УДК 004.056

СУЧАСНІ ПІДХОДИ ДО ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

М. В. Грайворонський[a]

Національний технічний університет України «Київський політехнічний інститут»

Анотація

Зроблено аналіз сучасного розуміння поняття кібербезпеки, проведено порівняння з традиційними поглядами на безпеку інформації. Проведено огляд кіберзагроз і засобів їх реалізації — шкідливого програмного забезпечення. Проаналізовано заходи із забезпечення кібербезпеки.

Ключові слова: безпека інформації, інформаційна безпека, кібербезпека, захист інформації

Вступ

Останні кілька років у пресі регулярно висвітлюються інциденти комп'ютерної безпеки, а на рівні урядів, парламентів і міждержавних організацій обговорюються заходи для протидії зростанню комп'ютерної злочинності і атакам на комп'ютерні системи з боку інших держав і терористичних організацій. При цьому широко застосовуть такі терміни як кібератаки, кібервійни, кібервійська, кібертероризм, і, відповідно, кібербезпека. У цій роботі спробуємо розібратись з цими термінами і визначити, що нового вони фактично вносять в сферу захисту інформації в комп'ютерних (інформаційно-комунікаційних) системах. Також розглянемо загрози безпеці сучасних інформаційно-комунікаційних технологій, засоби здійснення атак, і заходи протидії.

1. Поняття кібернетичної безпеки

У цьому розділі спробуємо розібратись з тим, що відрізняє кібернетичну безпеку (або *кібербезпеку*) від більш усталених понять інформаційної безпеки. Спочатку нагадаємо основні терміни, як вони визначені у нормативних документах.

1.1. Традиційні поняття із захисту інформації

Згідно Закону України про захист інформації в інформаційно-телекомунікаційних системах (ІТС), *захист інформації в системі* — діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі (тобто, діям, які порушують режим доступу до інформації, встановлений у відповідності до законодавства), зокрема, *технічний захист інформації* — вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації [1]. Терміни, використані у Законі, відповідають визначенню термінів у ДСТУ 3396.2-97 [2].

Згідно нормативних документів системи технічного захисту інформації в Україні (НД ТЗІ), *безпека інформації (information security)* — це стан інформації, в якому забезпечується збереження визначених політикою безпеки властивостей інформації. При цьому *політика безпеки* визначена як сукупність законів, правил, обмежень, рекомендацій, інструкцій тощо, які регламентують порядок обробки інформації і спрямовані на захист інформації від певних загроз [3, 4]. До властивостей інформації, які визначаються політикою безпеки, відносять *конфіденційність*, *цілісність* і *доступність*.

Поняття *інформаційна безпека*, яке широко застосовується в російській термінології, в нормативних документах України взагалі не вводилось, і традиційно розглядалось як значно ширша сфера, що охоплює як питання захисту інформації, так і питання захисту від інформації, наприклад:

- інформаційні війни,
- захист від неправдивої інформації,
- захист дітей від інформації із ЗМІ і Інтернету.

Термін *інформаційна безпека* був застосований розробниками галузевих стандартів ГСТУ СУІБ 1.0/ISO/IEC 27001:2010 і ГСТУ СУІБ 2.0/ISO/IEC 27002:2010, введених Національним банком України [5, 6]. Визначення цього терміну, наведене в обох документах: «Збереження конфіденційності, цілісності та доступності інформації; крім того, можуть враховуватися інші властивості, такі, як автентичність, відстежуваність, неспростовність та надійність». Виходячи з чинних НД ТЗІ, у цьому випадку слід було застосовувати термін *безпека інформації*.

1.2. Кібербезпека

Поняття *кібернетичної безпеки*, а точніше — *кібербезпеки* почали застосовувати порівняно нещодавно (у окремих публікаціях підкреслюють, що замість *cyber security* слід застосовувати саме термін *cybersecurity*). Цей термін стрімко набув значної популярності. Однак різні автори (а також різні організації, що мають повноваження тлумачення термінів і регулювання їх застосування) вкладають у

[a]mykola.graivoronskyi@gmail.com

цей термін зовсім різні значення. Розглянемо кілька характерних поглядів на це поняття (для більш детального ознайомлення з різноманітними тлумаченнями для початку можна порекомендувати публікації [7, 8]).

1.2.1. Кібербезпека — еволюційний розвиток поняття безпеки інформації

Перша точка зору полягає в тому, що кібербезпека не несе в собі нічого принципово нового. Інформаційно-комунікаційні технології (ІКТ) поширюються, охоплюють все більше сфер життя і діяльності людей, стають все доступнішими, а вимоги із захисту інформації стають все жорсткішими, але це все — еволюційні зміни. Революції трапилися раніше — з появою персональних комп'ютерів, Інтернету, а потім — мобільного зв'язку. Але про кібербезпеку заговорили згодом. Отже, на думку прихильників такої точки зору, кібербезпека — це просто нове слово, яке дозволяє обґрунтувати зростання вимог щодо фінансування заходів з безпеки інформації, а можливо і створення нових чиновницьких структур і спеціальних служб.

