УДК 004.056:004.031.4

АКТУАЛІЗАЦІЯ ІНФОРМАЦІЇ З ОБМЕЖЕНИМ ДОСТУПОМ У МЕРЕЖНИХ РЕСУРСАХ

Денис Самойленко

Для включення інформації з обмеженим доступом (ІзОД) до мережного інформаційного ресурсу (МІР), розміщеного у публічній, глобальній чи відкритій мережі іншого типу, необхідно вживати заходів з її додаткового захисту. Існуючі вимоги забороняють існування ІзОД у відкритих каналах зв'язку, проте не обмежують її існування у складі МІР – програмному коді, базах даних, тощо. У статті запропоновано схему взаємодії користувача з мережним інформаційним ресурсом для безпечної актуалізації ІзОД з відмовою від її існування у відкритому вигляді на усіх ланках схеми, окрім останньої. Запропоновано розділення автентифікаційних даних користувача на дві категорії, виділення трьох архітектурних шарів серверної частини та реалізацію контролю цілісності інформаційного обмінного процесу шляхом розподілу загального секрету за різними структурними елементами. Реалізація запропонованих заходів дозволить покращити інформаційну безпеку публічних МІР, особливо тих, що містять ІзОД.

***Ключові слова**: інформаційна безпека, мережні ресурси, захист даних, ІзОД.*

Постановка проблеми у загальному вигляді. Збереження інформації з обмеженим доступом (ІзОД) у мережних інформаційних ресурсах (МІР), а також її актуалізація для користувачів вимагає дотримання ряду вимог інформаційної безпеки. Як правило, мова іде про криптографічне перетворення (шифрування) ІзОД на всіх етапах її «руху» до користувача. Причому шифрування здійснюється різними паролями для різних користувачів. Сама ж ІзОД, як правило, існує у базах даних МІР у неперетвореному вигляді.

Тенденція до розширення функціональності сучасних МІР неодмінно відбивається на ускладнені їх внутрішньої будови і, як наслідок, на збільшенні їх вразливості до зовнішнього впливу. Атаки, спрямовані на підміну транзитних вузлів, можуть спричинити витік ІзОД на етапі її перекодування для передачі користувачу. Спроба перехоплення автентифікаційних даних, що передаються від клієнта, можуть призвести до несанкціонованого доступу (НСД) нелегальних користувачів. Відповідно, додатковою задачею виступає контроль цілісності усієї ланки актуалізації ІзОД – від бази даних (БД) до візуальної складової клієнтської частини МІР.

У разі успішної атаки чи НСД виникає додаткове питання щодо особливостей розподілу відповідальності за вчинені дії та їх наслідки. Особливості правового регулювання зазначеного питання також вимагають корегування підходів до забезпечення гарантованого транзиту ІзОД, оскільки різні ланки обмінного процесу можуть бути у власності різних суб'єктів мережного трафіку у т.ч. іноземного підпорядкування. Актуальність поставлених задач встановлюється положеннями Доктрини інформаційної безпеки України та Закону України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки».

Аналіз останніх досліджень і публікацій. Основні принципи класифікації інформації, вимоги до її захисту, розмежування чи гарантування доступу до неї а також відповідальність за забезпечення захисту встановлюються законами та нормативними актами України [1-4]. Ключовими для детального розгляду в рамках поточного дослідження можна визначити наступні вимоги.

Головною вимогою до існування ІзОД є впровадження комплексної системи захисту інформації (КСЗІ) [1: ст. 8], забезпечення вільного доступу до публічної (відкритої) інформації [2], передача ІзОД з однієї системи до іншої виключно у зашифрованому вигляді [3: п. 13], захист об'єктів від несанкціонованого ознайомлення з інформацією, що міститься в них, під час їх експорту/імпорту через незахищене середовище [4: п. 7.2.2]. Також слід відзначити, що положеннями тих самих документів відповідальність за забезпечення захисту інформації покладається на власника системи [1: ст. 9; 3: п. 17].

Відокремлення складових елементів, що є безпосередніми об'єктами захисту становить окрему задачу. Загальна парадигма захисту інформації, запропонована у роботі [5], дозволила її автору виділити та сформулювати означення «середовища впливу» як розширену концепцію

середовища поширення інформації. Розширення переліку об'єктів захисту, зокрема тих, що стосуються передачі інформації, проаналізовано у роботі [6]. Висновки реферованих робіт безпосередньо можуть бути враховані у задачах захисту МІР при створенні топографічної моделі процесу інформаційного обміну.

