nated magneto-sensitive elements embedded in grooves of the magnetic system in the working area of ore pulp supply. A source of stabilized power supply and a potentiometer were installed in the prototype of the system. The prototype has been experimentally studied in industrial environment of magnetic enrichment plant. Scheme of experimental studies, results of chemical analysis of selected technological samples and registrations of secondary device, which measures magnetic induction in the area of magnetic separator feeding with ore pulp are presented. Static characteristic of the prototype of the system for automatic control of mass fraction of iron in ore enriched has been determined as a regression equation. Confidence intervals of the regression have been determined. Accuracy of the automatic control of mass fraction of iron in the ore makes 5% in relative units.

We have developed the method and the system for automatic control of mass fraction of iron in ore pulp inflowing to the enrichment by the signal of the magnetic induction received in the area of magnetic separator feding.

Originality. For the first time it was found that the magnetic induction of spatially distributed magnetic field in the working zone of the feeding supply of the magnetic separator, measured along separator drum generatrix, perpendicularly to the axis of pulp supply to the bath of the separator is directly proportional to the mass fraction of iron in the ore.

Practical value. The result allows automating the process of sampling and analysis of the mass fraction of iron in ore pulp and reducing technological control costs.

Keywords: *automatic control, magnetic separator, mass fraction of iron, ore*

Рекомендовано до публікації докт. техн. наук В.В. Ткачовим. Дата надходження рукопису 20.02.12.

УДК 004.056

Т.В. Бабенко, д-р техн. наук, доц.,
О.М. Третяк, О.В. Кручінін, Д.С. Тимофєєв

Державний вищий навчальний заклад „Національний гірничий університет“, м. Дніпропетровськ, Україна, e-mail: Babenko@nmu.org.ua

ПРОБЛЕМИ ЗАХИСТУ ОСВІТНІХ ЕЛЕКТРОННИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ

T.V. Babenko, Dr. Sci. (Tech.),
O.M. Tretiak, O.V. Kruchinin, D.S. Tymofieiev

State Higher Educational Institution “National Mining University”, Dnipropetrovsk, Ukraine, e-mail: Babenko@nmu.org.ua

INFORMATION SECURITY PROBLEMS OF EDUCATIONAL ELECTRONIC INFORMATION RESOURCES

Мета. Метою статті є аналіз рівня захищеності інформації, що обробляється в автоматизованій системі електронного документообігу для роботи ВНЗ та абітурієнтів з Єдиною державною електронною базою з питань освіти (ЄДЕБО).

Методика. Для аналізу ризиків інформаційної безпеки в рамках досліджуваної системи було використано якісну методику, яка дозволила проранжувати вірогідні інциденти, що можуть виникнути під час роботи з ЄДЕБО, та визначити ті, що потребують обробки.

Результати. У результаті проведеного аналізу було визначено найбільш критичні загрози для інформації, що обробляється в автоматизованій системі ЄДЕБО. Крім того, під час дослідження було розглянуто чинні нормативні документи у сфері захисту інформації й визначено вимоги до системи захисту. Розроблено рекомендації щодо формулювання функціонального профілю захищеності для побудови комплексної системи захисту інформації.

Наукова новизна. Наукова новизна полягає в розробці рекомендацій щодо однозначної ідентифікації та автентифікації абітурієнтів під час електронної реєстрації заяв в особистому електронному кабінеті автоматизованої системи ЄДЕБО.

Практична значимість. Запроваджена в 2011 році експериментальна система „Електронний вступ“ після проведення певної модернізації в 2012 році перетворилася на повноцінну систему електронної реєстрації заяв для абітурієнтів, яким тепер немає потреби особисто відвідувати ВНЗ для подання документів на участь у конкурсному відборі. Збирання, верифікація, обробка та захист даних абітурієнтів здійснюється в ЄДЕБО, що розглядаються як окремий випадок системи електронного документообігу. Запропоновані в роботі рішення дозволять підвищити ефективність засобів, що використовуються для забезпечення захисту інформації, зокрема, персональних даних, що циркулюють в автоматизованій системі ЄДЕБО.

