Аникин Игорь Вячеславович,
заведующий кафедрой системы информационной безопасности КНИТУ-КАИ (г. Казань), к.т.н., доцент

Организация программы профессионального обучения работе на компьютерном полиграфе в казанском национальном исследовательском техническом университете им. А.Н. Туполева – КАИ

Высочайшая степень автоматизации современных предприятий ставит в зависимость надежность и эффективность их функционирования от степени защищенности информационных систем, обеспечивающих автоматизацию бизнес-процессов. Повсеместное применение информационных технологий (ИТ), с одной стороны, позволило предприятиям, выйти на качественно новый уровень достижения своих бизнес-целей, а с другой — привело к чрезвычайной уязвимости бизнес-процессов по отношению к угрозам информационной безопасности (ИБ). При этом исследования показывают, что основные угрозы ИБ реализуется сотрудниками. Большая часть государственных структур и коммерческих предприятий относят внутренние угрозы к наиболее опасным, о чем свидетельствуют аналитические отчеты таких известных компаний, как Perimetrix, Infowatch, Ernst&Young [1]. Внутренние угрозы для современных предприятий составляют около 68% от общего их числа. Такие угрозы, реализуемые внутренними сотрудниками организации, получили также название инсайдерских угроз. Риски, связанные с инсайдерскими угрозами, в настоящее время наиболее велики. Более чем 40% предприятий имеют долю потерь из-за инсайдерских атак более 50% в общем ущербе финансовых потерь. Естественно, таким потерям в настоящее время уделяется все большее внимание.

К наиболее серьезным инсайдерским угрозам в настоящее время относятся утечки информации, незаконное хищение активов, преднамеренное внедрение вредоносного программного обеспечения внутренним персоналом в информационные системы предприятий. Все более часто появляется информация об инцидентах, связанных с утечками конфиденциальной информации из коммерческих организаций и государственных структур. Исследования компании Perimetrix показывают, что наибольший объем утечек связан с персональными данными, а также коммерческой тайной предприятия.

Примерами крупных внутренних инцидентов ИБ являются [2, 3]:
- утечка информации о банковских картах из компании Heartland Payment Systems (январь 2009 года);
- утечка персональных данных о 30 млн. клиентов из компании Deutshe Telecom (август 2008 года);
- мошенничество с кредитными картами, реализованное внутренними сотрудниками регионального медицинского центра им. Джона Хопкинса (март 2009 года);
- мошенничество с кредитными картами, реализованное внутренним сотрудником фирмы Revenue Enterprices (декабрь, 2008 года);
- утечка информации о неблагонадежных заемщиках банка «Росбанка» (сентябрь, 2006 год);
- утечка персональных данных о 2 млн. абонентов компании «Мобильная Цифровая Связь» (сентябрь, 2006 год).

Ряд практических исследований показывают, что лишь около 30% сотрудников современного предприятия не имеют серьезных проблем. Остальные 70% являются проблемными сотрудниками, нарушающими корпоративные правила обеспечения информационной безопасности или склонными к таким нарушениям. Инсайдерские угрозы поэтому являются особо серьезными для современных предприятий и государственных структур. В связи с этим подбор надёжных, лояльных и компетентных людей для работы на критичных должностях является одной из основных задач любого работодателя. Последствия ошибки из-за некачественного подбора персонала в плане информационной безопасности трудно переоценить.

Одним из эффективных методов проверки внутренних сотрудников является использование специализированных устройств: детекторов лжи или полиграфов [1, 4].

При проведении кадровых проверок с использованием полиграфа выделяют следующие их виды:
- скрининговые проверки нанимаемого персонала;
- периодические проверки;
- проверки увольняемого персонала;
- служебные расследования;
- проверки в случае сделок с повышенной степенью риска.

Скрининговые проверки нанимаемого на работу персонала

Данные проверки используются для определения возможных рисков, связанных с наймом новых сотрудников, а также возможностью сокращения затрат, обусловленных некомпетентностью нанимаемого персонала. Здесь, как правило, определяют следующие характеристики нанимаемого персонала:

- некомпетентность в делах по работе, постоянные опоздания, хроническое забывание;
- нерегулярное или постоянное употребление спиртных напитков и различных видов наркотиков;
- выявление возможных нарушений закона, их тяжести и отношение сотрудника к своим деяниям;
- азартные игры на денежные суммы, способные привести к кражам и хищениям на предприятии;
- хищения на рабочем месте — фальсификация документов, изменение смет.

С помощью детектора лжи можно выявить, как работал сотрудник на прошлом месте работе. Определить, совершал ли он противоправные действия или нет.

В итоге возможно:

- определить замыслы кандидата, устраивающегося на работу;
- спрогнозировать поведение нового работника на рабочем месте;
- узнать все о рабочем прошлом кандидата;
- выявить лучших кандидатов на должность.

Периодические проверки

Данные проверки используются для осуществления контроля над сотрудниками, определения хищений финансовых ресурсов и товаров компании, выявления дополнительных доходов, получаемых при использовании служебного положения. В данном случае существует возможность определить факты:

- хищения товаров или информации;
- сотрудничества сотрудников с конкурентами;
- получения взяток/откатов;
- несерьезного отношение к своим служебным обязанностям;
- пользования служебным положением в корыстных целях;
- преднамеренного выявления действий, подрывающих работу компании.

