є досить складним. Це зумовлено такими факторами:

– можливостями Nb_i щодо формування різних типів атак та можливостями їх модифікації;
– наявністю загроз в *IS*, які необхідні для реалізації атак певного типу;
– можливостями середовища *IS*, що відомі Nb_i^N, які сприяють реалізації послідовності подій, які відтворюють атаку;
– цілями, для досягнення яких може використовуватися та чи інша атака;
– можливостями розвитку атак у процесі їх реалізації.

Наведені фактори, що використовуються для забезпечення успішної дії атаки, крім фактора моменту часу появи атаки, досить тісно між собою пов'язані. Це дасть змогу здійснювати прогноз за параметром одного з факторів, які є додатковими до фактора часу. Врахування інших факторів переважно реалізується шляхом встановлення залежностей між цілими параметрами. Це стосується передусім можливостей Nb_i, можливостей середовища *IS*, цілей реалізації атак та можливості розвитку атак, яка являє собою таку характеристику атаки, як самомодифікація в процесі реалізації атаки. Проблеми встановлення таких залежностей в нашому випадку не будуть розглядатися, оскільки вони потребують детальнішого дослідження різних класів атак [5].

У рамках задачі оцінювання рівня гарантії безпеки приймемо, що між переліченими факторами існує певна залежність, яку подамо у вигляді: $y=F(x_1, ..., x_n)$, де у є деяким інтегральним параметром, що залежить від параметрів інших факторів. Цей інтегральний параметр будемо називати загрозою небезпеки Nb_i, оскільки він переважно об'єднує характеристики Nb_i. Позначатимемо цей параметр символом Zn_i.

Для того щоб сформувати співвідношення для визначення оцінки рівня безпеки C_B, необхідно скласти співвідношення для визначення оцінки C_{NB}, яка визначає рівень небезпеки, що зумовлюється невідомими атаками, ініційованими в Nb_i^N. Оскільки в основі визначення факту виникнення атаки At_i з Nb_i^N лежать методики прогнозування, то оцінка рівня небезпеки або рівня безпеки C_{NB} визначається точністю процесу прогнозування виникнення атаки At_i. Якщо точність прогнозування атак є близькою до 100%, то можна стверджувати, що атака At_i, яка прогнозується з високою точністю або з високою ймовірністю, переходить у статус атак, що є відомими, і складова C_{NB} переходить у складову C_Z. Точність прогнозування здебільшого вимірюється ймовірністю виникнення спрогнозованої події. Точність прогнозування деякої події можна оцінювати величиною ймовірності виникнення спрогнозованої події за обраними параметрами прогнозування. В цьому випадку процес прогнозування будемо оцінювати в діапазоні [0, 1].

У разі оцінювання невідомої небезпеки C_{NB} прогнозувати відповідну атаку будемо за параметром часу t_i, який визначає момент виникнення атаки, та за параметром, що загалом характеризує атаку Zn_i, який характеризує загрозу небезпеки Nb_i. В загальному випадку параметр Zn_i складається з ряду параметрів, що характеризують Nb_i^N і між собою взаємопов'язані. Може виникнути

ситуація, коли параметр Zn_i відповідає тільки одному параметру, що характеризує Nb_i^N. Прикладом такого параметра може бути міра повноти даних про деяку загрозу, що існує у *IS*, які розміщаються в Nb_i^N. Приймемо, що параметр Zn_i має визначений масштаб вимірювання величини цього параметра. Очевидно, що однією з ключових інтерпретацій параметра Zn_i є інтерпретація, яка дозволяє ідентифікувати тип можливої атаки. Оскільки для встановлення такої відповідності потрібний детальніший аналіз вибраного типу атак та аналіз зв'язку між типом атаки і даними про особливості середовища *IS* та наявність відповідної загрози в *IS*, що потребує окремого дослідження, то обмежимося декларуванням такого зв'язку між типом атаки та параметрами Nb_i^N. Таким чином, у випадку, коли необхідно визначити оцінку гарантії безпеки системи *IS*, потрібно розв'язувати задачу прогнозування моменту t_i виникнення атаки At_i, починаючи від активізації процесу прогнозування до моменту t_{i+1}, де $t_i \prec t_{i+1}$. Крім того, треба провести прогнозування по параметру Zn_i, що дасть змогу визначити тип атаки, можна було б і не прогнозувати Zn_i, а дочекатися t_{i+1}, коли виникне атака At_i, а після цього провести ідентифікацію атаки, і на основі розпізнаних даних про атаку активізувати засоби захисту, які можуть протидіяти відповідній атаці. Процеси прогнозування типу атаки є фактором, на підставі якого можна вести мову про гарантовану безпеку. Це означає, що при розпізнаванні типу атаки збільшується гарантія того, що дія відповідної атаки може бути елімінована. Зрозуміло, що для цього повинен в *SB* існувати відповідний Zg_i. В аналізованому випадку на основі даних про тип атаки At_i реалізується необхідна модифікація засобу захисту, який найбільше надається для протидії атакам відповідного типу. Наведені базові функції, про які йшлося, реалізуються в *SB* і є ознаками гарантії безпеки. Отже, гарантія безпеки реалізується в рамках системи *SB* і являє собою можливість *SB* реалізувати:

