Аналіз цих результатів показує, що є два різних, але взаємодоповнюючих способи покращення енергетичного дозволу детектора: оптимізація його конструкції, в першу чергу електродів, і відбір сигналу за часом наростання.

**Висновки.** Аналіз результатів дослідження показав, що:

- обґрунтовано електрофізичні параметри кристалів CdZnTe, що задовольняють вирішенню поставленого завдання. Кристали виготовлені заводом чистих металів (м. Світловодськ Кіровоградської обл.);
- виготовлені на основі таких кристалів 5 груп експериментальних елементів датчика гамма-випромінювання, ці групи відрізняються розмірами приймаючої площі, геометрією і топологією контактів;
- досліджено вплив розмірів кристала й геометрії контактів на чутливість, точність і можливості застосування первинного перетворювача.

1. Мокрицкий В.А., Ленков С.В., Маслов О.В., Савельев С.А. Обработка монокристаллов CdZnTe для применения в датчиках γ-излучения // Технология и конструирование в электронной аппаратуре. – 2001. – № 3. – С. 9–10. 2. Лєнков С.В., Банзак О.В., Карпенко О.В. Порівняльний аналіз методів отримання та управління властивостями телуридів цинку і кадмію // Нові технології. – Кременчук, – 2011. – № 4(34). – С. 3–10. 3. Маслов О.В., Банзак О.В., Карпенко А.В. Исследование увеличения эффективности датчиков гамма-излучения с использованием монокристаллов CdZnTe // Вісник інженерної академії України. – 2012. – № 1. – С. 143–145. 4. Маслов О.В., Банзак О.В., Карпенко А.В. Конструкторско-технологические методы усовершенствования датчиков гамма-излучения на основе монокристаллов CdZnTe // Вісник інженерної академії України. – 2012. – № 2. – С. 25–28. 5. Олейник С.Г., Маслов О.В., Максимов М.В. Анализ возможностей применения однотипных технических средств и методического обеспечения для контроля состояния ядерного топлива и ядерных материалов в реальном времени / Ядерная энергетика. – 2004, № 1. – С. 87–97. 6. J.M. Perez, Z. He, D.K. Wehe. Stability and Characteristics of Large CZT Coplanar Electrode Detectors // IEEE Trans. Nucl. Sci. – June 2001, vol. 48, No 3. – P. 272–277. 7. High Resolution CdTe Detector and Applications to Imaging Devices / Takahashi T., Watanabe S., Kouda M., Okada Y., Sato G., eds. // IEEE Trans. Nucl. Sci. – June 2001. – Vol. 48, No 3. – P. 287–291. 8. Evaluation of CZT crystals from the former Soviet Union / Hermon H., Schieber M., James R.B., Antolak A.J., Morse D.H., Brunett B., Hackett C., Tarver E., Komar V., Goorsky M.S., Yoon H., Kolesnikov N.N., Toney J. – 2000. – P. 136–151.

**Надійшла до редколегії 06.02.12**

**УДК 005.03**

**А.А. Мочалов, д-р техн. наук, проф.,**
**А.А. Гайша, канд. техн. наук, доц., П.А. Степанов, асп.**

# АНАЛИЗ ИНФОРМАЦИОННЫХ ПОТОКОВ СИСТЕМЫ ДИСТАНЦИОННОГО ОБРАЗОВАНИЯ С УЧЕТОМ НЕОБХОДИМОСТИ ОБЕСПЕЧЕНИЯ ИХ БЕЗОПАСНОСТИ

***Проаналізовано можливі інформаційні загрози виникаючі в процесі роботи системи дистанційної освіти. Запропоновано механізм її захисту.***

***Ключові слова: менеджмент, інформаційні потоки, керування процесами, дистанційна освіта.***

***The possible threats of the information arising in the process of distance education are analysed. Mechanism of its protection is offered.***

***Keywords: management, clearing flows, office of the process, distance education.***

**Введение.** В наше время всё большее распространение в сфере образования, за счёт присущих только ей качеств, приобретает дистанционное образование (ДО) [1]. Параллельно актуализируется проблема защиты информационных потоков, которые несут конфиденциальную информацию и принадлежат системе ДО или направлены к ней. Существующие же решения [2, 3, 5] способны лишь частично осуществлять эту задачу.

