Охрана предприятия

№1 (71), 2020

Оглавление

С какими рекрутинговыми фирмами лучше иметь дело?

Книжное обозрение

Critical Infrastructure: Homeland Security and Emergency Preparedness

Кибербезопасность в 2020 году: главные тенденции

Онлайновый журнал Chief Security Magazine опубликовал 12 декабря обзорно-аналитическую статью о главных киберрисках в 2020 году и способах их минимизации. Автор публикации, старший редактор журнала Майкл Надо, использовал исследования и отчеты ведущих мировых организаций в этой сфере: Лаборатории Касперского, Sophos Labs, Verison, IDG, ряда других.

Вирусные инфекции

Согласно данным Лаборатории Касперского, практически половина всех организаций сталкивалась в 2019 году с проблемой занесения вируса на офисные компьютеры и принадлежащие сотрудникам гаджеты.

В 2020 году ожидается, что компании, стремясь к экономии средств, развитию форм дистанционной работы, а также идя навстречу пожеланиям своих работников, будут в больших, чем прежде, масштабах, разрешать использование персональных гаджетов. В результате хакеры получат дополнительные возможности преодоления средств корпоративной киберзащиты, тем более, что индивидуальные агрегаты по защищенности, как правило, уступают корпоративным средствам информзащиты.

Следовательно, считает эксперт Лаборатории Касперского Дмитрий Галов, число зараженных вредоносами гаджетов будет неуклонно увеличиваться. Наилучшие способы минимизации рисков, по его мнению, это «жесткие, строгие инструкции по безопасности, обеспечение сотрудников адекватными решениями киберзащиты при соблюдении права личности». Наряду с техническими мерами важнейшее значение имеют регулярные тренировки персонала компании, помогающие внедрять стандарты кибергигиены.

Фишинг

Согласно статистике экспертов, почти треть всех хакерских вторжений приходится на фишинг. Там, где дело касается промышленного шпионажа, фишинг достигает уровня 80% атак. Плохая новость в том, что фишеры год от года совершенствуют методологию и инструменты обмана. Образовался своеобразный рынок, где фишеры продают свои наработки. Цена начинается с 99 долларов.

По данным IDG Security Priorities Study, 44% опрошенных в разных странах компаний заявили, что рассматривают тренинги, специализированные программы ознакомления с методами фишеров в числе главных приоритетов 2020 году. Хакеры, в свою очередь, несомненно, ответят повышением качества фишинговых атак путем более тщательного сокрытия признаков обмана. Все чаще ими используется форма деловых электронных писем, отправляемых либо с ложных, либо реальных, но скомпрометированных сайтов и адресов.

Лучший совет: регулярно обновляйте программу тренингов с учетом изменений, происходящих в этой сфере мошенничества, включайте в инструкции требования безопасности, к примеру, обязательную перепроверку электронных финансовых поручений по телефону или лично.

Вымогательские атаки

Такие атаки встречаются реже, но они в числе наиболее «дорогостоящих» по своим последствиям. В 2019 году примерно 40% средних и малых предприятий были их объектом, полагают эксперты Лаборатории Касперского. Потери от инцидента могут исчисляться миллионами долларов.

Хотя инструменты защиты от вымогательских атак год от года совершенствуются, приемы и способы хакерства тоже не стоят на месте. Как считают специалисты Sophos Labs, в 2020 году уровень этого типа хакерских атак будет возрастать благодаря появлению новых способов обходить средства защиты. Чаще будут использоваться: а) рассылка от имени достоверного источника; б) для переговоров - автоматизированные инструменты, скрывающие организаторов и исполнителей преступления; в) технологии скрытого шифрования данных после вторжения в корпоративную сеть.

Что рекомендуют эксперты? Надежной защитой против хакеров-вымогателей является наличие современной, проверенной системы backup of critical data (резервное копирование на запасные носители). Держите резервные носители отдельно от общей корпоративной сети, чтобы хакеры не могли их зашифровать. Тренинги коллектива – критически необходимы. Также жизненно важно иметь в своем распоряжении современные системы контроля, мониторинга и реагирования, покрывающие все важные участки и объекты корпоративной сети, своевременно обновлять соответствующие программы.

Риски, связанные с поставщиками и партнерами

Инциденты с участием третьей стороны в 2019 году составили 43% всех инцидентов кибербезопасности среди крупных предприятий, 38% - в среднем и малом бизнесе. Подавляющее большинство организаций (94%) предоставляют партнерам доступ в свою сеть, причем 72% - привилегированный доступ. При этом только 22% компаний уверены, что партнеры не прибегают к попыткам неавторизованного доступа к их данным.

С другой стороны, три четверти организаций, вступая в деловые отношения с третьей стороной, заставляют их подписывать соглашение о мерах защиты информации, что дает им право требовать компенсации в случае ущерба по вине партнера.

В 2020 году продолжится тенденция расширения цифровых деловых отношений с поставщиками и партнерами, что повышает риски кибербезопасности. К тому же атаки

становятся все более изобретательными. Появляются новые группы хакеров, специализирующиеся на цепочках поставок. Компрометация одного звена грозит компрометацией всего бизнес процесса.

Рекомендации: необходимо хорошо знать своих партнеров, имеющих доступ в вашу компьютерную сеть, иметь в наличии документы, обязывающие третью сторону соблюдать строжайшие правила безопасности и предусматривающие ее конкретную ответственность за возможные инциденты.

6 вопросов, которые соискатель на должность руководителя СБ должен задать во время собеседований

Онлайновое издание Chief Security Magazine, September 18, 2019, публикует рекомендации для кандидатов на должность руководителя или старшего офицера корпоративной службы безопасности. Автор статьи, Дж. Поруб, формулирует шесть вопросов, которые соискатель просто обязан прояснить, прежде чем дать согласие на новую работу.

1. Сколько времени глава компании уделяет вопросам охраны и безопасности?

Культура безопасности начинается сверху. Если владелец/президент/генеральный директор компании не понимает значения функции безопасности для бизнеса, то вам предстоит борьба без шансов на успех. Что работодатель знает о безопасности? Отчасти информацию можно получить, изучая корпоративный сайт организации, личность руководителя в LinkedIn, но именно во время встречи с руководителями компании вы должны понять, является ли ваша предполагаемая работа для них высоким приоритетом. Если вы во время ознакомительных встреч увидите, что топ-менеджмент готов вникать в вопросы безопасности, обучаться им, что эти вопросы в повестке заседаний правления, тогда предлагаемая работа руководителем СБ, наверное, вам подходит.

