МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Институт информационных технологий и телекоммуникаций
Северо-Кавказского федерального университета (г. Ставрополь)

Институт компьютерных технологий и информационной безопасности
Инженерно-технологической академии Южного федерального университета (г. Таганрог)

Поволжский государственный университет телекоммуникаций и информатики (г. Самара)
Ростовский государственный экономический университет «РИНХ» (г. Ростов-на-Дону)

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

СБОРНИК МАТЕРИАЛОВ
III ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ

(Ставрополь, 14-18 декабря 2015)

Часть 2

Ставрополь
2015

УДК 004.2/.9
ББК 32.97
С 88

Организаторы конференции:

Министерство образования и науки Российской Федерации
Институт информационных технологий и телекоммуникаций
Северо-Кавказского федерального университета (г. Ставрополь)
Институт компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета (г. Таганрог)
Поволжский государственный университет телекоммуникаций и информатики (г. Самара)
Ростовский государственный экономический университет «РИНХ»
(г. Ростов-на-Дону)

Оргкомитет конференции:

Председатель:

Лиховид А.А. – проректор по научной работе и стратегическому развитию СКФУ, доктор географических наук, кандидат биологических наук, профессор.

Члены оргкомитета:

Чипига А.Ф. – директор Института информационных технологий и телекоммуникаций СКФУ, заведующий кафедрой информационной безопасности автоматизированных систем, кандидат технических наук, профессор.

Мезенцева О.С. – заместитель директора по учебной работе Института информационных технологий и телекоммуникаций СКФУ, кандидат физико-математических наук, доцент.

Петренко В.И. – заместитель директора по научной работе Института информационных технологий и телекоммуникаций СКФУ, заведующий кафедрой организации и технологии защиты информации, кандидат технических наук, доцент.

Веселов Г.Е. – директор Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета, полномочный представитель ректора по развитию инженерного направления, доктор технических наук, доцент.

Самойлов А.Н. – заместитель директора Института компьютерных технологий и информационной безопасности Инженерно-технологической академии Южного федерального университета по научной и международной деятельности, кандидат технических наук, доцент.

Маслов О.Н. – заведующий кафедрой экономических и информационных систем Поволжского государственного университета телекоммуникаций и информатики, доктор технических наук, профессор.

Тищенко Е.Н.– заведующий кафедрой информационных технологий и защиты информации Ростовского государственного экономического университета (РИНХ), доктор экономических наук, доцент.

Ответственный секретарь:

Толстова Н.А. – доцент кафедры межинститутской базовой кафедры СКФУ, кандидат педагогических наук.

С 88 **Студенческая наука для развития информационного общества:** сборник материалов III Всероссийской научно-технической конференции. Часть 2. – Ставрополь: Изд-во СКФУ, 2015. – 374 с.

ISBN 978-5-9296-0813-1

Материалы конференции посвящены вопросам развития инновационных образовательных и инфокоммуникационных технологий, проблемам информационной безопасности объектов информатизации, изучению информационных систем и технологии. Изложены результаты научных исследований в области разработки информационных технологий решения экономических задач, затрагиваются вопросы создания и использования робототехнических систем.

УДК 004.2/.9
ББК 32.97

ISBN 978-5-9296-0813-1

Классификационные схемы являются устаревшими и нереалистичными. Для большей части, классификации данных является субъективным процессом. Два человека могут смотреть на ту же часть данных и давать очень различные уровни систематизации, особенно когда применяется сложная схема. У организаций с давно установившейся схемой классификации также могут возникнуть проблемы внесения изменений или колебаний. Во многих из подобных ситуаций, систематизация просто не пригодна или не реалистична для исполнения. Еще одна проблема, которая делает классификацию невозможной - не совпадение или противоречие с безопасностью и использование данных политики вместе внутри организации.

Глобальная рабочая сила добавляет дополнительную сложность классификации. Ворочать главную схему классификации данных для большой, многонациональной организации без ясного понимания местных или региональных соображений является первым шагом к неудачной реализации. Есть множество конфиденциально связанных правовых обязательств, которые рассматриваются и понимаются со стороны различных внутренних заинтересованных сторон, где визуальная маркировка или метки помогают создать единое понимание терминов этикеток.

Роли и обязанности ясны. Каждая организация имеет свою собственную историю ответственности и право собственности данных. Различные группы также имеют разнообразные представления о значение информации, обработке и потребности в их безопасности. Это необходимо для оппортунистической классификации, или систематизации данных, которая позволяет использовать его для нужд этой группы. Отсутствие сдержек и противовесов в роли данных и обязанности усугубляет проблему оппортунистической классификации.

