

УДК 373.51:004.056

Гризун Людмила Едуардівна

доктор педагогічних наук, професор, професор кафедри інформатики Харківського національного педагогічного університету імені Г.С. Сковороди

0000-0002-5274-5624

lgr2007@ukr.net

Суворова Ольга Василівна

вчитель інформатики Харківської ЗОШ I-III ступенів № 44 Харківської міської ради Харківської області

0000-0002-6003-2632

b1ack1ght@rambler.ru

ПРАКТИКО-ОРІЄНТОВАНИЙ ПІДХІД ДО ВИВЧЕННЯ ОСНОВ ЗАХИСТУ ДАНИХ У РАМКАХ ІНФОРМАТИЧНОЇ ОСВІТИ

Анотація

Виходячи з проведеного аналізу наукових та навчально-методичних джерел та вимог до здобувачів сучасної інформатичної освіти, в роботі встановлено актуальність впровадження практико-орієнтованого підходу до вивчення основ захисту даних та визначено необхідність розробки комплекту відповідних практичних завдань. Відповідно до мети, в роботі схарактеризовано розроблений комплект дидактичних завдань різних типів для реалізації практико-орієнтованого підходу до вивчення основ захисту даних у рамках інформатичної освіти. Завдання усіх типів спрямовані на формування досвіду використання отриманих знань під час розв'язання реальних життєво-значущих проблем із захисту даних. Застосування розроблених завдань сприятиме одержанню молоддю стійких навичок застосування сучасних інструментів захисту даних, формуванню їх соціально-свідомого відношення до реальних загроз інформаційній безпеці та коректної поведінки при виникненні небезпечних ситуацій.

Ключові слова: основи захисту даних, практико-орієнтований підхід, інформаційна безпека.

Постановка проблеми в загальному вигляді

У зв'язку зі зростаючим глобальним рівнем інформатизації суспільства та широкомасштабного використання інформаційних ресурсів особливого

значення набувають сьогодні проблеми захисту даних та інформаційної безпеки усіх членів суспільства. Інформаційна безпека у своїх дослідженнях зосереджується на визначенні стану загроз для пристроїв, систем та людини, ймовірності виникнення таких загроз, а також на розробці та впровадженні заходів щодо захисту даних. Інформаційна безпека розглядається також як державне завдання, що полягає у забезпеченні відсутності загроз на рівні суспільства, окремих груп та кожної людини. Це висуває перед національною системою освіти завдання просвіти зростаючого покоління щодо грамотного залучення знань із різних інформаційних ресурсів, обізнаності з елементарних правил відбору, використання та захисту приватної інформації, що сприятиме розвитку системи захисту прав людини в інформаційному середовищі, збереженню його фізичного і духовного здоров'я.

Зрозуміло, що вивчення основ інформаційної безпеки та захисту даних посідає провідне місце в інформатичній освіті як середнього так і вищого рівнів. Відповідно до чинних навчальних програм для національних навчальних закладів, теми курсу інформатики, пов'язані із зазначеними проблемами, мають на меті засвоєння тими, хто навчається, системи відповідних знань та набуття певних навичок. Проте аналіз наявної освітньої практики та реалій життя засвідчує недостатню обізнаність молодого покоління щодо нагальних проблем захисту даних, слабку резистентність до впливу інструментів соціальної інженерії, які часто застосовуються кіберзловмисниками, а також брак практичних навичок із забезпечення інформаційної безпеки, що потребує пошуку оновлених підходів до вивчення основ захисту даних.

Аналіз останніх досліджень і публікацій

Окреслені проблеми інформатичної освіти знаходять своє відображення у низці робіт сучасних дослідників. Зокрема, визначенню сутності та завдань інформаційної безпеки сучасного суспільства, дослідженню основних загроз такій безпеці, формуванню відповідних заходів з боку держави, підприємства та людини присвячено роботи таких дослідників та педагогів-практиків [1; 2 та

ін.], як С. Попов, О. Барановський, Л. Бесєдіна, В. Богуш, О. Бойченко, В. Гавловський, Я. Жарков, Б. Заплотинський, Р. Калюжний, О. Степко та інші.

