УДК 35.073.515 / 477.62

Седікова І. О.

РОЛЬ ІНФОРМАЦІЙНОЇ СКЛАДОВОЇ У СИСТЕМІ ЗБЕРІГАННЯ ТА ПЕРЕРОБКИ ЗЕРНА

У статті проаналізовано сучасний стан діючої системи отримання інформації суб'єктами зернового ринку. Проведений аналіз чинної системи отримання інформації підприємствами зберігання та переробки зерна показав, що вона не відповідає новим умовам. Були виявлені основні недоліки: відсутність достовірних матеріалів; нестача ринкової і науково-технічної інформації виробничого призначення; функціонування системи базується на застарілих паперових технологіях збору, обробки й розповсюдження інформації; не налагоджені контакти і не забезпечений обмін інформацією з міжнародними та національними центрами наукової, інформаційної та ділової активності в повному обсязі. Обґрунтована доцільність створення єдиної інформаційної системи зернового ринку. Розглянуто основні положення системної концепції захисту інформації від несанкціонованого доступу в автоматизованих інформаційних системах та визначено чотири базові підсистеми системи захисту інформації від несанкціонованого доступу.

Ключові слова: ринок зерна, інформаційні системи, підприємства зберігання та переробки зерна, захист інформації, несанкціонований доступ

Рис.: 2. *Бібл.*: 10.

Седікова Ірина Олександрівна – кандидат економічних наук, доцент, кафедра менеджменту та логістики, Одеська національна академія харчових технологій (вул. Канатна, 112, Одеса, 65039, Україна)
Email: irina-sedikova@rambler.ru

УДК 35.073.515 / 477.62

Седикова И. А.

РОЛЬ ИНФОРМАЦИОННОЙ СОСТАВЛЯЮЩЕЙ В СИСТЕМЕ ХРАНЕНИЯ И ПЕРЕРАБОТКЕ ЗЕРНА

В статье проанализировано современное состояние действующей системы получения информации субъектами зернового рынка. Проведенный анализ системы получения информации предприятиями хранения и переработки зерна показал, что она не отвечает современным условиям. Выявлены основные недостатки действующей системы: отсутствие достоверных материалов; недостаток рыночной и научно-технической информации производственного назначения; функционирование системы базируется на устаревших бумажных технологиях сбора, обработки и распространения информации; не налажены контакты, не обеспечен обмен информацией с международными и национальными центрами научной, информационной и деловой активности. Обоснована целесообразность создания единой информационной системы зернового рынка. Рассмотрены основные положения системной концепции защиты информации от несанкционированного доступа в автоматизированных информационных системах и определены четыре базовые подсистемы системы защиты информации от несанкционированного доступа.

Ключевые слова: рынок зерна, информационные системы, предприятия хранения и переработки зерна, защита информации, несанкционированный доступ

Рис.: 2. *Библ.*: 10.

Седикова Ирина Александровна – кандидат экономических наук, доцент, кафедра менеджмента и логистики, Одесская национальная академия пищевых технологий (ул. Канатная, 112, Одесса, 65039, Украина)
Email: irina-sedikova@rambler.ru

UDC 35.073.515 / 477.62

Sedikova I. O.

ROLE OF INFORMATION COMPONENT IN THE SYSTEM OF STORAGE AND PROCESSING OF GRAIN

The article analyses the modern state of the existing system of obtaining information by the grain market subjects. The conducted analysis of the system of obtaining information by grain storing and processing enterprises shows that it does not meet modern requirements. The article reveals main shortcomings of the existing system: absence of trustworthy materials; shortage of the market and scientific and technical information of production purpose; the system functioning is based on outdated hard-copy technologies of collection, processing and distribution of information; contacts are not established, exchange of information with international and national centres of scientific, information and business activity is not arranged. The article justifies expediency of creation of a common information system of the grain market. It considers main provisions of the system concept of protection of information from unauthorised access in automated information systems and identifies four basic subsystems of the system of protection of information from the unauthorised access.

Key words: grain market, information systems, grain storing and processing enterprises, protection of information, unauthorised access

Pic.: 2. *Bibl.*: 10.