1.2.2. Кібербезпека — це захист кібернетичних систем

Прихильники другої точки зору вважають, що особливістю кібербезпеки є те, що вона стосується кібернетичних систем. До них належать системи, які включають цикл, у якому дія системи викликає зміну її середовища, яка через зворотний зв'язок спричиняє зміни системи. Деякі з галузей, що охоплює кібернетика, є дуже актуальними у сучасних ІКТ, як наприклад:

- штучний інтелект,
- системи керування,
- системи підтримки прийняття рішень,
- моделі соціальних систем.

Важливим прикладом кібернетичних систем, що відносяться до об'єктів захисту у кібербезпеці, є промислові системи керування [9], які часто називають абревіатурами: у російських джерелах — ЦСУ (*цифровые системы управления*), а в англомовних (і не тільки) — SCADA (*Supervisory Control And Data Acquisition*).

1.2.3. Кібербезпека включає наступальні дії проти супротивника

Третя, досить поширена точка зору була стандартизована авторитетним видавництвом Gartner для класифікації (рубрикації) публікацій. На замовлення видавництва аналітики Ендрю Уолс (Andrew Walls), Ерл Перкінс (Earl Perkins) і Юрген Вайс (Juergen Weiss) підготували звіт [10], в якому зробили такий висновок: ≪Застосування терміну "кібербезпека" як синоніму безпеки інформації або безпеки ІКТ вводить в оману споживачів і професіоналів з безпеки і приховує критичні відмінності між цими дисциплінами. [...] Кібербезпека відмінна у включенні нею

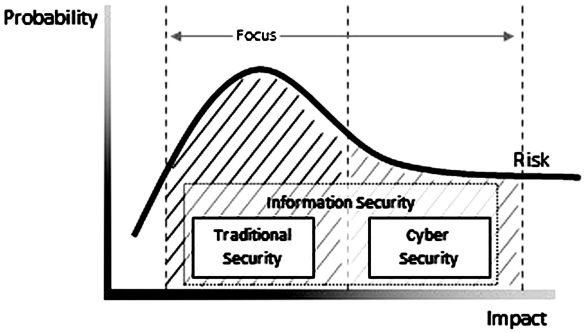

Рис. 1. Області традиційної безпеки інформації і кібербезпеки в термінах кібер-ризиків [12]

наступального характеру застосування інформаційних технологій для атаки на супротивника.≫

1.2.4. Визначення кібербезпеки через керування кіберризиками

Четверта точка зору визначає кібербезпеку через керування *кібер-ризиками* (*cyber risk*). Кібер-ризик — це будь-який ризик фінансових втрат, порушення або шкоди репутації організації, викликаний деякими порушеннями функціонування її інформаційно-комунікаційної системи [11]. Ризики, що пов'язані з реалізацією певних загроз, обчислюють як добуток ймовірності реалізації загрози протягом певного періоду часу та збитків, які очікують внаслідок реалізації цієї загрози. На рис. 1 проілюстровано точку зору щодо сфер застосування кібербезпекі і традиційної безпеки у термінах відповідних кібер-ризиків [12]. Тобто, кібербезпека має справу з ризиками, що пов'язані з особливо великими збитками і порівняно невеликою ймовірністю.

Слід визнати, що у багатьох випадках загрози, протидія яким відноситься до заходів кібербезпеки згідно наведеним вище трактуванням цього поняття, призводять саме до ризиків з високими втратами. Як приклади можна навести можливість атак кібер-терористів на комп'ютерні системи керування системами очищення питної води або на системи керування атомними електростанціями. З іншого боку, можна навести багато контр-прикладів, коли подія відноситься до кібер-загроз, але потенційний збиток може бути незначним. Наприклад, перехоплення керування і викрадення безпілотного розвідувального літального апарату хоча і є інцидентом кібербезпеки (наприклад, США розглядають таку подію як військовий напад), найімовірніше не несе значних втрат. А з іншого боку збитки від традиційної загрози несанкціонованого доступу до інформації про перспективні розробки військової техніки можуть бути значними.

1.2.5. Рекомендації ITU-T — огляд кібербезпеки

Нарешті, в якості п'ятої точки зору розглянемо визначення з Рекомендацій ITU-T X.1205 *"Огляд кібербезпеки"* (*"Overview of Cybersecurity"* [13]). Згі-

дно цього документа, кібербезпека — це набір засобів, політик, концепцій безпеки, заходів безпеки, методичних вказівок, підходів щодо управління ризиками, дій, навчання, кращих практик, гарантій і технологій, які можуть бути застосованими для захисту *кіберпростору* а також *активів користувача і організації*. До активів користувача і організації належать

- з'єднані обчислювальні пристрої,
- персонал,
- інфраструктура,
- прикладні програми,
- сервіси,
- телекомунікаційні системи,
- сукупність інформації, що передається та(або) зберігається в кіберпросторі.

