



Трафик не ограничен
Perl + PHP + SSI
MySQL + Shell + EMail
Хостинг: 4 у.е.



#09/2003
Купить
Подписка

Увеличить

НЕ потеряйте голову

Симон Каплан
16.09.2003
Директор ИС, #09/2003

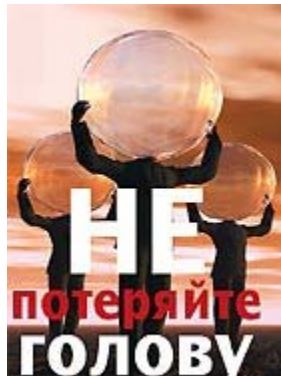
Версия для печати
Выскажите свое мнение

Новости по e-mail

- Новости ИТ
- Свежий номер

Введите Ваш e-mail

[Полная настройка подписки »](#)



Не всегда бывает просто определить, что относится к интеллектуальной собственности. Еще труднее защитить. Что во взаимодействии с другими сотрудниками может сделать руководитель службы безопасности для того, чтобы защитить будущее своей компании?

Вы полагаете, что обеспечить безопасность здания или компьютерной сети сложно, но попробуйте-ка защитить идею. Идеи нельзя увидеть; они имеют привычку возникать во время обсуждений — и не всегда с теми, кому следует их слышать. Они могут быть потеряны или украдены, и ни одна душа не будет знать об этом — до тех пор, пока конкурент не разобьет вас в пух и прах, используя изобретение, которое вы считали только своим.

И все же идеи значительно ценнее, чем многие из тех материальных активов, защиту которых должен обеспечивать директор службы безопасности. В роли интеллектуальной собственности может выступить что угодно — конкретный технологический процесс, планы запуска продукции, химическая формула или названия стран, в которых зарегистрированы ваши патенты. Этот вид корпоративной информации может означать ни много ни мало — конкурентоспособное будущее вашей организации.

Сегодня все чаще и чаще в должностные обязанности

руководителя службы безопасности включается пункт о защите подобных активов. Тем не менее иногда интеллектуальная собственность стоит в списке приоритетов ниже других — не потому, что она не важна, а просто потому, что с ней сложнее иметь дело. К тому же интеллектуальная собственность различается в зависимости от профиля компании и отрасли. Например, директор службы безопасности, работающий в индустрии развлечений, вряд ли отнесется к потере интеллектуальной собственности и ее краже так же, как его коллега из химической компании.

Понятно, что утрату интеллектуальной собственности и то, как это произойдет, можно с какой-то вероятностью спрогнозировать. Это дает некое преимущество. Но защита интеллектуальной собственности требует терпения и упорства. Как и многое в жизни, это не просто.

Разберитесь, что именно нуждается в защите

«Если компания теряет свои активы, она может погибнуть», — утверждает Джеймс Чендлер, президент Национального института законодательства по интеллектуальной собственности США. К интеллектуальной собственности относятся ключевые активы, благодаря которым компания получает возможность создавать свою продукцию или услуги. Если эти активы утеряны или украдены, компания может потерять устойчивую позицию на рынке. По словам Ричарда Айзекса, старшего вице-президента The Librinco Group, компании, специализирующейся на проблемах управления рисками, кражи интеллектуальной собственности стоят только американским компаниям около 300 млрд. долл. ежегодно.

Для руководителя службы безопасности лучший способ защитить частную информацию — понять самому и объяснить сотрудникам, что для организации представляет ценность. Если понять, что именно нуждается в защите, то легче разобраться в том, как и от кого это защищать. Для достижения такого результата необходим постоянный контакт с высшим руководством, которое в ответе за интеллектуальный капитал компании.

«Устраивайте встречи с генеральным директором, руководящими сотрудниками отдела кадров, продаж, маркетингового, юридического, производственного и научно-исследовательского отделов минимум раз в квартал, если не получается чаще, — советует Джон Понтрелли, директор по безопасности компании W.L. Gore & Associates. — Вы должны стать дружной

командой, чтобы обеспечить надежную защиту своей интеллектуальной собственности». Он подчеркивает, что подобное общение — непременно постоянный процесс, а не разовое мероприятие.