Sedikova Iryna O. – Candidate of Sciences (Economics), Associate Professor, Department of Management and Logistics, Odesa National Academy of Food Technology (vul. Kanatna, 112, Odessa, 65039, Ukraine)
Email: irina-sedikova@rambler.ru

Вступ. Україна є однією з найбільших виробників зерна в Європі, збираючи щорічно 40 – 53 млн тонн. За останні роки країна перетворилась на найбільшого експортера зерна. Зернова галузь має суттєвий потенціал розвитку, пов'язаний, перш за все, з наявністю багатих земельних ресурсів і достатньої кількості кваліфікованої робочої сили. Значною проблемою сучасного українського зернового сектору є певна обмеженість учасників ринку в різноманітній, різнобічній та достовірній ринковій інформації, що надходить з різних джерел.

Основні засади державної політики щодо формування та розвитку зернового ринку закладено у низці законодавчих актів, серед яких – Закон України «Про зерно та ринок зерна в Україні», який визначає державну політику щодо розвитку ринку зерна як пріоритетного сектору економіки агропро-

мислового комплексу України; Указ Президента України «Про невідкладні заходи щодо стимулювання виробництва та розвитку ринку зерна» – гарантує цивілізований рух зерна, прозору ринкову інфраструктуру, зниження негативних наслідків сезонних і кон'юнктурних коливань цін на зерно, підвищення рівня рентабельності та стимулювання його виробництва, а також низка нормативно-правових актів щодо функціонування аграрного ринку, а саме: Укази Президента України від: 6.06. 2000 р. № 767/2000 «Про заходи щодо забезпечення формування і функціонування аграрного ринку»; 8. 08. 2002 р. № 694/2002 «Про заходи щодо розвитку аграрного ринку»; 19. 09. 2007 р. № 1158 «Про затвердження Державної цільової програми розвитку українського села на період до 2015 р.». Незважаючи на наявність нормативно-правового забезпечення розвитку інфраструктури зернового ринку, в Україні її функціонування ще не забезпечує вільний прозорий рух продукції, а відсутність чіткої схеми реалізації «виробник – оптова торгівля – роздрібна торгівля – споживач» негативно впливає на цінову ситуацію на ринку, що досліджується, та не дає виробнику можливості отримати достатній дохід з вирощеної продукції. Об'єднання інформаційних ресурсів баз даних, пов'язаних зі станом та діяльністю учасників зернового ринку, є передумовою проведення всебічного аналізу діяльності гравців ринку та своєчасного прийняття превентивних управлінських рішень. Водночас, через ряд обставин, нерозв'язаними залишаються проблеми оперативного одержання (в тому числі в автоматизованому режимі) інформації з відповідних баз даних, необхідної для аналізу та оцінки заходів, щодо ефективного функціонування суб'єктів зернового ринку.

Постановка завдання. Метою даного дослідження є визначення реального стану щодо справ діючої системи отримання інформації суб'єктами зернового ринку, зокрема при торгівлі зерном, існуючих структур та сил, що впливають на функціонування об'єктів ринку, можливості виробників реагувати на сигнали ринку, можливості щодо підвищення ефективності каналів постачання. Визначення основної системи захисту інформації на підприємствах, які досліджуються.

Виклад основного матеріалу. Ефективність діяльності підприємств зберігання та переробки зерна у сучасних умовах залежить від якості управлінських рішень, що визначаються тим, наскільки вдало організовано рух інформаційних потоків як усередині підприємства, так і між підприємством та його зовнішнім середовищем. Вирішення проблеми раціональної організації руху інформаційних потоків неможливе без створення дієвої інформаційної системи, яка б забезпечувала неперервний процес збирання, оброблення, передавання та зберігання інформації. Для ефективного управління підприємством потрібно володіти великим обсягом різноманітної оперативної та об'єктивної інформації про структуру посівних площ, стан сільськогосподарських угідь, рослинності та ґрунтів, а також очікувану врожайність. Крім того, внаслідок зміни клімату (глобальне потепління) виникла необхідність перегляду існуючого агрокліматичного районування сільськогосподарських територій та стало актуальним питання корегування технологічних карт вирощування сільгоспкультур (оптимізація їх розміщення, корегування строків сівби та режимів зрошування).

