DOI: 978-966-301-265-0/1.2023.106

Пашорін В.І.
https://orcid.org/0000-0001-6165-1147
e-mail: v.pashorin@e-u.edu.ua

Доровська І.О.
https://orcid.org/0000-0001-8694-5395
e-mail: i.dorovska@e-u.edu.ua

Милашенко В.М.
https://orcid.org/0000-0002-1434-7609
e-mail: viktor.mylashenko@e-u.edu.ua

ПИТАННЯ БЕЗПЕКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ В УМОВАХ СУЧАСНИХ ВИКЛИКІВ

Виклад основного матеріалу. Питання безпеки інформаційних систем (ІС) та телекомунікаційних мереж у сучасному суспільстві стають все більш актуальними через постійно зростаючу кількість їх користувачів та розвиток технологій. Усвідомлення необхідності покращення стану кібербезпеки та важливості її для кожної країни значно посилилося за останні роки. Потрібно зазначити, що, в першу чергу, від обізнаності та навчання користувачів інформаційно-телекомунікаційних систем застосуванню принципів кібербезпеки залежить їх безпечне функціонування.

Необхідною умовою ефективності функціонування і високої конкурентноздатності організацій наразі є впровадження електронного бізнесу, який використовує інформаційні технології для підвищення ефективності всіх сторін ділових відносин (продаж, маркетинг, платежі, фінансовий аналіз, пошук співробітників, підтримка клієнтів і партнерських відносин, послуги інтернет-банкінгу, електронна комерція, миттєве переведення коштів тощо). Одночасно з впровадженням електронного бізнесу виникають проблеми, пов’язані, по-перше, з необхідністю захисту інформації від неправомірного її використання (розкрадання, розголошення, зміни, руйнування), по-друге, з порушенням працездатності інформаційних ресурсів організації (тимчасова недоступність ресурсів, або блокування), коли навмисно або помилково порушуються процеси обробки і передачі інформації.

Неправомірна зміна, блокування, знищення, розкрадання або розголошення інформації, так само, як і порушення працездатності інформаційних ресурсів організації, навмисно або помилково, коли порушуються процеси обробки і передачі інформації, завдають серйозної

матеріальної та моральної шкоди суб'єктам інформаційної взаємодії. Інтереси цих суб'єктів полягають у тому, щоб певна частина інформації (конфіденційна комерційна і персональна інформація), була б постійно легкодоступна і в той же час надійно захищена від неправомірного її використання.

Дані проблеми покликана вирішити *система безпеки інформаційних систем,* що захищає інформацію від несанкціонованого використання, а також інформаційні ресурси від впливів, спрямованих на порушення їх працездатності.

Чи поліпшується становище з безпекою електронного бізнесу? Ні, небезпека для сучасних інформаційних систем і комп'ютерних мереж, на жаль, не зменшується. Засоби злому інформаційних систем і маніпуляцій з електронною інформацією розвиваються так само швидко, як і всі високотехнологічні комп'ютерні галузі і тому є цілий ряд причин.

По-перше, інформація стає особливим продуктом, вартість якого часто перевершує вартість інформаційної системи, в рамках якої він існує.

З переходом до ринкових відносин у сфері надання інформаційних послуг інформація здебільш розглядається як товар. Це породжує проблему володіння цим ресурсом, його знищення або зміни, виходячи з державних, комерційних, приватних та інших інтересів. Неправомірні використання, фальсифікація, знищення розголошення інформації завдають серйозної матеріальної шкоди власникам цієї інформації.

По-друге, змінилося інформаційне середовище. Ще 20-30 років тому, проблема безпеки інформаційних систем могла бути ефективно вирішена за допомогою організаційних заходів (режимний доступ до систем, охорона, сигналізація) завдяки територіальної концентрації інформаційних ресурсів і відсутності тісного зв'язку із зовнішнім світом. Загрози безпеці виходили переважно від штатних співробітників.

Сучасне інформаційне середовище зовсім інше, сьогодні поширенні територіально розподілені системи і системи з віддаленим доступом до спільно використовуваних ресурсів. Комп'ютери розміщуються в різних офісах організації і об'єднуються між собою за допомогою мереж, створюючи єдину ІТС, як показано на рисунку 1.

