Автор: Balladonis
08.08.2009 00:36 -

При массовых сокращениях на улице оказывается большое количество специалистов. При этом бывшие сотрудники достаточно хорошо осведомлены о деятельности «обидевшей их» организации, об обрабатываемых данных, технологиях и о многом другом, касающемся ее бизнеса. Как это все скажется на функционировании компании, уволившей работника, и развитии ее бизнеса? Не «уйдет» ли из компании ценная информация вместе с человеком, который – санкционировано или случайно – имел к ней доступ? Кто даст гарантию, что именно эта конфиденциальная информация не станет «пропуском» в другую, конкурирующую с вашей компанией, организацию?

Известная американская компания Cyber-Ark, специализирующиеся на информационной безопасности, опубликовала аналитическую записку о возросших угрозах информационной безопасности в условиях кризиса.

В ходе опроса офисных служащих (США, Великобритании, Амстердама, Голландии) выяснилось следующее: чтобы сохранить работу, служащие готовы буквально на все. Но если всё-таки уволят, то уже ничто не сможет остановить их от передачи в чужие руки ценной информации, принадлежащей бывшему работодателю. 46 (!!!) процентов опрошенных признались, что поспешат уйти не с пустыми руками. И тут же уточняют, что если самостоятельно не смогут найти что-либо ценного, то готовы предложить взятку коллеге-итэшнику, чтобы с его помощью приобрести заветную информацию.

«Работодатель имеет право рассчитывать на лояльность своего персонала, но в эти темные времена, когда большинство компаний планирует сокращения, служащие боятся «попасть под раздачу». Инстинкт подсказывает им, что нужно искать самое ценное…»
Адам Босниан (вице-президент компании Cyber-Ank)

По результатам того же опроса стало известно, что в случае увольнения более половины респондентов заранее приготовились «вынести сор из избы» и готовы пренебречь этическими нормами. Они УЖЕ скопировали ценную корпоративную информацию (самое нужное, по их мнению: клиентские базы, контактная информация, планы и предложения, информация о продуктах, пароли и коды доступа), чтобы использовать ее как козырь при поисках новой работы.

Самыми предусмотрительными с этой точки зрения оказались голландцы: 71% из них

заранее скопировали все ценное, что могли. На втором месте американцы - 58% из них уже в состоянии «боевой готовности». Третье место и показатель в 40% принадлежат британцам. 71% из общего числа всех респондентов точно будут использовать на новом месте работы конфиденциальные данные прежнего работодателя.

«Никто и не подумает оставить деньги на столе, чтобы не искушать тех, кто проходит мимо. Точно так же нужно скрывать и шифровать любую конфиденциальную информацию в цифровых хранилищах. Мы советуем давать к ней доступ только тем, кто в ней действительно нуждается» **Адам Босниан (вице-президент компании Cyber-Ank)**

В России компания Cyber-Ark исследования не проводила. Но вряд ли кто-то посмеет предположить, что россияне окажутся менее предприимчивыми, чем их потенциальные собратья по несчастью из-за рубежа…

В сложившейся обстановке к тактическим задачам защиты информации добавляется ещё несколько особенно актуальных во время кризиса: построение и поддержка систем защиты от инсайдеров, различные службы цензуры, мониторинга деятельности сотрудников и борьба с мошенничеством.

Вопросы защиты информации в столь не простое время будут рассмотрены на семинаре-тренинге компании «**Благовест-В**», который будет проходить **с 17 по 19 февраля в г. Санкт-Петербурге**
. Наши преподаватели (совместно с ведущими российскими экспертами с области защиты информации) расскажут о принципах оценки источников угроз безопасности информации, о возможных каналах утечки и последовательности проведения работ по организации комплексной защиты информации.

На семинаре-тренинге **«ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ»** будут рассмотрены организационно-правовые основы защиты информации ограниченного доступа. Законодательство РФ в области защиты и неправомерного использования информации (в том числе и инсайдерской) постоянно изменяется, корректируются требования по хранению и раскрытию служебной информации и критически важных персональных данных. По информации ФСТЭК, требования только одного Закона "О персональных данных" обязаны исполнять более 7 миллионов частных предпринимателей и юридических лиц на территории РФ.

Программа семинара-тренинга корректируется под запросы каждой группы слушателей: будь то особенности построения системы защиты информации для организаций с большим ежедневным объёмом конфиденциальной информации (органы соцзащиты, страховые фирмы, банки), или структура для компаний, работающих с персональными данными с допуском персонала низкой квалификации (операторы на телефоне, в центрах продаж и т.д.)

Успешное решение всех этих задач даст положительный импульс к следующему витку развития. Но лишь в том случае, если нынешний «кризисный» период пройдёт без информационных и финансовых потерь.

Ведь вслед за кризисом всегда наступает новый этап развития. И с каким заделом ваша компания его начнёт – решать только вам.

Подробнее о программе семинара-тренинга «ОРГАНИЗАЦИЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ» можно узнать на сайте http://cdat.ru/