Разобравшись в производственной, исследовательской и интеллектуальной базе организации и определив модель взаимодействия с другими подразделениями, вы тем самым сформируете основу, на которой можно начинать выстраивать план защиты интеллектуальной собственности. Специалисты, занимающиеся защитой интеллектуальной собственности долгие годы, рекомендуют провести на этом этапе анализ рисков и уязвимостей, а также анализ затрат и выгод. Создайте карту активов вашей компании, пометив наиболее ценные из них. Определите, в случае утери какой информации компании будет причинен наибольший ущерб. Затем решайте, какие из этих активов подвергаются наибольшему риску быть украденными.

Внутренние угрозы

Может показаться, что вашей интеллектуальной собственности угрожают в основном внешние опасности, но обычно дело не в них. Независимо от того, в какой отрасли вы работаете, причины утери или кражи интеллектуальной собственности типичны: незащищенные ИТ-системы, ненадежные сотрудники и социотехника (введение пользователей или системных администраторов в заблуждение с целью узнать пароль, необходимый для проникновения в защищенную систему).

Беспечность, незнание или явный злой умысел тому виной, но именно ваши сотрудники являются тем каналом, по которому чаще всего утекает секретная информация. Служащие легко забывают о том, какую роль они играют для организации в целом, и не всегда помнят о том, что, обсуждая какой-то проект на вечернем коктейле, они могут подвергнуть свою компанию риску. Бизнес-ланчи и в особенности авиаперелеты — это «черные дыры» для интеллектуальной собственности. Пока ваши сотрудники беседуют с одним человеком, другой может подслушать их разговор или подсмотреть, что у них на мониторе ноутбука.

Многие сотрудники тратят массу времени, прилагают немалые усилия на определение важности их работы по отношению ко всему проекту, утверждает Линн Мэттис, директор по корпоративной безопасности компании Boston Scientific.

«Они считают, что, раз их работа — лишь крошечная часть огромной головоломки, то большой беды не будет,

если они и обсудят ее за ужином. Вы должны заставить их понять, как персональная утечка информации может повлиять на общее дело».

Иногда ваши сотрудники выдают крайне ценную информацию по личным причинам, не подозревая об этом. Например, вашей индустрии требуются люди с учеными степенями, которые, для того чтобы постоянно подтверждать свою квалификацию, должны публиковать исследования по своей теме. Часто это выливается в проблему для работодателей, которые не хотят, чтобы принадлежащая им интеллектуальная собственность становилась общеизвестной.

«Мы хотим, чтобы они публиковались, — говорит Понтрелли, — но нельзя позволить им говорить о том, над чем они работают в данный момент, потому что это представляет слишком большой интерес для конкурентов».

Опасное любопытство извне

Поставщики всегда проявляют любопытство по поводу того, над чем в данный момент работает компания, а ее сотрудники иногда слишком общительны и готовы поделиться такой информацией. Кроме того, вы можете привлекать работников со стороны, однако, как правило, их ничто не обязывает хранить полученную информацию в тайне, особенно если они ведут дела с вашими конкурентами.

«Всегда найдутся люди за пределами компании, которые будут выискивать ваши слабые места, чтобы получить выгоду», — утверждает Джефф Услан, директор по защите информации в Sony Pictures Entertainment. Даже при наличии хорошего программного инструментария и постоянных проверок любой из методов, с помощью которых ваша компания хранит или передает информацию, потенциально уязвим для проникновения.

Еще один способ проникновения в тайны компании — с помощью социотехники. Это может выглядеть, например, как звонки от людей, представляющихся студентами, пишущими дипломную работу, или бывшими сотрудниками компании, пытающимися разыскать своего любимого начальника. ИТ-руководители называют данный вид атаки «звонком под вымышленным предлогом», и, даже когда сотрудники компании знают, что происходит, они зачастую думают, что могут сами справиться с этой ситуацией. По мнению Мэттиса, они не понимают, что имеют дело с обученными профессионалами, которые способны по крошечным обрывкам сведений восстановить общую картину того, чем занимается компания.

