

## КОМПЬЮТЕРНЫЕ ВИРУСЫ И АНТИВИРУСНОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

**Костин И.В.**, студент 1 курса экономического факультета  
**Научный руководитель – Солнцева О.В.**,  
кандидат экономических наук, доцент  
**ФГБОУ ВО Ульяновская ГСХА**

**Ключевые слова:** вирус, антивирусное программное обеспечение, интернет, файл, персональный компьютер.

*В данной статье рассматриваются пути распространения компьютерных вирусов, их стадии и типы. Причины заражения ПК вирусом. А также некоторые способы защиты от них.*

Как мы знаем, сейчас компьютеры и мобильные устройства являются неотъемлемой частью нашей жизни. Интернет хранит информацию и файлы, среди которых, есть полезные и вредные. Существует много программ, которые могут навредить данным хранящимся на наших ПК и мобильных устройствах. Речь идет о вирусах-вредителях просторов «Всемирной паутины».

Компьютерный вирус – это вредоносное ПО, способное внедряться в код других программ, системные зоны памяти, загрузочные сектора, а также создавать копии самого себя и распространять их посредством различных путей: Интернет, съемные носители, диски.

Мобильный вирус – вредоносное ПО меньшего размера, предназначенное для вмешательства в работу мобильного устройства, также повреждения или удаления данных, распространяемое посредством сети Интернет и SMS.

На данный момент существует множество классификаций вирусов, различающихся в основном по способу распространения и функциональности. Если раньше вирусы могли перемещаться на съемных носителях, то теперь они имеют куда больше путей для распространения.

Различают вирусы по следующим категориям:

- поражаемый объект (файловые вирусы, загрузочные вирусы, сценарные вирусы, макровирусы, вирусы поражающие код);
- механизм заражения (паразитирующие – добавляют себя в файлы, перезаписывающие – невосстановимо портят файл, «спутники» идущие отдельным файлом);

- тип поражаемой ОС и платформы (DOS, Microsoft Windows, Unix, Linux);
- язык написания вируса (Assembler, C+);
- технология вируса (полиморфные вирусы, стелс-вирусы, руткиты);
- дополнительная вредоносная функциональность (бэкдоры, кейлоггеры, шпионы, ботнеты и др.)

На настоящий момент самым простым способом заражения ПК является заражение через Интернет. А именно социальные сети, электронная почта, непроверенные сайты и игры. Разработчикам вирусов и шпионских ПО удобно текущее положение пользователей, а именно их неосторожность. Зачастую люди просто не обращают внимания на все те мелочи, которые могут привести к заражению: реклама на сайте, всплывающие диалоговые окна, неизвестные источники и сайты. Этим и пользуются злоумышленники. Ведь вирус может не только погубить файлы или систему, но и «украсть» какие-либо данные. Например, логины и пароли аккаунтов, онлайн кошельков и платежных карт.

Вирусы существуют в системе в разных стадиях функционирования:

- латентная стадия (безвреден/не активен, может быть вычислен сканированием файлов);
- инкубационная стадия (активен, создает свои копии, снижает производительность системы, рассылает копии);
- активная стадия (активен, заметен – пропадают файлы, нарушается функционирование сети, происходит порча системы).

Различают вирусы так же по месту их пребывания:

1. Загрузочные вирусы (жесткие диски, переносные запоминающие устройства, нарушение работы загрузчика ОС, изменение файловой таблицы, что делает недоступными определенные файлы).

2. Файловые вирусы (находятся в модулях программ, активируются при доступе к файлу, изменяет код или создает модифицированную копию файла. Являются самым распространенным типом вируса).

3. Файлово-загрузочные вирусы.

4. Сетевые вирусы (Распространение посредством сетевых служб и протоколов).

5. Документные вирусы (Макровирусы). Заражают файлы типа Microsoft Office, Open Office.

Чтобы обезопасить свой ПК от угрозы заражения вирусом следует использовать Антивирусные ПО, Брандмауэр и своевременно обновлять систему на наличие обновлений. В сети Интернет существует множество Антивирусных ПО. Бесплатные: Oihoo 360 Total Security

8.0, Avast 2015 Free, Comodo IS; Платные: Kaspersky IS 2015, Norton Security 2015, G Data IS 2015 являются наиболее эффективными антивирусными ПО.