**Анализ последних исследований и публикаций** в этом направлении показывает, что наиболее эффективным подходом является построение системы управления информационными потоками (ИП) на основе разделенной иерархии целей её работы [1-3, 5]. Возьмём его принципы за основу.

**Цель работы.** Целью работы является создание структуры системы, позволяющей должным образом контролировать информационные потоки, циркулирующие в системе ДО, и защищать её от произвольных информационных атак.

**Изложение основного материала.** На текущий момент различают два ключевых вида угроз, которые могут повлиять на финальный уровень знаний у обучаемых и на работоспособность системы. Среди них:

- внешняя угроза – дистанционное воздействие злоумышленника, направленное на создание возможности неправомерного проникновения в систему;
- внутренняя угроза – неправомерное введение злоумышленником инородного ИП внутрь информационной системы в обход внешних систем защиты.

При этом, чтобы быть рентабельной и конкурентоспособной, любая система должна обладать следующими качествами:

- оперативно и качественно обрабатывать все ИП, циркулирующие как в самой системе, так и вне её;
- обеспечивать непрерывный и стабильный цикл работы системы;
- обеспечивать конфиденциальность циркулирующей информации.

Опираясь на предъявляемые требования, была разработана структура, приведенная на рис.1, которая позволяет их реализовать в полном объеме.

