УДК 004.415.2 (045) Мазур В.І., Мазур О.Ю., Іванкевич О.В., Мелешко О.О.

ІНФОРМАЦІЙНА БЕЗПЕКА - ОДНА З ОСНОВНИХ СКЛАДОВИХ УСПІШНОГО БІЗНЕСУ СУЧАСНОГО ПІДПРИЄМСТВА

1. Система забезпечення інформаційної безпеки авіапідприємства

Глобальне проникнення інформаційних технологій у всі сфери нашого життя, а також поступовий перехід до електронних способів ведення бізнесу ставить перед учасниками ринку нові завдання забезпечення інформаційної безпеки. Великі компанії, а саме їм в першу чергу доводиться вирішувати питання організації роботи віддалених користувачів корпоративних інформаційних систем, надзвичайно уважно відносяться до проблеми забезпечення безпеки інформації. І насправді, коропоративна інформаційна система, яка не забезпечує достатнього рівня захисту інформації від несанкціонованого доступу - потенційна загроза благополуччю компанії. І якщо для локальної мережі це питання стоїть не настільки гостро, то у випадку, коли комунікаційним середовищем виступає Інтернет, питання безпеки, в які входять і несанкціонований доступ, і шифрування інформаційних потоків, і захист клієнтських комп'ютерів від зараження вірусами, стоять дуже гостро. Як загрозу для інформації розглядають несанкціоновані ознайомлення, знищення, зміну, копіювання, а також блокування санкціонованого доступу до даних.

Під корпоративною інформаційною системою підприємства зазвичай розуміють програмно-технічний комплекс («набір» серверів, комп'ютерів користувачів, комутаторів, маршрутизаторів, операційних систем та програмних прикладень), за допомогою якого відбувається накопичення та автоматизована обробка виробничої інформації.

Під уразливістю інформаційної системи розуміється будь-яка її характеристика, використання якої зловмисником може привести до порушення працездатності інформаційної системи або викривлення інформації, що обробляється за її допомогою.

Під інформаційною безпекою організації будемо надалі розуміти стан захищеності інформаційних ресурсів, технологій їх формування і використання, а також прав суб'єктів інформаційної діяльності. Тут важливо відмітити наступне:

- об'єктом захисту стає не просто інформація як якісь відомості, а інформаційний ресурс, тобто інформація на матеріальних носіях (документи, бази даних, інструкції, технічна документація і т.і.), право на доступ до якої юридично закріплено за її власником і ним же регулюється;
- інформаційна безпека користувачів забезпечує захищеність їх прав на доступ до інформаційних ресурсів для задоволення їх інформаційних потреб;
- з погляду економічної доцільності захищати слід лише ту інформацію, розголошування (витік, втрата) якої неминуче приведе до матеріального і морального збитку.

Основні задачі забезпечення інформаційної безпеки:

попередження реалізації загроз інформаційній безпеці підприємства;

зниження рівня збитків для організації при реалізації загроз інформаційній безпеці (виникнення інцидентів інформаційної безпеки);

забезпечення високого рівня довіри (надання обґрунтованих гарантій досягнення цілі забезпечення інформаційної безпеки).

Один з варіантів вирішення задачі забезпечення інформаційної безпеки організації базується на створенні системи забезпечення інформаційної безпеки. Систему забезпечення інформаційної безпеки зазвичай розглядають як сукупність організаційних і процедурних мероприємств, а також технічних засобів забезпечення інформаційної безпеки.

Організаційні засоби служать для створення структури забезпечення інформаційної безпеки, включаючи визначення ролей і обов'язків користувачів. Процедурні засоби направлені на визначення і документування процесів забезпечення інформаційної безпеки, які виконуються персоналом. Сукупність технічних засобів забезпечення інформаційної

безпеки – це набір спеціальних підсистем (криптографічний захист інформації, антивірусний захист, виявлення і виключення атак, міжмережеве екранування, моніторинг і т.і.)

