информационно-деловой
# ВЕСТНИК
## ОАО ЦНПО «КАСКАД»
Качество - достойное Державы!

www.kaskad.ru vestnik@kaskad.ru Издается с 2005 года ноябрь 2010 № 11 (69)

В ознаменование 91-летия образования ОАО ЦНПО «КАСКАД» ПОЗДРАВЛЯЕМ

Хранить и приумножать традиции! ПОЗДРАВЛЯЕМ

Боевой Интернет. Чем ответит Россия? Продолжение ТЕХНОЛОГИИ

Среда безопасности. Рынок охранных и антивирусных программ РЫНОК

## ТЕМА НОМЕРА: «КАСКАДУ» 91 год

ПОЗДРАВЛЯЕМ!

# В ознаменование 91-летия со дня образования ОАО ЦНПО «КАСКАД»

По сложившейся традиции награждение сотрудников Объединения приурочено ко дню рождения предприятия. В этом году в связи с 91-й годовщиной образования ОАО ЦНПО «КАСКАД» за добросовестный труд и большой личный вклад в развитие предприятия медалями Федерации космонавтики России награждены 23 человека

*Стрелки часов продолжают свой размеренный бег, оставляя за собой годы и десятилетия. Вот наше Объединение и разменяло десятый десяток.*
*91 год – солидный возраст. Возраст мудрости и подведения итогов. Мы измеряем свой жизненный путь не днями и годами. На этом пути – вехи новых проектов, новые километры кабельных трасс, пуски ракет. У нас за спиной годы безупречной работы командных пунктов и измерительных систем.*

С ДНЕМ РОЖДЕНИЯ, НАШ ВЕЧНО МОЛОДОЙ «КАСКАД»!
ТРУДОВЫХ СВЕРШЕНИЙ, АКТИВНОГО ДОЛГОЛЕТИЯ И НОВЫХ ПОБЕД ТЕБЕ!

*А нам всем – мирного неба и семейного счастья!*

**Медалью им. С. П. Королева:** Белов Сергей Дормидонтович, исполнительный директор; Куликов Илья Юрьевич, начальник монтажного участка Мирнинского филиала.

**Медалью им. В. Н. Челомея:** Гречаник Сергей Анатольевич, директор Армавирского филиала; Кукарин Сергей Николаевич, начальник управления по вводу объектов.

**Медалью им. М. К. Янгеля:** Крентик Александр Егорович, электромонтажник Армавирского филиала; Суворов Василий Валерьевич, заместитель генерального директора по производству.

**Медалью им. М. В. Келдыша:** Богатырев Сергей Валентинович, руководитель группы Белгородского филиала; Сердюк Вера Михайловна, ведущий специалист аналитического отдела Представительства ОАО ЦНПО «КАСКАД» (г. Харьков).

**Медалью им. К. Э. Циолковского:** Плоскун Александр Иванович, главный специалист отдела социологических исследований Представительства ОАО ЦНПО «КАСКАД» (г. Харьков); Третьяков Анатолий Васильевич, начальник ремонтно-восстановительной группы Мирнинского филиала.

**Медалью им. Ю. А. Гагарина:** Долголевец Николай Михайлович, сварщик 4-го разряда Мирнинского филиала; Чудаков Владислав Юрьевич, начальник отдела закупок; Меладзе Ираклий Бадриевич, заместитель генерального директора по безопасности

**Медалью им. Г. С. Титова:** Иванов Александр Валентинович, наладчик КИПиА 3-го разряда Мирнинского филиала; Бездетко Владимир Сергеевич, инженер по наладке и испытаниям РЭО 1-й категории Белгородского филиала.

**Медалью им. В. В. Терешковой:** Христофорова Вера Михайловна, инженер 2-й категории аналитического отдела Представительства ОАО ЦНПО «КАСКАД» (г. Харьков); Ясюкевич Марина Васильевна, главный бухгалтер Мирнинского филиала.

**Медалью им. А. М. Исаева:** Воробьев Юрий Иванович, начальник технического отдела Белгородского филиала.

**Медалью им. М. Л. Миля:** Грицаенко Иван Иванович, электромонтажник Армавирского филиала.

**Медалью им. В. П. Бармина:** Давлеткалиев Роман Куанышевич, руководителя группы Белгородского филиала.

**Медалью им. Н. А. Пилюгина:** Даньков Вячеслав Яковлевич, инженер-конструктор 2-й категории Белгородского филиала.

**Медалью им. Г. Н. Бабакина:** Твердохлеб Виталий Викторович, ведущий специалист аналитического отдела Представительства ОАО ЦНПО «КАСКАД» (г. Харьков).

