УДК 681.5.033.2

д.т.н., доц. **Бойченко О.В.** (ОДАТРЯ)
к.військ.н., доц. **Пашков С.О.** (ВІКНУ)
Охрамович Л.В. (ВІКНУ)

РОЗВИТОК ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АВТОМАТИЗОВАНИХ СИСТЕМ УПРАВЛІННЯ

У статті розглянуті проблеми захисту інформаційних ресурсів автоматизованих систем управління (АСУ). Дослідження функціонування сучасних АСУ та засобів інформаційного захисту доводить що, ефективно вирішувати завдання щодо захисту інформації, що циркулює в АСУ, а також забезпечити надійний захист інформаційно-телекомунікаційних систем державних органів від злочинних посягань (у тому числі з-за меж України) можна лише шляхом створення в їх складі комплексних систем захисту інформації, що поєднують правові, організаційні, інженерні заходи, а також технічні і програмні засоби захисту.

Ключові слова: інформаційна безпека, автоматизовані системи управління, засоби захисту.

Вступ та аналіз останніх досліджень і публікацій. Актуальність вирішення проблеми захисту інформаційних ресурсів автоматизованих систем управління (АСУ) обумовлюється зростанням доступу до мереж загального користування окремих категорій протиправно налаштованих категорій громадян, певною вразливістю окремих мереж, зростанням попиту з боку злочинних елементів на здобування або руйнування інформації, що циркулює в спеціальних мережах зв'язку, інформаційних ресурсів (ІР) об'єктів критичної інфраструктури.

Інформаційна безпека є невід'ємним напрямком розбудови інформаційного суспільства, розвиток якого повинен йти не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, але й через глибоке усвідомлення усіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо захисту ІР та забезпечення інформаційної безпеки держави.

Як свідчить досвід [1,2], ефективно вирішувати завдання щодо захисту інформації, що циркулює в АСУ, а також забезпечити надійний захист інформаційно-телекомунікаційних систем державних органів від злочинних посягань (у тому числі з-за меж України) можна лише шляхом створення в їх складі комплексних систем захисту інформації, що поєднують правові, організаційні, інженерні заходи, а також технічні і програмні засоби захисту.

Основна частина. Відомо що, серед внутрішніх факторів, які стають внутрішніми загрозами національній безпеці держави з позиції формування стратегічних напрямків діяльності щодо забезпечення її інформаційної безпеки, є:

− помітне відставання України від провідних держав світу в галузі створення і впровадження сучасних інформаційних технологій, у сфері розвитку індустрії інформаційних послуг та, як наслідок, вимушене широке використання закордонних програмно-технічних засобів обміну інформацією та її захисту при розбудові національної інформаційної інфраструктури. Наслідком такого відставання може стати реалізація стратегій інформаційного протиборства проти України, поява реальної можливості несанкціонованого проникнення в інформаційні системи та бази даних, блокування систем та мереж, особливо тих, що функціонують в інтересах управління державою;

− недостатній рівень захищеності державних ІР, розповсюдження комп'ютерних вірусів, програмних та апаратних закладок спричиняють появу реальної можливості втрати стратегічного важливої інформації, порушення її цілісності та блокування доступу до неї. Крім того, це може призвести до порушення нормального функціонування систем управління об'єктів критичної інфраструктури. Протягом останніх років спостерігається стійка тенденція до різкого збільшення загроз з точки зору кількості спроб

несанкціонованого втручання в роботу інформаційних та телекомунікаційних систем та несанкціонованого доступу (НСД) до інформації, яка в них циркулює, а також появи нових методів та алгоритмів щодо їх здійснення. Зазначене являє собою реальну загрозу національному інформаційному простору України та у разі неприйняття необхідних заходів може призвести у найближчому майбутньому (у тому числі до 2015 року) до втрати державою контролю над частиною її інформаційного простору та, відповідно, неможливості забезпечення прав громадян у цій сфері;

− недостатня узгодженість діяльності державних органів України щодо формування і реалізації єдиної державної політики забезпечення інформаційної безпеки, порушення встановлених режимів функціонування інформаційно-телекомунікаційних систем органів державної влади та місцевого самоврядування, інформаційно-телекомунікаційних систем, які забезпечують потреби оборони та безпеки держави, кредитно-банківської та інших сфер економіки держави, систем управління життєзабезпеченням;

− об'єктивна неспроможність промисловості України задовольнити попит на сучасне комп'ютерне обладнання та обладнання зв'язку сприяє широкому застосуванню закордонних засобів обчислювальної і комунікаційної техніки.