Аналіз окремих норм законодавства, проведений у роботі [7], дозволив автору відзначити певні недосконалості, зокрема, у означеннях суб'єктів інформаційних відносин. З метою чіткого розмежування відповідальності, а також задля покращення показників безпеки МІР вбачається за доцільне реалізацію ряду додаткових заходів щодо логічного окреслення меж відповідальності на усіх етапах передавання інформації.

Метою даної роботи є формування схеми актуалізації ІзОД у розумінні її передачі від БД до користувача з урахуванням нормативних вимог та трансформації сучасних підходів до захисту інформації.

Виклад основного матеріалу. При введені у дію МІР, як програмно-апаратного комплексу, досить поширеною є ситуація, коли власники сервера, як інформаційно-телекомунікаційної системи (ІТС) та МІР, як програмного продукту, розрізняються між собою. У такому разі природно можна очікувати від них взаємного обмеження доступу до своєї матеріальної та інтелектуальної власності.

Однак, інформаційна безпека МІР не дозволяє простого однозначного поділу: недостатня захищеність ІТС може погіршити функціонування МІР, так само, як і «дірки» у захисті МІР можуть надати зловмиснику можливість нелегального впливу на ІТС шляхом «зламу» захисної системи МІР. Більш того, розмиваються межі відповідальності за обмінні процеси, оскільки функціонування файлової системи та системи управління базами даних забезпечується ІТС, хоча самі файли та інформація у БД є власністю МІР. Виявити, через який недолік стався витік інформації з фалу чи БД, як правило, досить складно, якщо взагалі можливо.

Розділення відповідальності за захист інформації, очевидно, має віддзеркалювати поділ власності. З іншого боку, природній сумнів у декларованій «ідеальності» захисту ІТС та намагання відмовитись від сподівань на надійність ІТС (фільтрацію пакетів, стабільність файлової системи та серверу бази даних, тощо) має спонукати розробника МІР вживати заходів з покращення показників безпеки шляхом їх реалізації у складі самого ресурсу.

У такому разі, достатньо логічним вбачається впровадження розглянутого вище терміну середовища впливу [5] у задачі захисту МІР як узагальнення під однією назвою усіх процесів, пов'язаних з актуалізацією ІзОД. Під об'єктами захисту при цьому слід вважати дані не лише у незахищених обмінних каналах, а й на усіх стадіях програмного перетворення чи збереження.

Потенційна вразливість файлової системи ІТС та системи управління базами даних (СУБД) має посилити вимогу заборони на використання незашифрованої ІзОД при міжсистемному обміні до повної відмови від її існування у МІР чи ІТС у відкритому вигляді.

У відповідності до правил побудови криптографічного захисту, відомих також як правила Керкгофса [напр. 8], його головна надійність має забезпечуватись паролем. Оскільки пароль має бути відомим лише легальному користувачу, необхідне забезпечення умов, за яких актуалізація ІзОД можлива лише за його безпосередньої участі. Будь-який інший спосіб вилучення ІзОД зі складу МІР чи ІТС (з файлів, програмного коду чи БД) має супроводжуватись обчислювальною працеємністю, не гіршою за повний криптоперебір.

З метою уникнення вразливості до атак підміни, які базуються на підборі паролю через аналіз кількох перехоплених пакетів від користувача [9], доцільно використовувати тимчасові (сеансові) ключі, що змінюються при кожному обміні між користувачем і МІР та забезпечують при шифруванні непередбачувану трансформацію автентифікаційних даних користувача [10].

Складність сучасних МІР, розподіленість їх апаратних та обчислювальних складових супроводжуються появою атак вторгнення, за яких нелегальних мережний вузол намагається звертатись до інформаційної БД МІР від імені її легального віддаленого вузла. Такі атаки підвищують вимоги до контролю цілісності інформаційних процесів, особливо при передачі ІзОД.

Як один з заходів покращення контролю цілісності можна запропонувати розподіл загального секрету (пароля) на декілька частин, що зберігаються у різних складових елементах (вузлах)

МІР. При цьому доступ до ІзОД має додатково обмежуватись контролем відновлення повного секрету.

Взявши до уваги те, що програмний код МІР розділюється на клієнтську і серверну частини, причому, останню рекомендовано реалізовувати за шаруватою архітектурою відповідно до вимог стандарту [11], з урахуванням висловлених зауважень та пропозицій схема взаємодії користувача і МІР при актуалізації ІзОД виглядатиме наступним чином.