Кібербезпека прагне забезпечити досягнення і підтримання властивостей безпеки активів користувача і організації проти відповідних ризиків безпеки в кіберпросторі. Загальні цілі безпеки охоплюють доступність, цілісність, яка може включати *автентичність* і *неможливість відмовлення від причетності*, і конфіденційність.

Легко побачити, що точка зору, яку ми назвали п'ятою, і яка сформульована ITU-T — однією з найавторитетніших організацій, яка є джерелом міжнародних стандартів у сфері телекомунікацій, зокрема й безпеки телекомунікацій, практично нічим не відрізняється від "точки зору номер один", оскільки фактично повторює усі традиційні уявлення про безпеку інформації й ІКТ. Єдиною помітною відмінністю є постійне згадування *кіберпростору*. Можна було б припустити, що саме з кіберпростором пов'язана новизна поняття кібербезпеки. На жаль, це жодним чином не внесе ясності. Адже термін "кіберпростір", який спочатку з'явився у науковій фантастиці, а тепер застосовується також і у різних державних і міжнародних нормативних документах, має безліч суттєво відмінних трактувань, визначень і тлумачень. Деякі фахівці нараховують до 28 різних визначень терміну "кіберпростір" [14, стор. 4].

Таким чином, фактично на сьогодні немає єдиної точки зору щодо застосування термінів "кібербезпека" і "кіберпростір". Виходячи з цього, у цій доповіді ми будемо розглядати сучасні аспекти забезпечення безпеки інформації, які можуть, але не зобовїязані включати проактивний (наступальний) захист, у сучасних інформаційно-комунікаційних системах, які безумовно включають, але не обмежуються кібернетичними системами.

2. Кіберзброя — шкідливе програмне забезпечення

2.1. Кіберзагрози

Коли ведуть мову про кібербезпеку, традиційно намагаються підкреслити нові, специфічні загрози, що характерні для сучасного стану розвитку інформаційно-комунікаційних технологій і рівня впровадження їх у повсякденне життя. Назвемо деякі з них.

Таргетовані атаки В залежності від цілей, можна виділити дві протилежні тактики атак на комп'ютерні системи.

Перший варіант — застосувати для атаки програмне забезпечення (вірус, троянський кінь, черв'як), маючи на меті компрометацію якомога більшої кількості систем. Програмне забезпечення, створюване для таких атак, повинно стрімко поширюватись, а компрометація кожного конкретного комп'ютера значення не має, тут важливою є кількість. В результаті створюють так званий *ботнет* — мережу скомпрометованих комп'ютерів для використання у своїх цілях. В подальшому ботнети застосовують для організації розподілених атак на відмову в обслуговуванні (DDOS) або для іншої злочинної діяльності в Інтернеті. Така тактика характерна саме для злочинців. Зазначимо, що через стрімке поширення програмне забезпечення, що було використано для такої атаки швидко потрапляє в поле зору розробників антивірусів і додається до баз сигнатур. Це не заважає подібним атакам бути дуже небезпечними і наносити значні збитки, але скорочує життєвий цикл такої атаки.

Другий варіант — проводити атаку прицільно (звідки й назва «*таргетовані*», тобто *націлені*), для компрометації комп'ютерів конкретної установи або навіть конкретних користувачів (як правило, посадових осіб високого рангу або їхніх помічників, науковців, взагалі людей, які мають справу з особливо цінною інформацією). У такому випадку якщо спроба атаки була неуспішною, готують нову спробу — і так до тих пір, поки компрометація не вдасться. Через це такі атаки спочатку назвали *Advanced Persistent Threats (APTs)*, підкреслюючи, що для атаки застосовують передові технології, а загроза атаки буде постійною.

Для таких атак так само застосовують шкідливе програмне забезпечення, але у цьому випадку воно не повинно безконтрольно розповсюджуватися. Навпаки, воно повинно непомітно функціонувати на скомпрометованих комп'ютерах тривалий час, не потрапляючи у поле зору антивірусних компаній. При цьому заради успіху атаки на розробку таких програм виділяють значні кошти, що дозволяє застосовувати викрадені чинні сертифікати, експлойти вразливостей нульового дня тощо. Програми конструюють для конкретної атаки, ретельно тестуючи їх на те, що вони не виявляються антивірусами.

Крім суто програмних засобів для таргетованої атаки може здійснюватись впровадження в атаковану організацію шпигунів і інформаторів (що ніяк не є новою тактикою), а також атаки на "треті сторони", що надають сервіси тим, кого атакують.