**Медалью им. В. П. Глушко:** Кохан Борис Дмитриевич, начальник отдела Армавирского филиала.

**Медалью им. В. П. Макеева:** Прудников Владимир Евгеньевич, электромонтажник Армавирского филиала.

## ПОЗДРАВЛЯЕМ!

### Почетной грамотой ОАО ЦНПО «КАСКАД» награждены:

Бондаренко Анна Максимовна, секретарь Представительства ОАО ЦНПО «КАСКАД» (г. Харьков);

Брусенский Роман Петрович, руководитель группы Белгородского филиала;

Воронов Жорж Владимирович, монтажник-бригадир Мирнинского филиала;

Вондрухов Анатолий Васильевич, электромонтажник 5-го разряда Мирнинского филиала;

Дмитриев Андрей Александрович, инженер-программист Белгородского филиала;

Дель Виталий Александрович, электромонтажник 5-го разряда Мирнинского филиала;

Зарецкий Александр Эдуардович, ведущий инженер Армавирского филиала;

Зуев Алексей Николаевич, сварщик 4-го разряда Мирнинского филиала;

Кабаченко Дмитрий Викторович, инженер Армавирского филиала;

Козлов Александр Анатольевич, начальник управления специальной техники;

Котова Елена Александровна, нормоконтролер Белгородского филиала;

Крехалев Алексей Владимирович, монтажник 5-го разряда Мирнинского филиала;

Куров Владимир Геннадьевич, инженер-конструктор 2-й категории Белгородского филиала;

Лукашов Максим Юрьевич, инженер-программист Белгородского филиала;

Минасян Амаяк Самвелович, техник по наладке и испытаниям Белгородского филиала;

Мирохина Александра Валерьевна, начальник юридического отдела;

Мисюра Юрий Александрович, начальник отдела технологических систем;

Новгородцева Татьяна Олеговна, ведущий инженер отдела социологических исследований Представительства ОАО ЦНПО «КАСКАД» (г. Харьков);

Попов Павел Вячеславович, монтажник 5-го разряда Мирнинского филиала;

Погребной Владимир Иванович, начальник управления по ремонту технологических систем;

Подлужный Алексей Николаевич, начальник сектора сопровождения государственных контрактов;

Савчук Олег Иванович, инженер-конструктор 2-й категории Белгородского филиала;

Старицын Павел Михайлович, электромонтажник 5-го разряда Мирнинского филиала;

Сяркин Алексей Николаевич, слесарь 3-го разряда Мирнинского филиала;

Тертычный Дмитрий Юрьевич, инженер Армавирского филиала;

Токарев Александр Геннадьевич, электромонтер 4-го разряда Мирнинского филиала;

Фадин Юрий Михайлович, начальник отдела кадров и режима Мирнинского филиала;

Федотов Александр Михайлович, электромонтажник 5-го разряда Мирнинского филиала;

Шидловский Олег Анатольевич, инженер отдела техники телеметрических измерений Знаменского филиала;

Шумар Константин Михайлович, электромонтажник 5-го разряда Мирнинского филиала.

### Также благодарностью руководства Объединения отмечены:

Белобров Михаил Николаевич, электромонтажник Армавирского филиала;

Белов Сергей Дормидонтович, исполнительный директор;

Одиноченко Николай Михайлович, начальник сектора технологических систем;

Фищиленко Константин Александрович, электромонтажник Армавирского филиала;

Ершов Сергей Анатольевич, электромонтажник Армавирского филиала;

Дмитриенко Михаил Алексеевич, электромонтажник Армавирского филиала.

Соответствующий приказ подписан генеральным директором ОАО ЦНПО «КАСКАД» Геннадием Семеновичем Симухиным 19 ноября 2010 г.

## ПОЗДРАВЛЯЕМ!

# Хранить и приумножать традиции!

Близится к завершению очередной календарный и финансовый год. Наше предприятие перешагнуло в следующее свое десятилетие. Трудно себе представить, но это уже десятое десятилетие Объединения. Мы с гордостью смотрим на трудовые награды предприятия, непроизвольно вспоминаем тех из ветеранов, которых мы знали, и тех, которых никогда не видели

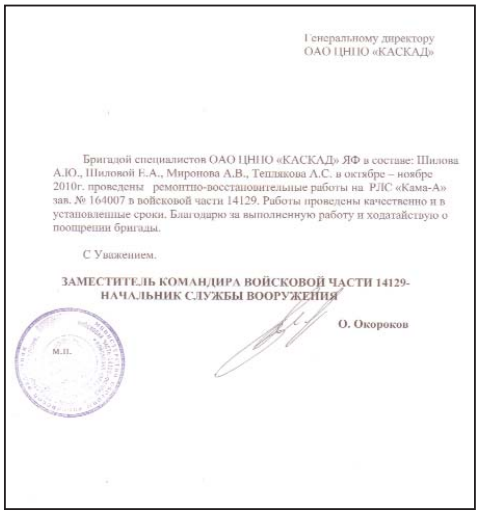
В конце года мы сконцентрировали все свои силы, чтобы своевременно завершить все контракты и договоры. Из года в год повторяются все те же шаги, которые из поколения в поколение делали наши предшественники. То есть наш нынешний коллектив продолжает те трудовые традиции, которые зародились на нашем предприятии десятки лет назад. Так же как и десятилетия назад, в настоящее время на важных объектах по всей стране трудятся специалисты «КАСКАДА» – Н. М. Одиноченко, Л. В. Кириченко, А. М. Ахметзянов, С. П. Чеканов, В. М. Шишкин, В. И. Погребной.