2. Как организация справляется с инцидентами безопасности?

Автор публикации советует избегать организаций, где людей увольняют только за то, что они проглотили фишинговую наживку. Задайте вопрос: «Допустим, сотрудник попался на удочку мошенников (например, фишинговое письмо по электронной почте), в результате компании нанесен финансовый ущерб. Как организация реагирует?».

Избегайте таких формулировок, где ответ может быть «да» или «нет». Собеседник, не исключено, может пытаться ввести вас в заблуждение, не говорить всю правду. Чем больше ложь, тем легче ее обнаружить. Конечно, не следует рассчитывать, что в ходе предварительного собеседования вам раскроют конфиденциальную информацию (сам этот факт уже должен вас насторожить). Но в самых общих выражениях они должны вам объяснить, как организация отвечает на инциденты.

3. Как появилась вакансия?

Если на этой должности у вас был предшественник, в тактичной форме спросите, почему он ушел, как он работал, что делал хорошо, а что не получалось, что ждет организация от нового человека на этой позиции. Уместен вопрос о текучке кадров в службе безопасности. Ответ на вопросы, как долго в среднем удерживаются на работе охранники и офицеры, давно ли уже открыта ваша вакансия, может сказать вам многое об организации.

4. Какова бизнес культура компании?

Если бизнес осуществляется по формуле «быстро и напролом», насторожитесь. Такой подход чреват пренебрежением элементарных норм предосторожности, игнорированием базовых инструкций по безопасности. В такой организации функция безопасности обычно не в числе главных приоритетов.

5. Считает ли организация вопросы безопасности «пустяшным делом»?

Задайте вопрос о программах ознакомления персонала с рисками и угрозами безопасности. Вам необходимо увериться, что такие программы, тренинги не «фиговый листок» для регуляторов, когда раз в год или полгода собирают сотрудников, чтобы показать им слайды, которые уже на следующий день никто не помнит. Поинтересуйтесь психологическим климатом в СБ. Спросите собеседника, на что больше всего там жалуются. И если услышите в ответ: «Ах, эти болваны.....», то, может быть, и не надо стремиться туда на работу?

6. Каков бюджет СБ?

Вы должны быть уверены, что выделяемые на охрану и безопасность средства обеспечат фундамент для успешной, результативной работы.

Карьера специалиста по кибербезопасности в 2025 году

Директор по информационной безопасности компании Polaris Alpha Эрик Шлезингер в своей работе опирается на принцип «люди и процессы», отдавая ему предпочтение перед технологиями. Но через пять лет все изменится, считает он. Машинное обучение и искусственный интеллект станут главным фактором безопасности. «Искусственный аналитик» заменит одного или нескольких специалистов, и будет принимать решения, опираясь исключительно на данные сети (Chief Security Officer, September, 23, 2019).

А что же будут делать те, кого машины вытеснят? Эксперт полагает, что для них найдется работа на более сложном, чем сейчас, уровне: облачные платформы, интернет вещей, борьба с эпидемией вымогательского фишинга… Многие должны будут пройти дополнительные курсы переобучения, повышения квалификации.

Искусственный интеллект лишь один из многих факторов, которые видоизменят карьеры киберспециалистов через пять лет. Хотя сегодня во всем мире испытывается острый дефицит таких экспертов (1.5 – 2 миллиона вакансий в мире по разным оценкам), спустя несколько лет эти, пока незанятые, позиции будут выглядеть совсем иначе.

В 2025 году наиболее востребованы будут знания и навыки в сфере облачной безопасности и интернете вещей, утверждает Алан Паллер, директор по исследованиям института SANS. Количество дивайсов, подключенных к интернету, инкорпорированных в повседневную жизнь, существенно увеличится. Соответственно возрастут и риски. Как полагают некоторые эксперты, в 2025 году в мире будет насчитываться 75 миллиардов подключенных к интернету устройств. В результате резко возрастет спрос на специалистов, разбирающихся в проблемах интернета вещей, способных отслеживать и анализировать трафик данных, обнаруживать потенциальные риски.

Еще один вызов представляют собой умные технологии городской среды обитания: сенсоры, измеряющие качество воздуха, системы автоматического контроля за автомобильным движением, на объектах энергетики и коммунальных услуг - программы распределения электричества в зависимости от спроса. Чем больше таких умных технологий, тем шире возможности хакеров осуществлять преступные замыслы.

Паллер считает, что будущее за «пен тестерами», которые, в отличие от систем, тестирующих защищенность компьютеров и сети, предназначены для проверки интернет приложений на предмет их надежности, устойчивости против хакерских атак.

Цифровая трансформация современных предприятий, охватывающая постепенно все сферы бизнеса и экономики, рождает необходимость в новых категориях специалистов по безопасности, например, в сфере развития продуктов. Здесь он (или она) в тесном контакте с инженерами, маркетологами, юристами должен идентифицировать и минимизировать риски, связанные с созданием и появлением на рынке новых продуктов и услуг. Для этого понадобятся дополнительные знания, в частности, в области защиты личных и интеллектуальных прав, где также постоянно происходят изменения.

На уровне высшего эшелона управления бизнесом следует ожидать рост числа позиций, носящих условное название «офицер/менеджер по безопасности бизнес информации», отмечает Эмили Моссбург (компания Delloitte Cyber - консалтинг, исследования, услуги по управлению киберрисками). Многие финансовые организации уже имеют такие должностные позиции в своих ключевых подразделениях, говорит она в интервью журналу Chief Security Magazine. Они обычно подчиняются напрямую главному офицеру по безопасности корпорации на уровне вице-президента.

Эксперты сходятся во мнении, что уже в недалеком будущем «героями кибербезопасности» станут те, кто смогут интегрировать результаты машинного обучения и искусственного интеллекта с процессами принятия решений.

Отделы кадров, принимая на работу специалиста, будут заинтересованы в более разнообразных, чем сегодня, компетенциях. По мере интеграции функции кибербезопасности непосредственно во все сферы и стороны бизнеса, роль и значение руководителя отдела по информационной защите будут возрастать и соответственно менять корпоративную культуру.

Как организована охрана монреальского морского порта

Примерно 2 500 грузовиков ежедневно въезжают и покидают порт Монреаля. До недавнего времени водители часами «загорали», ожидая разрешения на въезд. Новая инициатива, предпринятая администрацией порта, упразднила очереди и укрепила безопасность.