У роботах дослідників Ю. Богатирьової, І. Берест, Ковальчук, Т. Підгорної, О. Спіріна та інших розкриваються актуальні аспекти організації інформаційної безпеки дітей і підлітків, а також шляхи підготовки майбутніх учителів інформатики до забезпечення інформаційної безпеки навчального закладу [3; 4; 5; 6].

Дидактичні та методичні питання вивчення основ захисту даних, проблеми удосконалення інформатичної освіти у сказаній галузі розглядаються, зокрема, у роботах таких педагогів-дослідників, як О. Алтуф'єва, Л. Астахова, К. Виривода, В. Гріцик, І. Кірко, В. Поляков, Е. Татова та інші. Аналіз цих джерел, а також чинних навчальних програм з інформатики засвідчує, що питання інформаційної безпеки посідають в них значне місце. Проте, спостерігається переважно теоретичне наповнення навчально-пізнавальної діяльності тих, хто навчається. Так, передбачається їх ознайомлення та формування їх уявлення про необхідність захисту даних, етичні і правові основи їх захисту; класифікацію загроз; різновиди та загальні принципи дії шкідливих програм; особливості загроз, що виникають в процесі використання Інтернету, та відповідні способи боротьби із ними; основні стратегії кіберзлочинців тощо.

Разом із цим, слід зауважити, що вимоги до рівня здобувачів інформатичної освіти у цій галузі, сформульовані, зокрема у [7; 8; 9], перевищують їх реальні знання. Це частково пов'язано із тим, що теоретичні відомості не підкріплюються їх практичним застосуванням у реальному житті. У навчально-пізнавальній діяльності молоді щодо опанування основ інформаційної безпеки бракує практичної складової, спрямованої як на відпрацювання навичок застосування сучасних інструментів захисту даних, так і на формування особистого соціально-свідомого відношення до реальних загроз інформаційній безпеці та коректної поведінки при виникненні небезпечних соціальних ситуацій.

Отже, незважаючи на значний внесок авторів досліджень у розв'язання завдань удосконалення вивчення основ захисту даних, актуальним залишається впровадження саме практико-орієнтованого підходу до опанування засобів інформаційної безпеки. Метою роботи є презентація комплексу дидактичних завдань різних типів для реалізації практико-орієнтованого підходу до вивчення основ захисту даних у рамках інформатичної освіти.

Подання основного матеріалу дослідження

Виходячи з проведеного аналізу наукових та навчально-методичних джерел, вимог до здобувачів сучасної інформатичної освіти, а також сутності практико-орієнтованого навчання сформулюємо завдання щодо впровадження практико-орієнтованого підходу до вивчення основ захисту даних.

Відповідно до психолого-педагогічних досліджень, сутність практико-орієнтованого навчання полягає у побудові освітнього процесу на основі єдності емоційно-образного та логічного компонентів змісту; набуття нових знань і формування практичного досвіду їх використання під час вирішення життєво важливих проблем; емоційного й пізнавального насичення навчальної діяльності тих, хто навчається [10]. Автори зазначають також, що при практико-орієнтованому підході до навчання соціальна дійсність постає як сукупність людських практик, а саме: умінь, навичок, способів дії та звичаїв [11]. Акцентується також, що такий підхід фокусується на вивченні не навчальних дисциплін, а на розв'язанні справжніх проблем реального життя при активному навчанні в невеликих групах [12, с. 66; 13].

Зрозуміло, що реалізація такого підходу до вивчення основ захисту даних має спиратися на систему практичних завдань, які спрямовані на формування досвіду використання отриманих знань під час розв'язання реальних життєво важливих проблем із захисту даних. Крім цього, такі завдання мають забезпечувати емоційне і пізнавальне насичення навчальної діяльності тих, хто навчається, залучати їх до рефлексії власної поведінки у інформаційно-небезпечних ситуаціях.

Характеризуючи розроблену нами систему завдань для реалізації практико-орієнтованого підходу до вивчення основ захисту даних, зазначимо, що вона налічує загалом близько 40 дидактичних завдань різних типів, які можуть бути застосовані в рамках інформатичної освіти школярів та студентів.