1. Користувач звертається до МІР, набираючи його мережну адресу.

2. Сервер, отримавши дані без параметрів, на рівні узгоджувального архітектурного шару (УШ) встановлює сеансові параметри: M (модуль групи) і G (твірний елемент), генерує випадкове число A, обчислює $X = G^A \pmod M$ і включає величини M, G, X до складу html коду стартової сторінки, що передається клієнту.

3. Користувач вводить у завантаженій сторінці автентифікаційні дані C (логін, пароль, код та рівень доступу, тощо) та ініціює спробу отримання доступу (входу) до МІР.

4. Активна складова клієнтської частини МІР генерує випадкове число B, обчислює $Y = G^{Bo} (\mathrm{mod}\, M)$, $K = X^B (\mathrm{mod}\, M)$, шифрує за допомогою ключа K введені дані $D=F(C,K)$ та передає на сервер параметри Y та D.

5.1. Сервер, на рівні УШ обчислює $K = Y^A (\mathrm{mod}\, M)$, дешифрує передані дані $C = F^1(D, K)$ і передає їх на рівень автентифікаційного шару (АШ), додаючи частину секрету, що зберігається на даному шарі.

5.2. АШ перевіряє коректність даних, використовуючи власну БД. За умови підтвердження права доступу, передає запит до шару доступу (ШД), транслюючи секрет АШ та додаючи власну частину секрету.

5.3. ШД об'єднує усі частини секрету (користувача, АШ, ШД і власну), перевіряє його коректність. За позитивного результату перевірки, вилучає з власної БД ІзОД (у зашифрованому вигляді) I_S і передає її як відповідь.

5.4. АШ транслює I_S до УШ.

5.5. УШ шифрує дані ключем K: $I_{SK}=F(Is, K)$, встановлює нові значення A, M, G, X та передає клієнту у складі html відповіді параметри I_{SK}, M, G, X.

6. Клієнтська частина дешифрує отримані дані за ключем K: $I_S=F^{-1}(I_{SK}, K)$, дешифрує результат з використанням пароля, введеного клієнтом $I=F^{-1}(I_S, C)$. За вірного введення паролю користувач отримає ІзОД у відкритому вигляді I. При наступній комунікації повторюються пп. 4-6.

У схемі використані наступні припущення.

– Узгодження сеансового ключа К (пп.1-4) відбувається за протоколом Діффі-Хеллмана на дискретному логарифмі. Окремі деталі його реалізації для клієнт-серверної технології обміну за протоколом HTTP описано у [10]. Можливе використання довільного подібного протоколу із заданою технічними умовами на МІР криптографічною стійкістю чи швидкодією за умови наявності обмежень на обчислювальну потужність комунікаційних пристроїв (наприклад, для роботи зі смартфонами чи комунікаторами). Слід зазначити, що за зазначеним протоколом забезпечується убезпечення автентифікаційних даних користувача МІР. Захист ІзОД реалізується додатково, відповідно, до вибору протоколу узгодження вимоги можуть бути послаблені.

– У архітектурі серверної частини виділено три шари. Така кількість вбачається мінімальною для логічного відокремлення задач узгодження сеансових ключів, перевірки автентифікаційних даних користувача та отримання доступу до БД, що зберігає ІзОД. За наявності більшої кількості шарів, їх функція для «руху» ІзОД буде просто трансляційною, можливо, з додатковим контролем цілісності через додавання власних частин секрету за тим самим принципом, що і при русі в трьох наведених архітектурних шарах.

– Функція шифрування F може бути вибрана як з стандартизованих криптоалгоритмів, так і реалізована у авторський спосіб. Використання однакових F для різних задач перетворень даних застосовано для спрощення формулювання комунікаційної схеми, проте, цілком допускається використання множини F як у різних серверних архітектурних шарах, так і у різних етапах оброблення даних клієнтською частиною (п. 6).

– Автентифікаційні дані користувача складаються як з логіну-паролю для входу до МІР, так і з паролю для дешифрування переданої ІзОД. Дані для входу передаються від клієнта до сервера (у шифрованому вигляді), другий пароль зберігається виключно у користувача і саме його таємність визначатиме надійність усієї актуалізації ІзОД.