У розвинених країнах світу (США, Канада, Австралія, країни ЄС) для інформаційного забезпечення сільськогосподарського менеджменту всіх рівнів широко використовують різноманітні інформаційні системи, такі як:

- системи моніторингу стану агроресурсів та прогнозування урожайності сільськогосподарських культур;
- системи забезпечення контролю якості сільськогосподарської продукції;
- системи оперативного управління та оптимізації продукційних процесів;
- інформаційно-довідкові системи маркетингової спрямованості;
- аналітичні та моделюючі системи відстеження розвитку надзвичайних ситуацій та їх впливу на виробництво, якість сільськогосподарської продукції та багато інших спеціалізованих інформаційних систем різноманітної спрямованості та рівня деталізації.

Проведений аналіз діючої системи отримання інформації підприємствами зберігання та переробки зерна показав, що вона не відповідає новим умовам. Були виявлені основні недоліки, а саме: відсутність одного з основних базових елементів інформаційної системи – достовірних матеріалів; нестача інформаційних ресурсів, в першу чергу ринкової і науково-технічної інформації виробничого призначення; домінуючі інформаційні потоки не спрямовані на обслуговування виробничих структур; функціонування системи базується головним чином на застарілих паперових технологіях збору, систематизації, обробки і розповсюдження інформації і не забезпечує необхідної оперативності; не налагоджені контакти і не забезпечений обмін інформацією з міжнародними та національними центрами наукової, інформаційної і ділової активності в тому обсязі, якого потребують сучасні процеси.

Для визначення реального стану справ щодо діючої системи отримання інформації учасниками ринку та якого виду інформації бракує для прийняття ефективних рішень, було проведене опитування учасників зернового ринку Одеської області. В опитуванні прийняли участь респонденти, що працюють в регіоні. Опитування охопило декілька цільових груп: виробники зерна, зернові склади, переробники, торгівельні компанії, кредитно-фінансові установи, страхові компанії тощо (рис. 1).

Опитування показало різну поінформованість респондентів про зерновий ринок загалом і його учасників зокрема, але абсолютна більшість респондентів не володіє вичерпною і достатньою інформацією. Результати опитування показали, що учасники зернового ринку найменше поінформовані про світовий ринок зерна, майже 14 % респондентів взагалі не володіють такою інформацією, 40 % респондентів недостатньо поінформовані, 37 % поінформовані частково і лише 10 % володіють достатньою інформацією.

Рівень поінформованості про внутрішній зерновий ринок значно кращий, але 5 % респондентів зазначили, що володіють інформацією, 22 % володіють недостатньою інформацією, 50 % поінформовані частково, 23 % володіють достатньою інформацією. Наведені дані викривають неосяжне

Рис. 1. Учасники опитування

поле діяльності для проведення інформаційної роботи серед учасників зернового ринку.

Однією з умов ефективної і вдалої співпраці в межах ланцюга постачання зерна є високий рівень обізнаності всіх його учасників з вимогами партнерів та умовами співпраці з ними. В процесі пошуку і організації нових каналів постачання дуже важливо володіти інформацією і вміти реагувати на потреби ринку. Зважаючи на це, в ході опитування ми прагнули дослідити рівень обізнаності респондентів про учасників ланцюга постачання та їх потреби. Результати опитування показали, що майже 5 % респондентів не володіють інформацією про виробників, переробників, трейдерів та споживачів.

Найкраще респонденти поінформовані про виробників зерна: 28 % володіють достатньою інформацією, 44 % частково поінформовані і 24 % недостатньо поінформовані. Володіють достатньою інформацією про переробників зерна 24 % респондентів, 43 % поінформовані частково і 28 % недостатньо поінформовані. Про діяльність і вимоги трейдерів володіє достатньою інформацією 17 % респондентів, частково поінформовані 38 % і 40 % поінформовані недостатньо. Показовим є рівень обізнаності про споживачів зерна, які часто є кінцевою ланкою ланцюга постачання зерна. Лише 16 % респондентів володіють достатньою інформацією про українських споживачів і 9 % про споживачів зерна загалом, при цьому 38 % респондентів володіють недостатньою інформацією. Передбачаючи брак поінформованості респондентів, було вирішено визначити їх зацікавленість в отриманні додаткової інформації про своїх потенційних та/або існуючих партнерів.