Ключові слова: *захист інформації, аналіз ризиків, ЄДЕБО, система електронного документообігу, персональні дані, автентифікація*

Постановка проблеми. Запроваджена в 2011 році експериментальна система „Електронний вступ“ після проведення певної модернізації в 2012 році перетворилася на повноцінну систему електронної реєстрації заяв для абітурієнтів, яким тепер немає потреби особисто відвідувати ВНЗ для подання документів на участь у конкурсному відборі. Єдина державна електронна база з питань освіти

© Бабенко Т.В., Третяк О.М., Кручінін О.В., Тимофєєв Д.С., 2012

(ЄДЕБО) — автоматизована система, що призначена для збирання, верифікації, оброблення, зберігання та захисту даних, у тому числі персональних, щодо надавачів та отримувачів освітніх послуг в Україні [1]. А отже ми можемо розглядати її як окремий випадок системи електронного документообігу. Використання такої системи є, безумовно, прогресивним рішенням за умови виконання вимог із захисту інформації.

Невирішені раніше частини проблеми. У системі, що розглядається, підсистема електронної реєстрації заяв забезпечує електронний документообіг між абітурієнтом, вищим навчальним закладом та розпорядником єдиної бази – державним підприємством „Інфоресурс“, що належить до сфери управління Міністерства освіти і науки, молоді та спорту України. На рис. 1 наведено структурну схему взаємодії інформаційних підсистем системи електронного документообігу. Станом на серпень 2012 року кожна з підсистем, що приймає участь у електронному документообігу, належить окремому державному підприємству та має власну базу даних і систему розмежування доступу, що ускладнює контроль за діями користувачів.

Метою статті є аналіз рівня захищеності інформації, що обробляється в автоматизованій системі електронного документообігу, для роботи ВНЗ та абітурієнтів з ЄДЕБО.

Основний матеріал дослідження. Схема взаємодії інформаційних підсистем з ЄДЕБО (рис.1) досить складна, тому в рамках даної статті ми розглянемо процедуру електронної подачі заяви абітурієнтом та сконцентруємо нашу увагу на аналізі підсистеми взаємодії ЄДЕБО та ВНЗ з точки зору захисту інформації.