З методологічної точки зору створення системи забезпечення інформаційної безпеки базується на підходах широко відомого стандарту BS7799-2. Вказаний стандарт описує організацію управління інформаційною безпекою і використовує ISO17799 - стандарт, який вміщує каталог кращих світових практик забезпечення інформаційної безпеки. Стандарт BS7799-2 формулює принципи створення системи забезпечення інформаційної безпеки і базується на методології управління ризиками.

При вирішенні задачі забезпечення інформаційної безпеки можна виділити основні фактори успіху:

всебічна підтримка керівництва організації;

наявність в організації політики інформаційної безпеки, яка викладає: цілі забезпечення інформаційної безпеки, зформульовані на основі бізнес-планів організації; область дії системи забезпечення інформаційної безпеки і основні підходи до реалізації інформаційної безпеки;

наявність організаційної структури забезпечення інформаційної безпеки з виділенням ролей і обов'язків та схеми взаємодії програмних прикладень і користувачів;

наявність комплекту організаційно-розпоряджувальних документів, які регламентують забезпечення інформаційної безпеки;

обгрунтований вибір захисних мірориємств (з урахуванням адекватності, вартості та інших факторів);

реалізація дисциплінарного процесу та контроль виконання вимог і моніторинг.

Створення якісної системи забезпечення інформаційної безпеки забезпечує організації конкурентну перевагу поміж інших споріднених організацій на ринку, демонструючи здатність самостійно управляти інформаційними ризиками, які складають значну частину всіх операційних ризиків.

2. Створення та вдосконалення системи забезпечення інформаційної безпеки

Взагалі можна виділити три етапи реалізації належного рівня забезпечення інформаційної безпеки підприємства:

- розробка або вдосконалення організаційної структури забезпечення інформаційної безпеки, побудова або вдосконалення нормативно-методичної бази забезпечення інформаційної безпеки, що регламентує всі процеси забезпечення інформаційної безпеки і розробка або поліпшення архітектури підсистем забезпечення інформаційної безпеки;
- впровадження системи забезпечення інформаційної безпеки. Це складний і тривалий процес, реалізація якого не може бути здійснена за один день. Дуже часто вирішення цієї задачі можна досягти методом передачі в аутсорсинг зовнішнім фахівцям або фірмам;
- професійний супровід системи забезпечення інформаційної безпеки.

В процесі функціонування автоматизованих систем організації зовнішні умови постійно змінюються - висуваються нові вимоги до забезпечення інформаційної безпеки, з'являються нові системи, нові версії програмних і апаратних продуктів і засобів захисту. Супровід системи забезпечення інформаційної безпеки вимагає наявності кваліфікованих фахівців і організації процесу управління інформаційної безпеки на необхідному рівні. У зв'язку з цим часто представляється доцільним передати частину функцій супроводу системи забезпечення інформаційної безпеки надійним стороннім спеціалізованим організаціям.

Практикою створення якісної системи забезпечення інформаційної безпеки передбачено комплексне обстеження мережі та інформаційної структури, яка працює на підприємстві. Метою проведення комплексного обстеження системи забезпечення інформаційної безпеки є отримання об'єктивних даних про поточний стан забезпечення інформаційної безпеки і вироблення на їх основі рекомендацій по застосуванню набору захисних заходів (організаційних і процедурних заходів, а також технічних засобів захисту), направлених на забезпечення необхідного рівня інформаційної безпеки.

Можуть бути проведені роботи по оцінці відповідності системи забезпечення інформаційної безпеки вимогам вітчизняних і закордонних стандартів. В ході проведення оцінки проводиться ідентифікація невідповідностей вимогам стандартів і формулюються пропозиції з їх знешкодження.

Обов'язково повинні бути розроблені організаційно-розпоряджувальні документи, які визначають як стратегію і загальні принципи побудови системи забезпечення інформаційної безпеки, так і вимоги до її підсистем та порядок забезпечення інформаційної безпеки. Набір документів, який існує в організації, може бути доповнений і приведений у відповідність з сучасними вимогами.