– прогнозування моменту виникнення атаки по відношенню до *IS* у момент t_{i+k};
– прогнозування типу атаки, що можна розглядати як процес розпізнавання атаки, яка відбудеться в моммент t_{i+k};
– модифікація наявних засобів захисту Zg_i з системи *SB*, для того щоб останні могли здійснювати протидію атаці, що виникає в момент t_{i+k}, де t_i — це поточний момент часу процесу функціонування.

Система *IS*, що захищається засобами системи *SB*, крім наведених вище методів оцінки безпеки функціонування системи *IS*, на практиці часто використовується апостеріорний підхід до вирішення цього завдання.

Апостеріорний підхід до розв'язання завдання визначення рівня безпеки *IS* передбачає такі етапи його реалізації:

– вибір для системи безпеки найпоширеніших засобів захисту, враховуючи практику використання *IS*;
– виявлення в процесі експлуатації *IS* нових небезпек шляхом ідентифікації атак, що появляються в середовищі системи, яка захищається;

– введення до складу системи *SB* нових відповідних засобів захисту для протидії виявленим атакам;
– проведення переоцінки раніше задекларованого й ідентифікованого рівня захищеності.

Такий підхід повинен розширятися врахуванням вимог до системи захисту, які формуються в рамках стандартів, що орієнтовані на забезпечення певного рівня захищеності.

Наведені вище методи оцінки захисту *IS* стосуються насамперед інформаційних систем, що розв'язують завдання, для яких необхідні тільки засоби інформаційної системи. У випадку, аналізованому в цій роботі, йдеться про інформаційні системи управління технологічним процесом. У цьому разі основним завданням *IS* є не тільки забезпечення передбачуваних процесів управління засобами технологічного процесу, а й забезпечення необхідних умов реалізації випуску відповідних продуктів. У зв'язку з таким розширенням вимог до *IS* управління необхідно розширити клас небезпек, які можуть негативно впливати на технологічний процес і, відповідно, на систему управління. До небезпек належать такі їхні класи:

– небезпеки, зумовлені людським фактором;
– небезпеки, зумовлені відхиленнями в установках, що реалізують технологічний процес;
– небезпеки, зумовлені зовнішніми факторами.

Для друкарського технологічного процесу характерною є необхідність участі в його реалізації обслуговуючого персоналу. Персонал обслуги, незалежно від рівня кваліфікації та посадових технологічних інструкцій, може допускати помилки під час здійснення управляючих дій з системою управління виробничим процесом. У цьому випадку найпоширенішими методами протидії таким випадкам, які допускають інтерпретацію дії атак, є контроль виходу за допустимі границі величин відповідних втручань. Цей підхід до реалізації протидії є досить обмежений, оскільки взаємодія обслуговуючого персоналу з системою управління може мати складний характер і являти собою певну послідовність втручань у систему, ефект якої може не виявлятися безпосередньо після закінчення такого втручання. Тому відповідні засоби протидії повинні контролювати, проводячи його аналіз, і на основі такого аналізу переривати можливість втручання, інформуючи фахівця про необхідні зміни в його діях. Не розглядатимемо критичні ситуації такого втручання, наприклад, якщо воно не є санкціонованим.

