Data about the author
Natalya Solomianiuk
doctor of sciences, prof. Department of Marketing, National University of Food Technologies,
st. Vasilkovsky, 68, Kiev, 01601, Ukraine
e–mail: n.solomianiuk@gmail.com
Opulska Ludmila
fourth year student, University of Food Technologies,
st. Vasilkovsky, 68, Kiev, 01601, Ukraine
e–mail: liudmyla22st@gmail.com

УДК 004.056.53 *DOI: 10.5281/zenodo.1400688*

РУСІНА Ю.О.,
ЯРМАК А.І.

Інформаційна безпека як ключова складова фінансово–економічної безпеки підприємства

У статті розкрито принципи функціонування системи інформаційної безпеки підприємства та досліджено етапність створення системи захисту інформаційних ресурсів підприємства.

***Предметом дослідження** є сукупність заходів, етапів та принципів захисту системи інформаційної безпеки підприємства в контексті забезпечення його фінансово–економічної безпеки.*

***Метою статті** є дослідження особливостей формування ефективної системи забезпечення інформаційної безпеки як складової фінансово–економічної безпеки підприємства.*

***Висновки.** Інформаційна складова економічної безпеки підприємства виступає основним фактором забезпечення захищеності інформаційних ресурсів компанії та важливим чинником стабільного функціонування підприємств, ефективна реалізація якого сприятиме не тільки збереженню комерційних таємниць, але й дозволить попередити можливості непередбачуваних фінансових втрат. Впровадження ряду юридичних, організаційно–економічних та технологічних заходів забезпечення інформаційної складової фінансово–економічної безпеки підприємства дозволять створити ефективну систему інформаційної безпеки підприємства.*

***Ключові слова:** фінансово–економічна безпека, інформаційна безпека, інформаційні ресурси, підприємство.*

РУСИНА Ю.А.,
ЯРМАК А.И.

Информационная безопасность как ключевая составляющая финансово–экономической безопасности предприятия

В статье раскрыты принципы функционирования системы информационной безопасности предприятия и исследованы этапы создания системы защиты информационных ресурсов предприятия.

***Предметом исследования** является совокупность мероприятий, этапов и принципов защиты системы информационной безопасности предприятия в контексте обеспечения его финансово–экономической безопасности.*

***Целью статьи** является исследование особенностей формирования эффективной системы обеспечения информационной безопасности как составляющей финансово–экономической безопасности предприятия.*

***Выводы.** Информационная составляющая экономической безопасности предприятия выступает основным фактором обеспечения защищенности информационных ресурсов компании и важным фактором стабильного функционирования предприятий, эффективная реализация которого будет способствовать не только сохранению коммерческих тайн, но и позволит предупредить возможности непредсказуемых финансовых потерь. Внедрение ряда юридических, организационно–экономических и технологических мер обеспечения информационной составляющей финансово–экономической безопасности предприятия позволят создать эффективную систему информационной безопасности предприятия.*

Ключевые слова: *финансово–экономическая безопасность, информационная безопасность, информационные ресурсы, предприятие.*

RUSINA Yu.O.,
YARMAK A.I.

Information security as a main component of financial and economic safety of the enterprise

The article describes the principles of functioning of the information security system of the enterprise and explores the stages of creation of the system of protection of information resources of the enterprise.

The subject of the study *is a set of measures, stages and principles of protection of the enterprise information security system in the context of ensuring its financial and economic security.*

The purpose of the article *is to study the peculiarities of the formation of an effective information security system as an integral part of the financial and economic security of the enterprise.*

Conclusions. *The information component of the company's economic security is a major factor in ensuring the security of the company's information resources and an important factor in the stable operation of enterprises, whose effective implementation will contribute not only to the preservation of commercial secrets, but also to prevent unforeseen financial losses. Implementation of a number of legal, organizational, economic and technological measures to ensure the information component of the financial and economic security of the enterprise will allow to create an effective system of information security of the enterprise.*

Key words: *financial and economic security, information security, information resources, enterprise.*

Постановка проблеми. В реаліях сучасної української дійсності, що існує в умовах нестабільного зовнішнього та внутрішнього середовища, підприємства змушені будувати стратегію виживання, яка має базуватися на широкому застосуванні інформаційних технологій, одному з основних багатств економічно розвинутих держав. Інформатизація економіки, проникнення її у всі сфери діяльності людини та держави, призвели до того, що економічний потенціал будь–якого суб'єкта, в більшій мірі, визначається рівнем розвитку інформаційних структур, під впливом якого пропорційно зростає й потенційна уразливість економіки.