Можуть бути проведені роботи по створенню і вдосконаленню наступних підсистем забезпечення інформаційної безпеки:

захисту на рівні активного мережевого устаткування;

захисту мережевого рівня в глобальних мережах;

захисту периметра мережі;

виявлення і виключення атак;

захисту загальносистемного програмного забезпечення;

захисту прикладного програмного забезпечення і програмного забезпечення проміжного шару;

криптографічного захисту інформації;

антивірусного захисту;

управління подіями інформаційної безпеки.

Провідні компанії, які володіють знаннями та навичками для створення підсистем забезпечення інформаційної безпеки, використовують в своїй роботі найбільш сучасні технології відомих світових і вітчизняних виробників, таких як Aladdin Knowledge Systems, Baltimore Technologies, Computer Associates International, Check Point, Cisco Systems, Hewlett-Packard, IBM, Internet Security Systems, Oracle, RSA Security, Sun Microsystems, Інститут Системного Аналізу АН України, Лабораторія Касперського та інших.

3. Проблеми безпеки інформації в системах електронної комерції

У теорії інформаційної безпеки існує основна теорема безпеки системи, доведена до багатьох типів математичних моделей захищених систем та сформульована таким чином: «Якщо початковий стан системи безпечний і всі переходи системи із стану в стан безпечні, то система вважається безпечною». Абсолютно очевидно, що для безпечно захищеної системи електронної комерції умови наведеної теореми повинні підтримуватися на всіх стадіях життєвого циклу системи. При цьому під інформаційною безпекою електронної комерції розуміють захищеність інформації та підтримуючої інфраструктури від випадкових або навмисних впливів природного чи штучного характеру, здатних викликати нанесення збитку власникам або користувачам інформації і підтримуючої інфраструктури. Серед основних вимог до проведення комерційних операцій - конфіденційність, цілісність, аутентифікація, авторизація, гарантії і збереження таємниці. Перші чотири вимоги можна забезпечити технічними та програмними засобами, але виконання останніх двох - досягнення гарантій і збереження таємниці - однаково залежить як від програмно-технічних засобів та відповідальності окремих осіб і організацій, так і від дотримання законів, що захищають споживача від можливого шахрайства.

Для захисту суб'єктів інформаційних відносин при Інтернет-комерції необхідно поєднувати заходи наступних рівнів:

законодавчого (закони, нормативні акти, стандарти);

адміністративного (дії загального характеру організації, які виконуються керівництвом);

процедурного (конкретні заходи безпеки);

програмно-технічного (конкретні технічні заходи).

Законодавчий рівень. Законодавчий рівень є найважливішим для забезпечення інформаційної безпеки при електронній комерції. До цього рівня відноситься весь комплекс заходів, спрямованих на створення і підтримку в суспільстві негативного (в тому числі і карального) відношення до порушень і порушників інформаційної безпеки при електронній комерції. Найважливішим на законодавчому рівні є створення механізму, що дозволяє узгодити процес розробки законів з прогресом інформаційних технологій. Природно, що закони не можуть випереджати життя, але важливо, щоб відставання не було надто великим, оскільки на практиці, крім інших негативних моментів, це призводить до зниження інформаційної безпеки.

Адміністративний рівень. Основою заходів адміністративного рівня, тобто заходів, що розробляються керівництвом організації, є політика безпеки при електронній комерції. Під такою політикою безпеки розуміється сукупність документованих управлінських рішень, спрямованих на захист інформації і асоційованих з нею ресурсів. Політика безпеки визначає стратегію організації в галузі інформаційної безпеки, а також ту міру уваги і кількість ресурсів, яку керівництво вважає доцільним виділити. Вона будується на основі аналізу ризиків, які визнаються реальними для системи електронної комерції організації. Коли ризики проаналізовані і стратегія захисту визначена, назначаються відповідальні особи, встановлюється порядок контролю виконання програми. Розробка політики безпеки - справа відповідальна і тонка, оскільки кожна організація має свою специфіку.

Процедурний рівень. До процедурного рівня відносяться заходи безпеки, що реалізуються персоналом. У вітчизняних організаціях накопичено багатий досвід складання і здійснення процедурних (організаційних) заходів, однак проблема полягає в тому, що вони прийшли з докомп'ютерного минулого. Тому вони потребують істотного перегляду.