Всі учасники опитування зазначили, що хотіли б знати більше про того чи іншого учасника (групу учасників) зернового ринку. Загальний розподіл інформаційних потреб респондентів про діяльність і можливості співпраці з іншими учасниками ланцюга постачання зерна наведено на рис. 2.

Показово, що майже 70 % респондентів потребують більшої інформації про партнерів, так чи інакше пов'язаних із реалізацією зерна – трейдерів / експортерів (19 %), кінцевих споживачів (24 %) та переробників (27 %). Про виробників зерна бажають знати більше 17 % респондентів, ще 12 % зацікавлені в інформації про діяльність державних органів.

Крім інформації про партнерів по ланцюгу постачання зерна, респонденти висловлюють певну потребу і в загальній ринковій інформації. Найбільшу зацікавленість викликають попит і цінова інформація (загалом 54 %). Умовами зберігання на зернових складах цікавляться 16 %. Не надто цікавою для респондентів є інформація про урядові програми з підтримки зернового ринку (12 %), що може свідчити про певне

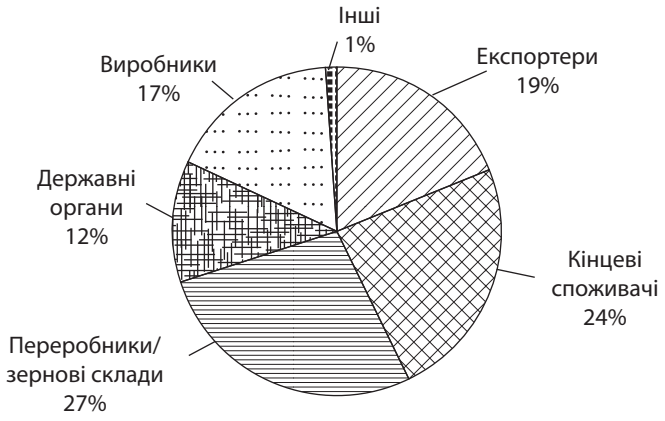

Рис. 2. Загальна потреба респондентів в інформації про інших учасників ринку

розчарування в державній політиці. Лише 10 % респондентів зацікавлені в інформації про умови постачання зернових до споживачів, що може свідчити про існування сталих і відпрацьованих партнерських відносин в ланцюгу постачання. При цьому лише 8 % респондентів хотіли б мати інформацію про баланси зернових, що може свідчити про недосконалість практики планування і прогнозування з використанням цієї інформації. В ході опитування дуже цікаво було дослідити використання респондентами тих чи інших напрямків та каналів збуту продукції. Результати опитування свідчать про використання декількох основних каналів збуту зерна. Вказані дані відображають лише частоту використання тих чи інших каналів і не відображають обсягів реалізації за цими каналами.

Слід зазначити, що реалізація зерна населенню має відношення, насамперед, до зерновиробників і дрібних індивідуальних локальних торговців, решта каналів використовується всіма учасниками ланцюга. Вибір каналу реалізації залежить від декількох факторів, перш за все ціни і стабільності відносин, по-друге, репутації партнера і, відповідно, рівня довіри. Крім цих критеріїв вибору каналу реалізації існують і інші.

Наприклад, зерновиробники надають перевагу роботі з оптовими компаніями (трейдерами / експортерами), адже вони часто беруть на себе транспортування зерна до місця призначення. Значна кількість зерновиробників зазначала, що і досі не завжди довіряють зерновим складам через заниження якості зерна, крім того, продаж зерновому складу чи переробному підприємству часто пов'язаний з транспортними витратами. Майже третина опитаних орієнтується в своїй діяльності на потреби переробних підприємств, 27 % – на кінцевих споживачів, 24 % – на трейдерів / експортерів, 16 % – на державу.