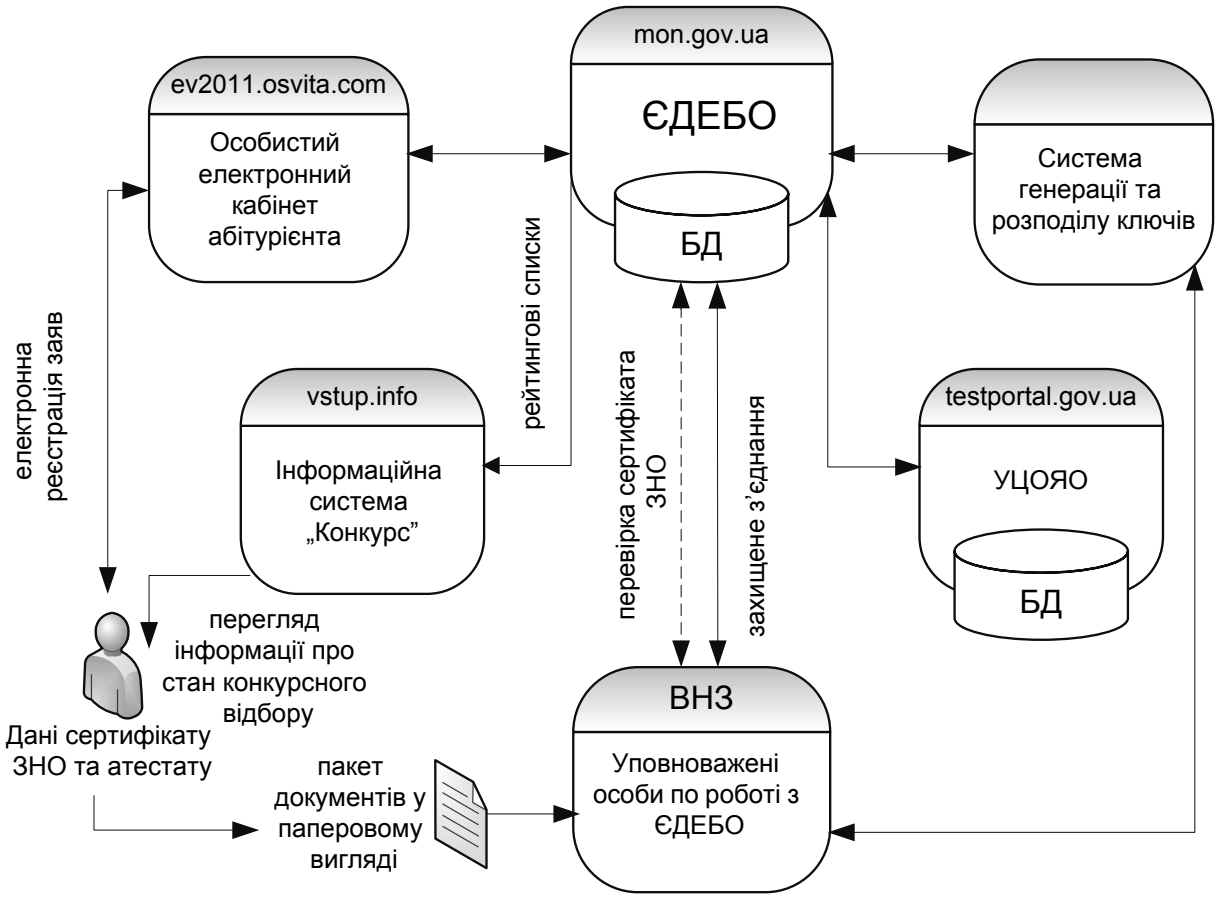

Рис.1. Схема взаємодії інформаційних підсистем з ЄДЕБО(2012р.)

Наказом МОНмолодьспорт № 1179 від 12.10.2011р. визначено „Порядок подання та розгляду заяв в електронній формі на участь у конкурсному відборі до вищих навчальних закладів“ [2].

Необхідною умовою подання електронної заяви є реєстрація абітурієнта на спеціальному інтернет-сайті, під час якої вступник має надати адресу електронної пошти, номер, пін-код та рік отримання сертифіката ЗНО, а також серію та номер атестата про повну середню освіту. Після успішно проведеної перевірки цих даних у ЄДЕБО на вказану адресу електронної пошти вступник отримує дані для проходження процедури автентифікації в електронному кабінеті, який використовується для подання та контролю статусу електронних заяв.

В особистому електронному кабінеті абітурієнта в ЄДЕБО заносяться його персональні дані та обраний вищий навчальний заклад і напрями підготовки. Подані електронні заяви відображаються в розділі Єдиної бази і розглядаються уповноваженими особами обраних вступником вищих навчальних закладів. Інформування абітурієнтів про хід подання заяв до ВНЗ та їх місце в

рейтингу здійснюється за допомогою Інформаційної системи „Конкурс“, що фактично візуалізує дані з ЄДЕБО. На жаль, системи погано синхронізуються, а вивантаження даних з ЄДЕБО інколи здійснюється із затримками, що призводить до ситуації, коли на сайті vstup.info абітурієнт бачить інформацію про перебіг вступної кампанії, яка не завжди є актуальною.

Розглянемо основні аспекти, пов’язані із захистом інформації у вище означеній системі. Система електронної реєстрації заяв підпадає під дію закону „Про електронні документи та електронний документообіг“, згідно зі статтями 5 та 6 якого „обов’язковим реквізитом електронного документа, що використовується для ідентифікації автора та/або підписувача електронного документа“ є електронний цифровий підпис. У такому разі, створення кожної електронної заяви абітурієнта повинно завершуватись електронним підписом вступника для забезпечення цілісності та підтвердження авторства документа. Зокрема, у ст. 12 закону „Про електронні документи та електронний документообіг“ [3] чітко визначено, що перевірка цілісності проводиться шляхом перевірки електронного цифрового підпису. Діючий сьогодні варіант системи не передбачає однозначної ідентифікації та автентифікації абітурієнтів, яка би дозволила стверджувати, що зареєстрований користувач дійсно є тим, за кого себе видає. Під час електронної реєстрації абітурієнт вказує тільки відомості про ЗНО (номер сертифіката, пін-код, рік отримання) та дані про атестат (серія та номер атестата, середній бал) – ці дані відомі не тільки йому й можуть бути використані іншими особами.