Інформаційні технології значно розширюють коло можливостей підприємств, забезпечують прискорення процесів обміну та співпраці, відкривають доступ до більш ефективних методів управління, однак, одночасно, й створюють умови для підриву власної економічної безпеки підприємств, впливають на зниження рівня стабільності їх фінансово–економічної діяльності. Інформація перетворилася на один із засобів конкурентної боротьби, за допомогою якого підприємство здатне не тільки отримувати реальний прибуток від її використання, але й забезпечувати стабільність свого розвитку. За таких умов набувають актуальності питання інформаційної безпеки як ключової складової фінансово–економічної безпеки підприємства.

Аналіз останніх досліджень та публікацій. Вагомий внесок у дослідження проблематики забезпечення фінансово–економічної зроблено такими вітчизняними та зарубіжними науковцями, як: С.П. Міщенко, В.І. Мунтіян, Г.В. Козаченко, Г. Пастернак–Таранушенко, В.Т. Шлемко, В.В. Тишаєв, Д.М. Прокоф'єва [2–8] та ін., якими визначено як понятійно–категоріальний апарат фінансово–економічної безпеки, так і розроблено механізм її реалізації. Однак, не дивлячись на це, в умовах випереджаючого розвитку інформаційних технологій, потребує уваги питання вивчення інформаційної складової економічної безпеки підприємства як фактора забезпечення фінансово–економічної стабільності підприємства.

Саме тому, ***метою*** даної ***статті*** є дослідження особливостей формування ефективної системи забезпечення інформаційної безпеки як складової фінансово–економічної безпеки підприємства.

Виклад основного матеріалу. Сучасний конкурентний механізм ринкового середовища побудований таким чином, що для забезпечення високих конкурентних позицій, власної економічної стабільності, підприємства змушені вдаватися до недобросовісних форм та методів бо–

ротьби, заснованих на відкритих протиборствах, знищенні матеріальних цінностей, привласненні та захопленні чужої власності. Це викликає посилену увагу бізнесу до проблем забезпечення власної фінансово–економічної безпеки, які виходять на передній план не лише в кризових умовах функціонування економіки, але й при стабільному її розвитку [6].

В загальному розумінні з поняттям «фінансово–економічна безпека підприємства» пов'язують здатність мобілізації та найбільш оптимального управління ресурсами підприємства з метою забезпечення його стабільного функціонування, активної протидії негативним впливам зовнішнього середовища. При цьому в умовах інформаційної ери – ери боротьби інформаційних технологій, все більша увага приділяється вивченню ризиків, пов'язаних з інформацією, системами її обробки, відводячи визначальну роль інформаційній складовій забезпечення фінансово–економічної безпеки підприємства.

Під інформаційною безпекою підприємства розуміють захист інформації, якою володіє підприємство (виробляє, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при надходженні. Не зважаючи на те, що інформатизація викликала формування ряду беззаперечних переваг для суб'єктів підприємницької діяльності, проникнення інформаційних технологій у всі сфери діяльності підприємств призвело до виникнення ряду істотних проблем [8]. Поширення комп'ютерних систем, об'єднання їх в комунікаційні мережі посилило можливість несанкціонованого проникнення в систему управління підприємством, що може не просто паралізувати роботу цілого підприємства, а й завдавати значних матеріальних втрат. Сьогодні втрати лише банківського сектору в результаті комп'ютерних злочинів щорічно нараховують сотні мільярдів доларів, а звичайні підприємства не одноразово піддаються набігу рейдерських атак. Саме тому, забезпечення інформаційної безпеки підприємства є невід'ємною частиною його фінансово–економічної безпеки.

Як визначено законом України «Про інформацію» захисту підлягає інформація, володіння якою дає змогу її дійсному чи потенційному власнику одержати виграш моральний, матеріальний чи політичний [1]. Отже, на перший план виходить проблема захисту таких параметрів інформації як конфіденційність, цілісність, достовірність, доступність, погіршення яких може призвести до порушення систем управління технологічними процесами та достовірності фінансової документації, розголошенню комерційних таємниць та несанкціонованому доступу до персональних даних.