Классификация данных имеет различные значения в пределах организации. Различные группы могут выделять виды классификации по-разному с точки зрения безопасности. Например, индивидуальный контроль управления информационных знаний может иметь инициативу классификации данных, которая включает в себя систематизацию данных (определение, если файл данных представляет собой договор) вместо чувствительности. Необходимо понимать плюсы и обоснование различных типов классификаций, которые могут существовать в рамках организации, и работать вместе с другими, объединяя усилия и представляя единую стратегию и бизнес-дела для классификации на предприятии.

Литература

1. Петренко С. А., Курбатов В. А. Политика информационной безопасности. [Электронный ресурс] Режим доступа: http://www.universalinternetlibrary.ru

2. Без автора. Компьютер + Локальная сеть + Интернет. [Электронный ресурс] Режим доступа: http://pgtk.edu.ru

МЕТОДЫ БОРЬБЫ С ВРЕДОНОСНЫМ ПРОГРАММНЫМ ОБЕСПЕЧЕНИЕМ НА СЪЕМНЫХ НОСИТЕЛЯХ

А. А. Честнов, З. А. Носиров
руководитель – ассистент кафедры информационной безопасности ***О. М. Князева***
Астраханский государственный университет, г. Астрахань

Введение. Вредоносное компьютерное программное обеспечение (ПО) — одна из наиболее широко известных угроз для сетей любой структуры [3]. Подобно живым микроорганизмам, они распространяются от компьютера к компьютеру, от носителя к носителю, «заражая» программы и файлы приложений и операционной системы [4]. Если пользователь часто использует USB накопители: подключает к различным компьютерам, переносит на них/ с них файлы, то вероятность того, что на них окажется вредоносное ПО достаточно велика. Примерно каждый десятый компьютер может стать причиной «заражения», приводящей к потере/искажению данных [4].

Ежедневно, студенты высших учебных заведений, абсолютно не задумываясь, пользуются различными флеш-накопителями в стенах университета. При этом в каждом учебном классе учреждения находится около 20 компьютеров. Таким образом, вредоносные программы переходят от одного устройства к другому, пополняя список «зараженных». Таким образом, одной из актуальных проблем высшего учебного заведения является распространение вредоносного программного обеспечения в пределах его локально-вычислительной сети.

Основная часть. Задачей исследования является выявление списка часто встречающегося вредоносного ПО, циркулирующего в локально-вычислительной сети университета на примере ФГБОУ ВПО АГУ и определение методов предупреждения и ликвидации последствий от их действий.

Для выявления списка часто встречающихся вредоносных программ при содействии отдела Эксплуатации Программного Обеспечения был проведен опрос студентов 1–4 курсов АГУ (364 человека). Опрос проводился методом анкетирования (рис. 1).

Анкета опроса студента

Форма обучения_____Специальность_____Курс_____Группа_____Год_____

Анкета «Вредоносное ПО в университете»

Уважаемые студенты! В университете проводится опрос с целью выявления угроз информационной безопасности посредством заражения устройств вредоносным ПО на основе изучения ваших мнений и пожеланий. Если затрудняетесь ответить, оставьте поле пустым.

Заполните таблицу.

Аудитория, № компьютера	**Название вредоносного ПО**	**Признаки заражения**

Рисунок 1. Пример анкеты для опроса студентов на предмет выявления вредоносного ПО на флеш-накопителях

По результатам анкетирования было выявлено, что наиболее часто встречающимися вредоносными программами в университете являются: 1) Флеш-вирус f4448e25.exe и 2) Вирус autorun.inf

Флеш вирус f4448e25.exe

Вирус f4448e25.exe довольно распространен в глобальной сети Интернет. Он скрывает файлы на внешнем запоминающем устройстве (ВЗУ), вследствие чего они становятся недоступными для пользователя.

К основным «симптомам заражения» относятся:

- визуальное исчезновение файлов на накопителе, при неизменном объеме памяти;
- визуальное исчезновение файлов на накопителе, при значительном уменьшении объема памяти;
- замена всех файлов и папок на носителе на соответствующие ярлыки.

Процесс ликвидации данного вредоносного ПО проводится в несколько этапов. Первоначально необходимо проверить Флеш-накопитель антивирусным ПО. После проверки следует перейти к восстановлению утраченных файлов. В рамках исследования для решения данной задачи (восстановления файлов) был написан bat файл, представленный на рис.2 [1].