Для забезпечення взаємовигідної співпраці на зерновому ринку необхідно не тільки знати потреби і вимоги споживачів і партнерів, але і враховувати їх у своїй діяльності. За результатами опитування 57 % респондентів враховують або намагаються враховувати потреби споживачів, 40 % не враховують і 3 % частково або інколи враховують потреби споживачів. Таким чином, в концептуальному баченні вимальовується перспективна структура єдиної інформаційної системи зернового ринку, яка будується на співпраці державних органів, підприємницьких структур інформаційно-консультаційного сервісу та інформаційно-аналітичних служб підприємств (асоціацій, об'єднань), елементи інфраструктури якої взаємодіють на принципах асоційованого співробітництва.

При створенні єдиної інформаційної системи зернового ринку виникає гостра проблема – захисту інформації, яка становить державну та іншу, передбачену законом, таємницю, а також конфіденційної інформації, що є власністю держави або спрямована на забезпечення потреб та національних інтересів суспільства і держави.

Серед загроз, які можуть призвести до розголошення інформації, за своїми небезпечними наслідками особливе місце займають несанкціонований доступ (НСД) до інформації, яка обробляється та циркулює на підприємствах зберігання та переробки зерна та в інформаційно-телекомунікаційних системах, а також витік інформації технічними каналами. Під НСД звичайно розуміється доступ до інформації, що порушує встановлену в інформаційній системі політику розмежування доступу. Під технічними каналами розглядаються канали побічних електромагнітних випромінювань і наводок, акустичні канали, оптичні канали та інші [1]. Захист від НСД може здійснюватися в різних складових інформаційної системи: прикладне та системне програмне забезпечення (ПЗ); апаратна частина серверів та робочих станцій; комунікаційне обладнання та канали зв'язку; периметр інформаційної системи.

Для захисту інформації на рівні прикладного та системного ПЗ використовуються: системи розмежування доступу до інформації; системи ідентифікації та автентифікації; системи аудиту та моніторингу; системи антивірусного захисту.

Для захисту інформації на рівні апаратного забезпечення використовуються: апаратні ключі, системи сигналізації; засоби блокування пристроїв та інтерфейс вводу-виводу інформації.

В комунікаційних системах використовуються такі засоби мережевого захисту інформації: міжмережеві екрани (англ. Firewall) – для блокування атак із зовнішнього середовища (Cisco PIX Firewall, Symantec Enterprise FirewallTM, Contivity Secure Gateway та Alteon Switched Firewall від компанії Nortel Networks). Вони керують проходженням мережевого трафіку відповідно до правил (англ. policies) захисту. Як правило, міжмережеві екрани встановлюються на вході мережі і розділяють внутрішні (приватні) та зовнішні (загального доступу) мережі; системи виявлення втручань (англ. Intrusion Detection System) – для виявлення спроб несанкціонованого доступу як ззовні, так і всередині мережі, захисту від атак типу «відмова в обслуговуванні» (Cisco Secure IDS, Intruder Alert та NetProwler від компанії Symantec). Використовуючи спеціальні механізми, системи виявлення вторгнень здатні попереджувати шкідливі дії, що дозволяє значно знизити час простою внаслідок атаки і витрати на підтримку працездатності мережі; засоби створення віртуальних приватних мереж (англ. Virtual Private Network) – для організації захищених каналів передачі даних через незахищене середовище (Symantec Enterprise VPN, Cisco IOS VPN, Cisco VPN concentrator). Віртуальні приватні мережі забезпечують прозоре для користувача сполучення локальних мереж, зберігаючи при цьому конфіденційність та цілісність інформації шляхом її динамічного шифрування; засоби аналізу захищеності – для аналізу захищеності корпоративної мережі та виявлення можливих каналів реалізації загроз інформації (Symantec Enterprise Security Manager, Symantec NetRecon). Їх застосування дозволяє попередити можливі атаки на корпоративну мережу, оптимізувати витрати на захист інформації та контролювати поточний стан захищеності мережі.