Обычно люди, которые стоят за хакерскими атаками, проникновением в систему обманным путем или через сотрудников компании, являются вашими конкурентами или кем-то, кто работает на них. Корпоративный шпионаж и «прощупывание почвы» — это нелегальные атрибуты мира бизнеса, и все знают об их существовании, но никто не любит о них говорить. Между тем они представляют собой реальную угрозу безопасности интеллектуальной собственности вашей компании. Конечно, есть и такие люди, которые выдадут ваши секреты специально. Недовольные сотрудники увольняются из компании и, несмотря на то что они подписывали в свое время соглашения о неразглашении, вносят свой вклад в конкурентную борьбу с вами или создают собственные компании, используя ваши коммерческие секреты. Важно понимать, какие факторы способствуют тому, что ваша закрытая информация разглашается, и как можно это предотвратить в будущем.

Уроки из практики

Для W.L. Gore защита интеллектуальной собственности — дело крайне важное; основные усилия в этом плане направлены на соответствующую подготовку сотрудников. Компания производит химические полимеры, которые используются для создания спецодежды по революционной технологии. Эту одежду для активного отдыха, с защитой от ветра и воды, известную под маркой Gore-Tex, очень ценят туристы.

Из-за того что в основе бизнеса W.L. Gore лежит такой интеллектуальный капитал, Понтрелли создал для сотрудников всех 45 филиалов компании специальные обучающие презентации по вопросам интеллектуальной собственности. У W.L. Gore множество конкурентов, и все они были бы счастливы заполучить закрытую корпоративную информацию. Понтрелли напоминает своим сотрудникам, что защита интеллектуальной собственности — дело каждого. Каждый несет ответственность за свои действия.

При приеме на работу все подписывают соглашение о неразглашении, и Понтрелли акцентирует особое внимание на том, что это обязательство необходимо выполнять.

«Все мы полагаемся друг на друга в том, что касается защиты наших коммерческих секретов, — говорит он. — Сохранение их в неприкосновенности дает нам возможность в конце года выдавать премии. Так что, если что-то произойдет, это затронет интересы каждого сотрудника».

Понтрелли также напоминает о правильном

использовании технологий, способном свести к минимуму возможности кражи данных, например о безопасном использовании электронной почты и сохранении данных в упорядоченном виде, чтобы посторонние не могли до них добраться.

Для инженеров, технологов и научных сотрудников компании W.L. Gore юридический отдел составил специальную презентацию. Она учит их общаться с производителями, поставщиками и журналистами так, чтобы случайно не выдать важной информации.

«Наши служащие — замечательные люди, но при телефонном разговоре с посторонними они не всегда думают о том, что следует и чего не следует говорить, — заявляет Понтрелли. — Непреднамеренная выдача конфиденциальной информации — та проблема, на борьбу с которой направлены наши обучающие программы по защите интеллектуальной собственности. Для всех нас своеобразной лакмусовой бумажкой является вопрос: 'Обладал бы я данной информацией, если бы не работал здесь, и хотел бы мой самый серьезный конкурент заполучить эту информацию?'

В 2000 году компания W.L. Gore создала комитет по интеллектуальной собственности, который осуществляет наблюдение за контактами с посторонними организациями и является важным инструментом защиты корпоративных активов. Если кто-то в компании захочет опубликовать свой комментарий в журнале, подать заявку на регистрацию патента или начать работу с новым поставщиком, ему придется пройти через этот комитет.

«Единая позиция — вот что предотвращает утечку секретных сведений», — говорит Понтрелли. В компании четыре крупных подразделения, и до создания комитета по правам интеллектуальной собственности часто бывало так, что они принимали собственные решения о том, какую информацию можно оглашать, а какую нет. «Не было общего подхода, и часто интересы конкретного подразделения диктовали, какие сведения разглашать, даже без серьезного обсуждения этого вопроса, — добавляет Понтрелли. — В основе проблемы защиты интеллектуальной собственности — люди. Нам пришлось найти способ повлиять на отношение наших сотрудников к этой проблеме, на их поведение, заставить их осознать необходимость защиты нашего интеллектуального капитала и указать пути к этому».

В качестве дополнительной меры защиты в W.L. Gore создали специальный информационный центр, куда служащие могут переправлять все поступающие к ним запросы о компании. Персонал центра умело отвечает на вопросы, обходя щекотливые моменты, так чтобы не выдать конфиденциальных сведений.

По мнению Понтрелли, лучший способ удержать интеллектуальную собственность внутри компании — бережное и уважительное отношение к сотрудникам.