После запуска Recovery.bat компьютер запросит букву, соответствующую «зараженному» ВЗУ. После того, как будут удалены ярлыки вместо папок и само вредоносное ПО, пользователю будет показано содержимое устройства.

Recovery.bat

```
:lable
cls
set /p disk_flash="Bukva fleshki: "
cd /D %disk_flash%:
if %errorlevel%==1 goto lable
cls
cd /D %disk_flash%:
del *.lnk /q /f
attrib -s -h -r autorun.*
del autorun.* /F
attrib -h -r -s -a /D /S
rd RECYCLER /q /s
explorer.exe %disk_flash%:
```

Рисунок 2. Recovery.bat

Вирус autorun.

Изначально безобидное предназначение файла автозапуска autorun.inf стало использоваться, как эффективный способ распространения компьютерного «червя» win32 autorun. Сам по себе файл autorun.inf не содержит исполняемый код вредоносного ПО, он является лишь средством запуска autorun «червя». Такие вредоносные программы распространяются посредством копирования исполняемого файла на съемные носители и прописываясь в файл автозапуска autorun.inf, таким образом заражая их. [1] Губительному воздействию подвержены абсолютно все внешние накопители.

«Симптомы заражения»:

- наличие файла autorun.inf и скрытой папки RECYCLER на внешнем накопителе. Данные файлы скорее всего будут скрытыми, поэтому необходимо предварительно убедиться, что поставлена соответствующая галочка в настройках вида папок;
- отсутствие возможности запуска (чтения, выполнения) или удаления файла autorun.inf;
- отсутствие в меню Проводника «Сервис» пункта «Свойства папки».

Для лечения «вируса» autorun.inf был написан следующий bat файл рис.3.

Antiautorun.bat

```
attrib -s -h -r autorun.*
del autorun.*
mkdir "\\?\%~d0\autorun.inf\name..\"
attrib +s +h %~d0\autorun.inf
```

Рисунок 3. Antiautorun.bat

На первом этапе файл Antiautorun.bat удаляет существующий вредоносный файл, а затем создает неудаляющуюся папку autorun.inf. Созданную папку таким методом уже ничем невозможно удалить. Единственный способ удалить папку – это отформатировать флеш-накопитель.

Приведенные выше bat файлы позволяют ликвидировать последствия от заражения ВЗУ вредоносным ПО. Однако более действенным методом борьбы с данными программами является предупреждение заражения носителей и распространения вредоносного ПО в сети.

В целях предупреждения угрозы распространения вредоносного ПО в локально-вычислительной сети АГУ и дальнейшего заражения съемных носителей была предложены мероприятия по защите ВЗУ студентов, включающие в себя организационные и программные средства и меры защиты информации:

1. Организационные меры по защите информации:

- Проведение лекционного курса на тему «Предупреждение заражения ВЗУ», дающего студенту базовые представления об основных источниках и признаках заражения ВЗУ вредоносным ПО, а также об эффективных средствах предотвращения заражения и ликвидации последствий от его действия.
- Создание ознакомительной инструкции пользователя студента по безопасной работе на компьютере в компьютерном классе. Инструкция содержит свод правил, выполнение которых сводит к минимуму угрозу заражения ВЗУ вредоносным ПО.

2. Программные средства защиты информации:

Рекомендация к профилактике и устранению последствий заражения ВЗУ вредоносным ПО на домашнем компьютере:

- Установка антивирусной утилиты «Зоркий глаз», способной обнаружить подавляющее большинство вредоносных программ, обитающих на флеш накопителях (даже новых и ранее неизвестных) [2].
- Установка скрипта Autostop, способного противостоять autorun-вирусам;
- Установка Panda Internet Security;
- Предоставление открытого доступа студентов к разработанным bat файлам.

Внедрение данных мероприятий должно позволить значительно снизить угрозу заражения ВЗУ студентов ФГБОУ ВПО АГУ посредством распространения вредоносного ПО на различные носители данных.

Заключение. В ходе исследования был проведен опрос студентов АГУ, в результате которого был выявлен список наиболее часто встречающихся вредоносных программ в локальной сети

университета и предложены методы борьбы с ними путем предупреждения и ликвидации последствий заражения. В результате был предложен комплекс мероприятий, позволяющий обезопасить взаимодействие различных накопителей информации и рабочего компьютера, избежав потери/искажения данных.

