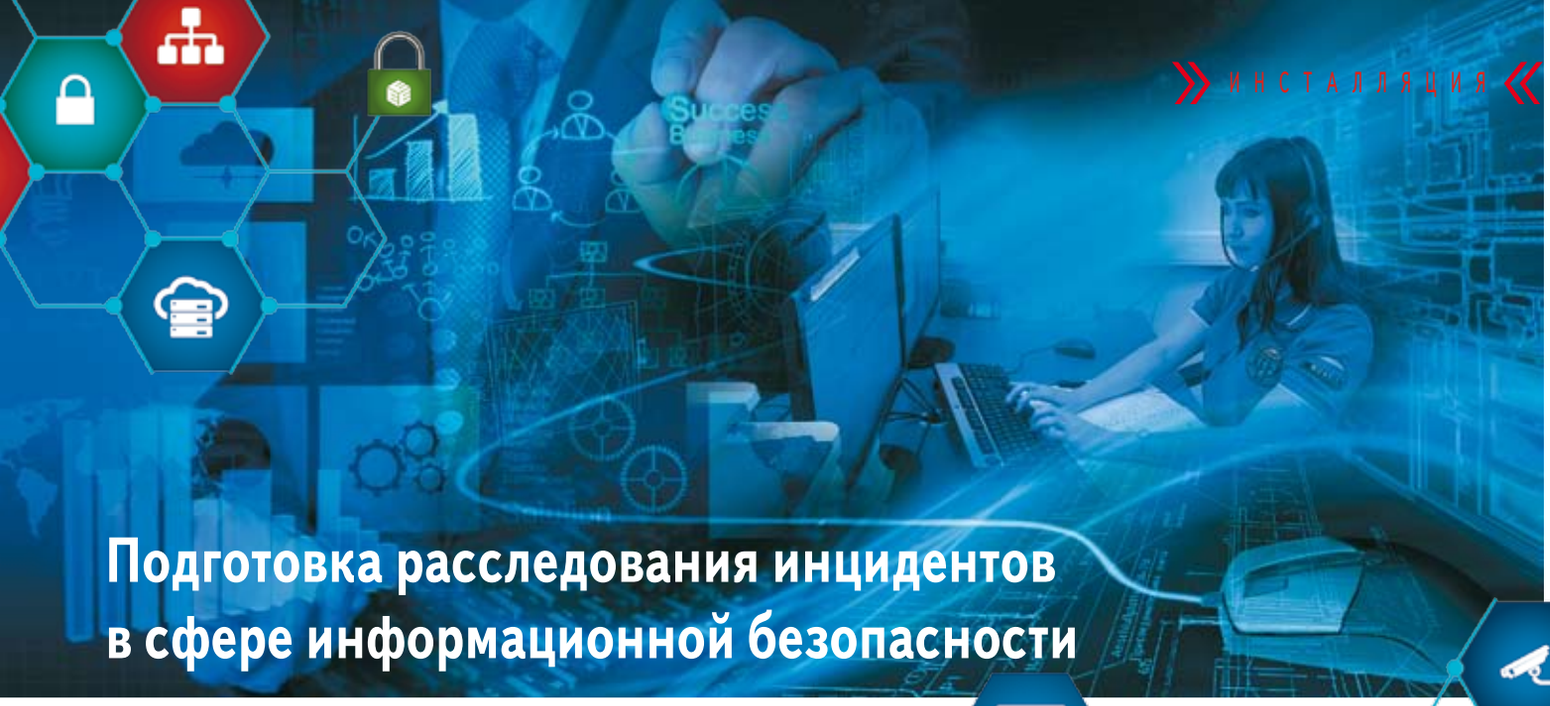


Подготовка расследования инцидентов в сфере информационной безопасности

Игорь СОБЕЦКИЙ,
завкафедрой экономической безопасности учебного центра «Информзащита»

«Он отправился в буфет покупать себе билет, а потом помчался в кассу — покупать бутылку квасу».

Попытка реализации плана, не проверенного на предварительной тренировке

Практика показывает, что руководители многих российских компаний твердо уверены, что уж с их-то бизнесом ничего дурного случиться не может. Нанят специалист по информационной безопасности (позитивный, идеально работающий в команде, обучался своему делу аж целых 72 часа, зарплата — 40 000 руб.), утвержден бюджет (на год запланировано 200 000, в феврале начали конкурс на закупку, к декабрю подведем итоги), утверждены нормативные документы по безопасности (специалист всю ночь печатал) — чего же еще желать? Всё будет в полном порядке. Поэтому планы реагирования на инциденты информационной безопасности либо отсутствуют в принципе, либо составлены, что называется, «на отвали». Когда же инцидент все-таки случается, попытки восстановить работоспособность системы подозрительно напоминают суету в горящем муравейнике. Провести же полное расследование инцидента и защитить интересы компании оказывается практически невозможно.

Одной из главных причин такой ситуации является неочевидность большинства инцидентов. Вмешательство в систему банковского обслуживания может оставаться незамеченным неделями, пока на счете компании не скопится привлекательная для мошенников сумма. Воровство конфиденциальных данных проявляется только в снижении доходов компании. Ну а в уничтожении важных документов виноват исключительно туповатый пользователь. В результате ни руководство компании, ни специалист по безопасности (если он вообще есть в штате) могут даже не подозревать о каких-то инцидентах.

