

«ДЯТЛЫ», ВОИНЫ СВЕТА...



Станислав Шевченко,
заместитель директора
департамента инноваций и
разработки «Лаборатории
Касперского»

«Дятлы у нас обрабатывают поток по сменному графику», «есть дятлы зрелые, матёрые, есть молодые, перспективные, есть ещё зелёные, учатся пока»... Слыша подобные фразы, непосвящённый человек испытывает недоумение: речь идет о птицах? О птицах, но птицах особого полета. Речь о «дятлах». Именно так в «Лаборатории Касперского» называют вирусных

аналитиков. О работе «дятлов», о том, как ими становятся и что нужно для того, чтобы стать настоящим «дятлом», рассказывает Станислав Шевченко, заместитель директора департамента инноваций и разработки «Лаборатории Касперского», руководитель антивирусной лаборатории.

Кто и когда придумал название «дятел»?

Вирусных аналитиков в «Лаборатории Касперского» всегда называли «дятлами». Наше эксклюзивное название, если хотите. Слово *woodpecker* теперь и в английском языке для нас имеет второе значение – вирусный аналитик. Авторство проследить сложно. Название зародилось в «Лаборатории Касперского», но сказать наверняка, кто придумал и стал первым использовать слово «дятел», не могу. Когда я пришёл в компанию (почти девять лет назад), слово уже существовало.

Что это название символизирует в среде вирусных аналитиков?

Этимология слова «дятел» тесно связана со спецификой работы вирусных аналитиков. «Дятлы» непрерывно обрабатывают всё возрастающий поток вирусов, червей и прочих троянцев. Иными словами, день и ночь «долбят» новых «зловредов». Неволь-

но прослеживается четкая ассоциация с дятлом. Хотя на самом деле всё гораздо глубже, не только на уровне ассоциаций.

На сайте антивирусной школы (<http://av-school.ru>), который ведем мы, аналитики, уже третий или четвертый раз проводится игра для всех пользователей Интернета, которая называется компьютерный биатлон. Отвечая на аналогичный вопрос, участники одной из команд предложили свою интерпретацию: дятел – санитар леса, наши «дятлы» – санитары Интернета. Такое толкование мне, честно скажу, очень нравится.

Расскажите, пожалуйста, кто был первым «дятлом», как долго он работал в компании и кем стал сегодня?

Первым «дятлом» был, конечно же, Евгений Касперский. Если говорить о «дятлах» следующего поколения, среди них я бы назвал Александра Гостева, который в настоящее время является

руководителем группы глобальных исследований и аналитики «Лаборатории Касперского». Как и все, Саша начал с должности вирусного аналитика. Работа ответственная и напряженная: получение объекта, анализ, принятие решения, детектирование и так далее. Этот период становится своего рода школой профессионального выживания и роста, выявляет способности человека и определяет его призвание. Саша научился не просто обрабатывать информацию, а анализировать ее, замечать тенденции, фиксировать индивидуальные особенности каждого анализируемого объекта и наиболее интересные случаи. Перефразируя поговорку о том, что за деревьями леса не видно, можно сказать, что Саша способен и лес увидеть, и каждое деревце рассмотреть.

Какова миссия «дятлов»?

Антивирусная лаборатория (в просторечье – «вириаб») – одно из центральных подразделений нашей компании, в котором работают «дятлы». Девиз лаборатории – «Мы спасаем мир!» Мы действительно спасаем мир – от компьютерных угроз и даже компьютерного терроризма. Для кого-то это громкие слова, для нас же – просто работа.

Какой путь проходят «дятлы»? Как становятся ведущими аналитиками?

Когда я пришёл в компанию в 2000 году, вирусной лаборатории как таковой не было. У нас работало около семи человек, которые, кроме антивирусного движка, занимались обработкой входящего потока. Это был обыкновенный почтовый ящик, существующий и сегодня, который переключался на сотрудников, причем переключался вручную. Тогда его в основном обрабатывал



Евгений Касперский. Вирусные коллекции были небольшие.

За прошедшие восемь-десять лет мы нарабатывали уникальный инструментарий, который позволяет нам оперативно собирать информацию о новых вредоносных программах со всего мира. Сегодня вирлаб можно с полным основанием назвать научно-исследовательской лабораторией.



Дятел – лесная птица с длинным и сильным клювом, которым она добывает насекомых из щелей и трещин древесной коры.

«Современный толковый словарь русского языка»,
Москва, Российская академия наук

У нас построена чёткая схема: мы находим вирусных аналитиков, отбираем их, принимаем на работу, ведём «дятлов» до какого-то определённого момента. Учебных заведений, где учат на вирусного аналитика, к сожалению, нет. Существуют факультеты компьютерной безопасности, но работать с вредоносным

«Дятел» – офисная «птица», санитар Интернета, с острым умом и высоким чувством ответственности. Стучит по клавиатуре со страшной силой, безжалостно «долбит» любых «зловредов».

