

работников службы по освоению автоматизированных систем учета.

**Библиографический список:**

1. Финансово-кредитный энциклопедический словарь. Колл. авторов под общ. ред. А.Г. Грязновой, 2004 г.
2. Формы отчетности о финансово-экономическом состоянии товаропроизводителей АПК за 2008 – 2010 гг.

**COST ACCOUNTING FOR AUTOMATION IN DAIRY CATTLE**

*N.A. Kaskurov, Ju. V. Kuznecov*

*Key words: automation, accounting, analysis, response, cost.*

*The work is devoted to the use of automated accounting costs in dairy farming. Examine and determine the effectiveness of the introduction of automation in agriculture accounting for example SEC "Elm-Gai."*

**УДК 681.3**

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РОССИИ**

*А.Ю. Миронов, студент 4 курса экономического факультета  
Научный руководитель - С.В. Голубев, к.э.н., ст. преподаватель  
ФГБОУ ВПО «Ульяновская государственная  
сельскохозяйственная академия»*

**Ключевые слова:** *информационная безопасность, защита, криптография, несанкционированный доступ, конфиденциальность, ключ.*

*Работа посвящена определению информационной безопасности и методов ее защиты, так как в данное время осуществляется быстрый рост глобальной сети Internet и стремительное развитие информационных технологий, как во всем мире, так и в России, которые привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Однако, несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается.*

*Быстрый рост глобальной сети Internet и стремительное раз-*

витие информационных технологий, как во всем мире, так и в России привели к формированию информационной среды, оказывающей влияние на все сферы человеческой деятельности. Новые технологические возможности облегчают распространение информации, повышают эффективность производственных процессов, способствуют расширению деловых отношений. Однако, несмотря на интенсивное развитие компьютерных средств и информационных технологий, уязвимость современных информационных систем и компьютерных сетей, к сожалению, не уменьшается. По данным «Лаборатории Касперского», в 2011 году для проведения 946 393 693 атак через интернет злоумышленники воспользовались 4 073 646 доменами. Серверы, на которых был размещен вредоносный код, были обнаружены в 198 странах мира. 86,4% всех зафиксированных в Сети вредоносных хостингов были размещены в интернет-пространстве двадцати стран. Из них на Россию пришлось 14,6% всех атак: это второе место после США.

Без знания и квалифицированного применения современных технологий, стандартов, протоколов и средств защиты информации невозможно достигнуть требуемого уровня информационной безопасности компьютерных систем и сетей.

Защита данных в компьютерных сетях становится одной из самых открытых проблем в современных информационно-вычислительных системах. На сегодняшний день сформулировано три базовых принципа информационной безопасности, задачей которой является обеспечение:

1. целостности данных - защита от сбоев, ведущих к потере информации или ее уничтожения;
2. конфиденциальности информации;
3. доступности информации для авторизованных пользователей.

Любая комплексная система защиты информации после того, как производится аудит информационной безопасности объекта, начинает опираться на наиболее распространенные пути перехвата конфиденциальных данных, поэтому их важно знать, для того чтобы понимать, как разрабатывается комплексная система защиты информации.

Проблемы информационной безопасности в сфере технической защиты информации:

- перехват электронных излучений;
- принудительное электромагнитное облучение (подсветка) линий связи с целью получения паразитной модуляции несущей;
- перехват акустических излучений и восстановление текста принтера;
- копирование носителей информации с преодолением мер защи-

ты;

- маскировка под зарегистрированного пользователя;
- маскировка под запросы системы;
- использование программных ловушек;
- использование недостатков языков программирования и операционных систем;
- незаконное подключение к аппаратуре и линиям связи специально разработанных аппаратных средств, обеспечивающих доступ информации;
- злоумышленный вывод из строя механизмов защиты;
- расшифровка специальными программами зашифрованной информации;

Вышперечисленные пути утечки информации по оценке информационной безопасности требуют высокого уровня технических знаний для того чтобы использовать наиболее эффективные методы и системы защиты информации.

Соответственно, если есть угрозы утечки информации, то есть и средства, предотвращающие это. На сегодняшний день можно выделить следующие основные виды технических средств защиты:

- средства криптографической защиты информации;
- средства разграничения доступа пользователей к ресурсам АС;
- средства межсетевого экранирования;
- средства анализа защищённости АС;
- средства обнаружения атак;
- средства антивирусной защиты;
- средства контентного анализа;
- средства защиты от спама.