Кібертероризм Явище тероризму не нове, але протягом кількох останніх десятиліть воно поши-

рилося і протидія йому не дуже ефективна. ІКТ надають терористам кілька інструментів.

- Застосування комп'ютерних мереж для керування, координації дій і підготовки терактів.
- Можливість терористам напряму звертатись до широкого кола людей, використовуючи сервіси сучасного Інтернету. Така можливість дуже важлива для терористів, і сам факт її наявності певною мірою стимулює їх діяльність.
- Те, що власне і називають *кібертероризмом* — можливість впливу через комп'ютерну мережу (зокрема, Інтернет) на системи керування транспортом, промисловими об'єктами, будинками та будь-якими технологічними процесами.

Потенційно будь-який технологічний процес, яким керує цифрова система керування (або SCADA), може стати об'єктом атаки кібертерористів. Фахівці, які проводять аудит таких систем керування, підтверджують, що з їх безпекою існують величезні проблеми. На сьогодні значна частина систем керування або підключена до Інтернету напряму, або має приховані зв'язки з Інтернетом, про які не завжди знають навіть ті, хто ці системи експлуатує. Але відключення системи від Інтернету теж не гарантує повної безпеки, як це було продемонстровано черв'яком Stuxnet — він успішно і непомітно проникав у мережу з заражених пристроїв flash-пам'яті.

Інтернет речей Крім систем SCADA в Інтернеті взагалі багато об'єктів, керування якими або просто доступ до яких може бути вкрай неприємним для людей. Такі об'єкти складають те, що прийнято називати «*Інтернет речей*» (*the Internet of things*). Це камери спостереження, давачі систем охорони, світлофори, медичні пристрої. Вся ідея систем «розумних будинків» побудована на таких пристроях. А загальна кількість таких пристроїв в Інтернеті вже, за деякими оцінками, у 6 разів перевищує кількість людей-користувачів. І якщо несанкціонований доступ або несанкціоноване використання таких пристроїв і не буде мати характер кібертероризму, все одно це є значною загрозою.

Кібервійни Щойно згаданий Stuxnet — це якраз і є прообраз кіберзброї для ведення кібервійни. Його ціллю були центріфуги для збагачення урану. Але цілі можуть бути й іншими, зокрема військовими. Військова техніка зараз теж знаходиться під керуванням комп'ютерних систем, а отже може бути атакована аналогічним чином. Можливі сценарії — здійснення диверсій або відключення систем (наприклад, комплексів протиповітряної чи протиракетної оборони). Малоймовірно, але не повністю виключено й одержання керування над окремими системами супротивника. Якщо додати до цього проведення розвідувальних операцій у мережі, то стає зрозумілим, що помітна частина військових операцій може бути перенесена у кіберпростір.

«**Хактивізм**» «Хакери-активісти» — явище, яке набуло поширення кілька років тому. Деякі хакерські угруповання ставлять за мету видобування конфіденційної (іноді таємної) інформації і розкриття її шляхом розміщення в Інтернеті у вільному доступі. Як правило, мова йде про викриття таємних операцій, змов, корупції та інших дій на рівні урядів чи окремих політичних сил, які суперечать закону, принципам демократії й іншим загальнолюдським цінностям. Звичайно, не все і не завжди так просто, і у багатьох випадках такі дії наносять шкоду не лише вузьким колам зацікавлених осіб, а й країнам у цілому. Таку діяльність також можна віднести до «кібервійни», оскільки розкриття інформації, що наносить шкоду одній стороні, автоматично дає перевагу іншій стороні.

Банківські системи Маніпуляції з банківськими системами стали відомі задовго до появи Інтернету і розмов про кібербезпеку. Чим ширше у банківській сфері застосовуються інформаційно-комунікаційні технології, тим більше можливостей для махінацій у цій сфері. Дуже поширеними є фішинг (отримання шахрайським шляхом атрибутів користувача для доступу до його рахунків), викрадення і використання атрибутів платіжних карток, а також застосування дуже складного і досконалого шкідливого програмного забезпечення для втручання в роботу систем клієнт-банк. У багатьох випадках програмне забезпечення онлайн-банкінгу є недосконалим і вразливим, хоча банки не схильні це визнавати.

Саме втрати у банківській сфері вносять найбільший внесок у втрати від кіберзлочинів (за деякими даними - більше 100 мільярдів доларів на рік).

«**Електронний уряд**» Це — інформаційно-комунікаційна система, або об'єднання інформаційно-комунікаційних систем, що автоматизує інформаційну взаємодію органів державної влади та органів місцевого самоврядування з громадянами та суб'єктами господарювання з метою підвищення ефективності надання державних послуг. Електронний уряд вважають важливим чинником боротьби із корупцією і поширення принципів демократії в країнах, що розвиваються. Атаки на електронний уряд можуть зашкодити функціонуванню такої системи, а у країнах з низьким рівнем впровадження інформаційно-комунікаційних технологій — підірвати довіру до демократичних перетворень і технічного прогресу.