Персональні дані абітурієнтів, що циркулюють в ЄДЕБО, підпадають під дію статті 8 закону „Про захист інформації в інформаційно-телекомунікаційних системах“ і повинні оброблятися із застосуванням комплексної системи захисту інформації (КСЗІ).

Згідно з нормативними документами, аналіз ризиків є одним із перших етапів створення КСЗІ. Але, перш ніж визначати ризики та механізми контролю, що дозволять забезпечити оптимальний захист електронних заяв під час їх обробки та зберігання, проаналізуємо процес роботи ВНЗ із системою електронного документообігу.

Таблиця 1

Матриця визначення вірогідності інциденту

Вірогідність загрози	Низька			Середня			Висока		
Рівень вразливості	Н	С	В	Н	С	В	Н	С	В
Значення вірогідності сценарію інциденту	**0**	**1**	**2**	**1**	**2**	**3**	**2**	**3**	**4**

* Н - низька, С – середня, В – висока.

Таблиця 2

Фрагмент таблиці аналізу вірогідності інцидентів

Інцидент	**Потенційно можливі загрози**	**Рівень ризику реалізації загрози**	**Потенційно можливі вразливості**	**Рівень вразливості**	**Вірогідність інциденту**
Недоступність сервісу	Відмова в обслуговуванні через запуск експлоітів, що використовують вразливості операційної системи (Dos-атаки / DDos-атаки та ін.)	В	Не використовується система виявлення вторгнень	В	3
		С	Не використовуються засоби захисту програмного стеку від перевантажень	В	
		В	Не виконується регулярне встановлення оновлень для усунення відомих вразливостей	С	
	Відмова в обслуговуванні через запуск експлоітів, що використовують вразливості мережевих служб (Dos-атаки / DDos-атаки та ін.)	В	Не використовується система виявлення вторгнень	Н	
		С	Не використовуються засоби захисту програмного стеку від перевантажень	С	
		В	Не виконується регулярне встановлення оновлень для усунення відомих вразливостей	В	
	Відмова в обслуговуванні мережевої служби (внутрішній збій програмного забезпечення)	В	Відсутність систем моніторингу мережевих служб, що працюють у режимі реального часу	С	
		С	Відсутність систем відновлення робочих конфігурацій мережевих служб	С	
	Видалення критично важливої інформації	В	Відсутність процедур резервного копіювання	Н	
	Навмисне чи ненавмисне псування резервних копій	С	Відсутність організаційних заходів контролю цілісності резервних копій	С	

Співробітники приймальної комісії, так само як і абітурієнти, працюють з ЄДЕБО через загальнодоступні мережі, але використовують захищене з'єднання. Для попередження несанкціонованого доступу до Єдиної бази працівники приймальної комісії пройшли складну процедуру реєстрації, після чого отримали дані для здійснення двофакторної автентифікації та шифрування даних. Такий підхід дозволяє зменшити вірогідність отримання несанкціонованого доступу до інформації, що циркулює в системі. Проте на практиці, у реалізованому підході, спостерігаються недоліки. Двофакторна автентифікація була реалізована не в повній мірі, що дозволяло виконати доступ до системи з чужими ідентифікаційними даними.

Найбільш небезпечні вірогідні інциденти та потенційно можливі причини їх виникнення оцінювали за допомогою якісної методики аналізу ризику[4]. У відповідності до цієї методики, для визначення вірогідності інциденту була використана матриця визначення вірогідності інциденту, що базується на експертній оцінці (табл. 1). У табл. 2 наведено фрагмент таблиці аналізу вірогідності інцидентів, в якому проаналізовано один із найбільш вірогідних інцидентів для системи ЄДЕБО.