Что заставляет людей ехать работать на дальние объекты? Конечно же, стремление заработать. А вот что заставляет людей выполнять свою работу с высоким качеством? Можно ответить просто – традиции. Если работника приучили на предприятии работать только на отлично, если он знает, что на этом предприятии принято только так, то он всегда будет стремиться выполнять свою работу с высоким качеством. Это уже будет традицией. Когда-то в нашем коллективе на основе опыта совместной деятельности сложились и прочно укоренились нормы, правила и стереотипы поведения. Из года в год, из десятилетия в десятилетие они передавались каждому последующему коллективу «КАСКАДА».

В современный «КАСКАД» эти традиции передавались через ветеранов – нашего предыдущего генерального директора В. В. Титова, нынешнего главного конструктора В. В. Стешенко, директора ярославского филиала Е. П. Колесникова, руководителя дочернего предприятия «Харьковский филиал» А. Г. Краморенко, главного инженера проекта А. М. Белоусова, А. А. Шмелева.

За период своей современной деятельности наше предприятие выросло в большой коллектив опытных специалистов, который способен проводить широкий спектр работ, начиная с проектирования и заканчивая монтажом и наладкой сложнейшего оборудования. Мы стремимся сохранить позиции динамично развивающегося предприятия, сочетающего трудовые традиции прошлого, успешную деятельность в настоящем, новые достижения в будущем.

Почему мы с удовольствием празднуем день рождения нашего предприятия, почему с уважением смотрим в его прошлое? Потому что нам в наследство досталась славная традиция уважительного отношения к каждому специалисту нашего коллектива. Кажется, что этим пропитаны стены «КАСКАДА». Меняются поколения, приходят в «КАСКАД» новые люди, а коллектив остается все таким же дружным, работоспособным, профессиональным. Это подтверждают даже те, кто по каким-либо причинам оставил работу в Объединении. Нетрудно найти массу благодарственных отзывов о результатах работы предприятия о профессионально выполненной работе от многих инстанций.



Генеральному директору
ОАО ЦНПО «КАСКАД»

Бригадой специалистов ОАО ЦНПО «КАСКАД» ЯФ в составе: Шилова А.Ю., Шиловой Е.А., Миронова А.В., Тепляков А.С. в октябре – ноябре 2010г. проведены ремонтно-восстановительные работы на РЛС «Кама-А» зав. № 164007 в войсковой части 14129. Работы проведены качественно и в установленные сроки. Благодарю за выполненную работу и ходатайствую о поощрении бригады.

С Уважением.

ЗАМЕСТИТЕЛЬ КОМАНДИРА ВОЙСКОВОЙ ЧАСТИ 14129-
НАЧАЛЬНИК СЛУЖБЫ ВООРУЖЕНИЯ

О. Окороков

М.П.

Важнейшей традицией Объединения, одним из важнейших активов нашей компании, одним из ключевых факторов является профессионализм сотрудников. Забота о этом – задача каждого руководителя и каждого специалиста. В подразделении Ю. А. Мисюры во главу всей деятельности поставлен именно высокий профессионализм, который, как твердо уверены в отделе, обеспечит успешное будущее их коллектива.

ОАО ЦНПО «КАСКАД» способно сконцентрироваться на любом объекте в любом месте и в любое время. Эта работа по силам лишь предприятиям, владеющим, помимо современных технологий и оборудования, многолетним опытом практической работы и новейшими знаниями, вкладывающим немалые средства в развитие производственной базы. Всеми этими качествами в полной мере обладает наше предприятие.

Можно быть уверенным, что славные трудовые традиции, передающиеся из поколения в поколение, останутся залогом устойчивой работы Объединения.

*Начальник управления специальной техники*
*А. А. Козлов*

## ТЕХНОЛОГИИ

# Боевой Интернет. Чем ответит Россия?

***Продолжение. Начало в № 10/2010***

В прошлом номере мы рассмотрели возможности боевого применения сети, аналогичной Интернету, на примере ВС США. Вице-адмирал ВМС США Артур Себровски и эксперт КНШ Джон Гарстка ввели даже специальный термин Network Centric Warfare (NCW), или «сетецентрическая война». Действительно, отчасти это лицо войны будущего, но практические результаты применения подобных разработок на сегодняшний день далеко не однозначны

Впрочем, есть и примеры очень успешного использования «сетецентрических» технологий. Новые возможности продемонстрированы при организации адресного тылового снабжения – основы боевого применения войск в маневренной войне. В Ираке успешно использовалась распределенная информационная система MTS (Army's Movement Tracking System). В ней на основе радиоизлучающих датчиков, стационарных и портативных сканеров, системы GPS, беспроводного доступа и тактического Интернета непрерывно отслеживается положение всех наземных подвижных объектов (танков, БТР, БМП) на ТВД, от экипажей которых органы тыла получали запросы на поставку топлива, боеприпасов, ЗИП и других видов обеспечения. В системе было задействовано около 4000 бортовых компьютеров и 100 серверов. Система MTS обошлась армии США в 418 млн долл. и формировалась в тече-

***Продолжение на стр. 3***

**ТЕХНОЛОГИИ**

# Боевой Интернет. Чем ответит Россия?

***Начало на стр. 2***

ние трех лет. Компьютеры штаба 5-го армейского корпуса – основной ударной силы группировки в Ираке – были способны самостоятельно сопровождать до 1000 наземных объектов. Командиры эскадрилий палубной авиации планировали вылеты своих экипажей вместе с коллегами из армейской авиации, также пользуясь общей информационной системой.