В итоге данные проверки удерживают персонал от недостойного поведения, так как одно только знание об обязательных периодических проверках на полиграфе в значительной степени дисциплинирует сотрудников.

Проверки увольняемого персонала

Данные проверки позволяют предотвратить утечку информации, узнать мотивы увольняемого сотрудника. В данном случае существует возможность предотвратить:

- хищение коммерческой информации;

Занятия с курсантами по программе «Компьютерные полиграфные системы» в КНИТУ-КАИ

- шантаж компании;
- передачу закрытой информации конкурентам.

В итоге пресекаются попытки уволенного сотрудника рассекречивать или передавать третьим лицам конфиденциальную информацию о компании.

Служебные расследования

Данные проверки позволяют выявить кражи и хищения сотрудников, использование служебного положения в своих корыстных целях. В данном случае существует возможность:

- узнать, совершалась ли незаконная деятельность, сузить круг возможных подозреваемых;
- выяснить участников незаконной деятельности и их сообщников;
- выявить роль каждого исполнителя и добиться признательных показаний.

В итоге определяется виновный сотрудник и снимаются подозрения с других сотрудников.

Проверки в случае сделок с повышенной степенью риска

В данном случае осуществляется проверка сотрудников в ситуациях, связанных с передачей больших финансовых ресурсов (деньги, ценные бумаги, кредит) из рук в руки.

Особенно эффективны полиграфные проверки на тех предприятиях, где безопасность и успешность работы во многом зависит от лояльности сотрудников. По сути, полиграф можно эффективно использовать как средство повышения эффективности деятельности предприятия.

Таким образом, в настоящее время для современных предприятий и государственных структур значительную актуальность приобретает подготовка профессиональных кадров для работы на компьютерных полиграфах. Актуально осуществление такой подготовки (переподготовки) кадров на базе образовательных учреждений с привлечением ведущих специалистов-полиграфологов, а также специалистов силовых ведомств.

На кафедре систем информационной безопасности Казанского национального исследовательского технического университета им. А. Н. Туполева — КАИ реализуется программа дополнительного профессионального образования «Компьютерные полиграфные системы». Обучение по данной программе реализуется в объеме 248 часов в течение 5 недель с отрывом от производства. Общий объем учебной нагрузки — 54 часа в неделю, включая: лекционные и практические занятия, самостоятельную работу, контроль знаний (экзамен). По окончании обучения выдается свидетельство о повышении квалификации государственного образца.

Цель обучения — обеспечить слушателей теоретическими и практическими навыками проведения психофизиологических исследований на компьютерных полиграфах.

Категория слушателей:

- служащие государственных и негосударственных учреждений;
- сотрудники правоохранительных органов.

В результате реализации программы обучаемые **должны иметь представление**:

- о способах и методах проведения психофизиологических исследований;

знать:

- естественно-научные основы проведения психофизиологических исследований (ПФИ);
- специальную терминологию;
- правовые основы проведения ПФИ;
- организационные требования к проведению ПФИ;
- характеристики технических средств, используемых при проведении ПФИ;
- методические основы проведения ПФИ;
- специфику формулирования выводов по результатам проведения ПФИ.

уметь:

- адекватно ситуации оценивать целесообразность и возможность проведения ПФИ в целях разрешения поставленных вопросов;
- использовать различные методики проведения ПФИ, методические основы производства ПФИ;
- применять специфику формирования выводов по результатам проведения ПФИ;
- учитывать в ходе проведения ПФИ индивидуально-психологические особенности обследуемого;
- составлять справку по результатам ПФИ;
- работать с техническими средствами, используемыми при проведении ПФИ.

К проведению занятий привлекаются ведущие специалисты-полиграфологи, а также специалисты силовых ведомств, в том числе МВД по РТ.

Практические занятия проводятся на базе кадровых агентств Казани, а также на базе МВД по Республике Татарстан.

В 2010–11 годах на базе кафедры систем информационной безопасности КНИТУ-КАИ было подготовлено более 20 специалистов-полиграфологов — сотрудников силовых органов, служащих государственных и негосударственных учреждений.

Еще раз отметим, что цену ошибки из-за некачественного подбора сотрудников трудно завысить. В силу этого профессиональная подготовка специалистов-полиграфологов становится все более актуальной.

Литература:

1. В. А. Варламов, Г. В. Варламов, Н. М. Власова, И. С. Зубрилова, М. Б. Котомин. Углубленные кадровые проверки. М.: Группа компаний Русичи, 2003.
2. Инсайдерские угрозы в России 2009 [электронный документ].— Perimetrix, 2009. (www.perimetrix.ru).
3. Скиба В. Ю., Курбатов В. А. Руководство по защите от внутренних угроз информационной безопасности. СПб.: Питер, 2006.
4. Варламов В. А. Детектор лжи. М.: ПЕР СЭ-Пресс, 2004.