Як підтверджують дані світової статистики [7], втрата тільки 20% інформації викликає руйнацію 65% фірм та компаній, а погіршення її параметрів може призвести до вкрай важких наслідків, пов'язаних з розривом партнерських відносин, невиконанням умов договорів, втратою вигідних контрактів, відмовою від прийнятих рішень, які стали неефективними в результаті розголошення конфіденційної інформації. І, як результат колосальні фінансові втрати компаній, які залишають свій відбиток не лише на обсягах виробництва та реалізації продукції, але й наносять «пляму» на авторитет та ділову репутацію компанії, призводячи в майбутньому в крайньому випадку або до повного банкрутства підприємства, або до більш жорстких умов отримання кредитів та труднощів в сфері співпраці з постачальниками. При цьому за даними досліджень близько 75% витоку інформації компаній відбувається виключно за рахунок її розголошення співробітниками фірм, зі 100% опитаних працівників 25% завжди готові продавати комерційну таємницю [10].

У 2017 році був зареєстрований 2 131 випадок витоку конфіденційної інформації. Обсяг даних, скомпрометованих в результаті витоків, склав 13,2 млрд. записів – номера соціального страхування, реквізити пластикових карт та інша критично важлива інформація. Кількісні показники витоків в 2017 році склали вибухово позитивну динаміку. Якщо в 2016 році приріст числа витоків до попереднього року склав 3,4%, то в 2017 році число витоків зросло на 36,9% [13]. Багато в чому, це зростання пов'язане зі зміною підходу до зберігання та обробки персональних і, пов'язаних з ними, даних. Раніше дані про клієнтів, співробітників, громадян зберігалися і оброблялися розрізнено, в філіях і підрозділах, набір таких даних був обмежений. Тепер, з розвитком технологій зберігання і обробки інформації, компанії та держави по всьому світу прагнуть об'єднати інформацію в єдине сховище, щоб максимально ефективно використовувати обчислювальні потужності і можливості сучасних

технологій вилучення нового знання на великих масивах даних.

Досліджуючи дані 2017р. щодо витоків інформації, можна зазначити, що скоротилася частка витоків через паперові документи (–2,6%), знімні носії (–1,9%), в результаті крадіжки або втрати обладнання (–1,5%). Але частка витоків по каналу «електронна пошта» збільшилися (+4,8%). Показники витоків з мережевого каналу, через миттєві повідомлення (текстові, голосові), за допомогою мобільних пристроїв залишилися на рівні 2016 року [13].

Розподіл витоків по каналах рік від року змінювався незначно, що дає підстави говорити про стійкість факторів, що лежать в основі такого розподілу. Найбільш очевидним фактором слід зазначити об'єктивні особливості інформаційних процесів, апаратного і програмного середовища, яке ці процеси забезпечує.

В зв'язку з цим, більшість підприємств вирішення проблем по забезпеченню власної фінансово–економічної безпеки, пов'язують зі створенням сучасної корпоративної системи інформаційної безпеки, здатної сприяти захисту конфіденційності інформації від несанкціонованого доступу та нейтралізації факторів погроз фінансово–економічній безпеці компанії. Така система повинна забезпечувати максимальне скорочення величини ризиків, пов'язаних з інформаційними технологіями, з мінімальним рівнем витрат на їх реалізацію та володіти високим запасом гнучкості для самостійної адаптації в умовах мінливого зовнішнього середовища [9]. На думку авторів статті, створення ефективної системи інформаційної безпеки підприємства вимагає розробки ряду юридичних, організаційно–економічних та технологічних заходів, спрямованих на:

– своєчасне виявлення та запобігання розголошенню конфіденційної інформації, аналіз причин та умов їх виникнення і реалізації;

– вивчення каналів розподілу інформації, виявлення та призупинення несанкціонованого доступу до них;

– розробку механізмів оперативного реагування на погрози, засновані на використанні різного роду юридичних, економічних, технічних засобів та методів їх виявлення і нейтралізації;

– організацію спеціальної системи документообігу, що виключає можливість несанкціонованого отримання інформації;

– попередження різного роду форм незаконного втручання в інформаційні ресурси підприємства, що створюють погрозу для підриву його фінансово–економічної безпеки.