Уже в операции в Афганистане 80% боевых вылетов производится «вслепую», то есть в память бортовых компьютеров заранее не вводятся координаты целей, информация о них поступает от наземных частей непосредственно с передовой. Для этого развернута специальная система боевого планирования и управления авиацией на ТВД – TBMCS (Theater Battle Management Core Systems). Более чем в семь раз по сравнению с 1991 г. увеличилась суммарная полоса пропускания (до 3 ГГц) арендованных Пентагоном каналов спутниковой связи для передачи информации. В результате в Ираке в 2003 г. в ходе воздушных ударов применено до 80% высокоточного оружия. Для сравнения: 10% применялось во время «Бури в пустыне» и 40% – в Югославии. Масштабы разрушений в Ираке нам сегодня неизвестны, но известно, что во время войны против Югославии (1999 г.). 900 гражданских и военных объектов были выведены из строя 1500 высокоточными ракетами. С их помощью разрушена нефтеперерабатывающая промышленность и уничтожено 40% нефтехранилищ. Уничтожено 80 мостов, не менее 50% оборонных предприятий, выведено из строя 70% автомобильных и железных дорог.

Сегодня американские офицеры не рисуют карт и не передают боевые донесения голосом по радио. Они используют распределенную информационную систему боевого управления

FBCB2 (Force XXI Battle Command Brigade or Below), охватывающую звенья «бригада–батальон–рота».

Чем отвечает Россия? Идея управления войсками с помощью интернетподобных технологий захватила умы военных и в России. В нашем Генштабе как о само собой разумеющемся говорят о «сетецентрических» войнах будущего. В Советском Союзе существовали системы высшего уровня («Редут», «Кентавр») и ПАСУВ «Маневр», охватывавшая органы управления тактического звена. Следует особо отметить, что одним из пионеров этой тематики в СССР выступило ЦНПО «КАСКАД». Полевая автоматизированная система связи фронта «Редут-2» подсистемы связи РВСН «Редут 1–3» в рамках объединенной автоматизированной системы связи ВС «Редут», автоматизированные системы управления связью РВСН «Багет» – все это работы Объединения в годы СССР. Активно работали в этом направлении и другие предприятия, так что появление полевой автоматизированной системы управления войсками (ПАСУВ) «Маневр», так напугавшей американцев, было вполне закономерно. Как считают эксперты, она была очень неплохой для 1983 г. (год принятия на вооружение) коллективной разработкой, с хорошим военным обеспечением, исходными данными. Системы «Маневр» состоят из двух частей: АСУ фронта–армии–дивизии и полевой системы связи. В разработке участвовали в том числе и страны Организации Варшавского договора (ОВД) – Болгария, ГДР и другие. Выпущены и поставлены в войска ОВД несколько дивизионных комплектов в двух вариантах. В СССР армейский комплект прошел государственные испытания, но развернуть его успели только в ПВО и ВВС Группы советских войск в Германии. Но к исходу 80-х гг. прошлого века работы по «Маневру» практически свернули. Изменения в заказывающих управлениях Минобороны РФ также не способствовали концентрации финансовых и организационных усилий на создании масштабной автоматизированной системы управления войсками. Работы велись только в интересах отдельных органов управления и соединений ВДВ. Системные работы по автоматизации пунктов управления уровней оперативного звена были возобновлены через 10 лет, а по тактическому звену – спустя еще пять лет.

Учесть все многообразие требований к организации и временным показателям циклов управления в этих звеньях и скоординировать все работы по созданию средств поражения и разведки различного назначения, чтобы обеспечить их эффективное боевое применение, не брался никто. Поэтому в новой России пошли своим путем: с 1990-х гг. концерн «Системпром» разрабатывал АСУВ «Акация» для оперативно-стратегического звена. К концу 2012 г. российская армия при достаточном финансировании может быть полностью оснащена мобильным вариантом системы «Акация-М» – военным аналогом Интернета. Сегодня такими комплексами оснащены один из пунктов управления Генштаба, а также Московский военный округ и 20-я армия. Это позволяет офицерам находиться в одном и том же информационном пространстве, как в местах постоянной дислокации, так и при выходе в поле или в ходе боевых действий.