Захист інформації від її витоку технічними каналами зв'язку забезпечується такими засобами та заходами: використанням екранованого кабелю та прокладка проводів та кабелів в екранованих конструкціях; встановленням на лініях зв'язку високочастотних фільтрів; побудовою екранованих приміщень («капсул»); використанням екранованого обладнання; встановленням активних систем зашумлення; створенням контрольованої зони [2, с.128].

Функціонування системи технічного захисту інформації здійснюється з урахуванням необхідності забезпечення гарантії відповідності рівня захищеності інформації вимо-

гам нормативних документів. При цьому необхідну якість робіт з технічного захисту інформації можна забезпечити за умови залучення спеціалістів, які мають відповідну фахову підготовку та досвід роботи, при відповідному технічному оснащенні.

Обов'язковою умовою забезпечення захисту інформації, яка циркулює в інформаційно-телекомунікаційних системах та на об'єктах інформаційної діяльності, є одержання об'єктивної оцінки рівня захищеності інформації. Це здійснюється через систему державної експертизи та атестації. Ефективність робіт з технічного захисту інформації може бути досягнуто за умови застосування захищених засобів обробки інформації та засобів її захисту, які мають відповідні сертифікати та експертні висновки. Для цього зазначені засоби, які надходять на український ринок і споживачі яких належать до сфери державного управління, проходять перевірку на відповідність вимогам технічного захисту інформації в Українській державній системі сертифікації продукції УкрСЕПРО, а також через державну експертизу у сфері технічного захисту інформації.

Важливе місце в системі технічного захисту інформації відіграє державний контроль за її функціонуванням, який здійснюється Інспекцією Департаменту шляхом проведення контрольно-інспекторських перевірок виконання вимог нормативно-правових актів у сфері технічного захисту інформації.

Згідно з критерієм безпеки комп'ютерних систем TCSEC США (1983 р.), інакше відомому як «Оранжова книга», захищеність інформації в будь-якій комп'ютерній системі в цілому оцінювалась за трьома її класами: клас С2 – мінімальний рейтинг захищеності від несанкціонованого доступу, клас В2 – відносно стійкий захист від несанкціонованого доступу, клас В3 – стійкий захист від несанкціонованого доступу [2, с. 215]. Згідно європейському критерію безпеки інформаційних технологій ITSEC (1991 р.) її країн – розробників (Німеччина, Франція, Англія, Нідерланди) захищеність інформації в будь-якій комп'ютерній системі в цілому оцінювалась також за трьома її класами: клас FC-2 – мінімальний рейтинг захищеності від несанкціонованого доступу, клас FB-2 – відносно стійкий захист від несанкціонованого доступу, клас FB-3 – стійкий захист від несанкціоно-ваного доступу [2, С. 215; 3, С. 20]. У подальшому пріоритетність захисту від загроз несанкціонованого доступу одержала подальший розвиток в Єдиних міжнародних критеріях CCITSE (1996 – 1997 роки), потім в міжнародних стандартах ISO 15408, ISO 17799 [4 – 7]. Серед міжнародних нормативно-правових документів особливе місце по вагомості займає Конвенція Ради Європи про кіберзлочинність. У цій концепції особисто виділяються чотири групи суспільно небезпечних діянь, які вимагають міжнародного співробітництва і контролю [8 – 10]. Це злочини проти конфіденційності, цілісності і доступності комп'ютерних даних і систем; злочини, пов'язані з використанням комп'ютерів; злочини, пов'язані з порушенням авторських і суміжних прав на інтелектуальну власність тощо.

В Україні в 1999 р. було вперше введено в дію вітчизняний пакет із п'яти нормативних документів з питань технічного захисту інформації (ТЗІ) комп'ютерних систем від несанкціонованого доступу.