В условиях тотального антикризисного сокращения штатов существенно выросла нагрузка на рядового бизнес-пользователя. Поэтому многие работники просто не имеют возможности тратить драгоценное время на взаимодействие со специалистом по безопасности. Прекращать работу, дозваниваться до специалиста, ждать, пока тот что-то сделает? А на подходе дедлайн, а этот специалист мою работу за меня делать не будет. И вместо информирования об инциденте работник отчаянно пытается его скрыть, выступая невольным пособником хакеров. Тем более практически у любой проблемы есть простое и очевидное для работника неправильное решение. Не работает сеть? Не беда, все данные можно перетащить на flash-накопителе. Нет доступа в интернет? Не беда, вместо корпоративного канала подключимся через смартфон. В системе торчат какие-то левые и сомнительные платежки? Ну, так быстренько сотрем их, а то еще на меня подумают.

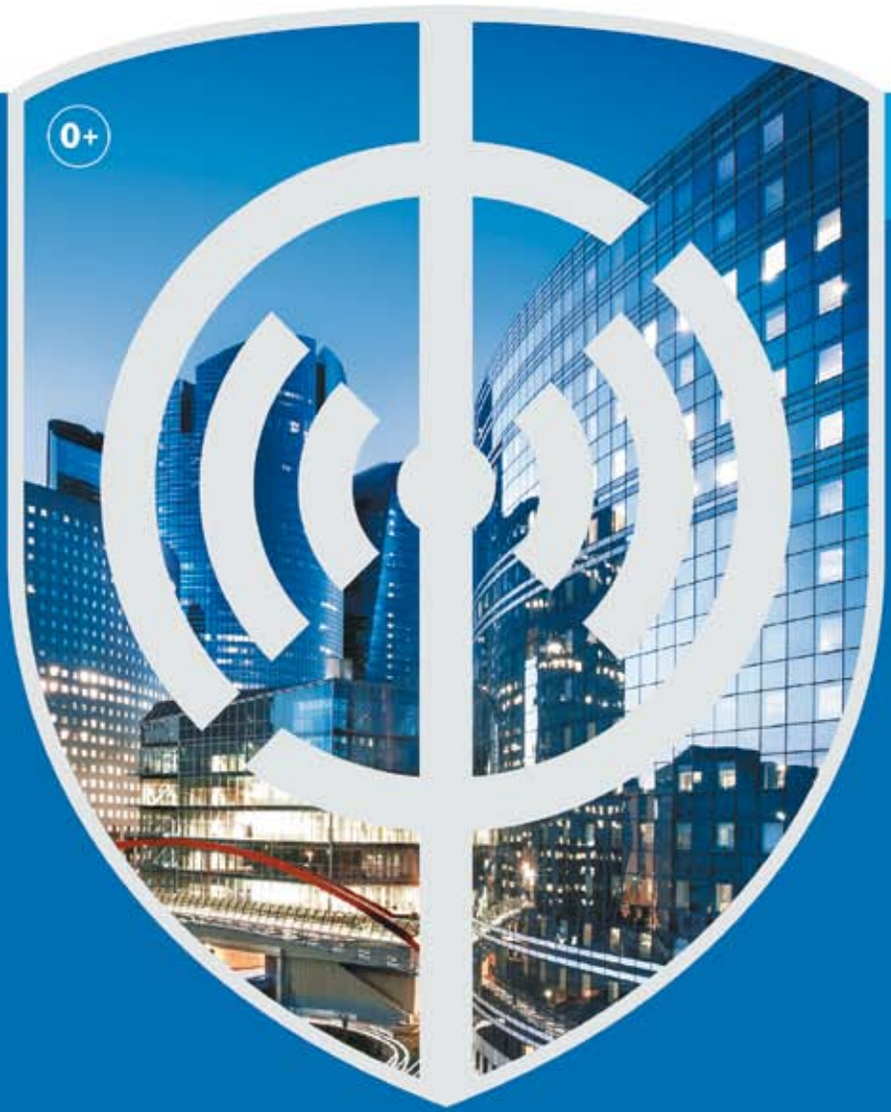
Для того чтобы избежать негативного развития событий, подразделение информационной безопасности компании еще в спокойной обстановке должно подготовить четкий план расследования инцидентов. Желательно, чтобы такой план предусматривал как минимум два класса мер: технические и организационно-административные. К техническим относятся меры по обеспечению сохранения в автоматическом режиме уликовых данных, а также защите их от неправомерного удаления и/или модификации. Организационно-административные меры включают обеспечение доказательственного значения собранных материалов и своевременной защиты интересов компании. Очень важно понимать, что меры обоих классов могут эффективно сработать только вместе. Применение мер только одного из классов станет лишь бессмысленной тратой времени и средств.

