собі не тільки позитивні риси, а й потенційні та вже реальні загрози. Усунення цих загроз традиційними методами навряд чи є скільки-небудь можливим і вимагає нових системних підходів, адаптації усієї системи державного управління до нової суспільної ситуації.

III Висновки

Узагальнюючи викладене, можна зробити висновки про те, що існування віртуальних спільнот, побудованих шляхом використання сучасних телекомунікаційних технологій є суттєвим чинником, що впливає на національну та міжнародну безпеку. Формування таких спільнот обумовлено як розширенням інформаційної сфери, залученням до неї традиційних акторів, так і диверсифікацією активності в рамках кіберпростору. Діяльність зазначених віртуальних акторів має виражений транснаціональний характер і, з одного боку, виражає певні законні інтереси громадськості, а з іншого – несе у собі певні загрози та виклики, що мають враховуватися при напрацюванні систем та заходів забезпечення інформаційної безпеки. З іншого боку, можна передбачити розширення сфери впливу таких структур, що відіграватимуть все більшу роль у формуванні не лише інформаційного середовища, а й широкому спектрі процесів суспільного життя.

Література: ***1.*** *Jopling. Information and National Security.171 CDS 11 E: Draft General Report. General Rapporteur: (United Kingdom). – 01. 06. 2011 [Електронний ресурс]. Режим доступу: http://www.nato-pa.int.* ***2.*** *Denning E. D. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. Georgetown University [Електронний ресурс]. Режим доступу: http://www.iwar.org.uk/ cyberterror/resources/denning.htm.* ***3.*** *Arquilla J., Ronfeldt D. Networks and Netwars. The Future of Terror, Crime, and Militancy. – 2001 [Електронний ресурс]. Режим доступу: www.rand.org.* ***4.*** *Norton Q. Anonymous Skeptical of Proposed Attack on Zetas Drug Cartel. – October 31, 2011 [Електронний ресурс]. Режим доступу: www.wired.com.* ***5.*** *Mexico: Video threatens to disclose Zetas allies : Associated Press – 31.10.2011 [Електронний ресурс]. Режим доступу: www.ap.org.* ***6.*** *John P. M. Jr. Anonymous Takes On Mexican Drug Cartel : PCWorld. – 30. 10. 2011 [Електронний ресурс]. Режим доступу: www.pcworld.com.* ***7.*** *Anonymous: Борьба с детской порнографией – 09. 11. 2011 [Електронний ресурс]. Режим доступу: http://it-sektor.ru.* ***8.*** *Shane S. F.B.I. Admits Hacker Group's Eavesdropping. – 03. 02. 2012 [Електронний ресурс]. Режим доступу: http://www.nytimes.com.* ***9.*** *Heylighen, F. & Bollen J. The World-Wide Web as a Super – Brain: from metafor to model, in: Cybernetics and Systems 96, R. Trappl (ed.), (Austrian Society for Cybernetics, 1996, p. 917–922.* ***10.*** *Heylighen, F . Bootstrapping knowledge representations: from entailment meshes via semantic nets to learning webs. – International Journal of Human-Computer Studies, 1997.* ***11.*** *Казанський А. Б. Модели организационно замкнутых систем и контуры развития новых подходов в области искусственного интеллекта и когнитивной науки [Електронний ресурс]. Режим доступу: spkurdyumov.narod.ru/kazanskiy.html*

УДК 621.391

МОДЕЛЬ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ БАЗ ДАННЫХ В ОРГАНИЗАЦИЯХ, ИСПОЛЬЗУЮЩИХ СВЕДЕНИЯ, СОДЕРЖАЩИЕ ГОСУДАРСТВЕННУЮ ТАЙНУ

Давуд Рустамов, Мирза Рзаев
Министерство Национальной Безопасности Азербайджанской Республики

Анотація: **Запропонована модель забезпечення безпеки реляційних баз даних (РБД) відомостей, що містять державну таємницю. Такі типи баз потребують особливого підходу до забезпечення їх безпеки. Рішення питання про визначення грифа секретності документів, тобто розподіл інформації за категоріями конфіденційності, а також розподіл користувачів на групи з різними рівнями доступу і обмеженнями в доступі до електронних документів, що визначається структурою організації і штатною структурою подрозділів (начальники, заступники, рядові службовці, і т. п.), свідчать про актуальність методики, що запропонована авторами.**

Summary: **Offered model of providing of safety of relyaciynikh bases of these (RBD) information, that mistyat'derzhavnu secret. Such types of bases need the special going near providing of their safety. Decision of question about determination of vulture of secrecy of documents, that distributing of information is after the categories of confidentiality, and also distributing of users on groups with the different levels of access and obmezheniyami in access to the electronic documents, that is determined the structure of organization and regular structure of podrozdiliv (chiefs, deputies, ordinary office workers, and others like that), testify to actuality of method which is offered authors.**

Ключові слова: **Безпека баз даних, відомості, що містять державну таємницю.**

I Введение

Предлагаемая модель обеспечения безопасности реляционных баз данных (РБД) сведений, содержащих государственную тайну, состоит из двух частей:

1. управление доступом к РБД по архитектуре multi-level system (MLS)[3];
2. контроль деятельности пользователей, получивших доступ к РБД.