1. НДС ТЗІ 1.1-002-99 «Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу». В цьому нормативному документі визначаються та регламентуються: постановка проблеми захисту інформації в комп'ютерних системах від несанкціонованого доступу за основними напрямами захисту; концепція забезпечення захисту інформації: основні загрози інформації; політика безпеки інформації; комплекс засобів захисту і об'єктів комп'ютерної системи; визначення несанкціонованого доступу; модель порушника; основні принципи забезпечення захисту інформації: планування захисту і керування системою захисту; основні принципи керування доступом (безперервний захист, атрибути доступу, довірче й адміністративне керування доступом, забезпечення персональної відповідальності); послуги безпеки; гарантії безпеки; основні принципи реалізації програмно-технічних засобів: функції і механізми захисту; реалізація комплексу засобів захисту; концепція диспетчера доступу.
2. НД ТЗІ 2.5-004-99 «Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу». В цьому нормативному документі визначаються та регламентуються критерії: побудови та структури захищеності інформації; конфіденційності (довірча, адміністративна, повторне використання об'єктів, аналіз прихованих каналів, конфіденційність при обміні); цілісності (довірча, адміністративна, відкат, цілісність при обміні); доступності (використання ресурсів, стійкість до відмов, гаряча заміна, відновлення після збоїв); спостереженості (реєстрація, ідентифікація та автентифікація, достовірний канал, розподіл обов'язків, цілісність комплексу засобів захисту, самотестування, ідентифікація й автентифікація при обміні, автентифікація відправника, автентифікація отримувача); гарантій (архітектура, середовище розробки, послідовність розробки, середовище функціонування, документація, випробування комплексу засобів захисту).
3. НД ТЗІ 2.5-005-99 «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу». В цьому нормативному документі визначаються та регламентуються: класифікація автоматизованих систем за трьома їх класами (клас 1 – персональна ЕОМ, клас 2 – локальна обчислювальна мережа), клас 3 – глобальна обчислювальна мережа); функціональні профілі захищеності (визначення і призначення, семантика профілю, стандартні профілі); стандартні функціональні профілі захищеності для АС класу 1, 2, 3.
4. НД ТЗІ 3.7-001-99 «Методичні вказівки щодо розробки технічного завдання на створення комплексної системи захисту інформації (КСЗІ) в автоматизованій системі». В цьому нормативному документі визначаються та регламентуються: загальні вимоги до

розробки технічного завдання на створення комплексної системи захисту інформації в автоматизованій системі (порядок розробки і зміст технічного завдання); вимоги до змісту розділів технічного завдання (загальні відомості, мета і призначення КСЗІ, загальна характеристика автоматизованої системи і умов її функціонування, вимоги до КСЗІ в частині захисту від НСД та в частині захисту від витоку інформації технічними каналами); вимоги до складу проектної та експлуатаційної документації; етапи виконання робіт; порядок внесення змін і доповнень до технічного завдання; порядок проведення випробувань КСЗІ.

5. НД ТЗІ 1.1-003-99 «Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу». В цьому нормативному документі визначаються та регламентуються основні терміни і поняття: властивості інформації і загрози; створення і експлуатація захищених систем; принципи, послуги і механізми забезпечення безпеки.

Висновок. Проведене дослідження дало змогу проаналізувати сучасний стан діючої системи отримання інформації суб'єктами зернового ринку. Встановлено що, діюча система отримання інформації підприємствами зберігання та переробки зерна не відповідає новим умовам. Були виявлені основні недоліки, а саме: відсутність одного з основних базових елементів інформаційної системи – достовірних матеріалів; нестача ринкової і науково-технічної інформації виробничого призначення; функціонування системи базується головним чином на застарілих паперових технологіях збору, обробки і розповсюдження інформації; не налагоджені контакти і не забезпечений обмін інформацією з міжнародними та національними центрами наукової, інформаційної і ділової активності в повному обсязі. Обґрунтована доцільність створення єдиної інформаційної системи зернового ринку. Розглянуто основні положення системної концепції захисту інформації від несанкціонованого доступу в автоматизованих інформаційних системах та визначено чотири базові підсистеми системи захисту інформації від несанкціонованого доступу.