Речь идет о развертывании централизованной системы СКУД с использованием технологии «мобильного резервирования», позволяющей водителям заблаговременно, за несколько часов или дней, запрашивать разрешение на въезд в порт. Для этого им необходимо закачать на свои смартфоны специальное приложение, с помощью которого они связываются с администрацией порта и сообщают, когда ориентировочно им надо прибыть в порт для погрузки-разгрузки. Получают в ответ точные данные по часам и, тем самым, могут заранее планировать свое время, не тратя его впустую на ожидание в очередях.

Новая система также позволяет водителям заблаговременно и виртуально заполнять необходимые бланки и формуляры, ускорить необходимый на въезде и выезде из порта процесс аутентификации, который осуществляется с помощью биометрии (отпечатков пальцев), специальных электронных карт-пропусков, а также с применением технологии аналитического отслеживания государственных номеров транспорта.

Эти инновации существенно ускорили разгрузочно-погрузочные операции в порту, через который ежегодно переваливают 35 миллионов тонн различного груза. Выигрывают водители, экономя время и горючее. В выигрыше и таможенники, отслеживающие в онлайновом режиме движение контейнеров с корабля в терминалы, а оттуда в грузовики. Архивация данных необходима для проведения расследования в случае пропажи груза.

Ключевую роль во внедрении и эксплуатации новой системы играет служба безопасности, возглавляемая Феликсом Бергероном. Он персонально отвечает за охрану порта, провоз опасных материалов и грузовой транспорт. Именно он в 2001 году, когда только пришел сюда работать, ввел систему электронных ID карт для всего персонала. «Никакой революции, все инновации внедрялись постепенно», говорит он в интервью журналу Security Management, October, 2019.

Сегодня допуск на территорию порта имеют 37 000 человек. Их идентификационные карты различаются по цвету. Например, голубые карты - у чиновников, зеленые – у работников терминалов, пурпурного цвета – у работающих по временному контракту, желтые – у водителей грузовиков, серые - у грузчиков.

Порт – место шумное. Поэтому световая сигнализация, развернутая по всей территории, здесь не лишняя. Красный цвет специальных мощных ламп предупреждает об инциденте, опасном для жизни (к примеру, об утечке опасного для жизни ядовитого вещества). Белый цвет означает требование к охране немедленно прибыть на место возможного инцидента. Желтая лампа означает просьбу о технической помощи, поддержке. Зеленый, как и везде, показывает, что все в

порядке.

Конфигурация порта с береговой протяженностью без малого 20 км довольно сложная. Несмотря на наличие буферных зон, отделяющих его территорию от города, которые включают ограждения и заборы, автомобильные и железнодорожные подъезды, жилые кварталы, тем не менее, подходят впритык.

«Город совсем рядом и моя задача – не допустить, чтобы какой-либо инцидент в порту отразился на жизни простых горожан», замечает Бергерон. Весь груз, проходящий через порт, подвергается проверке на радиоактивность, как того требует правительство Канады. Для этого охранники вооружены специальными детекторами радиации.

На территории порта расположены около 20 сооружений и зданий, принадлежащие разным ведомствам. Некоторые из них управляются на основе правил морской безопасности. Но все без исключения охвачены единым, централизованным планом (и соответственно программой) охраны и безопасности. Если какое-либо ведомство допускает отклонения от требований плана, например, при досмотре грузов, на место отправляется старший офицер по безопасности для мониторинга ситуации, а нарушители привлекаются к административной ответственности.

Система видеонаблюдения интегрирована с аналогичными системами, принадлежащими местной полиции и береговой охране.

С рабочими порта проводятся тренинги. Если они замечают кого-либо или что-либо, вызывающее подозрения, то обязаны немедленно сообщать дежурному офицеру по безопасности, который отправляет на место потенциального инцидента находящийся поблизости патруль.

Как Фольксваген защищается от дронов и использует их в интересах своей безопасности

Фольксваген столкнулся с проблемой промышленного шпионажа с помощью дронов во время испытаний новых моделей на своих полигонах. Таких полигонов у корпорации несколько. Каждый из них надежно охраняется по периметру безопасности. Но не с воздуха до недавнего времени.

«Мы уже несколько раз фиксировали появление дронов», - говорит М.Шмидт, директор по безопасности Volkswagen Group (Security Management, September, 2019). Каждый раз удавалось засечь местоположение оператора, но попытки задержать злоумышленника проваливались. Он ускользал на автомобиле с фотографиями на руках.

Чтобы справиться с новой проблемой, Фольксваген пять лет назад начал изучать рынок анти-дроновых технологий. К сожалению, тогда не удалось найти отвечающую требованиям и условиям корпорации систему. «Мы хотели передвижную систему, поскольку нуждаемся в такой защите только во время испытаний или закрытых

демонстраций», - отмечает Шмидт.

В конце концов, удалось найти в Германии подходящих партнеров - ESG, Diehl и Rohde & Schwarz – и договориться с ними о создании мобильной системы обнаружения дронов GUARDION, напоминающей те, которые использовались в ФРГ во время G20 в Гамбурге и визита президента США Обамы. Помимо камер наблюдения система включает сенсоры, радарную и радио аналитику. Одно из преимуществ - низкий уровень ложных сигналов, в том числе от пролетающих птиц.

Система установлена на грузовике с прицепным трейлером, что вполне достаточно для комфортного размещения двух рабочих станций и обслуживающего персонала.

Всякий раз во время проведения испытаний новых моделей неподалеку от полигона размещается GUARDION. Как только фиксируется появление дрона, об этом сообщается специальной службе, которая отвечает за поиск и обнаружение оператора. У службы безопасности корпорации нет разрешения на самостоятельный захват потенциальных злоумышленников, поэтому вся необходимая информация тут же передается в ближайшее управление полиции для задержания оператора и конфискации шпионского оборудования. В рамках партнерства с полицией служба безопасности время от времени проводит совместные тренинги по защите от дронов.

Помимо мониторинга испытательных площадок система GUARDION уже дважды использовалась во время проведения футбольных матчей премьер лиги Германии с участием клуба, которым владеет Фольксваген. В последнее время владельцы и управленцы футбольных стадионов в этой стране серьезно озаботились потенциальными рисками от использования дронов как в конкурентских, так и в террористических целях.