Як свідчить досвід провідних країн світу, ефективна діяльність у сфері забезпечення інформаційної безпеки АСУ повинна проходити шляхом нарощування потужностей тих структур, на які покладено реалізацію державної політики за основними, технологічними її складовими, а саме заходів щодо захисту ІР, захисту інформації, забезпечення безпеки інформаційного обміну.

Це дозволяє не тільки створити додаткові важелі впливу на процеси реалізації державної політики у сфері інформаційної безпеки, але й забезпечити, в умовах подальшої демократизації суспільства, відкритість заходів, що впроваджуються для підтримання та забезпечення інформаційної безпеки особи, суспільства і держави.

Разом з інтенсивним розвитком АСУ все більш актуальною стає проблема забезпечення інформаційної безпеки. Заходи безпеки направлені на запобігання несанкціонованому отриманню інформації, а також фізичного знищення або модифікації конфіденційної інформації.

Аналіз зарубіжних публікацій останніх років показує, що можливості зловживань інформацією, яка передається по каналах зв'язку, розвивалися та удосконалювалися не менш інтенсивно, ніж засоби їх попередження. В такому випадку для захисту інформації потрібна не просто розробка окремих механізмів захисту, а організація комплексу заходів у складі спеціальних засобів і методів з метою запобігання втраті інформації. Зазначене стало базою для заснування сучасної технології захисту інформації в АСУ і в мережах передачі даних.

Дослідження функціонування сучасних АСУ та засобів інформаційного захисту показує, що наявні системи захисту доки не можуть забезпечити збереження достатнього рівня конфіденційності інформаційних ресурсів.

Засобами реалізації загрози розкриття конфіденційної інформації можуть бути НСД до баз даних, а також прослуховування каналів. У будь-якому випадку отримання інформації, що є надбанням деякої особи або групи осіб, іншими особами наносить її власникам істотний збиток.

Компрометація інформації, як правило, реалізується за допомогою внесення несанкціонованих змін до баз даних, внаслідок чого її споживач вимушений або відмовитися від неї, або робити додаткові зусилля для виявлення змін і відновлення дійсних відомостей. У разі використання скомпрометованої інформації споживач наражається на небезпеку прийняття невірних рішень зі всіма наслідками, що з цього витікають.

Несанкціоноване використання ІР, з одного боку, є засобом розкриття або компрометації інформації, а з іншої – має самостійне значення, оскільки, навіть не стосуючись призначеної для користувача або системної інформації, може завдати певного збитку користувачам і адміністрації. Цей збиток може змінюватися в широких межах – від скорочення надходження фінансових коштів до повного виходу комп'ютерної техніки з ладу.

Помилкове використання IP, будучи санкціонованим, проте, може привести до руйнування, розкриття або компрометації вказаних ресурсів. Дана загроза найчастіше є наслідком помилок в програмному забезпеченні.

Несанкціонований обмін інформацією між користувачами може привести до отримання одним з них відомостей, доступ до яких йому заборонений, що по своїх наслідках відповідно розкриттю змісту маркетингової інформації.

Відмова від інформації полягає в невизнанні одержувачем або відправником інформації фактів її отримання або відправки. В умовах маркетингової діяльності це, зокрема, дозволяє одній із сторін розривати укладені фінансові угоди «технічним» шляхом, формально не відмовляючись від них і наносячи тим самим другій стороні значний збиток.

Відмова в обслуговуванні є вельми істотною і поширеною загрозою. Подібна відмова особливо небезпечна в ситуаціях, коли затримка з наданням ресурсів абонентові може привести до тяжких для нього наслідків. Так, відсутність у користувача даних, необхідних для ухвалення рішення, протягом періоду, коли це рішення ще може бути ефективно реалізоване, може стати причиною його нераціональних або навіть антимонопольних дій.

