*Борис Мирошников:*

# «Решающим является «человеческий фактор»

**Еще лет десять назад дюжие охранники на входе и прочные решетки на окнах могли обеспечить безопасность фирмы. Однако многим сегодняшним преступникам они не помеха — активное развитие Интернета и информационных технологий дало им новый инструментарий, методики нападений и значительно усложнило защиту организаций. День ото дня ценность информационных ресурсов организаций растет, и стоит посмотреть правде в глаза: осведомленность руководителей о высокотехнологичных новинках и стремление поставить их на службу бизнесу соседствует с непростительной невнимательностью к информационной безопасности компании. Надежная защита организации сегодня без нее немыслима — потеря информации и разрушение баз данных в одночасье может привести предприятие к банкротству. Поэтому именно о защите информации мы беседовали с руководителем главного российского ведомства по борьбе с преступлениями в сфере высоких технологий — начальником Бюро по специальным техническим мероприятиям МВД РФ Борисом Мирошниковым.**

**– Борис Николаевич, как вы охарактеризуете сегодняшнюю ситуацию с защитой российских предприятий от преступных посягательств?**

— Как это ни печально, но ведение дел многими сегодняшними бизнесменами напоминает наполнение дорогостоящими вещами дома, в котором нет замков, либо их роль выполняют шпингалеты. Многие руководители не жалеют денег, «окутывая себя дорогими проводами», и получают за счет внедрения информационных технологий повышение эффективности производства. Но защита всего этого мудреного хозяйства объективно в свою очередь тоже требует немалых вложений. Если этого не сделать, однажды наступает момент расплаты. Например, все понимают, что на серьезную систему защиты дорогой автомашины нужно потратить до 15% ее стоимости, но когда речь заходит о защите информации на предприятии, адекватное понимание встречается гораздо реже. Как сказал один умный человек, лучше раньше потратиться на безопасность, чем позже на адвоката. Потери вследствие некачественной защиты информационных ресурсов фирмы могут многократно перекрыть так называемую экономию. За решением вопросов информационной безопасности надо обращаться к добросовестным квалифицированным специалистам, но делают это сегодня, к сожалению, немногие.

**— Вследствие желания сэкономить?**

— Не только. Помимо элементарного легкомыслия и стремления сэкономить существует и проблема знаний. Пока еще немало руководителей высокого ранга представляют старшее поколение, не имеющее соответствующих знаний в области информатизации. Поэтому они зачастую становятся наиболее легкой жертвой для шарлатанов. Псевдоспециалисты с помощью эквилибристики специальными терминами «убалтывают» их выделить средства на предлагаемые именно ими «лучшие», а на деле крайне уязвимые системы защиты. Причем часто речь идет об очень больших суммах. Рост подобных случаев заставляет специалистов соседних с нами ведомств напряженно работать над проблемами сертификации, лицензирования тех, кто предлагает такие услуги.

**— Тем не менее дилетантов на рынке пока много. Какие меры вы посоветуете предпринять, чтобы не попасть на крючок неквалифицированных специалистов?**

— Сегодня существует достаточно большое количество сертифицированных изделий, специалистов и фирм, которые на высоком уровне обеспечивают такого рода работы. Подлинность сертификатов можно установить, позвонив в организации, их выдавшие. Выдают их ФСТЭК России (бывшая Гостехкомиссия при Президенте РФ) либо Центр лицензирования и сертификации ФСБ РФ. После подтверждения компетентности фирмы нужно точно сформулировать, как и что руководитель хочет защитить. Если у вас существует некий информационный ресурс, подлежащий защите, нужно спросить себя, какая доля этого ресурса подлежит особой защите? Все ли необходимо равноценно защищать? Какой ущерб получит фирма в случае утечки той или иной информации? Наиболее дорогостоящие средства нужно использовать для защиты самого критичного информационного ядра ор-

ганизации. Все остальное допустимо защитить на менее высоком техническом уровне. Далее специалисты проанализируют информационные потоки, выяснят, какие средства связи и телекоммуникаций, программные продукты применяются. И уже на этой базе предложат конкретные, прошедшие испытания системы защиты. Но вообще, любые советы теряют смысл, если конкретный бизнесмен позволяет себе слабость смешивать деловые интересы и чисто человеческие эмоции...