Соціальні мережі Соціальні мережі є специфічною ціллю для кібератак. Через соціальні мережі можна здійснювати вплив на свідомість людей, формувати суспільну думку, поширювати інформацію (і дезінформацію) і організовувати масові заходи. Люди схильні довіряти інформації з соціальних мереж значно більше, ніж інформації, яку поширюють ЗМІ. Існують вже апробовані методики впливу. Таким чи-

ном, соціальні мережі – це одна з основних територій інформаційних війн.

Апаратні закладки у мікросхемах і прошивках комп'ютерного і мережного обладнання Як специфічну кіберзагрозу можна назвати можливість наявності апаратних закладок у мікросхемах і прошивках. Слід пам'ятати, що більшість важливих мікросхем (процесори, чіпсети) проектуються в США, а виготовляються в Китаї або на Тайвані. Зрозуміло, що саме названі держави можуть мати можливість впроваджувати апаратні закладки. До можливих функцій таких закладок слід віднести можливості несанкціонованої роботи з мережею, дистанційного блокування систем, знищення або копіювання інформації, і навіть впровадження додаткового прихованого рівня віртуалізації. Подібні побоювання останнім часом висловлюють все більше, хоча прихованих закладок такого типу поки що не виявляли. А вот функція дистанційного знищення усієї інформації на комп'ютері (захист від викрадення портативних комп'ютерів) реально існує і документована. Відкритим залишається питання, чи не може ця функція бути активована всупереч бажанню законного власника?

2.2. Класифікація і схеми застосування шкідливого програмне забезпечення

Вище було зазначено, що особливу роль у кібератаках грає *шкідливе програмне забезпечення* (*malware*). Це програмні засоби, які несанкціоновано впроваджуються в комп'ютерну систему і призначені для порушення політики безпеки, нанесеня шкоди інформаційним ресурсам, а в деяких випадках — і апаратним ресурсам комп'ютерної системи.

Існують різні підходи до класифікації шкідливого програмного забезпечення. Доцільно провести класифікацію шкідливого програмного забезпечення за способом розповсюдження:

- Класичні комп'ютерні віруси (virus)
- Мережні хробаки (worms)
- "Троянські коні" (trojan)
- Спеціальні засоби (експлойти, генератори ключів тощо)

2.2.1. Віруси

Класичні комп'ютерні віруси — це програмні засоби, які здатні самостійно відтворюватись, тобто розмножуватись, і які використовують в якості носія інший програмний код, який вони модифікують таким чином, щоби впровадити в нього свою копію. Середовище існування — системні області комп'ютера, операційні системи, прикладні програми, у певні компоненти яких впроваджується код вірусу. Спосіб зараження — різні методи впровадження вірусного коду в об'єкти, які він заражає. За такими об'єктами розрізняють:

- Файлові віруси
- Завантажувальні (boot) віруси
- Макро-віруси
- Скриптові віруси (віруси у сценаріях)

Термін «комп'ютерний вірус» часто застосовують узагальнено, маючи на увазі будь-яке шкідливе програмне забезпечення. Саме у такому сенсі говорять про захист від комп'ютерних вірусів і антивіруси. Слід визнати, що зараз класичні комп'ютерні віруси є менш популярними, поступившись місцем іншим різновидам шкідливого програмного забезпечення.

2.2.2. Троянські коні

Троянський кінь (троян, троянець) — це програма, яка використовуючи різні методи *соціальної інженерії* приваблює довірливого користувача і таким чином провокує його на її запуск. У деяких троянських конях шкідливі функції добре приховані, так що користувач може і не підозрювати, що його комп'ютер вже скомпрометований.

Троянські коні є одним з основних засобів доставки шкідливого коду в таргетованих атаках. Здебільшого, їх оформлюють у вигляді документів у форматі DOC або PDF, які надсилають користувачам електронною поштою.

2.2.3. Мережні черв'яки

Класичні *мережні черв'яки* здатні самостійно, без втручання користувача, розповсюджуватись у комп'ютерній мережі, забезпечуючи щонайменше дві функції:

1) передавання свого програмного коду на інший комп'ютер,
2) запуск свого програмного коду на віддаленому комп'ютері.

Для цього черв'яки використовують вразливості комп'ютерних систем (тобто, вони містять експлойти). На відміну від класичних вірусів, черв'яки, як правило, не використовують в якості носія код іншої програми, оскільки не намагаються примусити користувача таким чином запустити їх.

Іноді черв'яками називають також програми, які здатні автоматично передати себе на інший комп'ютер, але не здатні самостійно запустити себе на виконання на віддаленій системі (для запуску вони використовують принцип троянського коня).