У табл. 3 наведено матрицю для визначення ризиків, в якій запропоновано оцінювати результуючий ризик за шкалою від 0 до 8. Відповідно: 0-2 – низький ризик, 3-5 – середній, 6-8 – високий.

Таблиця 3

Матриця для визначення рівня ризику

	Вірогідність сценарію інцидента	Дуже низька	Низька	Середня	Висока	Дуже висока
Рівень негативного впливу	Дуже низький	0	1	2	3	4
	Низький	1	2	3	4	5
	Середній	2	3	4	5	6
	Високий	3	4	5	6	7
	Дуже високий	4	5	6	7	8

Висновки. Таким чином, за результатами виконаного аналізу можна зробити висновки, що найбільш критичні рівні ризику мають: інцидент недоступності сервісу (розглянутий у табл. 2) та спотворення персональних даних абітурієнтів під час їх обробки. Основною причиною виникнення означених інцидентів є недостатній рівень захищеності інформаційних ресурсів системи від несанкціонованого доступу через відсутність програмно-апаратних засобів захисту та/або невиконання організаційних вимог.

Як відомо, необхідною умовою формалізації вимог до комплексу засобів захисту є визначення функціонального профілю захищеності. Відповідно до НД ТЗІ 2.5-004-99 та НД ТЗІ 2.5-005-99, система електронного документообігу, що розглядається, представляє собою АС класу 3, в якій циркулює інформація з обмеженим доступом, зокрема, персональні дані, що потребує чіткого розподілу прав доступу користувачів – вимоги до конфіденційності. Крім того, постійний обмін інформацією між вузлами системи потребує налагодженої синхронізації та гарантованого рівня доступності сервісу – вимоги до доступності. Модифікація персональних даних у ЄДЕБО може привести до спотворення інформації та неправильних результатів рейтингування – вимоги до цілісності.

Таким чином, СЕД належить до підкласу 3. КЦД з підвищеними вимогами одночасно до конфіденційності, цілісності та доступності. Взаємодія ВНЗ з ЄДЕБО передбачає двофакторну автентифікацію, а отже це повинно бути відображено у профілі послугою НИ-3 (множинна ідентифікація і автентифікація), для попередження недоступності сервісу пропонуємо включити до профілю послуги ДР-2 (недопущення захоплення ресурсів) та ДС-3 (стійкість без погіршення характеристик обслуговування).

Що стосується абітурієнтів, то, для вирішення проблеми однозначної ідентифікації абітурієнтів при роботі з системою електронної реєстрації заяв, пропонується кожному абітурієнту особистий таємний ключ. За допомогою ключа він зможе подати заяву в електронному вигляді на участь у конкурсному відборі, не боячись, що його дані буде використано іншими особами. Для забезпечення захисту інформації, при передачі її каналами зв'язку, доцільно було би вивчити варіант використання відповідного програмного забезпечення на стороні абітурієнта, де буде виконуватись заповнення заяви, її підписання ЕЦП та шифрування. У зашифрованому вигляді заява надходитиме до центру електронної реєстрації заяв, де заяву буде розшифровано та перевірено ЕЦП. Отже, підсумовуючи одержані результати слід зазначити, що система електронного документообігу потребує певного доопрацювання для надійної та захищеної реалізації всіх закладених до неї функцій з метою відповідності вимогам чинного законодавства.

Список літератури / References

1. Постанова №752 від 13.07.2011 р. „Про створення Єдиної державної електронної бази з питань освіти" [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/752-2011-%D0%BF

Decree no.752 dated July 13, 2011 "About creation of unified state education electronic database", available at: http://zakon2.rada.gov.ua/laws/show/752-2011-%D0%BF

2. Наказ МОНмолодьспорт №1179 від 12.10.2011 р. „Порядок подання та розгляду заяв в електронній формі на участь у конкурсному відборі до вищих на-

вчальних закладів“ [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/z1222-11