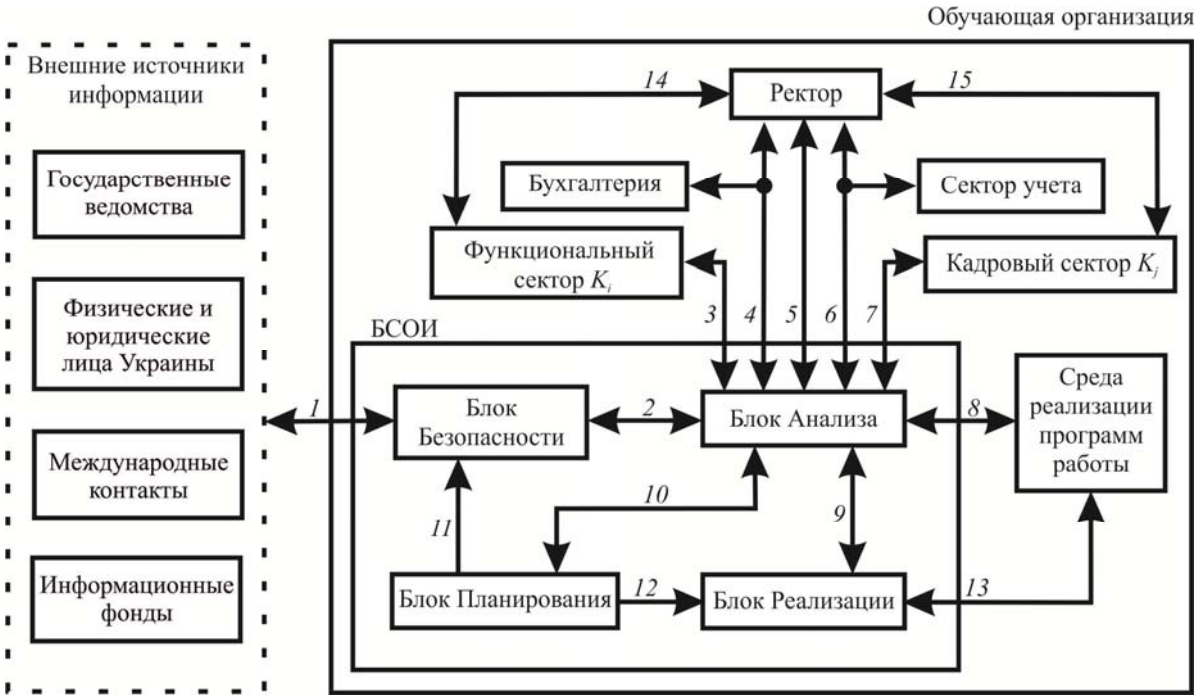


**Рис.1. Структура защищенной обработки ИП системой ДО**

При возникновении внешнего информационного потока *1*, он, прежде чем попасть в систему, проходит предварительную обработку блоком сбора и обработки информации (БСОИ) [4]. В нем реализовано 4 области функционирования:

- безопасности (представлена в блоке безопасности (ББ), производит защиту от внешних угроз);
- анализа (представлена в блоке анализа (БА), который производит:

а) мониторинг ИП – отслеживание всех циркулирующих ИП и их учёт;

б) анализ ИП;

в) кодирование-декодирование, формирование специализированных ИП;

г) маршрутизацию ИП;

д) защиту от внутренних угроз);

- планирования (представлена в блоке планирования (БП), производит сбор, хранение и резервное дублирование информации, циркулирующей в системе);
- реализации (представлена в блоке реализации (БР), производит имплементацию разработанных планов работы из БП).

Каждая из этих областей обладает уникальным набором функций, комплексная работа которых позволяет реализовать поставленные выше задачи. При попадании ИП в систему *1*, он направляется в ББ, где подвергается проверке на соответствие типу "вредоносный информационный поток". На этом этапе отсеиваются внешние угрозы, в частности вирусные программы и информационные потоки, которые представляют собой спам. При успешном прохождении проверки, он передаётся *2* в БА, где подвергается первичной обработке, процесс представлен на рис.2.

Блок анализа анализирует и обрабатывает все циркулирующие ИП в системе, регистрирует и проводит их анализ на соответствие статусу "закодированный информационный поток". Если он не соответствует принятому в системе виду циркулирующих ИП, он проходит кодировку, в ходе которой на основании множества смысловых элементов и множества целей работы системы, полученных их БП, формируется новый, закодированный ИП. Структуру закодированного ИП допустимо представить в виде множества:

$$M_{\text{ЗИП}} = \left[ \underbrace{M_{ind}}_{1}, \underbrace{M_{key}}_{2}, \underbrace{M_{body}}_{3} \right],$$

где 1 – множество индекс–адресов принадлежности закодированного ИП; 2 – множество смысловых элементов, выделенных с изначального ИП; 3 – множество, содержащее изначальное тело ИП.

После того как ИП приобретает статус "закодирован", он подвергается анализу, в ходе которого определяется его актуальность для системы, если она меньше допустимого порогового значения, он выводится из системы *2*.