Схарактеризуємо типи означених завдань. Зокрема, система включає завдання, розроблені із залученням апарату семантичних мереж. Вони, як правило, містять графічне відтворення фрагменту навчального матеріалу із візуальним відображенням зв'язків та відношень між елементами знань. Деякі із таких відтворень можуть бути напівпорожніми, що дозволить тим, хто навчається, самостійно, шляхом відповідей на запитання, встановити відповідні зв'язки між навчальними елементами, сформулювати коректні факти і положення, швидко пригадати вивчені теоретичні знання та усвідомити їх практичну значущість.

Наступний тип являє собою практичні завдання, виконувані за алгоритмом та спрямовані на формування і відпрацювання конкретних необхідних умінь тих, хто навчається, щодо забезпечення їх особистої інформаційної безпеки; налаштувань стаціонарних та мобільних пристроїв для забезпечення захисту даних, їх безпечного зберігання та пересилання; налаштування коректної і безпечної роботи поштових сервісів; обачної поведінки при роботі в Інтернеті.

Ще одним типом розроблених завдань є практичні задачі із залученням різноманітних програм-емуляторів, які імітують роботу із усілякими сервісами (соціальними мережами, платіжними системами, сайтами знайомств), навмисно створюють небезпечні обставини і у такий спосіб спонукають тих, хто навчається, розв'язувати реальні проблеми з інформаційної безпеки та відпрацьовувати необхідні навички.

До окремого типу практико-орієнтованих завдань слід віднести розроблені авторами соціально-виховні ситуації, що імітують реальну життєву проблему, яка потребує залучення знань з основ інформаційної безпеки, спонукає до критичного осмислення конкретної небезпечної ситуації і власної

поведінки при її виникненні та забезпечує емоційне й пізнавальне насичення навчальної діяльності тих, хто навчається.

Схарактеризовані завдання можуть бути використаними в рамках інформатичної освіти підлітків та студентів на різних етапах навчання та з різною дидактичною метою. Наведемо приклади та методичні рекомендації щодо їх впровадження в освітню практику. Так, з метою актуалізації знань, тим, хто навчається, слід запропонувати завдання, розроблені із залученням апарату семантичних мереж. Наприклад, до семантичної мережі (Рис. 1) можна запропонувати низку запитань, виду: (1) які відомості про види загроз ви можете сформулювати? (2) який тип (видовий або ієрархічний) класифікації загроз відтворено? (3) чи є така класифікація повною, яких видів бракує? тощо.

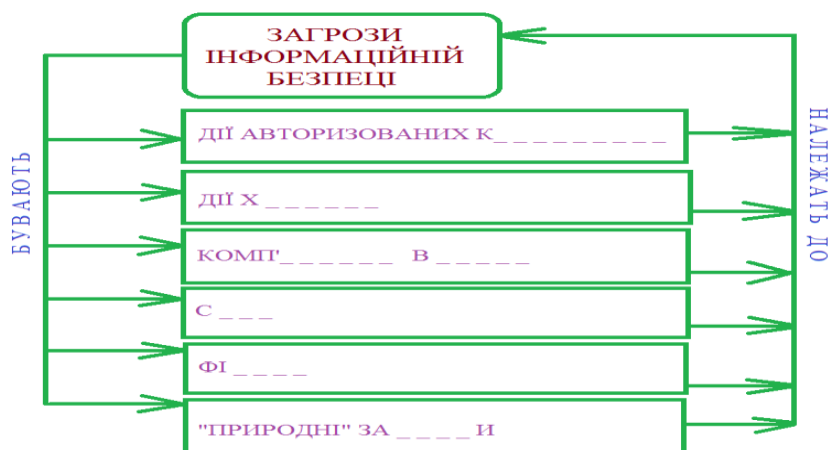


Рис. 1. Фрагмент завдання із залученням апарату семантичних мереж

Відповідно до вікових особливостей, для актуалізації та закріплення знань можна долучити школярів (студентів) до розв'язання термінологічних загадок, ребусів, кросвордів, що спонукають не тільки назвати термін, пов'язаний із проблемами кібербезпеки, а й надати йому вірне тлумачення, пригадати зв'язок із іншими поняттями тощо.

Значне місце у розробленій системі посідають практичні завдання на формування і відпрацювання конкретних необхідних умінь, що можуть бути використані для закріплення нових знань. Наприклад, при виконанні серії завдань «Управління доступом до конфіденційних даних на різних пристроях»

пропонується за вказаним покроковим алгоритмом здійснити на усіх можливих пристроях налаштування конфіденційності особистої інформації у сервісах Google; управління доступом до власної сторінки у соціальній мережі; створення резервної копії історії чату Viber тощо.