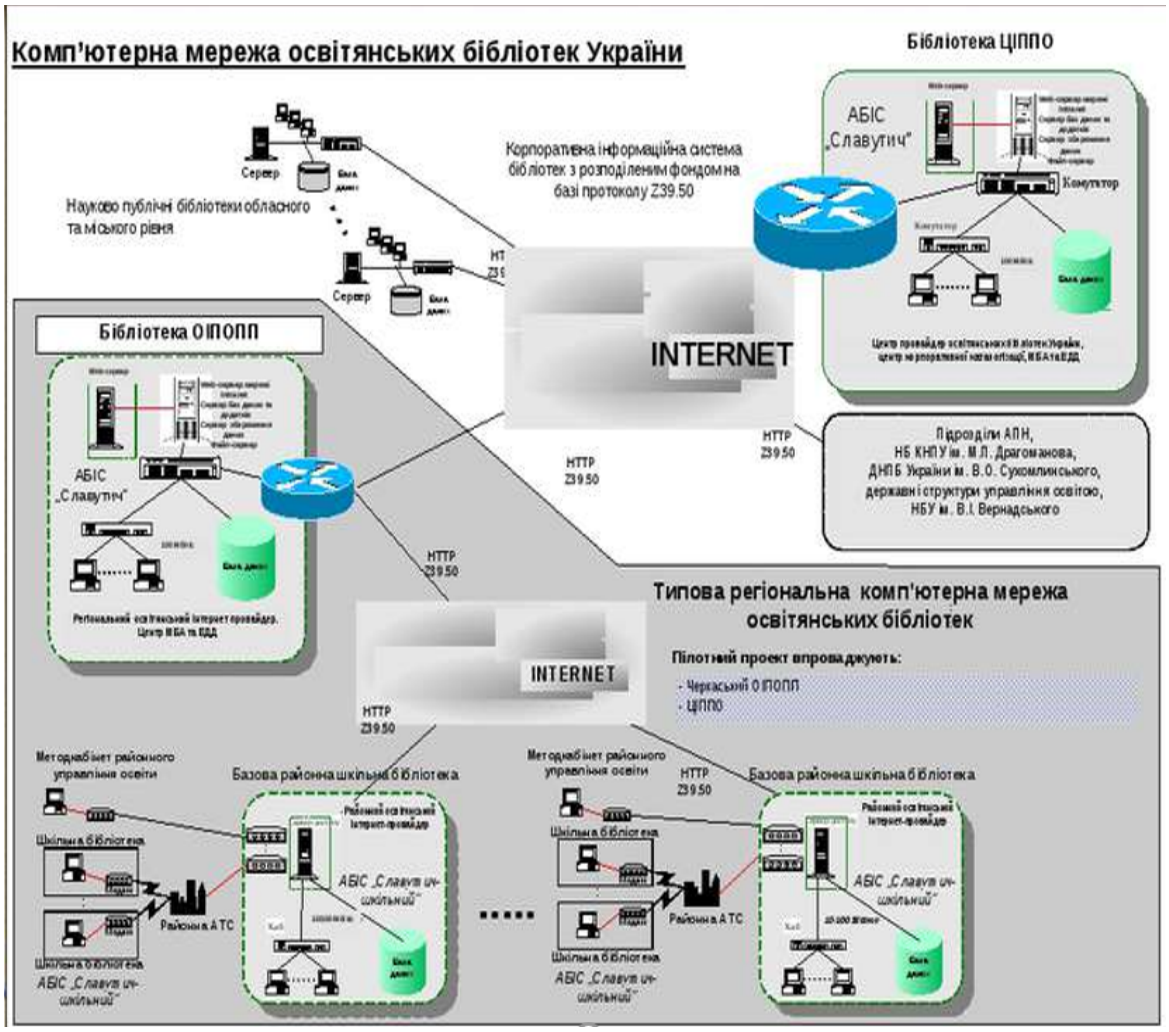

Рис. 1. Розподілена інформаційна система

Доступ до такої розподіленої інформаційної системи мають не тільки співробітники даної організації, а й зловмисники, які не мають відношення до організації і можуть проникнути в систему віддалено й отримати інформацію, незважаючи на те, що знаходяться за тисячі кілометрів. Виникають нові можливі канали несанкціонованого доступу до інформації.