Одним из самых распространенных и качественных средств защиты информации является криптографическая защита информации посредством криптографического шифрования. Криптографические методы защиты информации применяются для обработки, хранения и передачи информации на носителях и по сетям связи. Криптографическая защита информации при передаче данных на большие расстояния является единственно надежным способом шифрования.

Защита конфиденциальной информации, основанная на криптографической защите информации, шифрует данные при помощи семейства обратимых преобразований, каждое из которых описывается параметром, именуемым «ключом» и порядком, определяющим очередность применения каждого преобразования.

Важнейшим компонентом криптографического метода защиты

информации является ключ, который отвечает за выбор преобразования и порядок его выполнения.

Один и тот же алгоритм криптографической защиты информации может работать в разных режимах, каждый из которых обладает определенными преимуществами и недостатками, влияющими на надежность информационной безопасности России и средства информационной безопасности.

Для обеспечения наивысшей защиты вашей информации можно использовать два продукта – это «Контур информационной безопасности SearchInform» и «BestCrypt».

На сегодняшний день «Контур информационной безопасности SearchInform» признанный лидер на рынках информационной безопасности России и стран СНГ. «Контур информационной безопасности SearchInform» позволяет выявлять утечки конфиденциальной информации и персональных данных через электронную почту; ICQ; голосовые и текстовые сообщения Skype, посты на форумах или комментарии в блогах; внешние устройства (USB/CD); FTP; файл-серверы; ноутбуки, в том числе отключенные от корпоративной сети; документы, отправляемые на печать; а также появление конфиденциальной информации на компьютерах пользователей.

BestCrypt — платный пакет проприетарных программ для создания на жёстком диске компьютера виртуального зашифрованного диска (контейнера) — одного или нескольких. Виртуальный диск работает, как обычный дисковый раздел.

Шифрование и расшифровка идут в фоновом режиме, и пользователь не замечает разницы в работе с обычным и зашифрованным диском, который, при необходимости, можно превратить в обычный, но нечитаемый, файл. У программы BestCrypt есть опция создания «скрытого» контейнера, который криптографически гарантированно нельзя определить никакими средствами. У BestCrypt есть возможность шифрования swap-файла (файла виртуальной памяти) — в нём хранятся временные данные, в том числе там могут оказаться документы и пароли, поэтому его шифрование является полезной возможностью с точки зрения защиты информации. Также присутствует функция шифрования системного диска с последующей загрузкой с него.

По данным отчета IDC Russia Security Software 2011-2015 Forecast and 2011 Vendor Shares, объём российского рынка программных систем обеспечения информационной безопасности (ИБ) в 2011 году достиг \$229 млн, что соответствует ежегодному приросту на 29,9 %. По прогнозам IDC, в последующие пять лет российский рынок программных

систем обеспечения ИБ будет ежегодно расти в среднем на 18,3%.

**Библиографический список**

1. В.Ф. Шаньгин. Информационная безопасность компьютерных систем и сетей, 2008;
2. Давлетханов М. Обзор BestCrypt Volume Encryption - программы для криптографической защиты данных;
3. <http://arhidelo.ru/article/detail-8746.html>;
4. [http://www.tadviser.ru/index.php/Статьи:Информационная\\_безопасность\\_\(рынок\\_России\)](http://www.tadviser.ru/index.php/Статьи:Информационная_безопасность_(рынок_России));
5. <http://www.searchinform.ru/main/full-text-search-information-security-product.html>.

**INFORMATION SECURITY IN RUSSIA**

*Mironov A.U., Golubev S.V.*

*Keywords: information security, protection, encryption, unauthorized access, confidentiality, key.*

*The rapid growth of the global Internet and the rapid development of information technologies, such as around the world and in Russia led to the formation of the information environment, affecting all spheres of human activity. New technological capabilities make it easier to disseminate information, increase the efficiency of manufacturing processes, contribute to the expansion of business relations. However, despite the rapid development of computer and information technologies, the vulnerability of modern information systems and computer networks, unfortunately, is not reduced.*