«Защита интеллектуальной собственности строится не столько на использовании специальных технологий или каких-то расследованиях и преследованиях, а в гораздо большей степени на правильном отношении к своим сотрудникам, — утверждает он. — Если вы сделаете так, что они не захотят причинить вам вред, то сведете к минимуму риск утраты конфиденциальной информации. Мы можем возвести самые мощные защитные барьеры в мире, иметь самые лучшие технологии и самую жесткую систему отбора персонала, но все это не является преградой, когда человек, покидая компанию, уносит ценную информацию просто-напросто в своей голове».

Не только люди

Услан предлагает свой рецепт: проверка, проверка и еще раз проверка. Успех его работы зависит от поддержания высокого уровня информационной безопасности, — это особенно важно для таких отраслей, где большие объемы закрытых сведений хранятся и передаются в электронном виде. Поэтому неудивительно, что Услан держит корпоративные ИТ-системы Sony Pictures под неусыпным надзором. Его отдел, который является частью общекорпоративной службы информационных технологий Sony, обеспечивает безопасность всей интеллектуальной собственности корпорации в цифровом виде.

«Если информация в компьютере, то защитить ее — моя работа», — говорит Услан. Поэтому он тщательно проверяет ИТ-системы Sony по всему миру, тестируя все используемые методы хранения и передачи данных, чтобы убедиться в том, что уровень их безопасности отвечает высоким корпоративным стандартам. Он и команда его сотрудников также регулярно предпринимают попытки проникновения, эта практика обычно вскрывает слабые места в системе защиты, которые в противном случае не будут обнаружены, пока кто-нибудь извне не воспользуется ими.

Проверки, которые устраивает Услан, напоминают засаду. Он и его команда приводят с собой группу экспертов по ИТ-безопасности, специализирующихся на той операционной системе или программном обеспечении, проверка которых производится в данный момент. (Услан подчеркивает, что системные администраторы компании весьма компетентны, но их задача — поддерживать системы Sony в рабочем состоянии, а не анализировать проблемы безопасности, — поэтому и нужны специалисты иной квалификации.) Группа экспертов начинает проверку на макроуровне,

анализируя корпоративные серверы и операционные системы, выискивая слабые места, исправляя ошибки. Затем эксперты просматривают каждую программу и каждый сетевой порт. После этого Услан проводит встречу с системными администраторами, чтобы сообщить им о проблемах и уязвимых местах, найденных благодаря проверке.

Как только заканчивается одна проверка, эксперты уже готовы начать весь процесс заново в другом месте.

«Кража интеллектуальной собственности означает прибыль, которую мы не сможем поделить между сценаристами, теми, кто занимается реквизитом, художниками по костюмам и всеми другими людьми, которые трудятся над созданием фильмов, — объясняет Услан. — Когда кто-то бесплатно скачивает фильм через Internet, например, вместо того чтобы пойти в кинотеатр, это пощечина им всем». А еще он не раз был свидетелем того, что происходит, когда люди перестают беспокоиться о безопасности своей интеллектуальной собственности. «Именно когда вы думаете, что все тылы у вас надежно прикрыты, и случается что-нибудь очень неприятное. Нужно всегда быть настороже».

Конечно, директору службы безопасности проще поставить защиту идей в списке первоочередных задач на много пунктов ниже, чем защиту зданий и сотрудников. Как говорит Услан, службы безопасности чувствуют себя увереннее и спокойнее, когда защищают то, что умеют защищать.

«Так или иначе, интеллектуальная собственность — это то, что делает вашу компанию жизнеспособной, — утверждает Чендлер. — И директора служб безопасности должны сделать защиту интеллектуального капитала одним из основных своих приоритетов».

Ведь от этого зависит всего лишь... будущее вашей компании.

Simone Kaplan. Don't Lose your Head. CSO, April 2003.

Определение интеллектуальной собственности

Для того чтобы лучше защитить интеллектуальную собственность своей компании, вы должны понять, что представляет ценность. Для этого необходимо уметь определять интеллектуальную собственность.

По словам Скотта Нельсона, бывшего вице-президента по безопасности компании AOL Time Warner, большинство руководителей служб информационной

безопасности не смогут как следует дать определение интеллектуальной собственности.