Програмно-технічний рівень. Згідно із сучасними переконаннями у межах систем електронної комерції повинні бути доступні принаймні такі механізми безпеки:

- ідентифікація і перевірка автентичності користувачів;
- управління доступом;
- протоколювання та аудит;
- криптографічний захист інформаційних потоків;
- екранування;
- відстеження подій, що являють загрозу інформаційній безпеці та протоколювання подій;
- забезпечення високого рівня доступності.

Весь спектр інтересів суб'єктів, пов'язаних з використанням системи електронної комерції, можна поділити на основні категорії:

- конфіденційність (захист від несанкціонованого ознайомлення);
- цілісність (актуальність і несуперечність інформації, її захищеність від руйнування і несанкціонованої зміни);
- доступність (можливість за прийнятний час одержати необхідну інформаційну послугу).

Конфіденційність. Це - найбільш відпрацьований у нашій країні аспект інформаційної безпеки. На варті конфіденційності стоять закони, нормативні акти, багаторічний досвід відповідних служб. Апаратно-програмні продукти дозволяють закрити практично всі потенційні канали витоку інформації.

Цілісність. Її можна поділити на статичну (зрозумілу як незмінність інформаційних об'єктів) і динамічну (що стосується коректного виконання складних дій (транзакцій)). Практично всі нормативні документи і вітчизняні розробки відносяться до статичної цілісності, хоч і динамічний аспект - не менш важливий. Приклад динамічної цілісності - контроль потоку фінансових повідомлень на предмет виявлення крадіжки, переупорядкування або дублювання окремих повідомлень.

Доступність. Системи електронної комерції створюються або придбаються для отримання певних інформаційних послуг (сервісів). Якщо за тих чи інших причин отримання цих послуг користувачами стає неможливим, це наносить збиток усім суб'єктам інформаційних відносин. Тому, не протиставляючи доступність іншим аспектам, ми виділяємо її як найважливіший елемент інформаційної безпеки. Особливо яскраво провідна роль доступності виявляється в таких системах електронної комерції, як:

підтримка електронної взаємодії різних служб при підготовці авіаційних, залізничних і автомобільних рейсів;

торгові системи, призначені для організації Інтернет-торгівлі і реалізуючі відносини типу продавець-клієнт; системи бізнес-бізнес, де реалізована схема повністю автоматизованої взаємодії бізнес-процесів двох сторін (організацій). Це можуть бути аукціони; фінансові, банківські, туристичні, медичні, страхові, інформаційні послуги; онлайнова оплата рахунків, тощо.

Зовні менш драматичні, але також вельми неприємні наслідки – і матеріальні, і моральні – може мати тривала недоступність інформаційних послуг, якими користується велика кількість людей, як то продаж залізничних і авіаційних перевезень, банківські послуги тощо.

Таким чином, інформаційна безпека повинна забезпечувати: конфіденційність інформації, цілісність даних, а також неможливість неавторизованого створення або знищення даних і високу доступність інформації для всіх авторизованих користувачів.

Для ефективного захисту інформації в системах електронної комерції широко використовують програмно-апаратні засоби захисту програмного забезпечення від несанкціонованого доступу і копіювання. Під програмно-апаратними засобами захисту в даному випадку розуміються засоби, засновані на використанні так званих апаратних (електронних) ключів. Електронний ключ – це апаратна частина системи захисту, що являє собою плату з мікросхемами пам'яті і в деяких випадках з мікропроцесором, вміщену в корпус і призначену для установки в один із стандартних портів ПК (COM, LPT, USB) або в слот розширення материнської плати. Так само можуть використовуватись і смарт-карти.

4. Вибір методології і основних принципів створення системи управління і адміністрування прав користувачів авіакомпанії

Інформаційна система сучасної авіакомпанії є безперечно складним об'єктом і вимагає системного підходу до забезпечення її безпеки. Забезпечення комплексної безпеки інформаційних ресурсів є необхідною умовою функціонування авіакомпанії. Ця "комплексність" полягає, перш за все, в продуманості, збалансованості захисту, розробці чітких організаційно-технічних заходів і забезпеченні контролю над їх виконанням. Побудова складних захищених інформаційних систем пов'язана з вирішенням наступних двох ключових взаємопов'язаних проблем:

- розподіл задач адміністрування засобами захисту інформації поміж суб'єктами управління системою;
- використання вбудованих механізмів захисту на всіх рівнях ієрархії системи.