Під час виконання практичних завдань такого типу доцільно акцентувати увагу учнів і студентів, на виборі осіб, яких можна долучити до кола тих, кому можна відкрити доступ до конфіденційних даних та до чатів. Слід також, спонукати їх сформулювати ознаки небезпечних ситуацій при роботі із відповідними сервісами; назвати цілі та дії зловмисників, які намагаються одержати доступ до конфіденційної інформації користувачів; сформулювати роль паролів та їх надійності для захисту даних, а також пригадати правила генерування надійного паролю.

Корисним уявляється виконання серії практичних завдань у середовищі програм-емуляторів, загальну характеристику яких наведено вище. Наприклад, емулятор може імітувати роботу із фейковими сторінками сайтів, які лише зовні нагадують відомий сервіс, а насправді планомірно збирають у користувача дані про доступ до власних даних. Також корисною є робота із емулятором деякої платіжної системи, яка містить в адресному рядку незахищену адресу, проте пропонує здійснити платіж. Окрему увагу при виконанні таких завдань рекомендується зосереджувати на аналізі інтерфейсу, характері повідомлень, даних адресного рядку, що надає емулятор. Після виконання вправ із емулятором доцільно провести обговорення дій кожного із учасників процесу навчання, спонукати їх до рефлексії власної поведінки при виникненні загроз.

Як зазначалося вище, до окремого типу практико-орієнтованих завдань належать спеціально розроблені соціально-виховні ситуації, які доцільно застосувати як для вивчення нового матеріалу з елементами проблемного навчання, так і для закріплення набутих знань.

У якості прикладу такого практико-орієнтованого завдання можна навести ситуацію «Електронне листування», яка полягає в наступному. Уявіть,

що Василь та Петро отримали однаковий електронний лист від свого однокласника Тараса із запрошенням разом пограти в онлайн гру, де також додавалось посилання на завантаження гри.

Наведемо орієнтовну схему опрацювання цієї ситуації в аудиторній роботі. Пропонується обрати дві-три групи із трьох осіб для інсценування ситуації за різними сценаріями, які ті, хто навчаються, визначають самостійно. Наприклад, «Василь» («Петро») у різних сценаріях можуть або проігнорувати листа, або спитати «Тараса», чи відправляв він такого листа із посиланням, чи одержане воно із надійного джерела, чи є гра вільно-розповсюджуваною тощо, або без зайвих вагань перейти за посиланням із різними наслідками.

Решта присутніх переглядають різні сценарії інсценування ситуації та аналізують поведінку усіх її героїв. Після інсценування та перегляду ситуації доцільно задати учням (студентам) запитання, що спонукають їх до критичного аналізу поведінки героїв ситуації та до власної емпатії. Доцільно також спонукати учнів (студентів) сформулювати ті правила інформаційної безпеки, які були порушені. Крім цього, можна запропонувати розіграти сценарій із найбільш коректною та із найбільш необачною поведінкою героїв з точки зору правил інформаційної безпеки.

Отже, аналіз розробленого та схарактеризованого комплекту дидактичних завдань засвідчує, що його застосування у рамках інформатичної освіти школярів та студентів здатне реалізувати практико-орієнтований підхід до вивчення основ захисту даних. Дійсно, впровадження таких завдань в практику навчання сприятиме поєднанню логічного та емоційно-образного компонентів змісту інформатичної освіти, а також забезпеченню практичного досвіду використання знань під час вирішення життєво-важливих проблем на основі поєднання емоційного й пізнавального насичення навчальної діяльності тих, хто навчається.

Висновки

Виходячи з проведеного аналізу наукових та навчально-методичних джерел та вимог до здобувачів сучасної інформатичної освіти, встановлено

актуальність впровадження практико-орієнтованого підходу до вивчення основ захисту даних та визначено необхідність розробки комплексу відповідних практичних завдань.

Відповідно до мети, в роботі схарактеризовано розроблений комплект дидактичних завдань різних типів для реалізації практико-орієнтованого підходу до вивчення основ захисту даних у рамках інформатичної освіти. Завдання усіх типів спрямовані на формування досвіду використання отриманих знань під час розв'язання реальних життєво-значущих проблем із захисту даних. Крім цього, розроблені завдання забезпечують залучення тих, хто навчається, до інсценування інформаційно-небезпечних ситуацій, що спонукають до емпатії та аналізу власної поведінки.