Всемирная организация по правам интеллектуальной собственности (World Intellectual Property Organization) дает определение интеллектуальной собственности как результата творческой деятельности человека. Это изобретения, литературные и художественные произведения, символы, названия, изображения и дизайн, используемые в коммерческих целях. Если рассматривать понятие интеллектуальной собственности более детально, то оно включает в себя (но не ограничивается ими) частные (запатентованные) формулы и идеи, изобретения (конкретные продукты и технологические процессы), промышленный дизайн и географические указания на первоисточник, а также литературные и художественные произведения, подобные романам, фильмам, музыке, архитектурному дизайну и Web-страницам.

Выражаясь юридическим языком, интеллектуальную собственность обычно делят на четыре категории: патенты, авторские права, товарные знаки и коммерческие тайны (см. врезку «У меня есть тайна»). Интеллектуальная собственность, относящаяся к одной из этих категорий и зарегистрированная специальным уполномоченным ведомством, находится под защитой закона, и в случае того или иного злоупотребления соответствующими правами собственности нарушители преследуются в судебном порядке.

В роли интеллектуальной собственности может выступать и нечто менее конкретное и материальное, например идея.

Защита «снаружи» и «изнутри»

Помимо средств охраны объектов интеллектуальной собственности, предусмотренных законом РФ «Об авторском праве и смежных правах», предприятия могут руководствоваться положениями статьи 139 Гражданского кодекса Российской Федерации.

ГК дает четкое определение того, какая информация может быть отнесена к коммерческой тайне. В частности: «Информация составляет служебную или коммерческую тайну в случае, когда она имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании, и обладатель информации принимает меры к охране ее конфиденциальности».

Кроме того, в отношении каждого объекта интеллектуальной собственности могут быть применены положения закона РФ «Об информации, информатизации и защите информации». Так, закон устанавливает, что собственник информационных ресурсов вправе:

- назначать лицо, осуществляющее хозяйственное ведение информационными ресурсами или оперативное управление ими;
- устанавливать в пределах своей компетенции режим и правила обработки, защиты информационных ресурсов и доступа к ним;
- определять условия распоряжения документами при их копировании и распространении.

Ряд мер поможет предприятию до некоторой степени обезопасить себя от утечки информации, составляющей коммерческую тайну. В частности, можно рекомендовать заключение договоров о материальной ответственности, а в правила внутреннего распорядка включить положения об ответственности за разглашение информации, отнесенной к коммерческой тайне.

Если информация размещается во внутренней сети предприятия, то при оформлении с сотрудником документов о приеме на работу следует специально ознакомить его с тем, что составляет коммерческую тайну, а в трудовом договоре установить ответственность и санкции за разглашение таких сведений. Также можно рекомендовать принять специальное положение о доступе к информации, которое должно быть подписано сотрудниками, в силу своих должностных обязанностей имеющими к ней доступ.

Существуют и иные методы защиты объектов интеллектуальной собственности. Прежде всего необходимо четко регистрировать во внутренней документации предприятия момент создания объекта интеллектуальной собственности. В случае когда это целесообразно, следует подать соответствующую заявку в Российское агентство по патентам и товарным знакам, зарегистрировать объект в качестве товарного знака или получить соответствующий патент. Наконец, информация, находящаяся во внутренней сети предприятия, должна быть надлежащим образом защищена от внешнего доступа.

Если же информация была получена и использована недобросовестными сотрудниками или третьими лицами, закон предоставляет правообладателю обширный набор инструментов по восстановлению своих прав и получению компенсации за причиненный вред.

Лица, незаконным образом получившие информацию, обязаны возместить убытки, причиненные

правообладателю; при этом такая обязанность возлагается не только на третьих лиц, но и на сотрудников, разгласивших коммерческую тайну в нарушение положений трудового договора. В соответствии с положениями ГК убытки должны быть возмещены в полном объеме, однако обязанность обосновать размер убытков возлагается на правообладателя, что затрудняет применение подобных средств защиты. Однако, если нарушитель использовал полученные им недобросовестно объекты с целью извлечения прибыли (говоря попросту, продал их), то становится возможным требовать компенсации в объеме не меньшем, чем выгода, полученная нарушителем.