Decree of Ministry of Education and Science, Youth and Sport of Ukraine no.1179 dated October 12, 2011 “Procedure of registration and consideration of applications in electronic form for participation in the competition for entering to the universities”, available at: http://zakon2.rada.gov.ua/laws/show/z1222-11

3. Закон України „Про електронні документи та електронний документообіг“ [Електронний ресурс]. – Режим доступу: http://zakon1.rada.gov.ua/laws/show/851-15

Law of Ukraine “On the electronic documents and electronic document circulation”, available at: http://zakon1.rada.gov.ua/laws/show/851-15

4. Астахов А. М. Искусство управления информационными рисками / Астахов А. М. – М.: ДМК Пресс, 2010. – 312 с.,ил.

Astakhov, A.M. (2010), *Iskusstvo upravlenia informatsionnimi riskami* [The Art of Information Risk Management], Press, Moscow, Russia.

Цель. Целью статьи является анализ уровня защищенности информации, обрабатываемой в автоматизированной системе электронного документооборота для работы ВУЗов и абитуриентов с Единой государственной электронной базой по вопросам образования (ЕГЭБО).

Методика. Для анализа рисков информационной безопасности в рамках исследуемой системы была использована качественная методика, которая позволила проранжировать возможные инциденты, которые могут возникнуть при работе с ЕГЭБО, и определить те, которые требуют обработки.

Результаты. В результате проведенного анализа были определены наиболее критичные угрозы для информации, которая обрабатывается в автоматизированной системе ЕГЭБО. Кроме того, в ходе исследования были рассмотрены действующие нормативные документы в области защиты информации и определены требования к системе защиты. Разработаны рекомендации по формулированию функционального профиля защищенности для построения комплексной системы защиты информации.

Научная новизна. Научная новизна заключается в разработке рекомендаций по однозначной идентификации и аутентификации абитуриентов при электронной регистрации заявлений в личном электронном кабинете автоматизированной системы ЕГЭБО.

Практическая значимость. Введенная в 2011 году экспериментальная система „Электронное поступление“ после проведения определенной модернизации в 2012 году превратилась в полноценную систему электронной регистрации заявлений для абитуриентов, которым теперь нет надобности посещать ВУЗ для подачи документов на участие в конкурсном отборе. Сбор, верификация, обработка и защита данных абитуриентов осуществляется в ЕГЭБО, которая рассматривается как частный случай системы электронного документооборота. Предложенные в работе решения позволят повысить эффективность средств, используемых для обеспечения защиты информации, в частности, персональных данных, циркулирующих в автоматизированной системе ЕГЭБО.

Ключевые слова: *защита информации, анализ рисков, ЕГЭБО, система электронного документооборота, персональные данные, аутентификация*

Purpose. The purpose of the article is to analyze the security level of the information processed in an automated electronic document management system for universities and students working with the United State Electronic Database on Education (USEDE).

Methodology. For the information security risk analysis within the investigated system we have used qualitative methods, which allowed us to rank probable incidents that may arise while working with USEDE, and identify those ones that require treatment.

Findings. The analysis identified the most critical threats to the information that is processed in the USEDE automated system. In addition, during the investigation the existing regulatory documents, in the area of information security, were examined, and this helped to define the requirements to the protection system. The recommendations on the formulation of the functional information security profile for the construction of an integrated information security system were suggested.

Originality. Scientific innovation consists in developing recommendations for unambiguous identification and authentication of university entrants during electronic registration of their applications in personal electronic office within automated system USEDE.

Practical value. The experimental system “Electronic entry” introduced in 2011, after certain modernization in 2012 has turned into a comprehensive system of electronic registration for the university entrants, who now don’t have to attend university personally to apply the documents for participation in the competition. The collection, verification, processing and data protection performed in USEDE, which is considered as a special case of electronic document management system. The suggested solutions will improve the effectiveness of information protection facilities, including personal data that circulate in the automated system USEDE.

Keywords: *information security, risk analysis, USEDE, electronic document management system, personal data authentication*

Рекомендовано до публікації докт. техн. наук М.О. Алэксээвим. Дата надходження рукопису 14.03.12.