Наведена схема забезпечує захист ІзОД від безпосереднього ознайомлення на усіх етапах руху від сервера до клієнта. Частина клієнтського паролю, що не передається жодним каналом, унеможливлює відновлення ІзОД через її перехоплення у каналах зв'язку і, навіть, при дискредитації СУБД, файлової системи сервера чи викрадення усіх програмних кодів МІР.

Використання сеансових ключів забезпечує стійкість схеми до атак з накопиченням переданих пакетів. У будь-якому разі, з перехоплених пакетів можливе відновлення лише автентифікаційного паролю користувача. Для одержання ІзОД у відкритому вигляді необхідна додаткова частина паролю, яка, як зазначалась вище, не передається при комунікаціях.

Криптографічна стійкість щодо перехоплення автентифікаційних даних забезпечується обраним протоколом асиметричної криптографії і може бути встановлена на довільному рівні, відповідно до вимог, що висуваються при створенні МІР.

Висновки. Розглянуто основні вимоги до роботи з ІзОД у відкритих мережах та принципи поділу відповідальності за їх порушення.

Запропоновано узагальнити вимогу до шифрування ІзОД на усі види зберігання чи перетворення, а не лише на трансляцію незахищеними каналами. З метою гарантування участі легального користувача у процесі отримання ІзОД пропонується розділення його паролю на дві частини.

Наведена структурна схема актуалізації ІзОД у відкритій мережі. У схему впроваджено принцип сеансових ключів та контролю цілісності через розподіл секрету на складові частини.

Перспективи подальших розвідок вбачаються у створенні програмної реалізації схеми та її випробувані за різних практичних умов.

ЛІТЕРАТУРА

[1]. Про захист інформації в інформаційно-телекомунікаційних системах: Закон України від 05.07.1994 № 80/94-вр [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua /laws / show/80/94-%D0%B2%D1%80

[2]. Про доступ до публічної інформації: закон України від 13.01.2011 № 2939–VI [Електронний ресурс]. – Режим доступу: http://zakon4.rada.gov.ua/ laws / show/2939-17

[3]. Про затвердження Правил забезпечення захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах: Постанова Кабінету Міністрів України від 29.03.2006 № 373 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua / laws / show/373-2006-%D0%BF

[4]. НД ТЗІ 2.5-010-2003 Вимоги до захисту інформації WEB - сторінки від несанкціонованого доступу. [Текст] / НД ТЗІ, затверджений наказом ДСТСЗІ СБ України від 02.04.2003 № 33.

[5]. Громико І. Загальна парадигма захисту інформації: визначення термінів [Текст] / Ігор Громико // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2006. – вип. 2 (13). – с. 130-137.

[6]. Василюк В. Об'єкти захисту інформації. методи та засоби захисту інформації [Текст] / Володимир Василюк // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, 2006. – вип. 2 (13). – с. 88-102.

[7]. Тимченко Н. М. Правовий механізм доступу до публічної інформації: сучасний стан та перспективи [Електронний ресурс] / Н. М. Тимченко. – Режим доступу: http://lib.uabs.edu.ua/library / P_Visnik/Numbers/1_6_2012/06_02_05.pdf

[8]. Климентов В.В. Криптосистема с «виртуальным ключом» [Текст] / Климентов В.В., Трощило А.С. // Захист інформації, 2010. – №1 с. 89-94.

[9]. Pei, D. Y. Authentication Schemes. [Електронний ресурс] / D. Y. Pei / Singapore: Institute for Mathematical Sciences. – 2001. – 36 p. Режим доступу: www2.ims.nus.edu.sg/ Programs/ coding/ files/dypei.ps

[10]. Самойленко Д. М. Комплексна система захисту інформаційного ресурсу Інформаційна безпека, 2013. – № 1 (9). с. 147-151 (ISSN 2224-9613)

[11]. ISO/IEC 7498-2:1989(E) Information technology – Open Systems Interconnection – Basic Reference Model: Security Architecture. [Text] / International Organization for Standardization, 1989. First edition. / Switzerland: ISO/IEC Copyright Office. – 34 p.