Наряду с использованием средств защиты, предусмотренных ГК, также возможно применить против нарушителя санкции, предусмотренные трудовым договором, например потребовать уплаты неустойки или штрафа.

Итак, если охрана объектов интеллектуальной собственности предприятия «снаружи» возможна средствами, предоставляемыми законами «Об авторском праве», «О товарных знаках» и «Патентным законом», то охрана «изнутри» возможна с применением мер, предоставляемых ГК в отношении коммерческой тайны и служебной информации.

- Андрей Миронов, юрист, «Студия Артемия Лебедева»,
mironov@design.ru

У меня есть тайна

Четыре типа защиты интеллектуальной собственности

ПАТЕНТ. Когда вы официально регистрируете свое изобретение, — а это процесс, который может занять больше года, — вы получаете законное право на эксклюзивное производство или сбыт соответствующей продукции. Патенты выдаются на материальные предметы. Их можно регистрировать за границей — это часто используемая практика, которая помогает справиться с излишне любопытными конкурентами, мечтающими выяснить, чем занимается ваша компания. Если вы являетесь владельцем патента, другие компании могут подавать заявки на лицензионное производство вашего продукта. Патенты действительны в течение 20 лет. Их можно возобновлять, но если срок действия патента кончился, а компания его вовремя не возобновила, она теряет эксклюзивное право на это изобретение.

ТОВАРНЫЙ ЗНАК. Товарный знак — это название,

фраза, звук или символ, используемый по отношению к конкретным услугам или продуктам. Товарный знак часто связывает бренд с уровнем качества, на котором компании строят свою репутацию. Срок защиты товарного знака после регистрации составляет 10 лет и может быть продлен, как и в случае с патентом. Но товарный знак не обязательно регистрировать. Если компания создает символ или название, на которое она хочет иметь эксклюзивное право, то она может просто добавить символ ТМ (Trademark) к названию. Это дает возможность преследовать другие компании в судебном порядке, если они попытаются использовать тот же символ для своих целей.

АВТОРСКОЕ ПРАВО. Законы об авторском праве защищают письменные или художественные произведения, зафиксированные на материальном носителе, — романы, стихи, песни или фильмы. Авторское право защищает воплощение идеи, но не саму идею. Владелец работы, защищенной авторским правом, имеет право воспроизводить ее, создавать на ее основе производные работы (например, создать фильм на основе книги), равно как продавать, исполнять или демонстрировать ее на публике. Для получения авторского права не нужно регистрировать ваш материал, но регистрация необходима, если вы хотите подать иск о нарушении авторского права. Авторское право действительно в течение всей жизни автора и в течение 50 лет после его смерти.

КОММЕРЧЕСКАЯ ТАЙНА. Коммерческая тайна — это формула, модель, устройство или набор данных, обеспечивающих их владельцу преимущество перед конкурентами. Обращаясь за защитой коммерческого секрета, необходимо доказать, что он приносит компании дополнительную прибыль и что внутри компании приняты соответствующие меры для охраны этого секрета, например, о нем знает только руководство компании. Скажем, Coca-Cola успешно хранит формулу своего напитка в тайне уже более 117 лет.

• [Версия для печати](#)

Интернет-университет информационных технологий представляет серию книг "Основы информационных технологий"

Программирование на Java

Вязовик Н.А.

Курс лекций посвящен современному и мощному языку программирования Java. В его рамках дается вводное изложение принципов ООП, необходимое для разработки на Java, основы языка, библиотеки для

работы с файлами, сетью, для построения оконного интерфейса пользователя (GUI) и др. Рекомендовано УМО в области прикладной информатики для студентов высших учебных заведений, обучающихся по специальности 351400 "Прикладная информатика".

Выскажите Ваше мнение:

Ваш e-mail:

Ваше имя:

показывать e-mail рядом с Вашими мнениями

Отправить

К сожалению, ни одного мнения по этой теме еще нет...

Предложения магазинов

BOLERO.RU: [Оптимизация производительности UNIX](#)

PCBOX.RU: [Жидкокристаллический дисплей на тонкопленочных транзисторах, 15" Sony N50PS](#)

TELESCOPE.RU: [70-мм телескоп-рефрактор на экваториальной монтировке с двигателем Konusmotor-70](#)



Copyright © 1992-2004 Издательство "[Открытые системы](#)"