Однак, безперервний захист інформації можливий лише при створенні спеціальної системи захисту, побудованої з урахуванням індивідуальних особливостей підприємства (організаційної структури, обсягу та характеристики інформаційних потоків, кількості та характерів виконуваних операцій, характерів клієнтів) та здатній забезпечувати комплексний характер захисту на всіх етапах життєвого циклу економічної системи. Відповідно до цього організація та функціонування системи захисту інформаційної складової фінансово–економічної безпеки підприємства повинні відповідати наступним принципам [8]:

1. Обґрунтованість.
2. Комплексність.
3. Безперервність.
4. Спеціалізація.
5. Взаємодія і координація.
6. Вдосконалення.
7. Централізація управління.

Останнім часом, для забезпечення збереження інформації підприємствами створюються цілі структурні підрозділи, які відповідають за збереження комерційних таємниць та захисту від несанкціонованих втручань з боку зовнішнього оточення. В цілому, основним етапами системи захисту інформації можна визначити [11]:

1. Аналіз можливих погроз. На цьому етапі визначається перелік реальних погроз, які можуть завдати серйозних збитків підприємству.

2. Розробка системи захисту (планування). Цей етап реалізації системи захисту інформації передбачає розробку комплексної системи захисту як сукупності засобів, здатних протидіяти впливам різного характеру. Результатом даного етапу є розробка плану захисту організації від несанкціонованих втручань, який містить перелік компонентів інформаційної системи підприємства, що підлягають захисту та можливий вплив на них, мету захисту інформації, правила її обробки та користування персоналом і користувачами інформаційної системи підприємства, детальний опис розробленої системи захисту.

3. На етапі реалізації системи захисту відбувається установка та настройка, визначених планом захисту, засобів захисту.

Етапність побудови системи захисту інформації підприємства

Джерело: Складено авторами на основі [8; 11]

4. Етап супроводження системи захисту передбачає постійний контроль над роботою системи, реєстрацію подій, які відбуваються в ній, їх аналіз з метою виявлення факт порушення безпеки функціонування інформаційної системи підприємства.

В загальному вигляді етапність побудови системи захисту інформації підприємства можна представити у вигляді схеми (див. рисунок).

У широкому розумінні підприємство володіє інформаційною безпекою, якщо забезпечується не тільки надійність роботи комп'ютерних мереж, збереження цінних даних, захист інформації від несанкціонованого доступу та збереження таємниці переписки електронним зв'язком, але й виконуються основні принципи інформаційної безпеки підприємства, а саме: принцип законності, невизначеності, мінімального ризику та мінімальної шкоди, безпечного часу, «захисту всіх від усіх», персональної відповідальності, обмеження повноважень, взаємодії та співпраці, комплексності та індивідуальності, послідовності рубежів безпеки тощо [11]. При цьому, більшість експертів та науковців, які цікавляться питанням інформаційного забезпечення фінансово–економічної безпеки, відводять визначальну роль в її забезпеченні економіко–математичним методам пошуку, збору, аналізу, обробки та використання інформації, які тим чи іншим чином сприяють підвищенню фінансово–економічного потенціалу підприємства та передбачають оцінку важливості інформації, що потребує захисту, та інформаційних ризиків підприємства; оцінку вразливості інформації та системи, в якій вона функціонує та економічне обґрунтування доцільності витрат на забезпечення інформаційної безпеки [12].

Однак, розглядаючи зміст процесу забезпечення інформаційної складової фінансово–економічної безпеки підприємства, необхідно зазначити, що будь–яка система повинна носити комплексний характер захисту та передбачати ряд заходів, здатних забезпечувати:

– постійний моніторинг каналів розподілу інформації, доступ працівників до інформаційних ресурсів підприємства з метою завчасного виявлення та попередження ймовірності її витоку за межі підприємства;

– постійний контроль за інформацією, що має характер комерційної таємниці підприємства з метою передбачення можливостей незаконного втручання на всіх рівнях обробки даних та можуть призвести до її знищення, руйнування, спотворення;

– організацію безвідмовної роботи інформаційних систем та ресурсів підприємства;

– прогнозування тенденцій розвитку науково–го та технологічного потенціалів підприємства з метою встановлення можливості факту незаконного заволодіння об'єктами інтелектуальної власності компанії;

Висновок

Таким чином, інформаційна складова фінансово–економічної безпеки підприємства в системі випереджаючого розвитку інформаційних технологій виступає основним фактором забезпечен–

ня захищеності інформаційних ресурсів компанії та важливим чинником стабільного функціонування підприємств, ефективна реалізація якого сприятиме не тільки збереженню комерційних таємниць, але й дозволить попередити можливості непередбачуваних фінансових втрат.