Перша проблема обумовлена ієрархічними принципами побудови складної системи. Як правило, можна виділити рівень платформи (операційна система), загальносистемний рівень (СУБД і інші системні засоби), рівень прикладень. Кожен рівень вимагає свого адміністрування.

В концепції безпеки авіакомпанії ключовим моментом виступає момент централізації безпеки інформаційної системи. Користувач повинен мати обмеження повноважень і прав доступу незалежно від того, з якого робочого місця і з яким завданням він має справу в рамках інформаційної системи.

Програмне забезпечення є однією з найбільш уразливих ділянок інформаційної системи організації. Безпека програмного комплексу складається із забезпечення безпеки самих прикладень і розумного адміністрування. Згідно сталих класифікацій, за умовами

появи уразливості додатків і програмного забезпечення можна розділити на наступні: проектування; реалізації; конфігурації; експлуатації.

Уразливості проектування – найскладніші. Такі уразливості, закладені безпосередньо в реалізовані алгоритми, виявляються і усуваються з великими зусиллями. Уразливості реалізації привносяться в додатки на етапі створення і часто пов'язані з невірною обробкою вхідних даних, а також передаваних між компонентами програмного забезпечення, або з невірною реалізацією алгоритмів. Ці помилки усуваються тільки розробником програмного забезпечення. Уразливості конфігурації – помилки, обумовлені діями адміністратора, який налагоджує програмне забезпечення всупереч вимогам політики безпеки і здорового глузду. Уразливості експлуатації виникають з вини користувача, який ухиляється від виконання вимог корпоративної політики безпеки.

Рівень доступу співробітника до інформації повинен визначатися його посадовими правами згідно посадової інструкції. Повноваження роботи з інформаційною системою повинні реєструватися відділом та комплексом, який приймає співробітника на роботу, відділом інформаційної безпеки та дирекцією з інформаційних технологій одразу при надходженні людини на роботу. За безпеку конкретних завдань повинні відповідати конкретні адміністратори. Кожен користувач для роботи в інформаційній системі повинен бути зареєстрований. На користувача повинна бути заведена реєстраційна картка, що є офіційним документом, який визначав би повноваження даного користувача у складі системи.

Автентичність користувача повинна перевірятись по методу імен і паролів. У зв'язку з тим, що у якості мережної операційної системи в компанії використається Microsoft Windows 2000 Server, логічно використати її засоби для доступу до ресурсів мережі. Всі користувачі реєструються у домені сервера під певним ім'ям і самостійно вводять пароль. Але для рівня безпеки авіакомпанії не є цілком достатньо таких засобів ідентифікації. Один з методів, що дозволяє уникнути несанкціонованого доступу до системи, - це дозвіл даному користувачеві працювати тільки з певними робочими станціями. Навіть у випадку, якщо ім'я і пароль користувача стали відомі іншій особі, можливість одержати доступ до системи існує тільки на конкретних робочих станціях, як правило, комп'ютерах того відділу, де працює користувач.

Неможливість зовнішнього доступу, тобто доступу через засоби Internet, повинна забезпечуватись наступними факторами. По-перше, сервер розмежування доступу в мережі і Internet-сервер повинні бути фізично різними комп'ютерами. Зв'язок між їх доменами повинен здійснюватись на основі довірчих відносин, тобто щоб дістатися до домену сервера розмежування доступу можна було тільки з паролем адміністратора. По-друге, багато функцій захисту від несанкціонованого доступу через Internet повинні брати на себе Windows 2000 Server і Proxy Server.

Ще один з немаловажних моментів, які стосуються прав роботи в мережі в цілому, - це доступ до ресурсів робочих станцій. В компанії всі комп'ютери, підключені до мережі, працюють під управлінням операційної системи Windows XP Pro. Таким чином, для кожного комп'ютера є можливість установлювати доступ до ресурсів машини на рівні користувача. Список користувачів береться із домену сервера. Адміністратор повинен стежити за характером доступних ресурсів і вести роз'яснювальну роботу з користувачами.