Відхилення в роботі технологічного обладнання не завжди може являти собою несправність, яка може бути виявлена засобами діагностики. Такі відхилення можуть не приводити до порушень технологічного поцесу так, як до цього приводять несправності. Відхилення цього типу можуть спричиняти відхилення параметрів продукції, які є недопустимими. Тому ці зміни необхідно розглядати як фактори, що негативно діють на процес виробництва, що є ана-

логом атак, про які йшлося вище. Якщо різні несправності виявляє та реагує на них система діагностики, то відхилення в параметрах технологічного процесу інтерпретуються як атаки, що активізуються в рамках самого обладнання, і тому вони виявляються і елімінуються системою безпеки. Для розпізнавання таких ситуацій в *SB* формуються емпіричні залежності між значеннями параметрів технологічного процесу та значеннями параметрів продукту, що виготовляється. Такі залежності є сталими для всього технологічного процесу, а константи, що в них використовуються, вводяться в процесі настройки технологічного процесу на конкретний режим його функціонування, при якому реалізується тираж певної продукції. Така настройка технологічного процесу друкування є характерною для поліграфічного виробництва.

Висновки. Небезпеки, зумовлені зовнішніми факторами, зазвичай є критичними, і через те що неперервний технологічний процес у друкарстві є порівняно коротким, то зовнішні фактори, що можуть впливати на технологічний процес, і є малоймовірні. Тому цей клас небезпек можна не брати до уваги. Враховуючи наведені вище розширення класів небезпек, для визначення загального рівня безпеки можна використовувати таке співвідношення:

$$C_B = C_Z + C_{NB} + C_{LF} + C_{TF},$$

де C_{LF} — оцінка небезпеки, що виникає через людські фактори, C_{TF} — оцінка небезпеки, що виникає через технологічні фактори.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Техника флексографической печати : Ч. 1; под ред. В. П. Митрофанова, Б. А. Сорокина. — М. : МГУП, 2000.
2. Соколов А. В. Защита информациии в распределенных корпоративных сетях и системах / А. В. Соколов, В. Ф. Шаньгин. — М. : ДМК–Пресс, 2002.
3. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин. — М. : Радио и связь, 2001.
4. Цвики Э. Создание защиты в Интернете / Э. Цвики, С. Купер, Б. Чапмен. — СПб. : Символ Плюс, 2002.
5. Зайцев О. В. ROOTKITS, SPYWARE/ALWARE, KEYLOGGERS & BACKDOORS, обнаружение и защита / О. В. Зайцев. — СПб. : ВХБ-Петербург, 2006.

REFERENCES

1. *Tehnika fleksograficheskoi pechati: ch. 1*; edited. V. Mitrofanova, B. A. Sorokin. (2000), M.: MGUP. [in Russian]
2. Sokolov A. (2002), *Zashchita informacii v raspredelennykh korporativnykh sietiah i sistemakh* / Sokolov A., V. Shan′gin. M.: DMP, Press. [in Russian]
3. Romanec Y. (2001), *Zashchita informacii v kompiuternyh sistems i sietiakh* / Y. Romanec, P. Timofeev, V. Shan′gin. M.: Radio and communications. [in Russian]
4. Cviki E. (2002). *Sozdanie zashchity v Internete* / E. Cviki, S. Cooper, B. Chapman. Spb.: Symvol Plus. [in Russian]
5. Zaitsev A. (2006), *ROOTKITS, SPYWARE/KEYLOGGERS, ALWARE & BACKDOORS, obnaruzhenie s zashchita* St. Petersburg: VHB-Petersburg. [in Russian]

ANALYSIS OF ASSESSMENTS OF THE INFORMATION SYSTEMS SECURITY LEVEL

B. V. Durniak, T. M. Maiba

Ukrainian Academy of Printing,
19, Pidholosko St., Lviv, 79020, Ukraine

It was analyzed the security of the evaluation methods and techniques to protect the evaluation of information control systems of technological process. The paper considers the processes forecasting different types of attacks.

Keywords: *assessment of the level of security, information system security, attack, forecasting.*

Стаття надійшла до редакції 23.06.2015.
Received 23.06.2015.