Список використаних джерел

1. Закон України «Про інформацію» [Електронний ресурс] // Сайт Верховної Ради України. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2657-12.

2. Мунтіян В.І. Економічна безпека України [Текст] / В.І. Мунтіян. – К.: КВІУ, 1999. – 464 с.

3. Козаченко Г.В. Економічна безпека підприємства: сутність та механізм забезпечення [Текст]: Монографія / Г.В.Козаченко, В.П. Пономарьов, О.М.Ляшенко. – К.: Лібра, 2003. – 280 с.

4. Пастернак-Таранушенко Г. А. Економічна безпека держави. Статика процесу забезпечення [Текст] / Г. Пастернак-Таранушенко; за ред. проф. Б. Кравченка. – К. : Кондор, 2002. – 302 с.

5. Шлемко В.Т Економічна безпека України: сутність і напрямки забезпечення [Текст]: монографія / В. Т. Шлемко, І. Ф. Бінько. – К.: НІСД. – 1997. – 144 с.

6. Тишаев В.В. Информационная составляющая экономической безопасности хозяйствующих субъектов и ее значение для обеспечения устойчивого развития национальной экономики [Текст] / В.В. Тишаев// Управление общественными и экономическими системами, 2007. – №.1. – С.1-11.

7. Прокоф'єва Д.М. Підприємницьке шпигунство в системі інформаційних злочинів [Текст] / Д.М. Прокоф'єва // Український центр інформаційної безпеки. 2008. – с.123-128.

8. Міщенко С.П. Інформаційна складова економічної безпеки підприємства [Текст] / С.П.Міщенко // Вісник економіки транспорту і промисловості, № 39, 2012. – с. 250-254.

9. Волков Я. Системы обеспечения информационной безопасности как часть корпоративной культуры современной организации [Текст] / Я.Волков // Финансовая газета, 2006. – №34. – С.15.

10. Ткачук Т. Формування системи інформаційної безпеки бізнесу [Текст] / Т.Ткачук // Бізнес і безпека, 2009. – №4. – С.19-23.

11. Ясенев В.Н. Информационная безопасность в экономических системах [Текст]: Учебн.пособ / В.Н. Ясенев. – Новгород: Изд-во ННГУ, 2006. – с. 253.

12. Гриджук Г.С. Систематизація методів інформаційної безпеки підприємства. [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/portal/natural/vntu/2009_19_1/pdf/64.pdf.

13. Глобальне дослідження витоків конфіденційної інформації 2017 році [Електронний ресурс]. – Режим доступу: https://www.ec-rs.ru/novosti/utechki-konfidentsialnoy-informatsii-v-2017-godu-globalnoe-issledovanie-infowatch.

References

1. Law of Ukraine «On Information» [Electronic resource] // Site of Verkhovna Rada of Ukraine. – Mode of access: http://zakon4.rada.gov.ua/laws/show/2657-12.

2. Muntian V. Economic security of Ukraine [Text] / V. Muntian – K .: KVIU, 1999. – 464 p.

3. Kozachenko G. Economic security of the enterprise: the essence and mechanism of providing [Text]: Monograph / G. Kozachenko, V. Ponomarev, O. Lyashenko. – K .: Libra, 2003. – 280 p.

4. Pasternak-Taranushenko G. Economic security of the state. Static of the process of providing [Text] / G. Pasternak-Taranushenko; for ed. prof. B. Kravchenko. – K.: Condor, 2002. – 302 p.

5. Shlemko V. Economic security of Ukraine: the essence and directions of providing [Text]: monograph / V. Shlemko, I. F. Binko. – K .: NISS. – 1997. – 144 p.

6. Tishaev V. Information component of economic security of economic entities and its importance for ensuring sustainable development of the national economy [Text] / V. Tishaev // Management of Public and Economic Systems, 2007. – No. 1. – P.1-11.

7. Prokofiev D. Entrepreneurial espionage in the system of information crimes [Text] / D. Prokofiev / / Ukrainian Center for Information Security. 2008. – December 12-128.