**— Что вы имеете в виду?**

— В нашей практике был случай, когда локальную сеть крупной организации монтировали студенты. Бригадиром у них был сын директора этой фирмы: любовь к ребенку застила ему глаза — он считал свое чадо «самородком». На поверку оказалось, что данный «специалист» имеет знания на уровне 3-го курса профильного вуза. Только беда смогла заставить бизнесмена трезво взглянуть на ситуацию. Хотя, с другой стороны, его тоже можно понять: особенность этого вида деятельности в том, что неспециалисту сложно определить, мощный «забор» ему соорудили или легкий «штакетник». Конечно, кустарную работу можно попытаться выявить, предложив специалистам по взлому проверить систему на прочность, но и в этом случае никто не может дать гарантии, что нанятые «хакеры» сами не дилетанты. Так что самодеятельность — тернистый путь.

**— Борис Николаевич, на ваш взгляд, какой подход к защите предприятия должен проповедовать его руководитель?**

— Смысл любой системы, обеспечивающей информационную безопасность, заключается в комплексности. При нынешнем развитии средств и методов, находящихся в руках преступников, невозможно обеспечить надежную защиту предприятия только техническими или только физическими методами противодействия. Они должны дополнять друг друга. Часто приходится сталкиваться с тем, что директор предприятия, уделяя пристальное внимание техническим средствам безопасности, оставляет без должного внимания организационные меры. Между тем низкоквалифицированный персонал и нелояльные сотрудники могут сделать бессмысленной даже самую надежную защиту. По общепризнанной мировой статистике, 70-80% преступлений против бизнеса вырастают из проблем с собственным персоналом. Пароли и системы шифрования находятся все-таки в руках человека. Так что решающим является «человеческий фактор».

**— Предположим, что фирма-таки не убереглась от виртуального нападения. Каким образом ее представители могут обратиться в правоохранительные органы за помощью?**

— Как и в случае физического нападения, существует стандартная процедура обращения в милицию. В последнее время ОВД стараются не допускать отказов в помощи обратившимся. То же касается и преступлений в сфере информационных технологий. Перед подачей заявления потерпевший должен подготовиться к разговору, так как ему придется отвечать на большое количество вопросов о деталях происшествия. Чем больше подробностей он изложит оперативному работнику или следователю, тем больше вероятность успеха при поиске преступников. Любая мелочь может иметь решающее значение. Преступления могут иметь разный характер. Случается, что киберпреступники, подобно обычным ворам, готовящимся к крупной краже, длительное время исследуют информационную систему, прощупывая ее с разных адресов и разными методами на предмет уязвимостей, режима и особенностей работы. Каждый отдельный эпизод может быть неприметен, но когда мы их накапливаем и анализируем, можно выявить почерк злоумышленников. Кстати, они сегодня склонны объединяться в криминальные сообщества, с делением на специализации. Последнее обстоятельство ощутимо усложняет оперативно-розыскные мероприятия. Потому-то очень многое зависит от грамотного администрирования информационной системы и локальной сети компании. Хороший системный администратор сохраняет информацию обо всех изменениях в системе в течение длительного времени, фиксируя следы внешних воздействий.

Нередко случаются и разовые нападения. В зависимости от целей они могут быть по-разному исполнены. Часто приходится сталкиваться с местью уволенных сотрудников, разрушающих информационную базу фирмы, или хищением данных, необходимых им для дальнейшей работы.

**— Как это можно предотвратить?**

— Это и есть элемент комплексного подхода, и называется он «работа с персоналом». Отбор и проверка, доверие и контроль... Ну и так далее. Если же вы видите, что сотрудник, допущенный к критическим для вас данным, внезапно увольняется, нужно оперативно «поменять замки», как вы поступаете у себя дома, когда ваш ребенок теряет ключ.

