ЗАЩИТА КЛИЕНТСКОЙ БАЗЫ

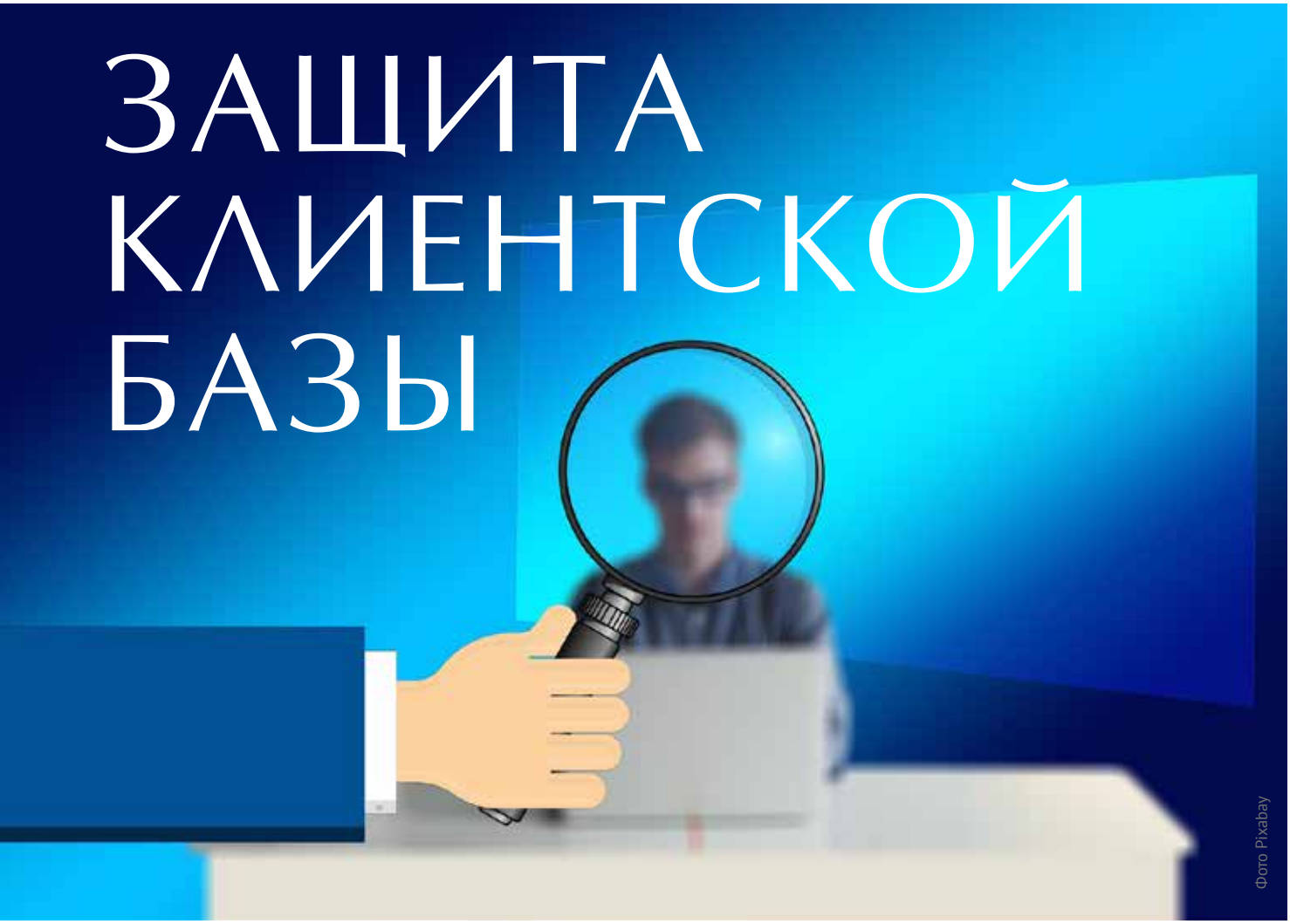


Фото Pixabay

Многие из нас помнят ставшую крылатой строчку из песни: «Если к другому уходит невеста, то неизвестно, кому повезло», но если от вас уходит менеджер по продажам и при этом уносит с собой клиентскую базу, то очевидно, что не повезло именно вам. Как же с уходом сотрудника не потерять и важных клиентов?

Почти в любом бизнесе клиенты привязаны к конкретному менеджеру по продажам, и потому его уход обычно означает их потерю. Если в компании работает не один менеджер, а целый отдел продаж, то в этом случае это становится реальной проблемой. Сложная финансовая ситуация, сокращение штата, ликвидация предприятий вынуждают людей использовать любую возможность для заработка, в том числе корпоративную информацию — для продажи или получения преимущества при трудоустройстве. Данные, которые представляют наибольший интерес (клиентская база, проектная документация, информация о счетах клиентов, коммерческие предложения и пр.).

Фото Pixabay

За такую сумму 20% сотрудников готовы продать пароли рабочих программ, говорится в исследовании софтверной компании SailPoin.