Однако без системы управления тактическим звеном, то есть уровнем «бригада–батальон–рота–солдат», автоматизация управления большого смысла не имеет. Задачу по созданию Единой системы управления тактическим звеном (ЕСУ ТЗ) решают с 2000 г. в «Концерне «Созвездие»», ведущем предприятии РЭП по созданию АСУ, средств связи для ВС РФ и силовых структур. Шифр разработки «Созвездие-М». В СССР действовали 16 разных систем управления. Теперь необходима одна.

Ее появление сулит технологическую революцию в области управления: зона ведения боевых действий бригады расширяется вдвое при двукратном сокращении цикла боевого управления. При этом возможно непрерывное ведение боевых действий и их обеспечение, что позволяет максимально использовать боевой потенциал тактических формирований. Испытания показали – отдельные нормативы «солдат с компьютером» выполняет в 40 раз быстрее, чем раньше. Собственно, это уже не просто компьютер, а коммуникатор. В этом году предложено решение в виде IP-телефонии, которая позволит выйти на отдельного военнослужащего простыми набором номера. Военные получают «мобильник» с WiFi-связью, GSM-модулем, ГЛОНАСС и радиостанцией шестого поколения. Вес аппаратуры – 500 г.

Единая цифровая защищенная полевая сеть связи создается с использованием мэдж-технологий на базе станций Wi-Fi. Можно сравнить ее возможности с передачей информации обычными средствами (радиостанция, проводная связь). Раньше время доведения команды или боевого распоряжения от командира бригады до командира подразделения исчислялось десятками минут. Сейчас, с использованием автоматизированных средств управления, – от нескольких секунд до десятков секунд.

Для обеспечения оперативных контуров управления в составе оперативного командования (армии) требования по взаимодействию заданы в обеих системах. Более того, ЕСУ ТЗ должна взаимодействовать не только с «Акацией», но и с другими АСУ видов и родов войск. Планируется не замещать одни средства автоматизации другими, а интегрировать их ресурсы.

На учениях «Кавказ 2009» обе системы вызвали ряд нареканий военных. Характер этих нареканий в принципе аналогичен американским. Анализируя опыт боевых действий в Ираке, американцы назвали одной из причин ошибок программные и иные недостатки архитектуры данной автоматизированной системы боевого управления. Во время испытаний сегмента ЕСУ ТЗ в позапрошлом году, продолжавшихся около недели, было зафиксировано 137 отказов и сбоев. Из них только 12 – из-за неправильных действий бойцов. Одновременно выявилась недостаточная устойчивость связи в условиях применения средств РЭП.

Сеть состоит из множества устройств, которые принимают и отправляют сигналы в самых разных диапазонах. Заблокировать эту систему можно, только если забить помехами практически весь существующий частотный диапазон. Но нельзя исключать, что противник окажется в состоянии это сделать.

Одна из главных задач на сегодня – отработка алгоритмов действий в условиях боя, так чтобы их понимал каждый участник. И здесь возникают определенные проблемы. Многие военные уже жалуются, что научиться работать с новой системой трудно. То есть, даже если будут решены все технические проблемы, интерфейс программы настолько сложен, что пока все комбаты разберутся в стрелочках и значках, уйдет масса времени.

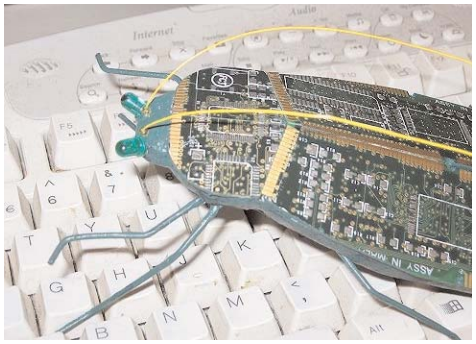
В марте 2010 г. на полигоне Струги Красные прошло КШУ 76-й Гвардейской десантно-штурмовой дивизии, в ходе которого отрабатывались элементы «сетецентрического» метода управления войсками. Основным событием боевой подготовки 2010 г. стало оперативно-стратегическое учение «Восток-2010», к маневрам привлекли 20 тыс. солдат и офицеров, около 70 самолетов, почти 2500 единиц техники и порядка 30 кораблей. Генштаб развернул на учении три общевойсковые бригады. Учитывая, что военные остались в целом довольны результатами, есть основания полагать, что работа по совершенствованию систем управления войсками ведется и уже дала положительные результаты.

**РЫНОК**

# Среда безопасности

## Рынок охранных и антивирусных программ

В 2009 г. Россия занимала 4-е место в мире по количеству вирусных атак. Впрочем, сам термин «вирус» уже несколько неточен. На смену пришло понятие «вредоносная программа». Постепенно изменилась сама цель создания вирусов: прошло время одиночек, которые писали вирусы из простого хулиганства или самоутверждения. Цель сместилась в область финансов, и поэтому классические вирусы, заражающие файлы и портящие «железо», практически исчезли



Сегодня появление вирусов связано с большим транснациональным бизнесом, в котором есть даже разделение труда – одни ищут и анализируют уязвимости, другие пишут эксплойты (программы, использующие уязвимости в ПО и применяемые для проведения атаки на вычислительную систему), третьи – вирусы, четвертые отвечают за финансовые аспекты.