2.2.4. Програмні закладки

Програмні закладки — це програми або окремі функції програм, які приховано впроваджують у комп'ютерну систему, і які протягом тривалого часу функціонують у системі, порушуючи політику безпеки. Програмні закладки можуть впроваджуватись вірусом, троянським конем, черв'яком або безпосередньо користувачем-зловмисником. У таргетованих атаках як правило застосовують програмні закладки, що мають функції перехоплення і передавання інформації (*spyware*) і віддаленого адміністрування (*backdoor*).

2.2.5. Руткіти

Руткітами (rootkit) називають програмні закладки або їхні компоненти, призначені для приховування слідів присутності зловмисника чи зловмисної програми у системі.

2.2.6. Експлойти

Експлойти (exploit) – це програми, які використовують (експлуатують) вразливості комп'ютерних систем. Вони можуть застосовуватись локально для отримання користувачем-порушником підвищених привілеїв у системі, або віддалено, для здійснення мережної атаки. На відміну від черв'яків, експлойти запускаються зловмисником вручну, не мають засобів самокопіювання, і переносяться з системи на систему (наприклад, завантажуються з мережі Інтернет) також вручну. Експлойти можуть міститися у троянському коні або мережному черв'яку для реалізації певних функцій, зокрема, для підвищення привілеїв.

3. Захист інформації або заходи з кібербезпеки

Перейдем до розгляду того, що ж можна і необхідно робити для запобігання тим небезпекам, які були розглянуті у попередньому розділі.

3.1. Антивірусний захист

Оскільки, як ми з'ясували вище, все актуальнішими стають атаки із застосуванням шкідливого програмного забезпечення (яке узагальнено називають *комп'ютерними вірусами*), першим і необхідним методом захисту можна назвати *антивірусний захист*. Принципово цей метод полягає в тому, щоби на підставі різних ознак виявити і знешкодити шкідливі програми. Нагадаємо основні методи виявлення шкідливих програм:

- Сигнатурний пошук;
- Поведінковий (евристичний) аналіз;
- Незмінність файлів і каталогів.

Антивірусний захист є одним із базових компонентів захисту сучасних систем. В якості альтернативи можна назвати дозвіл на запуск лише підписаного коду, але ця технологія по-перше обмежує можливості користувача і розробників вільних програм, а по-друге не гарантує від використання зловмисниками викрадених сертифікатів (Stuxnet містив цілих два таких сертифікати).

Переоцінювати надійність антивірусного захисту теж не слід — таргетовані атаки як правило успішно його обходять, і деякі з таких атак продовжувались роками без виявлення антивірусами. Крім того, користувачі можуть неправильно налаштовувати антивірус або відключати його, якщо він буде заважати їм спокійно працювати. Висновок простий — антивірус необхідний, але без комплексного підходу, а саме без відповідних організаційних заходів, він не зможе убезпечити інформацію.

Слід визнати, що компанії-розробники антивірусів вносять вагомий внесок в забезпечення кібербезпеки. Більшість таких компаній співпрацюють з уповноваженими органами і спецслужбами своїх держав. Через це у сучасному світі наявність вітчизняного антивіруса вважається необхідним елементом кібернетичної безпеки держави. Але важливо розуміти, що антивірус — це не просто програмний продукт, це насамперед інфраструктура збирання і оброблення інформації про виявлені атаки і вразливості, а також швидкого і ефективного дослідження підозрілих файлів.

3.2. Комплексні системи захисту інформації

Традиційний підхід до захисту інформації, закріплений в нормативних документах системи технічного захисту інформації в Україні, полягає у створенні і підтримці в дієздатному стані системи заходів, як технічних (інженерних, програмно-апаратних), так і нетехнічних (правових, організаційних), що дозволяють запобігти або ускладнити можливість реалізації загроз, а також знизити потенційні збитки. Система зазначених заходів, що забезпечує захист інформації, називається *комплексною системою захисту інформації (КСЗІ)* [15]. Закон України [1] вимагає, щоби державні інформаційні ресурси або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, оброблялися лише в інформаційно-телекомунікаційних системах із застосуванням КСЗІ з підтвердженою відповідністю. Підтвердження відповідності здійснюється за результатами державної експертизи в порядку, встановленому законодавством. Вимоги до створюваної КСЗІ конкретизовані у документі, що називається «Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах» [16]. А ці Правила у свою чергу посилаються на численні нормативні документи системи ТЗІ.

Можна стверджувати, що по своїй суті КСЗІ є абсолютно необхідною компонентою будь-якої інформаційної системи, безвідносно до вимог захисту інформації у конкретній системі. Інша справа, що для багатьох користувачів достатньою буде система, побудована на ліцензійній операційній системі, що регулярно оновлюється, з встановленими і налаштованими згідно рекомендацій розробника антивірусом і брандмауером. Складність побудови КСЗІ не в необхідності її побудови, а в необхідності (якщо така є) дотримання вимог щодо підтвердження відповідності.