К городе Вольфсбург, где расположен главный завод Фольксвагена, корпорация провела испытание новой системы охраны своего офиса, в которой дрон с помощью кабеля соединен с компьютерами СБ. Как только в центр контроля за безопасностью поступает сигнал тревоги, дрон с установленными на нем камерами наблюдения взвивается вверх и по кабелю передает видеоинформацию дежурному охраннику. Привязанный к зданию дрон, в отличие от устройств в свободном полете, позволил компании получить лицензию на его использованиие в целях безопасности в городских условиях. Важно, что кроме проводника, ведущего в компьютерную сеть, дрон по кабелю постоянно подключен к зарядному устройству.

Сколько стоит безопасность компании?

Сколько денег требует корпоративная безопасность? По мнению Б. Вайолино, автора статьи в журнале Chief Security Officer, August 20, 2019, ответ на этот вопрос очень простой: цена безопасности зависит от:

- профиля деятельности, вида бизнеса;

- категории персональной, служебной информации, интеллектуальной собственности;

- требований регулятора;

- конфигурации интернет инфраструктуры компании;

- привлекательности с позиции криминала.

Более важен по-иному сформулированный вопрос: «Как организация определяет, сколько денег необходимо тратить на безопасность?».

Редакция журнала Chief Information Officer с помощью экспертов опросила в разных странах 683 руководителя отделов IT, стремясь выяснить, какая часть их бюджета идет на обеспечение безопасности компании. Чаще всего называли цифру 15%. Четверть респондентов озвучили цифру 20 и более процентов.

При этом обнаружилось, что размер организации не имеет принципиального значения. Средние цифры в процентах у крупных и малых предприятий не сильно разнятся. Что же касается сфер деятельности, то больше всего денег на безопасность тратят организации, занятые в финансах, высоких технологиях и оказании профессиональных услуг.

Отвечая на вопрос: «Какие бизнес инициативы наиболее значимы для финансирования IT в их организациях?», 40% опрошенных на первое место поставили кибербезопасность.

В другом исследовании, проведенном IDG Communications, две трети из числа опрошенных руководителей в области корпоративной безопасности разных стран (664 человека), заявили, что планируют в следующем году увеличить бюджет в среднем на 13%.

Среди факторов, определяющих приоритет вопросов охраны и безопасности в распределении финансов и конкретное их использование, называют:

- опыт «лучших практик» (74%);

- контроль за соблюдением политик и инструкций по безопасности (69%);

- ответ на инциденты безопасности, подобные тем, что уже происходили в организации (35%);

- ответ на инциденты в других организациях (29%).

Не надо слишком доверять таким опросам, считает Фрэнк Диксон, вице-президент компании Data Corp. (IDC). Обычно организации на цели кибербезопасности тратят, по его мнению, от 7% до 10% от бюджета на IT. «Однако, вы можете тратить и 15%, но не добиться желаемого уровня безопасности, если у вас архитектура внутренних сетей и баз особенно сложная, или данные, подлежащие защите, чрезвычайно ценные. В то же время, потратив всего 5% от бюджета, предназначенного на IT, вы можете получить желаемый результат» (там же).

В компании HITRUST (некоммерческая организация, занимающаяся разработкой и сертификацией стандартов безопасности данных) финансовые средства, отпускаемые на безопасность, остаются неизменными вот уже на протяжении нескольких лет. Джейсон Таул, отвечающий за безопасность, объясняет это так: «Как и большинство

других организаций, мы сталкиваемся каждый год с растущим числом угроз и рисков. Но предпочитаем решать возникающие проблемы путем повышения оперативной эффективности. Если бы мы не фокусировали внимание на вопросах эффективности, тогда нам пришлось бы постоянно увеличивать бюджет». Важную роль играют измерения эффективности программ безопасности. Мониторинг с помощью специально выбранных метрик ведется постоянно, подчеркивает Таул.

Одновременно Таул отмечает, что требования регуляторов, клиентские ожидания, партнеры диктуют необходимость дополнительных расходов на безопасность. Обычно такие дополнительные расходы учитываются в ценовой политике. Но клиенты, как правило, считают, что это бремя должно ложиться не на них, а на бизнес.

Отвечая на вопрос о том, как определить уровень финансирования, исходя из результатов повседневного анализа ландшафта рисков, Таул говорит: «Если картина рисков и угроз существенно не меняется, то нет и необходимости в дополнительном финансировании. Но если мы приходим к выводу, что мы сталкиваемся с новыми и серьезными вызовами, то, конечно, надо что-то предпринимать в плане бюджета. Но важно, что ответ всегда не статичен».

Время для новой модели управления киберрисками настало

В этом уверен главный аналитик компании Enterprise Strategy Group ESG Джон Олтсик, чьи статьи с завидной регулярностью появляются не только в специализированных журналах, но и в таких ведущих изданиях как Business Week, Wall Street Journal, New York Times.

Очередная его публикация в онлайновом журнале Chief Security Officer, November 28, 2019, посвящена вопросу трансформации модели управления киберрисками. Олтсик утверждает, что нынешняя модель полностью себя исчерпала. «Специалисты по кибербезопасности уже не в состоянии успешно справляться с гигантским расширением киберпространства, с колоссальным ростом уязвимостей, с постоянно совершенствуемыми способами и методами киберкриминала», пишет он.

В подтверждение своего подхода Олтсик ссылается на недавнее исследование, проведенное корпорацией ESG, в котором и он участвовал. В упомянутой статье он делится некоторыми своими находками и размышлениями.

Бизнесмены более, чем когда-либо вовлечены в процессы безопасности

Еще десяток лет назад предприниматели и топ-менеджеры компаний снисходительно относились к вопросам безопасности бизнеса. Ситуация изменилась. Сегодня службы безопасности во многих организациях собирают и обрабатывают огромную массу данных, которые в приемлемой, доходчивой форме необходимо регулярно докладывать совету директоров. Содержимое отчетов и рекомендаций ясно указывает, что традиционные формы взаимоотношений между СБ и первыми лицами безнадежно устарели и требуют кардинальной перестройки.

Расходы на кибербезопасность увеличиваются, однако растут и ограничения

Бюджеты, выделяемые на кибербезопасность, пухнут год от года и конца этому не видно. Бизнесмены готовы вкладывать средства в сферу, призванную защищать их организации, но вместе с тем они хотят понимать и оценивать, какую реальную отдачу получают от этих инвестиций. К примеру, главный финансовый директор корпорации хочет знать, как именно улучшится безопасность, если вместо запланированных на год одного миллиона долларов на эту функцию будет выделено 1.2 миллиона, как того просит служба безопасности. Специалисты вынуждены тратить массу времени и сил на то, чтобы с помощью не всегда точных метрик исследовать далеко не полный трафик данных, чтобы наглядно, с цифрами на руках продемонстрировать конкретные выгоды от затрат на безопасность. В этом вопросе также нужные какие-то изменения и улучшения, пишет Олтсик.