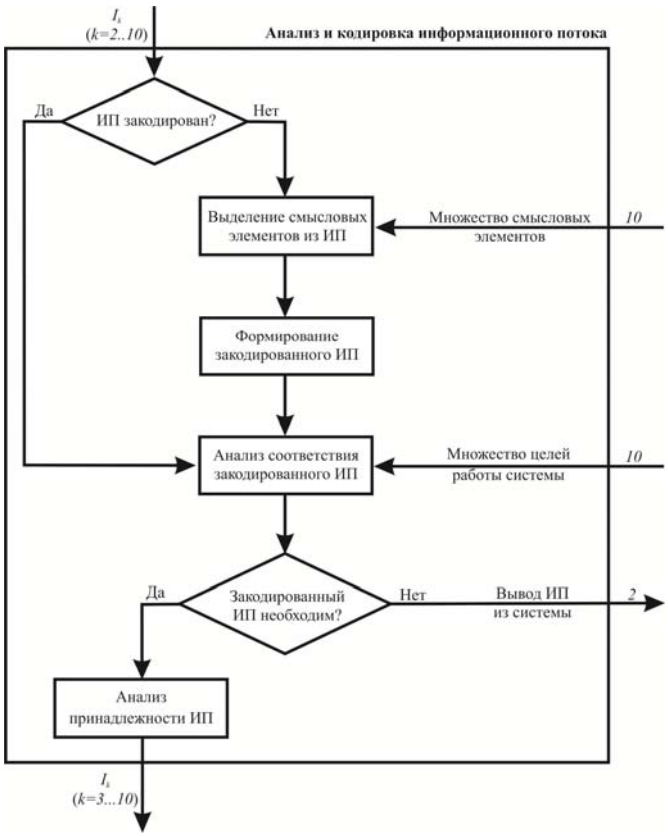


**Рис. 2. Структура алгоритма первичной обработки ИП в БА**

На этом этапе реализуется защита от внутренних угроз. Для того, чтобы инородный (вредоносный) ИП был обработан произвольным функциональным сектором, он должен сперва приобрести форму принятых к обработке ИП в системе, в противном случае он будет игнорироваться. При этом, как только он будет закодирован, он теряет свои первородные степени активности и в дальнейшем не представляет какой бы то ни было угрозы для системы и при обработке выводится из неё.

Если ИП отвечает всем предъявленным требованиям, БА руководствуясь определенным множеством индекс–адресов принадлежности потока, переадресовывает его секторам-адресатам, реализуя задачу маршрутизации *3-10*. Такой подход в оперировании ИП позволяет улучшить эффективность работы системы в целом, за счёт того, что каждый рабочий сектор обрабатывает лишь свою, актуальную лишь для него информацию.

Для формирования резервного хранилища информации, способного восстановить целостность информационного пространства системы, в случае сбоя, вся циркулирующая информация которая обладает достаточным уровнем актуальности сохраняется в БП.

В случае если ИП несёт в себе запрос и предоставлении некой услуги (учебного курса), в БА формируется ряд управляющих команд, направленных к БР и среде реализации работы, результатом выполнения которых является формирование виртуальной среды с элементами, способствующими реализации запроса, заложенного в пришедший ИП.

**Выводы.** Предложенная структура построения работы системы ДО, реализует на должном уровне механизмы контроля и обработки информационных потоков, циркулирующих в ней, при этом обеспечивая защиту от произвольных информационных атак. На её базе разработан алгоритм защиты ИП и идентификации пользователей. Следует отметить, что спектр применения предложенной структуры не ограничен лишь системой образования, и после некоторых предварительных настроек, может быть интегрирован в любую систему, нуждающуюся в механизмах контроля, маршрутизации и защиты ИП.

1. Вергазов, Р. И. Система автоматизированного дистанционного тестирования / Р. И. Вергазов, П. А. Гудков // Новые информационные технологии: Тез. докл. Восьмая международная студенческая школа семинар. – Крым: Пензенский государственный университет, 2000. 2. Ложников, П. С. Распознавание пользователей в системах дистанционного образования / П. С. Ложников // Educational Technology & Society. – 2001. – № 4. 3. Махутов, Б. Н. Защита электронных учебников в дистанционном обучении / Б. Н. Махутов, М. Ю. Шевелев // Образование XXI века: инновационные технологии, диагностика и управление в условиях информатизации и гуманизации: Материалы III Всероссийской научно-методической конференции с международным участием. – Красноярск: КГПУ, 2001. – С. 106 – 108. 4. Мочалов, А. А. Эффективный менеджмент системы дистанционного образования / А. А. Мочалов, П. А. Степанов // Зб. наук. пр. НУК. – Миколаїв: НУК, 2010. – №5 (434). С. 130 – 133. 5. Фурин, В. В. Направления в развитии правового обеспечения информационной безопасности в дистанционном образовании / В. В. Фурин // Информационные технологии в образовании: Матер. Всерос. науч.-практ. конф. – М.:МГУ, 2005. – С.83.

**Надійшла до редколегії 16.01.12**