REFERENCES

[1]. UKRAINE (1994) On information protection in information-communication systems [Online] Laws of Ukraine. Available from http://zakon4.rada.gov.ua / laws/show/80/94-%D0%B2%D1%80 [Accessed: 1st March 2014]

[2]. UKRAINE (2011) On access for public information [Online] Laws of Ukraine. Available from http://zakon4.rada.gov.ua/laws/show/2939-17 [Accessed: 1st March 2014]

[3]. UKRAINE (2006) Rules of information protection in information, communication and information-communication systems [Online] Laws of Ukraine. Available from http: // zakon2.rada.gov.ua/

laws/show/373-2006-%D0%BF [Accessed: 1st March 2014]
[4]. UKRAINE Security Service of Ukraine (2004) Requirements for information security of WEB-page from unauthorized access (2.5-010-2003). Kyiv: SSU
[5]. Gromyko I. (2006) «General paradigm of information protection: terms» *Law, normative and metrological provision of information protection system in Ukraine*, No. 2 (13), pp. 130-137.
[6]. Vasylyuk V. (2006) «Objects of information protection: methods and resources for protection of data» *Law, normative and metrological provision of information protection system in Ukraine*, No. 2 (13), pp. 88-102.
[7]. Tymchenko N. M. (2012) «Law mechanism of public information access: modern state and perspectives». [Online] Electronic library Available from http://lib.uabs.edu.ua/library/P_Visnik/Numbers/1_6_2012/06_02_05.pdf [Accessed: 1st March 2014]
[8]. Klimentov V.V., Troshilo A.S. (2010) «Cryptosystem with «virtual key»» *Information protection,* No 1, pp. 89-94.
[9]. Pei, D. Y. (2001) Authentication Schemes. [Online] Singapore: Institute for Mathematical Sciences. Available from: www2.ims.nus.edu.sg/ Programs/ coding/files/dypei.ps [Accessed: 1st March 2014]
[10]. Samoilenko D.M. (2013) «Complex protection system in information resource» *Information security* No. 1 (9), pp. 147-151 (ISSN 2224-9613)
[11]. ISO/IEC 7498-2:1989(E) Information technology – Open Systems Interconnection – Basic Reference Model: Security Architecture. First edition: Switzerland: ISO/IEC Copyright Office. – 34 p.

АКТУАЛИЗАЦИЯ ИНФОРМАЦИИ С ОГРАНИЧЕННЫМ ДОСТУПОМ В СЕТЕВЫХ РЕСУРСАХ

Для включения информации с ограниченным доступом (ИсОД) в сетевой информационный ресурс (СИР), размещенный в публичной, глобальной или открытой сети иного типа, необходимо проведение мероприятий по ее дополнительной защите. Существующие требования запрещают существование ИсОД в открытых каналах связи, но не ограничивают ее существование в составе СИР – в программном коде, базах данных и т.п. В статье предложена схема взаимодействия пользователя и сетевого информационного ресурса для безопасной актуализации ИсОД с отказом от ее существования в открытом виде на всех этапах схемы, кроме последнего. Предложено разделение аутентификационных данных пользователя на две категории, выделение трех архитектурных слоев серверной части и реализацию контроля целостности информационного обменного процесса путем разделения общего секрета по различным структурным элементам. Реализация предложенных средств позволит улучшить информационную безопасность публичных СИР, особенно тех, которые содержат ИсОД.
Ключевые слова: информационная безопасность, www-ресурс, защита данных ИсОД

RESTRICTED ACCESS INFORMATION ACTUALIZATION IN NETWORK RESOURCES

For including of restricted access information (RAI) in network information resource (NIR) especially for such placed in public, global and other open networks it is necessary to organize additional security actions. Existing requirements prohibit RAI transfer through the open channels, but state no limitations for RAI placing in NIR parts – program codes, files, databases etc. In the present work the user and network resource interconnection scheme is proposed for restricted access information actualization. RAI does not exist in open form in every part of scheme, except the last one – visualization. Authentic user's data is proposed to be divided onto two categories. Server part is constructed from three architecture layers. Integrity control is realized with secret distribution by different structural elements. Realization of the proposed scheme allows increasing of public NIR information security especially with RAI.
Keywords: information security, network resource, data protection, spoof action, restricted access information.

Самойленко Денис Миколайович, кандидат фізико-математичних наук, доцент, доцент кафедри електрообладнання суден та інформаційної безпеки. Національний університет кораблебудування імені адмірала Макарова.
E-mail: DenNikSam@gmail.com
Самойленко Денис Николаевич, кандидат физико-математических наук, доцент, доцент кафедры электрооборудования суден и информационной безопасности. Национальный университет кораблестроения имени адмирала Макарова.
Samoilenko Denys, PhD, docent of Ship Electrical Equipment and Information Security Department, National University of Shipbuilding after Admiral Makarov.