Можна припустити, що така система завдань для реалізації практико-орієнтованого підходу сприятиме одержанню молоддю стійких навичок застосування сучасних інструментів захисту даних, формуванню їх соціально-свідомого відношення до реальних загроз інформаційній безпеці та коректної поведінки при виникненні небезпечних ситуацій, а також підвищенню рівня резистентності молоді до впливу методів, що застосовуються кіберзловмисниками. До перспектив роботи слід віднести розробку критеріального апарату для детального вивчення впливу практико-орієнтованого підходу на результати вивчення основ захисту даних в рамках інформатичної освіти.

Список використаних джерел

1. Богуш В. Інформаційна безпека держави/ Володимир Богуш, Олександр Юдін; Гол. ред. Ю. О. Шпак. -К.: "МК-Прес", 2005. -432 с.
2. Попов С. В. Проблеми інформаційної безпеки України / // Форум права. – 2011. – № 1. – С. 798–801 [Електронний ресурс]. – Режим доступу: <http://www.nbuv.gov.ua/e-journals/FP/2011-1/11pcvibu.pdf>
3. Богатырева, Ю. И. Модель обеспечения информационной безопасности школьников при создании инфобезопасной среды образовательного

учреждения / Ю. И. Богатырева // Известия Тульского государственного университета. Гуманитарные науки. — 2013. — Выпуск № 3-2. — С. 14-25.

4.Ковальчук В. Н. Забезпечення інформаційної безпеки старшокласників у комп'ютерно-орієнтованому навчальному середовищі : дис. ... канд. пед. наук: 13.00.10 / Ковальчук Вікторія Наумівна. — Житомир, 2011. — 291 с.

5.Підгорна Т., Берест І. Деякі аспекти організації інформаційної безпеки учнів Педагогіка і психологія професійної освіти, 2014, № 6, с.70-77

6.Спірін О. М. Методика забезпечення он-лайн безпеки старшокласників у навчально-виховному процесі школи/ О. М. Спірін. Інформаційні технології і засоби навчання, № 1 (21). - 2011.

7.Державний стандарт базової і повної загальної середньої освіти [Електронний ресурс]. Режим доступу: http://osvita.ua/legislation/Ser_osv/28030/ (дата звернення 08.03.2019).

8.Закон України «Про освіту» від 05.09.2017 (розділ V ст. 41)

9.Закон України «Про вищу освіту» від 01.07.2014 № 1556VII (стаття 16. Система забезпечення якості вищої освіти)

10.Калугіна І. Ю. Освітні можливості практико-орієнтованого навчання учнів : дис. канд. пед. наук: 13.00.01/І. Ю. Калугіна—Єкатеринбург, 2001. – 215с.

11.Пальшкова І. О. Формування професійно-педагогічної культури майбутнього вчителя початкової школи: практико-орієнтований підхід : автореф. дис... д-ра пед. наук : спец. 13.00.04 «Теорія та методика професійної освіти» / І. О. Пальшкова. – Одеса, 2009. – 44 с.

12.Савицька А. В. Практико-орієнтований підхід у навчанні: огляд зарубіжної літератури та проблема реалізації в вузі / А. В. Савицька // European Social Science Journal. – 2013. - № 4(23). – С. 66-74.

13.Ohlsson L., Johansson C. A practice driven approach to software engineering education, in *IEEE Transactions on Education*, vol. 38, no. 3, pp. 291-295,1995. Mode of access:

<http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=406508&isnumber=9129>

References

1. Bohush V. Information security of a state / Volodymyr Bohush, Oleksandr Yudin; Hol. red. Yu. O. Shpak. -K.: "MK-Pres", 2005. - 432 p. (in Ukrainian)
2. Popov S. V. Problems of information security of Ukraine // Forum prava. – 2011. – № 1. – p. 798–801. Available at: <http://www.nbu.gov.ua/e-journals/FP/2011-1/11pcvibu.pdf> (in Ukrainian)
3. Bogatyreva, Yu. I. Model of students' information security to create info-safe environment in educational institution. // Izvestija Tul'skogo gosudarstvennogo universiteta. Gumanitarnye nauki (News of Tula State University. Humanitarian sciences), 2013. Issue 3-2. P. 14-25. (in Russian)
4. Kovalchuk, V. N. : Information security of senior school pupils in computer-oriented learning environment : Ph.D. thesis in Pedagogical Sciences 13.00.10. Zhytomyr, 2011.- 291 p. (in Ukrainian)
5. Pidhorna T., Berest I. Some aspects of students' information security. Pedagogika i psykhologhiia profesiinoi osvity, 2014, № 6, p.70-77. (in Ukrainian)
6. Spirin O. M. Technique for ensuring the online safety of high school students in the educational process of school /O. Spirin Informaciyni tehnologii i zasoby navchannya, № 1 (21). - 2011. (in Ukrainian)
7. State standard of basic and complete general secondary education. Available at: http://osvita.ua/legislation/Ser_osv/28030/ (accessed 08.03.2019) (in Ukrainian)
8. Law of Ukraine «On education» of 05.09.2017 (rozdil V st. 41) (in Ukrainian)
9. Law of Ukraine «On higher education» of 01.07.2014 № 1556VII (stattia 16. Systema zabezpechennia yakosti vyshchoi osvity) (in Ukrainian)
10. Kaluhina I. Yu. Educational Opportunities for Student-Oriented Learning : dys. kand. ped. nauk:13.00.01/I. Yu. Kaluhina–Yekaterynburh, 2001.–215 p. (in Ukrainian)
11. Palshkova I. O. Formation of the professional-pedagogical culture of the future elementary school teacher: a practice-driven approach : avtoref. dys... d-ra ped. nauk : spets. 13.00.04 «Teoriia ta metodyka profesiinoi osvity» / I. O. Palshkova. – Odesa, 2009. – 44 p. (in Ukrainian)
12. Savytska A. V. Practice-driven Approach to Education: Review of Foreign Literature and the Problem of Implementation in Higher Education / A. V. Savytska // European Social Science Journal. – 2013. - № 4(23). – S. 66-74. (in Ukrainian)
13. Ohlsson L., Johansson C. A practice driven approach to software engineering education, in *IEEE Transactions on Education*, vol. 38, no. 3, pp. 291-295,1995. Mode of access: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=406508&isnumber=9129> (in English)

Practice-driven approach to the learning of the fundamentals of data protection in the field of Informatics education

Gryzun L.E., Suvorova O.V.

Resume

Based on the analysis of scientific and methodical sources and requirements for the recipients of contemporary information education, the paper establishes the relevance of the implementation of a practice-driven approach to the learning of the fundamentals of data protection and the need to develop the set of relevant practical

tasks. According to the aim, the paper depicts the set of didactic tasks of various types for the implementation of the said approach in the field of information education. Tasks of all types are designed to form the students' experience of implementation the earned knowledge to the solution of real life problems on data protection issues. Solving of the developed set of tasks will help youth to acquire sustainable skills of using contemporary data protection tools, to form their socially conscious attitude to real threats to information security and correct behavior in case of dangerous situations.

Keywords: fundamentals of data protection, practice-driven approach, information security.

ПРАКТИКО-ОРИЕНТИРОВАННЫЙ ПОДХОД К ИЗУЧЕНИЮ ОСНОВ ЗАЩИТЫ ДАННЫХ В РАМКАХ ИНФОРМАТИЧЕСКОГО ОБРАЗОВАНИЯ

Гризун Л.Э., Суворова О.В.

Аннотация

Исходя из проведенного анализа научных и учебно-методических источников, в работе установлена актуальность внедрения практико-ориентированного подхода к изучению основ защиты данных и определена необходимость разработки комплекта соответствующих практических заданий. Согласно целям статьи, в работе охарактеризован разработанный комплект дидактических заданий различных типов для реализации практико-ориентированного подхода к изучению основ защиты данных в рамках информатического образования. Применение разработанных задач будет способствовать получению молодежью устойчивых навыков применения современных инструментов защиты данных, формированию их социально-сознательного отношения к реальным угрозам информационной безопасности и корректного поведения при возникновении опасных ситуаций.

Ключевые слова: основы защиты данных, практико-ориентированный подход, информационная безопасность.