Риски и угрозы быстро расширяются и растут

Базовая формула управления киберрисками сегодня выглядит так: «киберриск = уязвимости х угрозы х последствия». Все верно, но есть проблема: все составные части – киберпространство, бреши и уязвимости, последствия для бизнеса – увеличиваются быстрыми темпами. Один из выводов исследования ESG четко указывает на рост рисков и угроз, исходящих от третьей стороны (поставщиков, партнеров и т.п.).

Одновременно отмечается, что атаки становятся все более целенаправленными и изощренными. Организации сталкиваются с непрерывно увеличивающимся перечнем угроз: финансовые риски, операционные риски, наконец, репутационные риски. Естественно, что работа профессионалов по кибербезопасности требует большей специализации, концентрации усилий на все более узких направлениях, а это, в свою очередь, ставит вопрос о дополнительном обучении, повышении квалификации.

Способы управления рисками, такие как сканирование уязвимостей, аудит рисков, связанных с третьей стороной, тестирование возможностей для несанкционированного проникновения, обычно осуществляются периодически – раз в месяц, в квартал, несколько раз в год. Когда по требованию аудиторов, когда – регуляторов. Но редко исходя из продуманной и разработанной стратегии управления рисками.

Автор статьи видит проблему в методологическом подходе. В системе управления рисками всё взаимосвязано. Если меняется один фактор, то воздействие моментально распространяется на другие факторы и сегменты системы. Мы должны согласиться с этой реальностью и стремиться к созданию такой системы управления рисками, которая бы проводила мониторинг и оценку угроз на постоянной, непрерывной основе.

Кражи в торговле: высокие риски сохраняются

«Борцы с криминалом в торговой сфере, несмотря на зримые успехи, по-прежнему сталкиваются с ростом рисков и новыми вызовами», говорится в докладе Университета Флориды и организации National Retail Federation (NFR) «2019 National Retail Security Survey», с некоторыми результатами которого знакомит своих читателей онлайновое

издание Security Management, September, 2019.

Для большинства ритейлеров, согласно данным опроса, пять основных рисков представляют: 1) организованные преступные группы; 2) киберинциденты; 3) хищения, осуществляемые персоналом магазинов; 4) криминал в интернет торговле, 5) мошенничество, связанное с возвратом товаров. Эти риски сегодня более актуальны и остры, чем еще несколько лет назад.

Каждый год компания NFR оценивает убытки ритейлеров от воровства, мошенничества и других видов криминала. В 2018 году они составили более 50 миллиардов долларов или 1.4% от стоимостного объема продаж. Это больше, чем в предыдущем, 2017 году (46.8 миллиардов). При этом процент общих потерь в объеме продаж остался практически на том же уровне (1.33% в 2017 и 1.38% в 2018 гг.). Такой уровень убытков признается большинством ритейлеров «более-менее приемлемым». Хотя риски увеличиваются, они отчасти нейтрализуются такими факторами как более тесная координация между самими ритейлерами (корпоративными службами безопасности), между последними и правоохранительными органами.

Эксперт в области предотвращения убытков (loss prevention) Крис МакГойи отмечает, что наблюдаемая стабильность в потерях позволяет ритейлерам более эффективно планировать бюджет, если, конечно, торговля в целом успешна.

Две трети всех ритейлерских убытков обусловлены тремя факторами: организованной преступностью, индивидуальными кражами, хищениями со стороны персонала. Остальная треть потерь приходится на просчеты в бизнесе, документообороте.

Организованная преступность

По оценкам NFR, организованная преступность причиняет наибольший ущерб – около 30 миллиардов долларов. Криминал привлекают в первую очередь те товары, которые легче пронести через кассу – лекарства, бритвенные лезвия, батарейки, мобильники, некоторые виды модной одежды. Преступники работают группами, используют методы отвлечения внимания, другие изощренные способы преодоления систем контроля.

Организованные преступные группы опасны тем, что не пренебрегают никакими типами торговых предприятий. Будучи нацеленными на торговые центры, где сконцентрировано множество магазинов, они не проходят мимо и бакалейных лавок, и аптек, и небольших специализированных магазинов.

Злоумышленники используют самые современные пути и способы реализации похищенных вещей, затрудняющие поиск и разоблачение. Если ранее просто относили добычу барыгам, то сегодня, с распространением разных видов электронной, онлайновой торговли, скрытно сбывать краденное стало намного легче. Они выставляют вещи на веб-сайты, проводящие онлайновые аукционы, где реализуют товар быстро и по максимально высоким ценам.

Вместе с тем, эксперты затрудняются достаточно точно сопоставлять ущерб, наносимый организованными группами и ворами-одиночками.

Недавнее появление и распространение технологии TwinFlow обернулось ростом потерь. (TwinFlow: в отличие от привычных касс самообслуживания, где покупатели

сканируют свои товары, перекладывая их из одной корзины в другую, кассы Twin Flow оборудованы транспортной лентой, по которой товары отправляются в накопительный блок. Технология Twin Flow может обслуживать за определенный промежуток времени в 2-3 больше покупателей в сравнении с обычными кассами. Кассы Twin Flow активно используются в Западной Европе и странах Скандинавии, где показывают отличные показатели. «Лента» стала первой сетью, запустившей пилотный проект с кассовой технологией Twin Flow в России). Однако, как полагают эксперты, очевидный ущерб от новации полностью компенсируется экономией в результате сокращения обслуживающего персонала, в первую очередь, кассиров.

(окончание в следующем номере)

Транснациональные преступные организации

В 2013 году международная криминальная группа с помощью компьютерных специалистов в течение 10 часов похитила из банкоматов более чем 20 стран 45 миллионов долларов. Это больше, чем потери всех банков мира от физических грабителей в том же году.

Взрывное развитие цифровых технологий обусловило возникновение транснациональных преступных организаций (ТПО), криминальная деятельность которых по своим масштабам и последствиям превосходит традиционные виды правонарушения. Во-первых, они опираются на современные технологические инновации, в ряде случаев обгоняющие те, что появляются в легальной экономике. Во-вторых, они пользуются тем, что власти некоторых стран либо неспособны, либо не хотят серьезно с ними бороться. В числе таких стран журнал Security Management (August, 2019) называет Армению. По мнению автора публикации, Майкла Бреслина, «последние политические турбулентные события в этой стране способствовали увеличению числа ОПГ».