Теоретически при приеме на работу можно обязать менеджера подписывать соглашение о том, что он не будет «уводить» клиентов, но на практике эта бумага просто «филькина грамота».

По мнению Вячеслава Баженова, генерального директора бухгалтерско-аудиторской фирмы, лучший способ предотвращения утечки — это работа в системе 1С, в которой каждый сотрудник отдела продаж «видит» только своих клиентов. «При таком подходе менеджер по продажам может уволиться и прихватить только своих клиентов, и с такими потерями мы готовы смириться, потому что вся клиентская база останется у нас», — уточняет эксперт.

Также эксперты рекомендуют устанавливать DLP-систему (Data Loss Prevention – программа для предотвращения утечек конфиденциальной информации за пределы корпоративной сети). Это программное обеспечение позволяет определить, кто из сотрудников собрался сменить работу.

«Специалист, собирающейся сменить место работы, будет обсуждать свои планы в Skype, размещать резюме, просматривать ресурсы по трудоустройству и т.п. Система это отследит и оповестит службу безопасности. ИБ-специалисты начнут более внимательно следить за таким сотрудником, к

По данным аналитического центра ООО «СёрчИнформ», в 2015 году конфиденциальную информацию чаще остальных пытались украсть менеджеры (31%); прибегают к этому и руководители подразделений (19%); IT-специалисты находятся на третьем месте по количеству хищений данных (12%); четвертое место разделили бухгалтеры, экономисты и финансисты (10%); замыкают пятерку секретари (7%). Также среди инсайдеров стали появляться и разработчики.

Борис Ишкин, ведущий специалист по маркетингу киностудии:

— «Выгорев» у вас, менеджер по продажам может бодро встать под знамена конкурента и плавно переведет не только «теплых» потенциальных, но и ряд действующих клиентов. Ведь ему нужно доказать, что взяли его не зря, что у вас он был недооценен, и сделает это он за счет ваших же клиентов. Не спешите паниковать, если такое произошло, устройте оценку удовлетворенности для действующих клиентов, а для потенциальных – мероприятие, семинар. Преодолейте неприязнь и свяжитесь как с бывшим сотрудником, так и с руководителем фирмы, в которую он ушел, чтобы предупредить «войну мафии», от которой не выиграет никто. Наконец, найдите еще одного продажника, чтобы закрыть брешь.

ВСПОМНИТЕ, ВСЁ ЛИ ВЫ СДЕЛАЛИ ДЛЯ ПРЕДУПРЕЖДЕНИЯ СЛУЧИВШЕГОСЯ:

- *не оставили ли возможность сделать копию CRM?*
- *не открыт ли доступ к ней по интернету?*
- *чьи телефоны и адреса (корпоративные или личные) вы указываете в коммерческих предложениях и переписке с клиентами?*
- *возможны утечки информации сейчас?*
- *всё ли правильно сделано в отношении уволившегося сотрудника?*

Следите и наблюдайте за сотрудниками. Лояльность сотрудника, как и клиента, нужно уметь поддерживать, и тогда вашу компанию обойдут стороной и выгорание и увод клиентов.

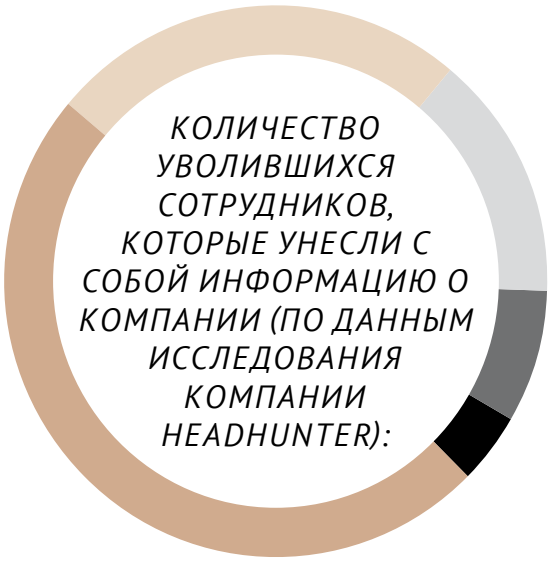
какой информации он имеет доступ, как ее использует, с кем общается», — поясняет принцип работы DLP-системы Сергей Ожегов, генеральный директор компании-разработчика средств информационной безопасности.

Однако, устанавливая какую-либо систему безопасности, работодатель всегда должен помнить, что увольняющийся сотрудник в любом случае унесет данные тех клиентов, с которыми он работал на протяжении какого-то времени, т.к. он мог вносить их номера в личный телефон, записывать контакты в блокнот и т. п., поэтому гораздо важнее, чтобы он не унес больший объем конфиденциальных данных – договоры, условия, коммерческие предложения. Также он может попытаться забрать всю базу клиентов компании или наработки других сотрудников. Потому, как только узнали, что сотрудник собирается уволиться, отслеживайте с помощью SIEM (Security information and event manager) и DLP-системы, чтобы он не собирал информацию в корпоративной сети, не отправлял и не сохранял большие объемы данных, не получил доступ к базам коллег и начальства. Это снизит риск масштабной утечки.