8. Mischenko S. Information component of economic security of the enterprise [Text] / S. Mishchenko // Bulletin of the Economy of Transport and Industry, No. 39, 2012. – p. 250-254.

9. Volkov Y. Information security systems as part of the corporate culture of a modern organization [Text] / Y.Volkov // Financial Newspaper, 2006. – No. 34. – P.15.

10. Tkachuk T. Formation of the system of information security of business [Text] / T. Tkachuk // Business and Security, 2009. – №4. – September 19-23.

11. Yasenev V. Information security in economic systems [Text]: Learning method / V. Yasenev – Novgorod: Publishing house of NNUU, 2006. – p. 253

12. Gridzuk G. Systematization of methods of enterprise information security. [Electronic resource].

– Access mode: http://www.nbuv.gov.ua/portal/natural/vntu/2009_19_1/pdf/64.pdf.

13. Global Survey of Confidential Information Origins 2017 [Electronic Resource]. – Access mode: https://www.ec–rs.ru/novosti/utechki–konfidentsialnoy–informatsii–v–2017–godu–globalnoe–issledovanie–infowatch.

Дані про автора

Русіна Юлія Олександрівна,

к.е.н., доцент кафедри фінансів та фінансово–економічної безпеки, Київський національний університет технологій та дизайну

e–mail: rusmaxrus@meta.ua

Ярмак Анна Іванівна,

студентка кафедри фінансів та фінансово–економічної безпеки, Київський національний університет технологій та дизайну

e–mail: yarmakanna2559@gmail.com

Данные об авторе

Русина Юлия Александровна,

к.е.н, доцент кафедры финансов и финансово–экономической безопасности, Киевский национальный университет технологий и дизайна

e–mail: rusmaxrus@meta.ua

Ярмак Анна Ивановна,

студентка кафедры финансов и финансово–экономической безопасности, Киевский национальный университет технологий и дизайна

e–mail: yarmakanna2559@gmail.com

Data about the author

Yulia Rusina,

PhD, Associate Professor of the Department of Finance and financial and economic security, Kiev National University of Technology and Design

e–mail: rusmaxrus@meta.ua

Anna Yarmak,

Student of the Department of Finance and financial and economic security, Kiev National University of Technology and Design

e–mail: yarmakanna2559@gmail.com

УДК 330.34.014–026.23:338.22:005.334:339.9–048.23(204) DOI: 10.5281/zenodo.1400796

КОЛОДІЙЧУК А.В.

Гідросферні екоризики впровадження ІКТ: класифікація та характеристика

У статті ідентифіковано і охарактеризовано підгрупи й класи потенційних загроз у складі групи гідросферних ризиків впровадження інформаційно–комунікаційних технологій в національній економіці та в рамках окремих її регіонів. Визначено сутність гідросферних ризиків ІКТ, доведена актуальність і необхідність їх вивчення та моніторингу за ними. Так, встановлено, що гідросферні екоризики впровадження ІКТ–технологій позначають усі можливі загрози від роботи та / або несправностей роботи комп'ютерно–комунікаційного та електронно–цифрового обладнання для природнього водного середовища (річки, озера, моря, океани тощо), в який вони поміщені або поряд з яким вони знаходяться. Запропонована і обґрунтована класифікація гідросферних екологічних ризиків інтрузії ІКТ–технологій. Зокрема, розглянуто океанічні, морські, річкові, водоймові, підземні, льодовикові підгрупи відповідного роду загроз; дано характеристику наступним класам ризиків: гідросферо–батискафні, субмаринні, ризики цифрової гідроенергетики, ризики аварій водних транспортних перевезень, ризики забруднень каналізаційними відходами, еколого–навігаційні ризики, захаращення гідросфери ІКТ–обладнанням. У рамках кожного класу ризиків наведені відповідні приклади. Обґрунтована необхідність посилення екологічних вимог до питань взаємодії ІКТ з ресурсами гідросфери.

Ключові слова: *гідросфера, екологія, ризики, інформаційні та комунікаційні технології, навігація, «розумні» технології, енергетика, забруднення.*

КОЛОДИЙЧУК А.В.

Гидросферные экориски внедрения ИКТ: классификация и характеристика

В статье идентифицированы и охарактеризованы подгруппы и классы потенциальных угроз