Що стосується безпеки СУБД, то вона повинна забезпечуватись на наступних рівнях: ідентифікація і перевірка дійсності користувачів, керування доступом до даних, механізм підзвітності всіх дій, що впливають на безпеку, захист реєстраційної інформації від перекручувань та її аналіз, очищення об'єктів перед їхнім повторним використанням, захист інформації, переданої по лініях зв'язку. У якості СУБД рекомендовано використання Microsoft SQL Server. Для визначення привілеїв використовується рольова політика.

Реєстрація дій користувачів - ще один фактор, що стримує потенційних зловмисників і дозволяє розслідувати порушення, які вже трапилися в системі. Така інформація може використовуватися для таких цілей, як виявлення незвичайних або підозрілих дій

користувачів і ідентифікації осіб, що здійснюють ці дії; виявлення спроб несанкціонованого доступу; оцінка можливих наслідків порушення інформаційної безпеки, що відбулося; надання допомоги в розслідуванні випадків порушення безпеки.

Для оптимізації процесу адміністрування доцільно спроектувати і реалізувати окремий модуль. В нього повинні входити всі адміністративні компоненти. Єдиний модуль адміністрування, на наш погляд, повинен виконувати наступні функції: реєстрацію користувачів, визначення прав доступу, перегляд адміністративних журналів, перегляд контрольної інформації в записах, створення і реєстрацію ключів безпеки.

Одним з важливих аспектів забезпечення безпеки роботи програмного комплексу є використання електронних підписів. У зв'язку із цим електронний підпис можна розглядати у двох аспектах: підпис як ознака візування операції або документа і підпис для контролю проходження інформації із зовнішніх каналів.

У додатках висока готовність апаратно-програмних комплексів є найважливішим чинником. Що стосується СУБД, то тут засоби підтримки високої готовності повинні забезпечувати нейтралізацію апаратних відмов, особливо тих, які стосуються дисків, а також відновлення після помилок обслуговуючого персоналу або прикладних програм. Подібні засоби повинні із самого початку інтегруватися в архітектуру комплексу. Наприклад, необхідно використати той або інший вид надлишкових дискових масивів. Звичайно, це зробить апаратно-програмне рішення більш дорогим, але натомість вбереже від можливих збитків під час експлуатації.

Найважливіше питання забезпечення високої готовності баз - це зберігання інформації. Всі системи захисту будуть марними, якщо дані буде втрачено. Для збереження інформації застосовуються різні методи. Найпоширеніший метод - це резервне копіювання або архівування баз даних. Архів відображує стан бази даних, що відповідає певному моменту часу. Резервне копіювання логічних журналів транзакцій зберігає файли журналів, заповнені і готові для копіювання. Логічні журнали транзакцій і, відповідно, їхні резервні копії зберігають відомості про дії сервера баз даних, зроблені після архівування або попереднього резервного копіювання. Інтерпретація цих журналів дозволяє відновити базу даних до стану, більш пізнього, ніж момент останньої архівації.

Важливим питанням при розгляді високої готовності системи є цілісність доменів серверів. Домен фактично є одним з елементів системи, який при руйнуванні операційного середовища неможливо відтворити. Це пов'язано з тим, що паролі користувачів відомі тільки їм. При відтворенні домена буде потрібна повна перереєстрація всіх користувачів, що може бути досить проблематично. Цю проблему простіше вирішити шляхом створення резервної копії домена на іншому сервері. У такому випадку навіть при повному руйнуванні операційної системи, або навіть фізично сервера, структуру основних компонентів можна відновити відносно швидко.

При проектуванні і реалізації політики безпеки варто враховувати, що для комерційних організацій потенційні загрози в порядку зниження розмірів збитку розташовуються в такий спосіб: помилки і недогляди обслуговуючого персоналу і користувачів, дії нечесних працівників, вогонь, зумисні дії скривджених працівників, вода, дії сторонніх несанкціонованих осіб.