По-третє, зростають потужності сучасних ІТС при одночасному спрощенні їх експлуатації. Збільшується кількість джерел інформації та коло користувачів, які мають безпосередній доступ до інформаційних ресурсів, збільшуються обсяги інформаційних потоків даних, що обробляються і передаються каналами зв'язку.

По-четверте, розширилися сфери застосування ІТС (наприклад, тільки в торговельно-економічній сфері це впровадження систем, що виконують фінансові операції, обслуговують банківські та торговельні структури, обробляють комерційну таємницю організації тощо) і, як наслідок, зростання

кількості розподілених баз даних різного призначення. Відбувається перехід до автоматизованих систем управління та обробки інформації.

По-п'яте, все більшої популярності набуває використання для підтримки бізнесу «хмарного» середовища, що вимагає перегляду підходів до забезпечення безпеки ІТС.

«Хмарні» обчислення (Cloud computing) – це технологія розподіленої обробки даних, при якій спільно використовувані комп'ютерні ресурси, програмне забезпечення (ПЗ) і дані надаються користувачам за запитом як сервіс через Інтернет. «Хмарний» сервіс являє собою особливу клієнт-серверну технологію – використання клієнтом ресурсів (процесорний час, оперативна пам'ять, дисковий простір, мережеві канали, спеціалізовані контролери, програмне забезпечення). На перший погляд, вимоги до безпеки «хмарних» обчислень нічим не відрізняються від вимог до звичайних центрів обробки даних (ЦОД), але «хмарна» інфраструктура виявляється більш складною, має нові властивості і, відповідно, нові, невідомі досі вразливості. Перехід до «хмарного» середовища призводить до появи принципово нових загроз.

По-шосте, зростання використання в бізнесі мобільних пристроїв та бездротових мереж, які можна вважати новими векторами атак, а також поява ефективних засобів технічної розвідки отримання інформації. Впровадження нових технологій приносить і нові ризики безпеки, оскільки старі підходи до захисту не працюють. Так, класичний метод пошуку вірусів на основі сигнатурного аналізу не підходить для сучасних мобільних операційних систем. Як виявилося, мобільну безпеку переважно зачіпає зберігання даних: додатки зберігають особисту інформацію, зображення, записи голосу, замітки, облікові дані, інформацію про бізнес, розташування тощо. Маючи номер телефона людини, можна отримати необмежений доступ до його особистого життя. Якщо врахувати, що мобільні пристрої легко губляться і викрадаються, а мобільні віруси зараз активно розвиваються, необхідність захисту даних стає ще більш очевидною.

По-сьоме, масове поширення інтернету речей (IoT). Пристрої інтернету речей ще не відповідають стандартам безпеки, що робить їх більш уразливими для атак. Зловмисники використовують їх для входу в мережу організації, а потім переходять до інших методів атак (рисунок 2).



Рис. 2. Інтернет речей

Цифровізація бізнесу і формування Інтернету всього (IoE) несе нові приводи для занепокоєння (рисунок 3). Кількість векторів атак неминуче збільшується, що призводить до розширення робочого простору для зловмисників.