Слід зазначити, що без належної організаційної підтримки програмно-технічних засобів захисту інформації від НСД і точного виконання передбачених проектною документацією процедур, вирішити проблему забезпечення безпеки інформації не вдається.

Тому до основних засобів захисту, що використовуються для створення механізму захисту АСУ, насамперед відносяться програмні засоби – це програмне забезпечення, спеціально призначене для виконання функцій захисту інформації.

Контроль цілісності програмного забезпечення проводиться за допомогою зовнішніх засобів (програм контролю цілісності) і внутрішніх засобів (вбудованих в саму програму). Контроль цілісності програм зовнішніми засобами виконується при старті системи і полягає в порівнянні контрольних сум окремих блоків програм з їх еталонними сумами. Контроль цілісності програм внутрішніми засобами виконується при кожному запуску програми на виконання і полягає в порівнянні контрольних сум окремих блоків програм з їх еталонними сумами. Такий контроль використовується в програмах для внутрішнього користування.

Висновки. Ефективним шляхом підвищення ефективності функціонування системи інформаційної безпеки АСУ є застосування системного підходу до проектування стійкого програмного забезпечення інформаційної системи, що дозволяє створити умови для розроблення специфікацій, що базуються на визнанні факту можливості виникнення перекручувань у роботі обчислювальних засобів і програмних засобів; розроблення програмних засобів контролю і виправлення помилок у роботі обчислювальних засобів; розроблення структури програмного забезпечення, що використовує зворотний зв'язок між підпорядкованим і верхнім рівнем, а також розміщення засобів контролю виконання програмного забезпечення відповідно до рівнів ієрархії в системі.

ЛІТЕРАТУРА:

1. Бойченко О.В., Лєнков О.С., Охрамович Л.В. Методика оцінки захищеності інформаційних ресурсів автоматизованих систем управління / О.В. Бойченко, О.С. Лєнков, Л.В. Охрамович // Збірник наукових праць Військового інституту Київського національного університету імені Тараса Шевченка. – 2013. – № 44. – С.79 – 81.

2. Бойченко О.В. Оцінка якості та оптимізація функціонування інформаційних систем / О.В. Бойченко // Захист інформації. – К.: НАУ, 2011. – № 2 (51). – С.105-107.

3. Бойченко О.В. Структурне проектування програмного забезпечення складних інформаційних систем реального часу / О.В. Бойченко С.В. Лєнков, П.А. Шкуліпа // Сучасна спеціальна техніка. – К.: ДНДІ МВС України, 2012. – № 4(31). – С. 92-97.

Рецензент: д.т.н., проф. Лєнков С.В., начальник науково-дослідного центру Військового інституту Київського національного університету імені Тараса Шевченка

д.т.н., доц. Бойченко О.В., к.воен.н., доц. Пашков С.АО., Охрамович Л.В.

РАЗВИТИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ

В статье рассмотрены проблемы защиты информационных ресурсов автоматизированных систем управления (АСУ). Исследования функционирования современных АСУ и средств информационной защиты доказывает что, эффективно решать задачи относительно защиты информации, которая циркулирует в АСУ, а также обеспечить надежную защиту информационно-телекомуникационных систем государственных органов от преступных посягательств (в том числе из-за пределов Украины) можно лишь путем создания в их составе комплексных систем защиты информации, которые объединяют правовые, организационные, инженерные меры, а также техническое и программное средства защиты.

Ключевые слова: информационная безопасность, автоматизированные системы управления, средства защиты.

O. Boychenko, S. Pashkov, L. Ohramovich

DEVELOPMENT INFORMATION SECURITY AUTOMATED CONTROL SYSTEMS

The article discusses the problem of protecting information resources of automated control systems (ACS). Research and functioning of modern automated information security software proves that effectively meet the challenges regarding the protection of information that circulates in the ACS , as well as provide reliable protection of information and telecommunication systems of state authorities against criminal offenses (including from outside Ukraine) is possible only by establishment in their part of integrated security systems that combine legal, organizational and engineering measures, as well as hardware and software protection .

Keywords: information security, automated control systems, means of defense.