Підтримка актуальних резервних копій і їхнє зберігання в безпечному місці – найбільш надійний засіб відновлення після крадіжок, пожеж, повеней і інших нещасть. Кластерна організація сервера баз даних важлива в ситуаціях, коли потрібна як дійсно безперервна робота протягом тривалого часу, так і потенційна масштабованість сервера. Захист від сторонніх користувачів може будуватися на основі використання сервера аутентифікації і брандмауера.

Висновки

Основну увагу варто звернути на систематизацію і автоматизацію дій адміністраторів баз даних і SQL-серверів. Але великий відсоток ручної роботи неминуче призведе до

помилок (ненавмисних), які можуть виявитися страшнішими за пожежу. Тому авіапідприємству з розгалуженою корпоративною інформаційною системою ми б рекомендували до використання автоматизовану систему управління і адміністрування прав користувачів, над створенням якої наразі працюють автори статті.

Надійшла 24.05.2007 р.

УДК 004.415 **Готун А.М.**

ВИКОРИСТАННЯ МЕРЕЖІ ІНТЕРНЕТ В ПОЛІТИЧНІЙ КОМУНІКАЦІЇ: ПРОБЛЕМИ КОНТРОЛЮ ТА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Щорічно у світі втрати від несанкціонованого втручання у роботу мереж, крадіжок і витоку інформації подвоюються. У 2004 році вони становили 10,2 млрд. доларів, у 2005-му – біля 20 млрд [1]. Але багато компаній відмовляються розголошувати збитки, пов'язані з втратою або витоком інформації, боячись зіпсувати свій імідж. Насамперед, це стосується соціально-економічної сфери. Не піддаються підрахункам, на жаль, втрати пов'язані з підготовкою і проведенням політичних кампаній. Адже до останнього часу хакерські атаки за замовленням з метою викрадення стратегічно важливої інформації із комп'ютерних мереж конкурентів ставили собі за мету переважно політики. Вони періодично замовляють зламування сайтів один одного, а найбільш гучний випадок – атака на сервер Центрвиборчкому у 2004 році (хоча слідство до цього часу не доказало, що мова йде про хакерів, а не про банальний підкуп адміністратора).

Безперечно, що все більш вагомим фактором розвитку сучасної політики стають нові інформаційно-комунікаційні технології. Глобальний віртуальний простір, а саме мережа Інтернет, є своєрідним викликом традиційним інститутам і механізмам політичного процесу. Глобальність й інтерактивність – найважливіші якісні ознаки нової віртуальної реальності, що не визнає умовностей державного суверенітету, форм політичної участі, ієрархічних структур політичних партій та інших інституціональних суб'єктів політики. Політичні наслідки нових технологій неоднозначні.

З розширенням масового доступу до мережі Інтернет вона почала відігравати все більш помітну роль не тільки у повсякденному житті людей, а й у сучасному політичному процесі. Інтернет сприяє більшій відкритості і транспарентності політичних інститутів і політики в цілому. В мережі з'являється все більша кількість сайтів різних державних органів, партійних структур, чисельних міжнародних неурядових організацій, які містять різноманітну інформацію, що суттєво збільшує політичну поінформованість широких мас. Різноманітні урядові публікації, які раніше були доступними лише небагатьом і тільки номінально подавали суспільну інформацію, з'являючись сьогодні в онлайновому режимі, стають у повному розумінні слова суспільно доступними. Завдяки Інтернету виникають нові, досить ефективні механізми політичної мобілізації громадян. Він виступає, зокрема, як засіб досить оперативної організації і координації дій політичних однодумців, які є прихильниками нетрадиційних соціальних рухів.

Інтернет являє собою надзвичайно потужний глобальний інструмент комунікації, освіти, розваг і інформованості. Але це – всього лише інструмент, значення якого не варто ані недооцінювати, ні ідеалізувати. Сила і характер його впливу залежать від того, ким і заради чого він використовується. Подібно будь-якому іншому інструменту або технологічному засобу, він може бути застосований як для блага так і для шкоди. Він може бути засобом освіти для людини у тій же мірі, що і засобом його розтління.