Далее автор пишет: «Структура организованной преступности в Армении представляется как базовая система взаимоотношений между разными сегментами общества. В отличие от обычных банд здесь нет формального «крестного отца», т.е. главы организации. И это затрудняет борьбу с ними. К примеру, одна армяно-американская преступная группировка, известная под именем «организация Мирзояна - Тер-Джаняна», занималась мошенничеством в сфере здравоохранения пяти стран, прибегая к краже персональных, идентификационных данных. Украденные деньги перекачивались через США в банки Армении. Организация насчитывала 70 человек, но не имела формального лидера. Члены ее постоянно курсировали между Арменией и США, претворяя в жизнь жульнические схемы. В конце концов, власти США их арестовали, предъявив множественные обвинения, включая отмывание средств».

Другая особенность ТПО – их анонимность, особенно характерная для криминала в сфере онлайновых трансакций. Они способны проникать всюду, оставаясь невидимыми для жертв и правоохранителей. Согласно данным исследовательской фирмы Verison («2019 Data Breach Investigations Report»), 71% организованных утечек информации финансово мотивированы отдельными инсайдерами, а 39% устроены

международными криминальными группами.

Киберкриминал, пишет Бреслин, негативно воздействует на доверие людей к институтам, к способности частных и общественных организаций защитить их жизненные интересы. Ежегодный урон от киберкриминала по разным оценкам варьируется от 50 до 100 миллиардов долларов. Удачная кибератака роняет цену акции. Только один пример. Компания Equifax (американское бюро кредитной истории, собирает информацию более чем о 800 миллионов физических лиц и более чем 88 миллионов компаний по всему миру) в сентябре 2017 года заявила о крупной утечке данных, касающихся 147 миллионов американцев. Акции компании тут же упали на 34%. Кроме того, компании пришлось выплатить 300 миллионов долларов на компенсацию ущерба.

Общим для ТПО является их удивительная гибкость, восприимчивость к технологическим новинкам, мощный технический интеллект. Они быстро приспосабливаются к новым методам и способам, коими правоохранительные органы пытаются им противостоять. Их способность подчинять своим целям технологические инновации, подчеркивает Бреслин, представляет собой пока непреодолимую преграду для противоборствующей стороны.

Борьба с ТПО осложняется рядом факторов. Они преследуют не политические, а финансовые цели. По этой причине они обычно не представляются властям столь же опасными как террористические группировки. Кроме того, они нередко рассматриваются как домашняя проблема, не выходящая за госграницу. Ими часто занимается уголовная полиция, а не службы государственной безопасности.

В то же время международный характер ТПО предоставляет им огромное преимущество. Многие их них родились, сформировались в сравнительно бедных странах, власти которых не имеют достаточных средств и сил с ними бороться. Вывод очевиден: только международная кооперация государств может обеспечить реальные позитивные результаты противодействия ТПО.

Женщины и терроризм

В конфликтных зонах по всему миру все больше женщин вливаются в ряды радикальных группировок и участвуют в террористических акциях.

Исследование, проведенное британским аналитическим центром по оборонным вопросам (Royal United Services Institute), показало, что женщины составляют сегодня 17% состава экстремистских организаций в странах Африки. В другом научном докладе, подготовленном организацией International Center for the Study of Radicalization, утверждается, что в Сирии и Ираке среди членов запрещенной в России организации ИГИЛ женщин насчитывается около 13%.

Хотя они и составляют существенное меньшинство, но, тем не менее, играют важнейшую роль в распространении экстремисткой идеологии, а также в деле придания легальной видимости террористическим организациям.

Эксперты из Global Extremist Monitor (организации, занимающейся изучением исламского экстремизма и возглавляемой бывшим премьер-министром

Великобритании Энтони Блэром) подсчитали, что только в одном 2016 году почти 200 женщин участвовали в террористических атаках, подрывая себя. В том же году они составили 26% арестованных в Европе террористов.

Хотя уровень участия женщин в экстремистской деятельности год от года заметно растет, эта тенденция не нова, она насчитывает многие десятилетия.

В Шри Ланке женщины еще в 70-е годы прошлого столетия активно участвовали в войне тамильских националистов за независимость. В 1989 году «тамильские тигры» даже образовали в своей организации военное женское крыло.

Еще ранее, в начале 20 столетия, женщины играли выдающуюся роль в борьбе за независимость Ирландии. О вкладе женщин России в революционные движения (особенно если иметь в виду террористов-народовольцев и партию эсеров) и говорить не приходится.

Вернемся в современность. Эксперты называют факторы, побуждающие женщин присоединяться к экстремистским организациям. Финансовая выгода и приверженность идеологии одинаково мотивируют экстремистов обоего пола. Но для привлечения женщин в ряды террористов в ход идут самые изощренные аргументы и доводы. Например, в организации Аш-Шааб (запрещенной в России) молодых девушек убеждают, что их стремление получить хорошее образование помешает перспективам удачного замужества. Активно пропагандируется восстановление «традиционной» в исламском обществе роли женщины как жены, матери детей бойцов за веру, домохозяек. Хотя известны случаи и сексуального рабства в той же Аш-Шааб.

Женщины часто служат рекрутерами, склоняющими на свою сторону других женщин. Заманивают обещанием работы и денег. ИГИЛ предлагает менее традиционные позиции: там немало женщин среди врачей и медсестер, а, кроме того, из женщин формируется «полиция нравов», призванная следить за соблюдением норм шариата среди населения.

С другой стороны, женщины обладают рядом преимуществ перед мужчинами в борьбе с терроризмом, утверждают авторы исследования «Women and Terrorism: Hidden Threats, Forgotten Partners», проведенного американской организацией в сфере международных связей Council on Foreign Relations. Они считают, что женщины по сравнению с мужчинами быстрее и лучше обнаруживают признаки терроризма, поскольку экстремистские группировки ориентированы, как правило, на ущемление их прав. И именно женщины наиболее успешны в деле разоблачения экстремизма: «женщины играют критически важную роль в опровержении догм фундаменталистов, работая в школах, социальных и религиозных организациях, региональных и местных органах власти».