Злоумышленники всегда акцентировали свое внимание на наименее защищенных зонах. Сейчас, пожалуй, это социальные сети на базе веб и системы мгновенных сообщений.

**Угрозы из Всемирной паутины**

Интернет повлиял не только на вирусы, но и на стратегию защиты. Стала доминировать эшелонированная защита с обязательной защитой периметра – интернет-шлюзов и почтовых серверов. Постепенно акцент был смещен с защиты только рабочих станций именно на эти узлы защиты.

Специалисты Вирусной лаборатории ESET выявили в августе 2010 г. самые распространенные интернет-угрозы. При этом использовалась технология раннего обнаружения ThreatSense.Net.

Статистические данные вредоносного программного обеспечения претерпели значительные изменения. Резкое падение активности червя Conficker привело к тому, что угрозой номер один в мире стало уже давно известное семейство злонамеренных программ INF\Autorun. Данный класс программного обеспечения использует для проникновения на компьютер пользователя функцию автозапуска Windows Autorun и распространяется на сменных носителях. Доля заражений INF\Autorun составила 7,76% по миру. Наиболее подвержены этой инфекции оказались ЮАР (10,48% от общего количества угроз), Израиль (5,66%), Австрия (3,58%) и Словакия (3,45%).

На втором месте рейтинга мировых угроз расположился червь Conficker. К концу лета его активность начала снижаться, и в августе доля распространения достигла абсолютного минимума за все время его присутствия в десятке – 4,89%, что на 7,58% меньше, чем месяцем ранее. Основные очаги инфекций сохранились на Украине (6,98%), в ОАЭ (3,83%) и Польше (2,48%).

Замыкают тройку лидеров кейлогеры Win32/PSW. OnLineGames, используемые хакерами для кражи аккаунтов игроков многопользовательских онлайн-игр. Уровень распространения этой угрозы составил 3,82%, что на 0,17% выше показателей предыдущего месяца. В числе пострадавших от заражения – пользователи из Словакии (3,36%) и Турции (4,09%).

Изменилась картина угроз и в российской двадцатке самого распространенного вредоносного ПО. Лидер ее, семейство троянских программ, предназначенных для кражи личных

***Продолжение на стр. 4***

**РЫНОК**

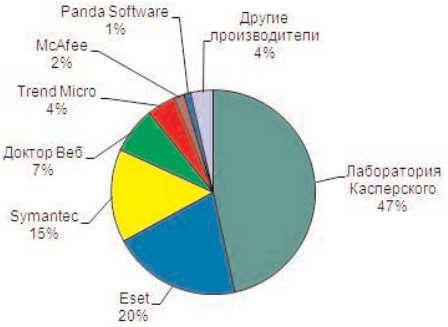
# Среда безопасности

***Начало на стр. 3***

данных пользователя, Win32/Agent, с показателем в 2,15% переместился на четвертое место, снизив долю присутствия в регионе на 3,38%. Однако эвристические технологии антивирусных продуктов ESET стали чаще срабатывать на вредоносные программы со схожим злонамеренным кодом, что отражено в статистике – с 14-е по 16-е место.

Главной угрозой вновь стала троянская программа Win32/Spy.Ursnif.A, которая крадет персональную информацию и учетные записи с зараженного компьютера и отправляет их на удаленный сервер. Кроме того, троянец может распространяться в составе другого вредоносного ПО. Процент проникновения Spy.Ursnif в России составил 4,38%.

Семейство INF\Autorun также угрожает безопасности компьютеров и российских пользователей. Несмотря на незначительное падение доли его распространенности в регионе (на 0,43%), данная вредоносная программа прочно занимает лидирующие позиции в рейтинге.




В августе доля присутствия INF\Autorun составила 4,31%. А общий процент проникновения всех модификаций этой угрозы – 5,50%. При этом значительно сдал позиции Conficker. Самой распространенной модификацией червя в России стал Win32/Conficker.AA с показателем 2,26%. Общая доля распространенности угрозы на локальном уровне упала в два раза и составила 5,25%.

Аналитики также наблюдали рост заражения программами класса Win32/Hoax.ArchSMS, который переместился на 6-е место российского рейтинга. Доля злонамеренного ПО составила 1,83%, что выше на 0,61% показателей прошлого месяца. Цели злоумышленников, которые распространяют данное вредоносное ПО, заключаются в вымогательстве денег за установку скачанного пользователем приложения. При этом появляется окно с просьбой отправить SMS на короткий номер. Распространяется данная угроза под видом различного популярного ПО.

В 2005 г. появился еще один вид вредоносного ПО – фальшивые антивирусы, применяемые мошенниками для получения нелегальных доходов. В западных странах и России они распространяются по-разному. Массовое распространение их на Западе началось осенью 2009 г. В англоязычных спам-рассылках используются модификации семейства Trojan. Fakealert, которые при заражении имитируют работу антивируса. В России, в свою очередь, стали распространяться мошеннические интернет-ресурсы. Ссылки на них под различными предлогами рассылаются по электронной почте, в социальных сетях и через средства мгновенного обмена сообщениями, а также фигурируют в контекстной рекламе некоторых поисковых систем. Графически имитируется процесс сканирования антивируса, причем компьютер не заражается никакой вредоносной программой.