Метод управления доступом представлен как в формальном, так и в схематическом виде. Контроль всех процессов над данными и их запись в структурированной форме позволяет применять различные методы их анализа (включая методы data mining и т. д.).

Основная цель предлагаемой модели безопасности – улучшение формы управления доступом к базам данных с информацией, классифицируемой как государственная тайна, и контроль всех действий (ввод, редактирование, удаление, и т. д.), производимых над информацией. Данная модель позволяет перекрыть большинство уязвимых, с точки зрения несанкционированного доступа и изменения информации, точек баз данных.

II Метод управления доступом к реляционным базам данных сведений, содержащих государственную тайну

Рассматриваемая ниже модель опирается на модель безопасности BPL (модель Bel-LaPadula), предлагаемой в [1, 2], согласно которой, управление доступом в систему формально можно представить в виде:

$$F : U \times D \rightarrow R \qquad (1)$$

где U – конечное множество пользователей СУБД; D – конечное множество хранимых в РБД документов; R – конечное множество прав доступа конкретного пользователя к конкретному документу; F – отображение, действующее в пространстве описанных выше множеств.

В предлагаемой системе проверки доступа к БД сведений, содержащих государственную тайну, предлагается трехэтапный процесс определения допустимого уровня работы пользователей с документами. Данный процесс представлен на рисунке 1 в виде блок-схемы.