Mastercard укрепляет периметр безопасности

Террористические атаки в Брюсселе в 2016 году, унесшие десятки жизней, заставили многие европейские компании критически переосмыслить состояние и возможности

своих систем безопасности, предпринять шаги по их модернизации и усилению.

Европейская штаб-квартира корпорации Mastercard еще в 2015 году взяла курс на конвергенцию физической охраны и кибербезопасности, что обусловило существенные изменения корпоративной культуры. Служба безопасности резко расширила свое присутствие и влияние практически во всех подразделениях и направлениях деятельности организации. Неизменным осталась ее миссия – защита критической инфраструктуры, в первую очередь, людей.

С ростом террористической активности возникла идея передислокации европейских офисов Mastercard численностью от 500 до 1000 сотрудников, традиционно отличавшихся открытой бизнес средой, в более безопасные места. Служба безопасности провела поиск и анализ возможных новых локаций и в результате рекомендовала отказаться от этой идеи. Вместо этого руководством корпорации было принято решение заняться укреплением периметра безопасности, в первую очередь, головного европейского офиса, расположенного в Ватерлоо.

Начинать надо было с плана действий. Опираясь на анализ потенциальных рисков и угроз, служба безопасности пригласила инженеров, технических специалистов обсудить технологические решения, касающиеся, в первую очередь, внешнего периметра (забора и входов на территорию). Нанятые по временному контракту консультанты помогли разработать подробный проект.

Он предусматривал кардинальное обновление систем СКУД, обслуживающих все пять зданий головного офиса. Процесс реализации несколько затянулся из-за бюрократических проволочек. Кампус расположен в оживленном, густонаселенном районе Ватерлоо, и потребовалось несколько месяцев, чтобы получить разрешение городских властей на работы.

Оборудование СКУД, установленное еще 15 лет назад, технологически и морально устарело, было изношенным. В числе проблем, которые предстояло решать – невозможность установки массивных, тяжелых заграждений, надежно перекрывающих доступ к зданиям для машин, начиненных взрывчаткой. Прямо за воротами – пешеходный тротуар. Внутри кампуса тоже нет достаточного простора для установки боллардов.

Обратились к английской фирме, выпускающей ворота с технологией crash ratings (аварийные самописцы, специальные регистраторы), позволяющей обходиться без массивных бетонных тумб ограждения. Технология совершенно новая, малоизвестная на рынке, но, как утверждают авторы статьи в журнале Security Management, September, 2019 (Меган Гейтс, Гэвин Гендерсон, Марко Мурру), «отвечающая требованиям безопасности и функциональным возможностям кампуса».

Ежедневно на территорию кампуса въезжают до 500 машин. Программа СКУД рассчитана таким образом, чтобы ворота открывались менее чем за 10 секунд, исключая возможность затора на городском проспекте, и быстро закрывались.

Кроме этого по всему периметру возведен двухметровый забор с системой инфракрасного излучения, предупреждающей об угрозе несанкционированного вторжения.

Заботясь о безопасности, корпорация не забыла о внешнем виде периметра, который

не должен выглядеть уж слишком устрашающе. Был нанят садовник-дизайнер, подобравший кусты и деревья, а также соответствующий цвет для забора.

Одновременно с технологическими решениями служба безопасности начала очень серьезно работать с персоналом компании, учитывая оправданные страхи и опасения людей после серии террористических актов в разных европейских городах. В структуре компании действует специальная комиссия, предназначенная для информирования коллектива о внутренней жизни. СБ тесно сотрудничает с комиссией, распространяя через нее новости о проводимых мероприятиях по безопасности, собирая и анализируя мнения работников корпорации. Проведены занятия по обучению новым правилам прохода на территорию и в здания Mastercard.

Завершив работы по укреплению периметра, служба безопасности совместно со специалистами в сфере IT сосредоточила усилия на вопросах совершенствования систем информзащиты, критичных для организации, деятельность которой основана на продуктах и услугах для безопасных трансакций.

Как малый бизнес должен реагировать на хакеров

Хакерские атаки и утечки информации, к сожалению, стали обыденной реальностью сегодняшнего бизнеса, пишет Сэм Бокетта в журнале Chief Security Magazine, 10 September, 2019. Десять лет назад объектами атак были, главным образом, крупные организации. Сейчас ситуация иная. По мере того, как крупный бизнес спешно укрепляет цифровой периметр безопасности, а малые предприятия все глубже погружаются в онлайн, криминал больше внимания стал уделять среднему и малому бизнесу.

Успешная атака может причинить серьезный ущерб крупной компании, но стать настоящей катастрофой для небольшой фирмы. По данным, которые приводит National Cyber Security Alliance, 20% малого бизнеса ежегодно сталкиваются с атаками хакеров. В результате 60% из них вынуждены закрываться в течение шести месяцев после инцидента.

Итак, как же надо реагировать малым предприятиям? Если вы задаете этот вопрос после атаки, то отвечать уже поздновато. Ключ к успеху – заблаговременная подготовка с целью предотвратить или минимизировать ущерб.

Начинать надо с разработки плана превентивных мер, пишет автор статьи. Персонал компании должен знать, как каждому реагировать на атаку. А, кроме того, понимать, как вести себя с клиентом, опасающимся утечки персональных данных.

В процессе планирования важно выделить приоритетные вещи, которые следует защитить в первую очередь и наиболее тщательно. Небольшие организации обычно не располагают возможностями покрыть защитным колпаком всю свою интернет инфраструктуру. Поэтому надо отдельно выделить те системы и базы данных, которые наиболее чувствительны и важны для бизнеса. Регулярные аудиты информационного трафика помогут обнаруживать те или иные утечки, бреши, вовремя подключить

внешних специалистов по кибербезопасности и правоохранительные органы к расследованию инцидента.

Что касается ответа на уже произошедший инцидент безопасности, то Бокетта рекомендует выделить кратко, средне и долгосрочные задачи.

В рамках *краткосрочных задач* необходимо добиться, чтобы ваши сотрудники умели распознать атаку на максимально раннем ее этапе. Чем быстрее атака обнаружена, тем легче идентифицировать преступника. Немедленный перевод всех систем в оффлайн Бокетта считает ошибкой, так как такая спонтанная реакция дает ясно понять хакеру, что его засекли, позволяет обрубить все концы. В таких случаях обозленный преступник может попытаться нанести компании максимальный ущерб и быстро исчезнуть. Поэтому, надо сначала определить, какие сегменты непосредственно затронуты в ходе атаки, а затем изолировать их от остальной инфраструктуры.