Кстати сказать, длительное хранение данных администрирования оказывается полезным и для собственных нужд. Руководителю предприятия, имеющему обширные внешние связи и большое количество сотрудников, допущенных к корпоративным сетям, может стать интересно, за что он платит, эксплуатируя свои телекоммуникационные и информационные системы. Нередко изучение данных администрирования открывает хозяину фирмы глаза на происходящее в ИТ-структуре.

**— Несомненно, ваше ведомство также имеет развитую информационную структуру. Возможно ли обращение в БСТМ МВД напрямую?**

— Конечно. Мы и получаем большое количество обращений напрямую в виде писем и заявлений. Кроме того, наш адрес в Интернете: ciber.mvd@gin.ru. Его знают и многие наши иностранные партнеры. Наши подразделения «К» находятся сегодня в каждом субъекте Российской Федерации и тесно взаимодействуют между собой. Поэтому при обращении в любой отдел или управление «К» при УВД или ГУВД к работе будут оперативно подключены компетентные специалисты любой точки страны, а при необходимости будут задействованы и наши зарубежные связи. Помимо борьбы непосредственно с компьютерными преступлениями линия «К» оказывает содействие другим подразделениям МВД в проведении расследований иных правонарушений, связанных с информационными технологиями.

**— Какие законы стоят сегодня на защите интересов организаций и граждан?**

— Сейчас нормативно-правовая база в информационной сфере продолжает эволюционировать. Мы можем гордиться, что в российском Уголовном кодексе статьи, посвященные компьютерной преступности, присутствуют с 1997 года. То есть когда законодатели представляли многие угрозы еще умозрительно, уже появилась глава 28, статьи 272, 273, 274 — гибкие инструменты в руках оперативников для борьбы со злоумышленниками. По мере накопления опыта мы вносим предложения по совершенст-

вованию текстов данных статей и комментариев к ним, предлагаем правоприменительную практику, свою методологию и стараемся выработать с нашими партнерами — следователями, юристами, судебными и прокурорскими органами — единый понятийный аппарат.

**— Насколько серьезные наказания несут киберпреступники?**

— Изучение судебной практики показало, что многие разоблаченные преступники получают небольшие условные сроки. И, оправившись от испуга, берутся за старое. Наш закон достаточно мягок. Возможно потому, что компьютерные преступления воспринимались законотворцами поначалу как мальчишеские шалости. Но сегодня мы видим, что группы преступников блокируют работу предприятий, учреждений и банков и способны выйти на так называемые критические инфраструктуры. Государству могут дорого обойтись отказы систем управления авиапредприятий, железных дорог или других жизненно важных для страны объектов. Законодательства иностранных государств в таких случаях предусматривают наказание до десяти лет лишения свободы, иногда и выше. Помните пословицу «Пока гром не грянет, мужик не перекрестится»? Боюсь, что и здесь нам нужен «гром», чтобы начать «креститься». А жаль.

**— Время от времени в прессе и из уст отдельных официальных лиц раздаются призывы «закрутить гайки» в плане свободы в Сети, поставить каждого пользователя под жесткий контроль. Эти меры, по мнению авторов ограничений, существенно снизят преступность в Интернете. Каково ваше мнение на этот счет?**

— Сегодня предостаточно как сторонников жестких ограничений, так и ратующих за полную вседозволенность в Сети. Думаю, что ни то ни другое неприемлемо. Идти путем запретов неверно. Мы же не запрещаем пользоваться автомобилями, ссылаясь на прямо-таки страшную статистику ДТП. Мы идем путем ужесточения правил и контроля. Это нормально. То же касается и такого достижения человеческого разума, как Интернет. То, что Интернет и информационные технологии в целом активно используются преступным миром, террористами, говорит лишь об острой необходимости введения единых, выгодных для общества норм. Возможно, и достаточно строгих. А еще — о необходимости предоставления обществом правоохранительным органам соответствующих полномочий для его защиты от киберкриминала. Мешкать с этим нельзя, иначе преступники будут убеждаться в собственной безнаказанности.