Чи можна вважати КСЗІ достатньою для забезпечення кібербезпеки? У більшості випадків це не так. КСЗІ, яка відповідає вимогам нормативних документів України, є занадто статичною системою для сучасного кіберпростору, що швидко розвивається. Вимоги до КСЗІ формулюються на підставі обстеження об'єкта, далі розробляють модель загроз, оцінюють ризики, розробляють політику безпеки, інтегрують КСЗІ і проводять заходи (державну екс-

пертизу) з метою підтвердження її відповідності. З практичного досвіду підтвердження відповідності КСЗІ у великих системах, які поступово (по мірі виділення коштів) розвиваються, можна стверджувати, що одразу після отримання сертифікату відповідності, який повинен бути чинним протягом 5 років, власники системи починають вносити в неї зміни, які фактично ставлять під сумнів чинність цього сертифікату. Будь-які зміни у технологіях оброблення інформації і інформаційних потоках у системі вимагають повторного обстеження і внесення змін у модель загроз, переоцінки ризиків, корегування політики безпеки і так далі. А це значає, що потрібна повторна державна експертиза.

Крім того, КСЗІ має інтегруватися з компонентів, які попередньо також пройшли процедуру підтвердження (державної експертизи або сертифікації). Але компоненти містять програми, а програми містять вразливості, які постійно знаходять. Після факту знаходження вразливості підтвердження відповідності теоретично повинно скасовуватися, і після усунення вразливості розробником необхідне повторне підтвердження. Така практика нам невідома. Тобто, строго кажучи підтвердження відповідності більшості КСЗІ побудовано на не зовсім коректному підтверджені відповідності їх компонентів.

3.3. Системи управління інформаційною безпекою

Система управління інформаційною безпекою (СУІБ) – *Information Security Management System, ISMS* – є більш досконалою системою захисту, ніж КСЗІ. СУІБ є складовою загальної системи менеджменту, що базується на підході бізнес-ризиків під час створення, впровадження, функціонування, моніторингу, аналізу, підтримки й удосконалення безпеки інформації.

Практичні правила, рекомендації та специфікації у сфері безпеки інформації для створення, розвитку і підтримки СУІБ містяться у серії стандартів ISO/IEC 27000. До них, зокрема, належать:

- ISO/IEC 27001:2005 «Інформаційні технології — Методики безпеки — Системи керування інформаційною безпекою — Вимоги» — стандарт, за яким організація може бути сертифікована;
- ISO/IEC 27002:2012 «Інформаційні технології – Методики безпеки – Практичні правила управління безпекою інформації» — набір практичних правил, які зручно застосовувати як для підвищення рівня безпеки інформації в організації, так і для аудиту
- ISO/IEC 27005:2008 «Інформаційні технології — Методики безпеки — Управління ризиками інформаційної безпеки» — стандарт, що надає рекомендації з управління безпекою інформації на основі підходу керування ризиками;
- ISO/IEC 27006:2007 «Інформаційні технології — Методики безпеки — Вимоги до організацій, що проводять аудит та сертифікацію систем менеджменту інформаційної безпеки» — настанова з акредитації сертифікаційних організацій.

Згідно з вимогами ISO/IEC 27001 в основу розроблення СУІБ покладено модель PDCA:

- Планування (Plan) — етап розроблення СУІБ, створення переліку активів, оцінювання ризиків і добирання заходів;
- Дія (Do) — етап реалізації і впровадження відповідних заходів;
- Перевірка (Check) — етап оцінювання ефективності та продуктивності СУІБ, що переважно виконують внутрішні аудитори;
- Удосконалення (Act) — виконання превентивних та коригуючих дій.

Завдяки прозорості та зручності практичного застосування, стандарти серії 27000 активно використовують у багатьох країнах світу. Стандарти 27001 і 27002 з деякими модифікаціями впроваджені в Україні в якості галузевих стандартів НБУ [5, 6].

3.4. Перевірка відповідності систем захисту

Перевірка якості систем захисту здійснюється шляхом перевірки на відповідність тим чи іншим стандартам.

3.4.1. Сертифікація систем і засобів захисту

Сертифікація є основною, міжнародно визнаною процедурою перевірки відповідності. Засоби захисту можуть проходити сертифікацію за різними стандартами, зокрема, за стандартом ISO/IEC 15408 (Common Criteria). СУІБ, як було зазначено вище, сертифікують за стандартом ISO/IEC 27001.