ЛІТЕРАТУРА

1. Захист_інформації [Електронний ресурс]. – Режим доступу: uk.wikipedia.org/wiki/
2. Ільніцький А. Ю. Базова модель експертної системи оцінки безпеки інформації в комп'ютерних системах органів внутрішніх справ України: [монографія] / А. Ю. Ільніцький, В. В. Шорошев, І. Л. Близнюк. – К.: Вид-во НАВСУ, 2003. – 316 с.
3. Шорошев В. В. Рекомендации по обеспечению безопасности конфиденциальной информации согласно европейским «Критериям оценки безопасности информационных технологий ITSEC» / В. В. Шорошев // Бизнес и безопасность. – 1998. – № 3. – С. 20 – 21.
4. Стандарт ISO/IEC 17799: 2000 (BS 7799). Практичні рекомендації з керування інформаційною безпекою.
5. Стандарт ISO/1EC 15408: 2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 1: Introduction and general model.
6. Стандарт ISO/IEC 15408: 2000. Information technology – Security techniques Evaluation criteria for IT security. – Part 2: Security functional requirements.
7. Стандарт ISO/IEC 15408: 2000. Information technology – Security techniques – Evaluation criteria for IT security. – Part 3: Security assurance requirements.
8. Шорошев В. В. Модель угроз для локальных вычислительных сетей по рекомендациям Конвенции Совета Европы о киберпреступности / В. В. Шорошев // Зв'язок. – 2005. – № 4. – С. 37 – 42.
9. Близнюк И. Л. Классификация угроз для компьютерных данных и систем по рекомендациям Конвенции о киберпреступности Совета Европы / И. Л. Близнюк // Бизнес и безопасность. – 2005. – № 1. – С. 36 – 39.
10. Шорошев В. В. Моделі загроз комп'ютерним даним і системам за Конвенцією Ради Європи про кіберзлочинність / В. В. Шорошев, І. Л. Близнюк // Наук. Вісн. НАВСУ. – 2005. – № 6. – С. 119 – 128.

REFERENCES

Blizniuk, I. L. "Klassifikatsiia ugroz dlia kompiuternykh dannykh i sistem po rekomendatsiiam Konventsii o kiberprestupnosti Soveta Evropy" [Classification of threats to computer data and systems on the recommendations of the Convention on Cybercrime of the Council of Europe]. Biznes i bezopasnost, no. 1 (2005): 36-39.

Ilnitskyi, A. Yu., Shoroshev, V. V., and Blyzniuk, I. L. Bazova model ekspertnoi systemy otsinky bezpeky informatsii v komp'iuternykh systemakh orhaniv vnutrishnikh sprav Ukrainy [The base model of the expert system safety assessment information in computer systems of internal affairs of Ukraine]. Kyiv: NAVSU, 2003.

"Information technology – Security techniques – Evaluation criteria for IT security" Standart ISO/IEC 15408: 2000.

"Praktychni rekomendatsii z keruvannia informatsiinoiu bezpekoiu" [Practical recommendations for information security management]. Standart ISO/IEC 17799: 2000 (BS 7799).

"Security techniques Evaluation criteria for IT security" Standart ISO/IEC 15408: 2000. Information technology.

Shoroshev, V. V. "Rekomendatsii po obespecheniiu bezopasnosti konfidentsialnoy informatsii soglasno evropeyskim "Kriteriiam otsenki bezopasnosti informatsionnykh tekhnologiy ITSEC"" [Recommendations to ensure the security of confidential information in accordance with European "Criteria for Information Technology Security Evaluation ITSEC"]. Biznes i bezopasnost, no. 3 (1998): 20-21.

Shoroshev, V. V. "Model uhroz dlia lokalnykh vychyslytelnykh setei po rekomendatsiiam Konventsyy Soneta Evropy o kyberprestupnosty" [The threat model for local area networks on the recommendations of the Council of Europe Convention on Cybercrime]. Zv'iazok, no. 4 (2005): 37-42.

Shoroshev, V. V., and Blyzniuk, I. L. "Modeli zahroz komp'iuternym danym i systemam za Konventsiieiu Rady IEvropy pro kiberzlochynnist" [Models threats to computer data and systems for the Council of Europe Convention on Cybercrime]. Naukovyi Visnyk NAVSU, no. 6 (2005): 119-128.

uk.wikipedia.org/wiki/