Литература

1. Некром О. Вирус скрыл файлы на флешке: [Электронный ресурс] /Некром О.// Компьютерная грамотность: интернет центр компьютерной грамотности,2014. – Режим доступа: www.url: http://osnov-computer.ru/. – 14.31.2014.

2. Зоркий глаз [Электронный ресурс]. – Режим доступа: http://www.exnax.narod.ru/antivir.htm. – 12.03.2012.

3. Михайлов, А.В. Компьютерные вирусы и борьба с ними/ Михайлов, А.В. – Москва: Диалог-МИФИ,2011. – 104 с.

4. Крис Касперски. Компьютерные вирусы изнутри и снаружи/ Крис Касперски. – СПб: Питер,2006. – 526 с.

ЧИСЛЕННОЕ РЕШЕНИЕ УРАВНЕНИЯ ВЫБОРА ОПТИМАЛЬНОЙ СТРАТЕГИИ СНИЖЕНИЯ РИСКА

М. М. Чудинов
руководитель – ассистент кафедры информационной безопасности ***Р. Ю. Дёмина***
Астраханский государственный университет, г. Астрахань

Введение. Оценка рисков и управление их уровнем занимает одну из ключевых позиций в сфере информационной безопасности.

Хранение конфиденциальной информации о своих клиентах (номера кредитных карт, адреса и т. д.) свойственно многим компаниям. При этом должен быть обеспечен достаточный уровень контроля хранения информации и процессов её обработки, потому что с каждым днём риск несанкционированного доступа к ней, либо утраты (повреждения) этой информации становится всё больше.

Решение о применении какой-либо политики обеспечения безопасности принимаются только после тщательной оценки рисков.

Существует множество подходов по исследованию проблемы управления рисками. Один из них рассмотрен в [1].

В статье рассмотрена математическая модель, позволяющая формализовать процедуру принятия управленческих решений в области риск-менеджмента. На её основе было выведено уравнение для выбора оптимальной стратегии снижения риска:

$$S_U^2 \cdot (U_0 - U) - S_P^2 \cdot a \cdot b \cdot e^{-bU} \cdot (P_0 - a \cdot e^{-bU}) = 0 \quad (1),$$

где *SU* – уровень затрат на снижение вероятности возникновения неблагоприятного события(НС); *SP* – уровень затрат на снижение ущерба от возникновения (НС); *a* – соответствует вероятности, с которой допускается возникновение незначимого ущерба; *b* – определяет скорость падения допустимой вероятности нанесения ущерба; *U0* – минимальное значение ущерба; *P0* – текущее значение вероятности возникновения ущерба *U0*.

Данное уравнение трансцендентно и не имеет аналитического решения. Поэтому необходимо задействовать численные методы.

На сегодняшний день существует множество разнообразных методов решения трансцендентных уравнений. Они различаются между собой по используемым подходам и, как следствие, эффективности, которая может оцениваться количеством итераций или временем вычисления.

Целью работы является анализ наиболее распространенных численных методов и выбор наиболее подходящего для рассматриваемой задачи.

Численные методы решения уравнений

Рассмотрим некоторые широко используемые численные методы. Для уравнений, не имеющих аналитического решения, используются итерационные методы с заданной степенью точности.

Решить уравнение *итерационным методом* значит установить, имеет ли оно корни, сколько корней и найти значения корней с нужной точностью.

СОДЕРЖАНИЕ

ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ РЕШЕНИЯ ЭКОНОМИЧЕСКИХ ЗАДАЧ

Научное издание

СТУДЕНЧЕСКАЯ НАУКА ДЛЯ РАЗВИТИЯ ИНФОРМАЦИОННОГО ОБЩЕСТВА

СБОРНИК МАТЕРИАЛОВ
III ВСЕРОССИЙСКОЙ НАУЧНО-ТЕХНИЧЕСКОЙ КОНФЕРЕНЦИИ
(Ставрополь, 14-18 декабря 2015)
Часть 2

Издается в авторской редакции

Компьютерная верстка М. И. Толмачёв

Подписано в печать 16.12.2015

Формат 60x84 1/8	Усл. п. л. 43,48	Уч.-изд. л. 42,72
Бумага офсетная	Заказ 295	Тираж 500 экз.

Отпечатано в Издательско-полиграфическом комплексе
ФГАОУ ВПО «Северо-Кавказский федеральный университет»
355028, г. Ставрополь, пр-т Кулакова, 2.