3.4.2. Державна експертиза систем і засобів захисту

В Україні проводять сертифікацію засобів захисту за рядом стандартів. Разом з тим, сертифікацію засобів захисту за НД ТЗІ 2.5-004-99, що встановлює вимоги до захисту інформації в комп'ютерних системах від несанкціонованого доступу, фактично не проводять. Перевірка відповідності за цим нормативним документом проводиться у вигляді *державної експертизи* згідно Положення про державну експертизу і ряду НД ТЗІ. Це стосується і КСЗІ. Результатом експертизи є *експертний висновок*, для КСЗІ в разі успішного проходження експертизи видають також *атестат відповідності*.

3.4.3. Аудит

Аудит – це незалежна перевірка стану безпеки інформації. Як правило, для цього залучають організації, які спеціалізуються на цій діяльності. Дуже часто аудит проводять на відповідність вимогам стандарту ISO/IEC 27002.

3.4.4. Тестування на проникнення

Тестування на проникнення (*penetration testing, pentest*) проводять окремо або як частину аудиту.

Тестування на проникнення передбачає здійснення модельних атак, метою яких є демонстрація можливості подолання систем захисту і компрометації системи. Цей вид випробувань систем набув особливої популярності в контексті кібербезпеки.

3.5. Навчання користувачів і підготовка фахівців

Рівень кібербезпеки критично залежить від коректності дій користувачів і кваліфікації фахівців. Навчання користувачів завжди було одною із важливих складових побудови системи захисту (КСЗІ або СУІБ). В наш час різні організації проводять навчання і сертифікацію фахівців. Такі сертифікації охоплюють широке коло завдань, які повинні розв'язувати адміністратори і менеджери систем. У контексті кібербезпеки варто окремо виділити доступні курси підготовки фахівців із конструювання експлойтів і такі сертифікації, як наприклад CEH – *Certified Ethical Hacker*. Все більшої популярності набувають також змагання з проникнення у комп'ютерні системи, які мають назву CTF – *Capture The Flag*.

Висновки

Можна зробити такі висновки:

- Кібербезпека – це еволюційний розвиток поняття безпеки інформації в комп'ютерних системах. Кібербезпека особливо стосується комп'ютерних систем керування і пристроїв, що функціонують з використанням Інтернету. Кібербезпека передбачає застосування наступальних дій, тобто атак на супротивника.
- Основним засобом реалізації кібератак є застосування шкідливого програмного забезпечення.
- Для протидії сучасним загрозам у кіберпросторі системи захисту повинні мати змогу швидко адаптуватися до змін.

Перелік використаних джерел

1. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах», від 05.07.1994 №80/94-ВР (Зі змінами).
2. ДСТУ 3396.2-97. Захист інформації. Технічний захист інформації. Терміни та визначення.
3. НД ТЗІ 1.1-003-99. Термінологія в області захисту інформації в комп'ютерних системах від несанкціонованого доступу. — Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
4. НД ТЗІ 1.4-001-2000. Типове положення про службу захисту інформації в автоматизованій системі. — Затверджено наказом ДСТСЗІ СБ України від 04.12.2000, № 53.
5. ГСТУ СУІБ 1.0/ISO/IEC 27001:2010. Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги. — Київ. — Національний банк України. — 2010.
6. ГСТУ СУІБ 1.0/ISO/IEC 27002:2010. Інформаційні технології. Методи захисту. Звід правил для управління інформаційною безпекою. — Київ. — Національний банк України. — 2010.
7. Joe Franscella. Cybersecurity vs. Cyber Security: When, Why and How to Use the Term. — Infosec Island. — July 17, 2013.
8. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности — 2014. — №1(2). — с. 22–27.
9. Новые кибернетические угрозы и некоторые методы обеспечения информационной безопасности в цифровых системах управления / Менгазетдинов Н. Э., Полетыкин А. Г., Промыслов В. Г. — Труды конференции «Технические и программные средства систем управления, контроля и измерения», Москва. — Октябрь 2010. — с. 851–862.
10. Definition: Cybersecurity. / Andrew Walls, Earl Perkins, Juergen Weiss. — Gartner. — 07 June 2013.
11. Cyber risk and risk management. — The Institute of Risk Management.
12. Menny Barzilay. A simple definition of cybersecurity. — ISACA Now Blog. — May, 2013.
13. ITU-T Recommendation X.1205, Overview of cybersecurity. — International Telecommunication Union. — April 2008.
14. Franklin D. Kramer. Cyberpower and National Security: Policy Recommendations for a Strategic Framework // Cyberpower and National Security / edited by F. D. Kramer, S. Starr, L. K. Wentz. — National Defense University Press, Washington (DC). — 2009. — 664 с.
15. НД ТЗІ 1.1-002-99. Загальні положення по захисту інформації в комп'ютерних системах від несанкціонованого доступу. — Затверджено наказом ДСТСЗІ СБ України від 28.04.1999, № 22.
16. Правила забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Затверджено Постановою Кабінету міністрів України від 29 березня 2006 р. № 373.