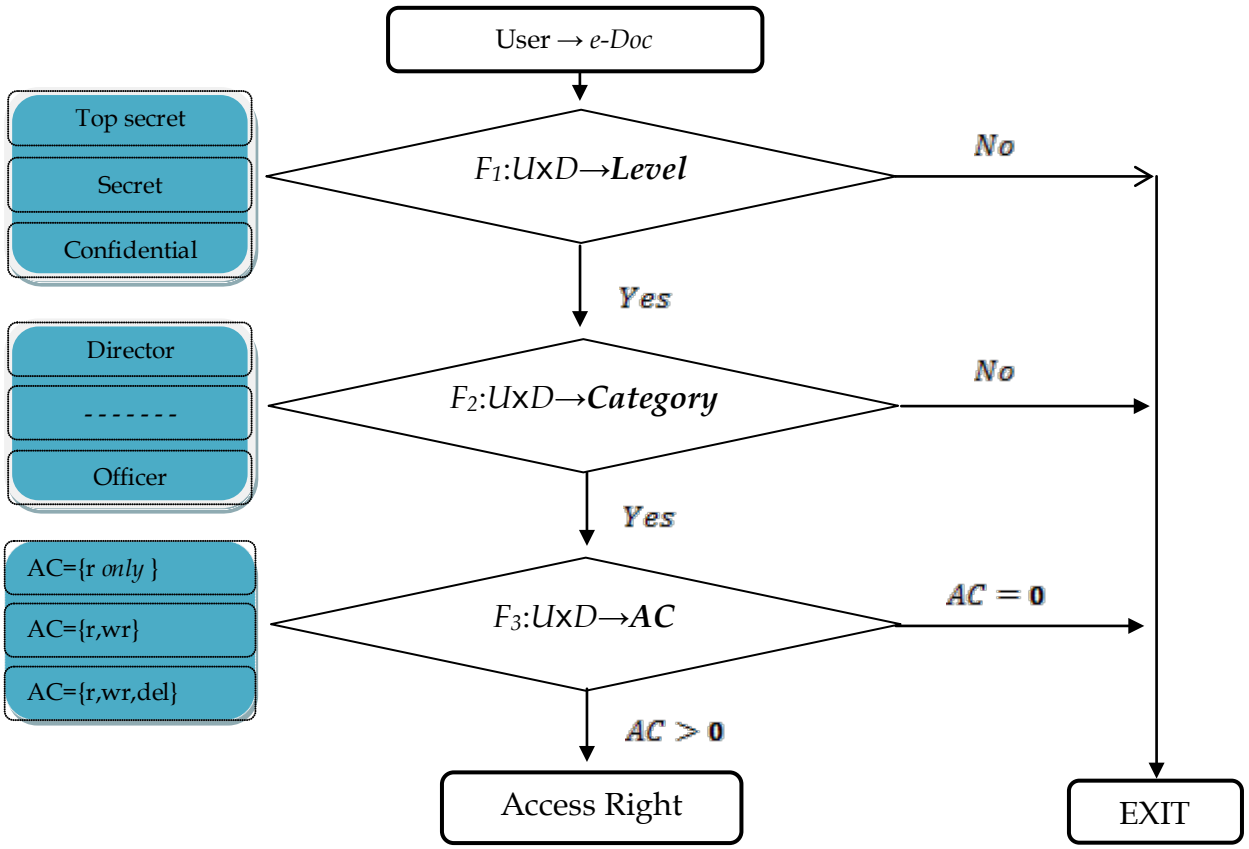

Рисунок. 1 – Блок-схема управления доступом к реляционным базам данных

Согласно данной схеме, отображение F из (1) представлено в виде 3-х последовательных вспомогательных отображений F_1, F_2, F_3, определяющих отдельные стадии проверки доступа к БД сведений, содержащих государственную тайну:

1. $F_1 : U \times D \to Level$ – проверка уровня доступа к секретной информации, иначе говоря, пересечение уровней доступа пользователя БД с грифом секретности документа (конфиденциально, секретно, сов. секретно, и т. д.);
2. $F_2 : U \times D \to Category$ – проверка уровня доступа согласно штатной структуре (или иной подобной) подразделения, где работает пользователь;
3. $F_3 : U \times D \to AC$ – код доступа пользователя к документу (только для чтения, возможность редактирования, удаления, распечатка и т. д.)

Введем в рассмотрение вспомогательные таблицы контроля уровня доступа:

$$\text{Users}(\text{User\_Id}, \text{User\_Level}, \text{User\_Category}) \text{ – множество } U, \quad (2)$$

$$\text{Documents}(\text{Doc\_Id}, \text{Doc\_Level}, \text{Doc\_Category}) \text{ – множество } D, \quad (3)$$

$$\text{Access}(\text{User\_Id}, \text{Doc\_Id}, \text{AC}) \text{ – множество } R. \quad (4)$$

Тогда, проверка доступа пользователя к документу начинается с сопоставления $\text{User\_Level} \Leftrightarrow \text{Doc\_Level}$ из (2) и (3). В случаи успеха, происходит проверка $\text{User\_Category} \Leftrightarrow \text{Doc\_Category}$. Последний этап проверки – вычисляется согласно (4) конкретный код доступа пользователя к документу. На любой стадии проверок пользователю может быть дан отказ в доступе к конкретному документу.

Следует отметить, что приведенная выше схема наиболее удобна для использования в военных организациях, с их сложной структурой прав доступа к секретным документам, т. к. легко можно учесть такие параметры, как гриф секретности, структурную организацию подразделений, должностную структуру и т. д.

III Контроль деятельности пользователей РБД

Рассматриваемый метод контроля деятельности пользователей баз данных является дополнением к приведенному выше методу контроля доступа в плане выявления нештатного обращения с данными тех, кто прошел законную аутентификацию и получил тот или иной уровень доступа к документам.

Как и выше, введем условные обозначения: U – конечное множество пользователей СУБД; D – конечное множество хранимых в РБД документов; OP – конечное множество операций, производимых пользователями над документами (ввод, редактирование, удаление и т. д.).

Учитывая отношения между отмеченными множествами легко видеть справедливость следующих утверждений:

1) если справедливо соотношение (1) и процесс проверки согласно представленной выше схеме завершен успешно, то деятельность пользователей, прошедших аутентификацию, можно отследить при помощи некоторого отображения:

$$G_1 : U \times OP \to D, \quad (5)$$

иначе говоря, можно определить множество документов, над которыми конкретные пользователи выполняли те, или иные операции;

2) если справедливо соотношение (1), а процесс проверки по известной схеме завершен успешно, то множество пользователей, совершивших определенные действия над документами, определяется при помощи некоторого отображения:

$$G_2 : D \times OP \to U \quad (6)$$

т. е., можно выявить всех пользователей, использовавших в своей работе конкретные документы.

На практике отображения (5), (6) можно построить с использованием вспомогательных системных таблиц, заполнение которых осуществляется исключительно на уровне самой СУБД с помощью набора триггеров. В этих таблицах отмечаются идентификаторы пользователей и документов, с которыми они работали, тип операций, дата проведения операции, старые и новые значения измененных данных.

Анализ данных таблиц позволяет определить все манипуляции пользователей над документами, выявить активность пользователей, сферу их интересов, а также те или иные тенденции их деятельности и т. д.