«Истории, когда при увольнении сотрудник уносит (или пытается унести) с собой клиентские базы, типичны по своему сценарию. Для примера, кейс нашего клиента. В кредитном учреждении один из сотрудников готовился к переходу на работу в конкурирующий банк. Чтобы не уходить с пустыми руками, скачал на личную флэшку информацию, составляющую коммерческую тайну банка. Служба безопасности вовремя заметила действия с конфиденциальной информацией и сумела предотвратить утечку. Если бы данные все-таки оказалась у конкурентов, кредитное учреждение только за один год потеряло от 5 до 20 млн рублей. Еще один случай произошел на предприятии по производству хлебобулочных изделий. С помощью DLP выяснили, что недавно устроившийся на работу менеджер по работе с торговыми сетями является «засланным казачком». Он устроился, чтобы иметь доступ в 1С и получить информацию о контрагентах. Если бы сведения попали к конкурентам, предприятию был бы нанесен немалый урон – произошел бы отток клиентов, а совокупные финансовые потери за год составили не менее 12 млн рублей», – подытожил Сергей Ожегов.

51% организаций России столкнулись с ситуацией, когда увольняющиеся сотрудники пытались забрать с собой конфиденциальные данные компании работодателя (по данным аналитического центра ООО «СёрчИнформ»).

Фото Pixabay



- *37% — скопировали собственные наработки;*
- *19% — взяли с собой уникальные методики и разработки, созданные в команде;*
- *11% — забрали базы клиентов и контакты партнеров;*
- *6% — унесли результаты труда своих коллег;*
- *3% – украли конфиденциальные сведения о компании.*

Еще один пример обеспечения защиты информации – установка CRM-системы (системы управления взаимоотношениями с клиентами). Это программное обеспечение позволяет сегментировать базу клиентов, а доступ к разным сегментам и операциям над ними четко разграничить на уровне прав. Подобные меры не вызывают какого-либо негатива со стороны сотрудников, поскольку «скрыты от глаз» пользователя.

По словам Михаила Пустовалова, руководителя отдела IT- разработки, приведенные выше меры по защите информации достаточно эффективны, но можно ввести и более жесткий контроль за действиями сотрудников, имеющих отношение к клиентской базе.

«Вы можете начать с банального отключения всех usb/cd приводов, жесткого регламента для списка используемого программного обеспечения, а также блокировки доступа к определенным интернет-ресурсам. Это повысит уровень сохранности данных, поскольку у сотрудника не будет физической возможности каким-либо иным, отличным от регламента, образом использовать данные. Но имея личный опыт работы в условиях подобного «тотального контроля», могу сказать, что работать в таких условиях, мягко говоря, некомфортно», – уточняет Михаил Пустовалов.

Николай Быстров

ПРАВО на БИЗНЕС

ЖУРНАЛ «ПРАВО НА БИЗНЕС» №1(8) август 2016 г.
Учредитель и издатель ООО «Инсайт Реклама»
Адрес: 350031, Краснодарский край, г. Краснодар, Ейское шоссе, д. 2

Главный редактор *ЮЛИЯ ОЛЕГОВНА КЛИНДУХОВА*
Шеф-редактор *СВЕТЛАНА БОГАТЫРЕВА*
Дизайн и верстка *ЕЛЕНА ГРИЦЕНКО*
Авторы *ЮЛИЯ КЛИНДУХОВА, УЛЬЯНА АЛФЕЕВА, СТАНИСЛАВ ЖАТИКОВ, ОЛЬГА КАРСЛИДИС, СВЕТЛАНА БОГАТЫРЕВА, ИРИНА ЮРЬЕВА, АЛИСА ЛЕСКОВА, НИКОЛАЙ БЫСТРОВ*
Фото *АППАРАТ УПОЛНОМОЧЕННОГО ПО ЗАЩИТЕ ПРАВ ПРЕДПРИНИМАТЕЛЕЙ В КРАСНОДАРСКОМ КРАЕ, ПРЕСС-СЛУЖБА МИНИСТЕРСТВА СЕЛЬСКОГО ХОЗЯЙСТВА И ПЕРЕРАБАТЫВАЮЩЕЙ ПРОМЫШЛЕННОСТИ КРАСНОДАРСКОГО КРАЯ, ЛИЧНЫЕ АРХИВЫ ЭКСПЕРТОВ И ОТКРЫТЫЕ ИСТОЧНИКИ*
Координатор проекта *МАРИНА ПОКУСАЕВА*
Отдел рекламы *АННА КОСЕНКО*
Адрес редакции: 350000, Краснодарский край, г. Краснодар, ул. Пашковская, д. 61,
тел: (861) 259-59-51, E-mail: pnb2014@mail.ru, www.правонабизнес.рф

Отпечатано в типографии ООО «Сочи-Пресс»
354008, г. Сочи, пер. Виноградный, 15а
тел: (8622) 96-08-08
www.sochipress.org

Тираж: 3 500 экз. Издание распространяется бесплатно.
Заказ № _____ от 15.08.2016 г.
Подписано в печать 15.08.2016 г.

www.правонабизнес.рф

16+