Различаются и способы оплаты лжеантивирусов. Если в России это платные SMS-сообщения, то в западных странах – безналичные платежи при помощи банковских карт (в среднем 50 долл.).

Признаки лжеантивирусов:
– лжеантивирус сканирует систему обычно очень быстро – всего несколько десятков секунд;
– злоумышленники обычно предлагают только один метод оплаты;
– стоимость отправляемого SMS не сообщается или намеренно занижена;
– на сайтах с лжеантивирусами не указаны банковские реквизиты, адрес офиса и другие контактные данные поставщика.

По сути, пользователи платят деньги просто за возможность использования своего компьютера. Самое главное – на самом деле не поверить, что на компьютере теперь установлен гениальный антивирус. Тогда система останется совсем беззащитной. Как сказано в отчете PandaLabs: «Эта новая тенденция в вымогательстве показывает, что либо пользователи становятся более опытными при опознании подобных угроз, либо антивирусные компании начинают перекрывать кислород мошенникам. Это бы объяснило, почему хакеры используют все более агрессивные методы принуждения своих жертв к платежам».

**Коробочные антивирусы**

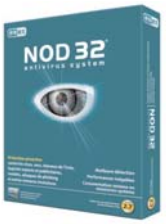
Более 25 лет компьютерные вирусы досаждают пользователям по всему миру, и более 25 лет антивирусные эксперты борются с ними. Однако практически все основные антивирусные технологии были придуманы еще к середине 1990-х гг., а сейчас продолжается их экстенсивное развитие, включающее в себя различные технологические совершенствования.

Антивирусы были далеко не первым направлением в области защиты информации. Гораздо раньше появились, например, системы контроля за доступом, защиты от взлома. Антивирусные программы в виде законченных коммерческих проектов впервые возникли около 20 лет назад.

Антивирусные программы, или антивирусы, служат для обнаружения компьютерных вирусов и прочих нежелательных (считающихся вредоносными) программ. Они восстанавливают файлы, зараженные такими программами, и предотвращают новые заражения (например, с помощью вакцинации). Антивирусные программы по своим функциям делятся на разные виды: фильтры, детекторы, программы-доктора или фаги, ревизоры, сторожа, программы-вакцины.

В современной России существуют десятки антивирусных программ, способные эффективно противостоять различного вида вирусным угрозам. Однако выделяется список лидеров, включающий такие антивирусные пакеты, как Kaspersky Anti-Virus, Panda Software, McAfee, «Доктор Веб», Eset и т. д.

**ESET (NOD32)**




Основные продукты:
- NOD32 Antivirus;
- NOD32 Smart Security;
- NOD32 Business Edition.

Эти пакеты обеспечивают безупречную защиту персональных компьютеров и корпоративных систем, работающих под управлением Microsoft Windows 95/98/ME/NT/2000/2003/XP, UNIX/Linux, Novell, MS DOS, а также для почтовых серверов Microsoft Exchange Server, Lotus Domino и других.

Главное преимущество NOD32 – быстрая работа и не раз доказанная способность ловить 100% вирусов. Работать с ним предельно просто. Включает четыре модуля: антивирусный монитор, монитор интернет-трафика, монитор документов MSOffice, защищающий от макровирусов, и антивирусный сканер.

**Лаборатория КАСПЕРСКОГО**

Основные продукты:
- Антивирус Касперского;
- Kaspersky Internet Security;
- Kaspersky Open Space Security.

Установка и использование Антивируса Касперского Personal очень проста. При настройке программы выбирается один из трех предопределенных уровней защиты: «максимальная защита», «рекомендуемая защита» и «максимальная скорость». У программы удобный интерфейс.

В Антивирусе Касперского Personal применяется современная технология защиты от вирусов, основанная на принципах эвристического анализа второго поколения. Двухуровневая защита почты.

Программа – бесспорный лидер по тщательности проверки подозрительных объектов. Антивирус Касперского обнаруживает вирусы в архивированных и упакованных файлах более чем 700 форматов, а также лечит файлы форматов ZIP, ARJ, CAB и RAR. Программа каждый час обновляется, организована круглосуточная техническая поддержка.

**DR.WEB32**

Основные продукты:
- Dr.Web Security Space Pro;
- Dr.Web Enterprise Suite;
- Dr.Web Бастион Pro.

Программа Dr.Web32 для Win32 выпущена в двух вариантах: с графическим интерфейсом (DrWeb32W) и без него (Dr.WebWCL). Оба варианта поддерживают одинаковый набор параметров (ключей) командной строки, но для варианта с графическим интерфейсом все настройки могут производиться и из диалоговых панелей, что обычно более удобно.

В то же время вариант без графического интерфейса несколько экономит ресурсы.

В составе антивируса идет антивирусный монитор, который немедленно («на лету») проверяет все файлы, а также электронную почту.