Табель о рангах «Лаборатории Касперского»

кодом в университетах не учат. Поэтому в вирлабе организован свой, внутренний процесс обучения «дятлов». Карьерный рост тесно связан с профессиональным развитием. Вирусный аналитик – ведущий аналитик – эксперт – антивирусный «гуру»...

Расскажите, пожалуйста, о трудных буднях «дятлов». В чем специфика работы вирусного аналитика?

Наша работа непростая. Сложная морально и физически. Во-первых, «дятлы» работают посменно – график достаточно напряжённый. Во-вторых, деятельность вирусного аналитика связана с высочайшим уровнем ответственности. Безответственных «дятлов» просто не существует в природе.

Всех людей, которые к нам приходят, можно назвать *потенциальными программистами*. Что такое программист? Он открывает чистый лист, пишет 'begin', определяет переменные, и... рождается программа – продукт деятельности, который можно посмотреть, показать коллегам. Иными словами, он пишет код, который что-то делает. Вирусные аналитики – люди иного плана. Они склонны, скажем так, анализировать, разбирать чужой код. В детстве они, наверное, часто ломали игрушки, чтобы узнать, что находится внутри. Им интересно посмотреть, как устроен тот и иной механизм. Не *выдать* конкретный продукт, а *разобраться* в каких-то технологиях. Это один из плюсов и минусов. Та самая психологическая составляющая.

Какими личностными качествами должен обладать «дятел»? Кто ни при каких условиях не сможет стать «дятлом», даже если все профессиональные качества говорят в пользу этого?

Никогда не сможет стать «дятлом» бывший вирусописатель. Мы в вирлабе чётко обозначаем наши, если можно так выразиться, позиции. Они на тёмной стороне, мы на светлой стороне. Причем мы – *только* на светлой. Здесь не может быть никаких полутонов. Существуют люди, которые *потенциально* могут «поменять сторону»: перейти с тёмной стороны на светлую, со

светлой – на тёмную... В принципе, это видно. Такого человека я не возьму на работу однозначно. Вирусному аналитику даётся в руки очень серьёзный инструментарий: технологии, знания, доступ к самой вирусной коллекции. В *неправильных* руках все это может нанести колоссальный ущерб Интернету и всему миру. Девиз «Мы спасаем мир» для нашей команды не пустой звук. Поэтому среди нас нет людей, которые смогут переметнуться на тёмную сторону. Хочу подчеркнуть: это не конкретный принцип «Лаборатории Касперского» – это жёсткий принцип всей индустрии.

Можно ли сразу распознать перспективного и даже талантливого вирусного аналитика? Какими критериями вы руководствуетесь, оценивая будущего кандидата?

Сложно, да и невозможно перечислить конкретные критерии. Как правило, уже во время первой встречи понимаешь, подходит кандидат или нет. Выбор определяют самые разные показатели. Соискателю предлагается выполнить небольшое тестовое задание, на основании которого я могу судить о его технической подготовке и навыках. При этом можно не знать инструментария – должна работать логика. Мы смотрим, «включает» ли человек мозг, в состоянии ли он мыслить логически. Выражаясь проще, я бы определил это следующим образом: «выдаёт результат, не выдаёт результат». Как правило, два-три стандартных вопроса плюс, как я уже упомянул, небольшое задание, ну а потом подробная беседа с успешным кандидатом.

Что представляет собой период обучения и адаптации?

Что касается последующего обучения, в вирлабе существует продуманная и тщательно выстроенная процедура. Вирусный аналитик, прошедший наш курс подготовки, максимум через три месяца в состо-

янии, выражаясь нашим языком, «сесть на KLAN» и начать обрабатывать поток. Иными словами, он может работать (или, как мы говорим, «обрабатывать поток») по сменному графику.

Изначально вирлаб был единым организмом. Сейчас структура немного раздробилась – сменных аналитиков у нас порядка тридцати человек, общий круг специалистов включает примерно шестьдесят сотрудников. Человек должен стать, если можно так выразиться, частью этого организма. Новый аналитик очень легко и естественно вливается в команду. Иного пути нет. Можно говорить, что многое происходит на уровне «впишется в коллектив, не впишется в коллектив». Смею утверждать, что такой подход к формированию командной работы в вирлабе очень верен. Благодаря четко выстроенной схеме в лаборатории работают только нужные нам люди, которыми мы дорожим. Компания вообще очень трепетно, по-другому не скажешь, относится к вирлабу. Наша лаборатория – фундамент, основа основ.

Можно ли утверждать, что ваша профессия заставляет постоянно «находиться в тонусе»: учиться, следить за новейшими тенденциями, технологиями развития отрасли?

Несомненно. Высокая интенсивность, жёсткий график, постоянная нагрузка – одновременно плюсы и минусы нашей работы. Часто слышу от друзей: «Знаешь, мы тебе по-хорошему завидуем». Вирлаб работает двадцать четыре часа, а значит, мы круглосуточно спасаем мир. Это важно, это нужно, это интересно. А самое главное, мы любим свою работу.

«Такой он умный, всегда бодрый, оживленный и деловой».

М.М. Пришвин «Этажи леса» (рассказ «Дятел»)