Наши коллеги за рубежом говорят о самой высокой латентности в сфере компьютерных преступлений. Банковские структуры и фирмы по понятным причинам не хотят распространяться о том, что их информационные системы оказались уязвимыми. То же наблюдается и у нас. Аргументация хозяев пострадавших организаций заслуживает понимания и сочувствия. Чтобы таких случаев было как можно меньше, мы неустанно стараемся своими расследованиями и результатами, профилактическими мероприятиями завоевать доверие у общества. Результативность нашей работы во многом зависит от взаимной уверенности и помощи.

**— То есть вы готовы дать гарантию сохранения конфиденциальности сведений, предоставленных любой обратившейся по линии «К» организации?**

— Я еще не помню ни одного случая, чтобы обратившийся к нам клиент или потерпевший упрекнул бы нас в том, что он пострадал от утечки информации по нашей вине. У нас существует жесткий внутренний режим. Мы много работаем над повышением квалификации собственных кадров.

**— Сеть не имеет государственных границ. Способны ли подразделения «К» расследовать так называемые трансграничные преступления?**

— Бюро развивает взаимовыгодное сотрудничество с множеством аналогичных иностранных организаций, что повышает раскрываемость атак, совершенных из-за рубежа. В рамках этого сотрудничества для синхронности и оперативности реакции на преступные действия во всем мире, в том числе и у нас в стране, развернуто большое количество национальных контактных пунктов. Они в круглосуточном режиме обеспечивают обмен оперативной информацией. Мы участвуем в работе специальной группы по киберпреступности стран «Восьмерки», к нашему опыту проявляют интерес на многих международных конференциях, посвященных информационной безопасности. Уверен, что все эти меры позволят укрепить доверие бизнеса и общества к правоохранительным органам, значительно повысить эффективность нашей работы.

## DVD-рекордеры теряют связь с ПК

Мировой рынок DVD-рекордеров растет за счет сегмента записывающих DVD-проигрывателей, которые не являются компьютерными компонентами. За 2004 год этот сегмент увеличился вдвое, а в 2005 году, согласно прогнозам исследователей In-Stat, его рост прогнозируется на уровне 87%.

«Вопреки нашим ожиданиям, рост продаж записывающих DVD-проигрывателей наблюдается во всех регионах, за исключением Японии, — сообщил Мишель Абрахам (Michell Abraham), аналитик In-Stat. — В Японии объемы продаж DVD-проигрывателей снизились, в то время как в других регионах возросли более чем вдвое».

Кроме того, специалисты In-Stat сделали вывод, что объем продаж записывающих DVD-проигрывателей вырастет с 9,4 млн. шт. в 2004 году до 67,7 млн. шт. в 2009 году. Подключение цифровых TV-тюнеров к DVD-плеерам позволит увеличить объем продаж в странах Северной Америки, Европы и в Японии. Согласно требованиям Федеральной комиссии по связи (FCC)с 1 июля 2007 года в США планируется включать в состав каждого продаваемого DVD-записывающего устройства DTV-тюнер.

На сегодняшний день уже три производителя поставляют в Японию проигрыватели следующего поколения на основе технологии Blu-Ray. При этом первые HD-DVD-проигрыватели будут доступны широкому пользователю только во второй половине 2005 года. К тому времени будет выпущено порядка 90 наименований кинофильмов в этом формате. Аналитики In-Stat считают, что объем продаж плееров и записывающих устройств, использующих технологию голубого лазера, достигнет к 2008 году 4 млн. шт., и это без учета игровых приставок.

По данным Reuters, ожидается, что мировые поставки DVD-рекордеров (в том числе и компьютерных) к 2008 году достигнут 47,8 млн. устройств, что на 12,3% превысит уровень 2004 года. Тайваньские производители, такие как Lite-On IT, Mustek и более мелкие компании (Sampo, Protop Innotech и Ya Hsin Industrial), как ожидается, выпустят в этом году 3 млн. DVD-рекордеров, в то время как в 2003 году этот показатель составлял лишь 742 тыс. устройств.