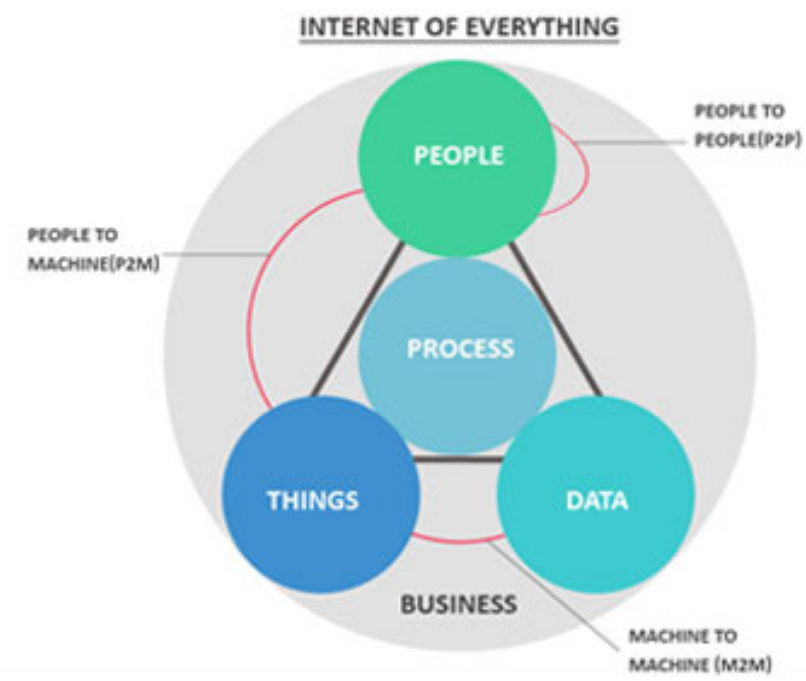

Рис. 3. Інтернет всього

Кожна нова технологія приносить нові ризики безпеки, спроба встигнути за цими змінами і є один з основних викликів, які стоять перед індустрією безпеки. Сторона захисту завжди на кілька кроків позаду. Спроби застосувати старий підхід: смартфони – це маленькі комп'ютери і мобільні додатки – звичайне програмне забезпечення, а значить, вимоги безпеки

абсолютно такі ж самі – невиправдані. Наприклад, класичний метод пошуку вірусів на підставі сигнатурного аналізу немає сенсу в сучасних мобільних операційних системах, тому що це несумісне з моделлю поширення мобільних додатків і тому, що деякі типи вразливостей, такі як переповнення буфера і XSS, менш релевантні до мобільних додатків, ніж до десктопних і вебдодатків.

Не дивлячись на прийняття ряду заходів законодавчого характеру, комп'ютерна злочинність зростає. Недбале ставлення до безпеки інформаційних систем призводить до відповідних наслідків. Наприклад, зловмисники можуть пошкодити вебсайт компанії, розмістивши неправдиву інформацію, що призведе до руйнування репутації компанії, яка будувалась багато років, втрати довіри клієнтів і партнерів, втрати доходу і порушення бізнес-процесів. Це також може призвести до витоку конфіденційних документів, розкриття комерційних таємниць та викрадення інтелектуальної власності. Основні наслідки порушення безпеки інформаційно-телекомунікаційних систем наведено на рисунку 4.



Рис. 4. Наслідки порушення безпеки ІТС

Тому в сучасних умовах відбуваються суттєві зміни в поглядах на безпеку ІТС. На великих підприємствах створюють спеціальні служби з чималим бюджетом, в завдання яких входить виявлення, локалізація і усунення загроз кібербезпеки підприємства. Вони використовують спеціальне дороге програмне і апаратне забезпечення, що потребує особливої підготовки персоналу для роботи з ним (рисунок 5).



Рис. 5. Центральний офіс підрозділу кібербезпеки компанії

У той же час, на малих підприємствах, які мають достатньо невеликий IT-бюджет проблеми кібербезпеки залишаються досить актуальними.

Висновки. Отже, питання питання безпеки інформаційних систем (ІС) та телекомунікаційних мереж у сучасному суспільстві є актуальними і постійно зростає потреба їх усвідомлення і системного вирішення. Авторами визначено основні чинники, що впливають на поширення ризиків та загроз кібербезпеці ІТС. Відзначено, що особливості сучасного інформаційного середовища, наприклад, поширенні територіально розподілені системи і системи з віддаленим доступом до спільно використовуваних ресурсів потребують нових методів і підходів до забезпечення безпеки, класичні методи пошуку вірусів не працюють, зокрема, для мобільних операційних систем. Авторами запропоновано системний підхід до вирішення проблем кібербезпеки, а саме, створення системи безпеки інформаційних систем, що захищає інформацію від несанкціонованого використання, а також інформаційні ресурси від впливів, спрямованих на порушення їх працездатності.

Література

1. Lakhno, V.A., Kasatkin, D.Y., Skliarenko, O.V., Kolodinska, Y.O. Modeling and Optimization of Discrete Evolutionary Systems of İnformation Security Management in a Random Environment // Machine Learning and Autonomous Systems. Smart Innovation, Systems and Technologies, vol 269. Springer, Singapore. – 2022 – p. 9-22.