Литература: ***1*** *Jensen C., et. al. "SDDM: A prototype of a distributed architecture for database security" Proceedings of Conference on Data Engineering,1989.* ***2.*** *Zhao Jia, Liu Ji-qiang, Chen Jing. A Multi-Level Security model Based on Trusted Computing / I International Symposium on Data, Privacy and E-Commerce / 2007 IEEE (DOI 10.1109/ISDPE.2007.71).* ***3.*** *"Formal Models For Computer Security", Carl E. Landwehr, Code 7593, Naval Research Laboratory, Washington D C. 20375, Received November 1980, final revision accepted April 1981.*

УДК 004.77:340: 347.121.1:347.121.2:341.1/8+341.215.4

ЗАКОНОДАВЧЕ ЗАБЕЗПЕЧЕННЯ ОХОРОНИ Й ЗАХИСТУ ПЕРСОНАЛЬНОЇ ІНФОРМАЦІЇ В МЕРЕЖІ ІНТЕРНЕТ

Олександр Радкевич
Національна академія внутрішніх справ

Анотація: **Висвітлено вітчизняне законодавство в сфері охорони й захисту персональної інформації. Приділено увагу міжнародному досвіду з урегулювання відносин при користуванні мережею Інтернет. Схарактеризовано основні аспекти, пов'язані з особливістю регулювання відносин у віртуальному просторі мережі Інтернет.**
Summary: **The article covers the national legislation in the Protection and defense personal information. Attention is paid to the international experience of regulating relations using the Internet. Author determined the main aspects relating to a regulation of relations in the cyberspace of the Internet.**
Ключові слова: **Законодавство, міжнародний досвід, мережа Інтернет, персональна інформація.**

Одним із негативних наслідків впровадження інформаційно–телекомунікаційних технологій у різних сферах суспільного життя стало порушення немайнових прав особи, що проявляється в незаконному зборі, використанні й поширенні інформації персонального характеру, у тому числі в мережі Інтернет. Ця проблема набула особливої актуальності у зв'язку з тим, що більшості громадян властивий правовий нігілізм, який виявляється у відсутності знань особистих прав і обов'язків у цій сфері. Водночас недостатньо розроблене законодавче забезпечення охорони й захисту персональної інформації в мережі Інтернет, тоді як такі правопорушення набувають широкого масштабу. Це пов'язано з тим, що дослідники присвячують увагу питанням захисту авторських прав у мережі Інтернет в загальному та мало уваги приділяють першоджерелу (першооснові) цих прав.

Наукові основи правового режиму охорони й захисту персональної інформації відображені в дослідженні українських учених: І. Арістової, О. Баранова, И. Бачило, В. Брижка, О. Задорожного, Е. Захарова, В. Наумова, А. Пазюка, А. Марущака, Р. Романова, В. Цимбалюка, М. Швеця та ін. Однак у дослідженнях поки що не розкривалися теоретичні та практичні проблеми правозастосування законодавства в сфері охорони й захисту персональної інформації в мережі Інтернет як елемент системи управління інформаційною безпекою країни.

Метою даної статті є обґрунтування законодавчого забезпечення, що регулює відносини з охорони і захисту персональної інформації в мережі Інтернет.

Охорона й захист є передбачена нормами права діяльність як державних, так і громадських органів, спрямована на примусове відновлення порушених прав. Дещо інакше трактує ці поняття І. Котерлін, вважаючи, що охорона й захист інформації зводиться до системи правових, організаційних, інженерних і технічних заходів, спрямованих на збереження інформації та запобігання її несанкціонованому витоку. Таким чином, охорону й захист персональної інформації можна розглядати як сукупність методів, засобів і заходів забезпечення інформаційної безпеки людини, суспільства й держави в усіх сферах життєдіяльності. На думку вченої, суть захисту інформації полягає у виявленні, вилученні й нейтралізації негативних джерел, причин та умов впливу на збереженість інформації [1, с. 34 – 35].

У цьому контексті персональна інформація розглядається з різних точок зору: вона може бути переліком конкретної інформації про особу та об'єктом, за допомогою якого можна конкретно ідентифікувати особу. Відтак ідентифікація є переліком конкретної інформації, що асоціюється із суб'єктом – утримувачем інформації (її власником). Ідентифікація різних осіб здійснюється по-різному. Для суб'єкта, якому особа знайома, вона може відбутись, а для іншого – ні. Що ж до персональної інформації, завдяки якій можна ідентифікувати особу, її можна визначити таким чином, це: «ім'я, адреса, дата народження, місце роботи, посада, номер паспорта, номер ідентифікаційного коду, номер страховки» тощо.

Щодо необхідності охорони й захисту персональної інформації А. Пазюком було висловлено думку про те, що «неправомірне збирання, використання й поширення персональної інформації завдає шкоду