Так же защиту может обеспечить браузер, и наиболее хорошо с этим справляются IE10 и Google Chrome. Но какой бы совершенной не была защита ПК или мобильного устройства, самой лучшей защитой остается бдительность пользователя.

#### **Библиографический список:**

1. Романов, В.В. Информационные системы и технологии в экономике: учебное пособие для специальностей экономического профиля/ В.В. Романов, О.В. Солнцева, А.В. Севастьянов, О.А. Заживнова. – Ульяновск: УГСХА, 2010. – 134 с.

2. Бунина, Н.Э. Информатика: учебно-методический комплекс для студентов экономического факультета. Часть 1. / Н.Э. Бунина, О.А. Заживнова, О.В. Солнцева. – Ульяновск: УГСХА им. П.А. Столыпина, 2012. – 101 с.

3. Видеркер, М.А. Тенденции потребительских онлайн-покупок в Ульяновской области / М.А. Видеркер, О.А. Заживнова, В.О. Семенова, О.В. Солнцева // Материалы международной научно-практической конференции «Наука сегодня: проблемы и перспективы развития». – Часть 3. – Вологда: ООО «Маркер», 2015. – С. 99–100.

4. Солнцева, О.В. Информационные технологии в науке и образовании: лабораторный практикум для аспирантов. / О.В. Солнцева, Н.Э. Бунина, М.А. Видеркер, О.А. Заживнова. – Ульяновск: УГСХА им. П.А. Столыпина, 2015. – 64 с.

5. Бунина, Н.Э. Компьютерная обработка информации: методические указания по изучению дисциплины для студентов заочного отделения биотехнологического факультета / Н.Э. Бунина, О.В. Солнцева – Ульяновск: УГСХА им. П.А. Столыпина, 2014. – 24 с.

6. Бунина, Н.Э. Информационные технологии в общественном питании: методическое пособие для студентов биотехнологического факультета / Н.Э. Бунина, О.В. Солнцева – Ульяновск: УГСХА им. П.А. Столыпина, 2014. – 21 с.

7. Солнцева, О.В. Информатика: учебно-методический комплекс для студентов специальности 080401.65 «Товароведение и экспертиза товаров (по областям применения)» / О.В. Солнцева, В.В. Романов, Н.Э. Бунина, О.А. Заживнова. – Ульяновск: УГСХА, 2009. – 117 с.

## **COMPUTER VIRUSES AND ANTIVIRUS SOFTWARE**

**Kostin V.I., Solntseva O.V.**

**Key words:** *virus, anti-virus software, Internet, file, PC.*

*This article discusses ways to spread computer viruses, their stage types. Causes of PC virus. As well as some ways to protect against them.*

УДК 338.5:633.1

## **РАСЧЕТА ФАКТИЧЕСКОЙ СЕБЕСТОИМОСТИ ПРОДУКЦИИ ПЕРЕРАБОТКИ ЗЕРНА**

**Кочержова Е.Н., студентка 4 курса  
учетно-финансового факультета  
Научный руководитель – Ельчанинова О.В.,  
кандидат экономических наук, доцент  
ФГБОУ ВО Ставропольский ГАУ**

**Ключевые слова:** *себестоимость, калькулирование, сортовые и односортовые помолы, попередельный метод, калькуляционная разница*

*В работе представлен расчет фактической себестоимости продукции переработки зерна примере мукомольного производства СПК «Племзавод Вторая Пятилетка».*

На сельскохозяйственных предприятиях переработку продукции растениеводства, а именно зерна, организуют промышленные производства. К основным из них относятся: мукомольные заводы, маслодельные заводы, консервные заводы, а также пункты по забою и переработке скота и птицы и другие.

В СПК «Племзавод Вторая Пятилетка» для переработки зерна развито мукомольное производство.

Калькуляция себестоимости представляет собой систему расчетов, с помощью которой может быть определена себестоимость, как всей произведенной продукции, так и единицы каждого ее вида. Рассмотрим некоторые особенности калькулирования в мукомольном производстве, а также определим, как следует организовать учет в таком случае.

Учет затрат на производство на мукомольных предприятиях осуществляется попередельным методом с применением элементов нормативного учета в части расходования сырья [1].

На мукомольных предприятиях могут получать односортовые помолы пшеницы и сортовые помолы. Во втором случае из одного сырья одновременно получают несколько сортов продукции. Для определе-