Также необходимо как можно скорее оповестить соответствующие правоохранительные службы, предоставив им максимум информации. Это не только облегчает отражение атаки, ликвидацию последствий, но и предоставляет легальную защиту вашей компании и клиентуры. Последний момент чрезвычайно важен с точки зрения сохранения репутации.

В качестве *среднесрочной задачи* необходимо выполнить работу детектива. А именно: исследовать, каким путем преступник проник в вашу сеть, найти и залатать бреши. Также следует восстановить поврежденные или утраченные данные, но не ранее того, как вы убедитесь, что инфраструктура в полной безопасности.

Наконец, *долгосрочная задача*: провести тщательный анализ, как вы реагировали на атаку хакера. Если правильно и глубоко разобраться в этом вопросе, то даже с учетом понесенного ущерба можно извлечь выгоду – использовать инцидент как возможность обучения персонала, внесения коррективов в план действий, в программу тренингов.

Десять признаков, что вас пытаются надуть

Рожер Гримс в публикации журнала Security Magazine, September, 19, 2019, называет десять индикаторов, позволяющих с большой вероятностью предположить, что к вам применена т.н. «социальная инженерия».

1. Запрос логина и (или) пароля

Когда по электронной почте или телефону (либо через веб-сайт) у вас запрашивают информацию о кодах и паролях, то почти наверняка вы стали объектом мошенничества. Чтобы уменьшить риски, необходимо пользоваться либо многофакторной аутентификацией, либо программным продуктом «password manager». Правда, следует оговориться, что «password manager» сам подвержен атакам хакеров. Автору известны около 30 случаев успешного взлома этой программы.

2. Просьба выполнить то или иное действие

Чаще всего речь идет о предложении «кликнуть» на ссылку, которое содержится в полученном вами сообщении по электронной почте или из социальных сетей. Ссылка отправляет вас на скомпрометированные сайты, где вам рекомендуется сделать то-то и то-то, чтобы оставаться на сайте. Например, обещают пикантное видео, для чего вам необходимо ввести ту или иную информацию, содержащую незаметный вирус, который впоследствии надолго поселится в вашем компьютере. Относитесь с подозрением к предложениям посмотреть видео в социальных сетях.

3. Плохой или подозрительный URL адрес

Следующий важный показатель фишинговой схемы – странно выглядящее название интернет домена или URL адреса. Следует учиться отличать реальные домены от фальшивых. Например, вы получили письмо со ссылкой «appleidicloudsupport», как бы подразумевающей службу технической поддержки Apple. Нажав на нее, вы на самом желе попадаете на домен «entertainingworkshop.com», ничего общего с Apple не имеющий.

4. Провоцирование стресса

Почти во всех сценариях социальной инженерии, в онлайне или по телефону, злоумышленник пытается внушить страх и стресс, убеждая немедленно предпринять те или иные действия. А именно:

- Сообщить коды, пароли, а то ваши счета будут заблокированы
- Немедленно обновить программу под угрозой исчезновения важного для вас контента
- Подтвердить персональной информацией, что банковская карта (или счет) принадлежит именно вам, в противном случае карта (счет) будет заблокирована
- Вас поймали на просмотре и записи порносайтов, о чем вскоре узнают все. Платите штраф
- Вымогательство денег под предлогом ущерба вашему бизнесу

Такие примеры можно продолжать до бесконечности.

5. У отправителя сообщения два URL адреса

Если вы получили письмо, отправленное с адреса, который не совпадает с предлагаемым ответным адресом (изменение мельчайшее – одна цифра или буква), будьте настороже. Два разных URL адреса – обычный фишинговый трюк. Случается, что такое вы увидите во вполне легальных рассылках, например, в рекламных объявлениях. Но в подавляющем большинстве случаев вы сталкиваетесь с мошенниками.

(окончание в следующем номере)

С какими рекрутинговыми фирмами лучше иметь дело?

Джерри Бреннан, постоянный автор публикаций в интернет издании Security Magazine, пишет в одном из последних выпусков, что к нему нередко обращаются с просьбой помочь выбрать рекрутинговую компанию для поиска новой работы. По его мнению,

следует избегать фирм, требующих солидную предоплату или предлагающих рассчитываться в течение какого-то времени процентом от будущей зарплаты. Это устаревшая модель на рынке труда. «Бегите от нее прочь», советует он.

Бреннан указывает, что сегодня наиболее надежны кадровые агентства, которые представляют не соискателя, а, напротив, потенциального работодателя. Они связаны с последним контрактом, по которому услуга оплачивается компанией, выходящей на рынок труда. В зависимости от контракта финансовые обязательства определяются следующим образом:

- компания платит разовый гонорар в размере процента от должностного оклада (обычно в пределах 20 – 35%);

- компания платит сразу или двумя частями: предварительно и по завершении контракта;

- компания платит только после того, как соискатель превращается в полноценного сотрудника, возмещение определяется, исходя из его/годовой зарплаты.

Опросы компаний в разных отраслях бизнеса и экономики показывают, что 37% в процессе поиска и найма работников обращаются к аутсорсингу. Бреннан считает эту цифру завышенной. Он полагает, что услуги высокопрофессиональных рекрутеров занимают не более 5% на рынке труда.

Бреннан предлагает как работодателям, так и соискателям следующие рекомендации:

1. Изучите репутацию, этические аспекты деятельности рекрутинговых компаний и работающих там людей.
2. Лишь очень небольшое число таких компаний действительно специализируются в определенных сегментах бизнеса и экономики. Проверьте, в каких отраслях работала компания до контакта с вами.
3. Посмотрите, как компания работает с информацией с точки зрения соблюдения мер конфиденциальности, надежности средств информационной защиты.
4. В качестве кандидата проявляйте максимум честности, отвечая на вопросы относительно ваших компетенций и опыта. Соблюдающая нормы профессиональной этики фирма никогда и никому не предложит резюме, содержащее неправду.
5. Будьте точны в предоставлении информации о себе. В нынешние времена перепроверить ее через социальные сети, общественно доступные источники не представляет большого труда.
6. При заключении контракта избегайте условий, которые бы вынуждали вас оплачивать любые предложения рекрутинговой фирмы, включая совсем для вас не интересные.
7. Когда рекрутер раскрывает вам имя (название) искомого объекта, не пытайтесь выйти на него самостоятельно, в обход компании. Это повредит вашей репутации и затруднит дальнейший поиск кандидата/работодателя.