Вероятность обнаружения вирусов, или, другими словами, надежность, антивирусной программы Dr.Web в апреле 2008 г. была рассчитана по методике российской «Лаборатории восстановления данных FS» и признана самой высокой среди подобных программ.

**PANDA**

Panda Titanium Antivirus 2004 быстро обнаруживает и уничтожает вирусы, троянцев, червей, программы-«дозвонщики», программы-«шутки», вредоносные коды ActiveX и опасные Java-апплеты.

Технология эвристического сканирования позволяет обнаруживать новые и неизвестные вирусы. Программа включает в себя мощные инструменты активной защиты.

Titanium Antivirus 2004 очень прост и удобен в использовании: у него интуитивно понятный интерфейс, прямые отчеты и полностью автоматические обновления.

Каждый раз, когда компьютер соединяется с Интернетом, TitaniumAntivirus 2004 находит и загружает ежедневные обновления файла вирусных баз, определяет и уничтожает вирусы еще до того, как пользователь открывает зараженное письмо.

В России представительство Panda Security зарегистрировано в 2001 г. и сейчас имеет развитую дилерскую сеть. Panda Security предлагает новую модель безопасности, специально разработанную для жесткой борьбы с новыми видами киберпреступности.

**Как выбрать лучший антивирус?**

Наиболее важные характеристики антивирусных программ:
– простота использования антивируса;
– эффективность защиты от вирусов, червей и других вредоносных программ;
– регулярность обновления антивирусной базы;
– возможности и характеристики защитного комплекса;
– простота установки антивирусной программы;
– уровень технического обслуживания.

Можно заметить, что каждый производитель ищет для себя нишу, которую считает некоей «фишкой».

Кроме того, все антивирусные пакеты проверяются на наличие международных сертификатов: 1) ICSA Certified, 2) VB100% Certified, 3) W.C.L Level 1 Certified, 4) W.C.L Level 2 Certified.

Пользователей особенно привлекают те продукты, которые можно использовать дома бесплатно. Например, NOD32 и Avast! в домашних версиях бесплатны. Бесплатен и самый популярный антивирус — AVG. Еще один плюс бесплатных защитных программ — они не обвешаны множеством «примочек», «экранов» и других инструментов безопасности для защиты всего и вся, а значит, не так прожорливы в отношении ресурсов компьютера. Если учесть, что сейчас тренд рынка ПК явно наметился в сторону удешевления, миниатюрности и энергоэффективности (актуально для нетбуков), то становится понятно, почему простой и легкий NOD32 популярнее, чем мощные орудия «Лаборатории Касперского», а тяжелейший продукт от Norton и вовсе находится в конце списка.

По результатам исследования компании «Комкон», 40% домашних пользователей выбирают в качестве антивируса продукцию Касперского, 23% — ESET, 17% — компании «Доктор Веб». При этом среди тех, кто предпочитает лицензионный софт, популярность «Лаборатории Касперского» еще выше — 44%. И лишь 19% покупателей лицензионных продуктов выбирают NOD32, а 16% — Dr.Web.

Примерно каждый пятый (22%) из покупателей лицензионного антивирусного программного обеспечения приобретает его в магазинах компьютерной и бытовой техники. Столь же часто этот софт скачивается из Интернета (зачастую нелегально), а 18% пользователей берут диски с нужными программами на работе. Еще одна неутешительная цифра для разработчиков: лишь 29% всех пользователей используют лицензионный софт.

Что ждет рынок антивирусного ПО в будущем? Очевидно, что доля использования нелицензионных программ будет снижаться, однако вряд ли за счет платных программ. По крайней мере есть все предпосылки для того, чтобы домашние пользователи использовали бесплатные программы, дающие возможность базовой защиты компьютера.

Разработчикам антивирусов также выгодно их продвигать: повышается уровень узнаваемости брендов и лояльности пользователей. А это дает основания полагать, что доля продвинутых платных версий программ будет расти в корпоративном сегменте. Вероятно, снижение доли «Лаборатории Касперского» как раз говорит о том, что у нее нет такого бесплатного домашнего продукта. Устаревают и традиционные каналы дистрибуции программного обеспечения: сегодня пользователям удобнее скачивать программы из Интернета, а не ходить за ними в магазины. Понятно, что быстрый доступ к Сети тоже упрощает скачивание бесплатных антивирусов. А платить в Интернете за контент наши пользователи еще не совсем привыкли.

***Продолжение следует***

*Главный редактор М. Сарбучев*
*Корректор О. Иванова*

*Россия, 125047, Москва,*
*1-я Брестская ул., 35*
*Телефон: (499) 978-58-73,*
*(495) 251-76-50*
*Факс: (499) 978-57-36*
*E-mail: vestnik@kaskad.ru*
*http://www.kaskad.ru*

*При перепечатке ссылка на «Информационно-деловой вестник ОАО ЦНПО «КАСКАД»» обязательна.*

*Тираж 999 экз.*

*Распространяется по уникальной базе ОАО ЦНПО «КАСКАД»*