Организационно-административные меры как минимум должны включать следующие шаги:

- Объявление всей существенной информации коммерческой тайной. В отсутствие на предприятии режима коммерческой тайны любые попытки обязать работников соблюдать какие-либо ограничения на распространение служебной информации лишены законного основания. Соответственно, вся информация компании де-юре является общедоступной, а наложение на излишне разговорчивых работников любых взысканий в дальнейшем легко может быть отменено в суде.
- Внесение соответствующих изменений в правоустанавливающие документы организации. В уставе организации — особенно ПАО — должны быть перечислены все виды деятельности, на которые компания получила или планирует получать лицензии. В противном случае деятельность, например, по технической защите конфиденциальной информации может быть признана незаконной.

26-я Международная выставка
технических средств охраны
и оборудования для обеспечения
безопасности и противопожарной защиты

securika St. Petersburg



Санкт-Петербург

7–9 ноября 2017

КВЦ «ЭКСПОФОРУМ»

Технические средства обеспечения безопасности

Системы охранного телевидения и наблюдения

Системы и средства обеспечения пожарной безопасности

Системы связи и оповещения

Технические средства и программное обеспечение для защиты информации

Организаторы:

primexpo

ITE

+7 (812) 380 6009/00
security@primexpo.ru
securika-spb.ru

Забронируйте стенд
securika-spb.ru

✔ Разработка и утверждение пакета организационно-распорядительных документов. В компании должен быть создан и утвержден руководством полный набор нормативных документов по защите коммерческой тайны, банковской тайны (для банков) и тайны связи (для операторов связи), а также персональных данных.
Работники должны быть ознакомлены с этими документами под роспись.

✔ Внесение соответствующих изменений в трудовые контракты всего персонала. На работника могут быть возложены только те обязанности, которые прописаны в его трудовом договоре. Поэтому необходимо убедиться, что типовые договоры с работниками включают в себя все обязанности по обеспечению режима конфиденциальности и ответственность за их неисполнение. Договоры с работниками, заключенные до введения в компании режима коммерческой тайны, предстоит переоформить.

✔ Практическая реализация мер по защите информации. Необязательно сразу же принимать чрезвычайные меры, включая закупку дорогостоящего оборудования. Но требуется предпринять хотя бы какие-то действия, которые потом подтвердят, что режим коммерческой тайны в компании действовал не только на бумаге. Например, табличка на дверях серверного помещения «Посторонним вход запрещен» тоже является одной из таких мер.

Для оперативной коммуникации с государственными органами в случае посягательства на корпоративные информационные ресурсы очень желательно назначить специального ответственного работника. Иными словами, начальнику подразделения информационной безопасности или же начальнику службы безопасности компании должно быть вменено в обязанность оперативное обращение в государственные правоохранительные органы, если они обнаружили, что действиями злоумышленников компании нанесен ущерб. Такому ответственному работнику должна быть выдана доверенность на право представительства интересов компании в государственных органах, а также заверенные копии всех правоустанавливающих документов компании.
Если в компании до сих пор отсутствуют системы внутреннего видеонаблюдения и СКУД (система контроля и управления доступом в помещения), целесообразно подумать о развертывании таких систем. В ряде случаев собранная с их помощью информация играет решающую роль в доказывании вины злоумышленников и защите интересов компании. Наконец, во избежание споров о размере нанесенного ущерба весьма желательно произвести предварительную оценку стоимости всех информационных ресурсов компании. Эту работу могут выполнить сторонние специалисты, например, из страховой или аудиторской компании. Данная мера существенно облегчит доказывание размера ущерба и его последующее возмещение в случае выведения этих ресурсов из строя.
Действующий в компании регламент расследования инцидентов информационной безопасности должен предусматривать как минимум следующие меры:

✔ Определение лица или лиц, в чьи обязанности входит расследование инцидентов информационной безопасности. При необходимости предусматривается формирование постоянных штатных или нештатных групп в филиалах компании. Также может быть предусмотрено предварительное заключение договора со сторонним подрядчиком по расследованию инцидентов.

✔ Быстрое выяснение размера ущерба. О необходимости предварительной оценки стоимости информационных ресурсов компании уже говорилось выше.

✔ Определение целесообразности обращения в государственные правоохранительные органы. Регламент должен содержать четкие критерии для принятия решения о подаче заявления в государственные правоохранительные органы. Такими критериями могут быть, например, размер нанесенного ущерба, размер потенциального ущерба, вероятность повторения аналогичных действий, последствия для деловой репутации компании, возможность возмещения всего или части ущерба за счет страховой компании или выявленных злоумышленников и т. д.

✔ Возмещение ущерба. Прописываются меры по возмещению нанесенного компании ущерба, включая обращение в суд в порядке гражданского судопроизводства, закрепление доказательств для гражданского процесса с помощью нотариуса и т. д.

✔ Интеграция расследования инцидентов в основные бизнес-процессы. Чтобы расследование инцидента не мешало нормальному функционированию компании, регламент должен предусматривать меры по недопущению конфликта интересов работников подразделения безопасности и бизнес-пользователей. Сюда могут входить использование резервного оборудования или носителей информации, временное увеличение численности бизнес-подразделений (например, за счет привлечения части работников к сверхурочной работе), проведение мероприятий по расследованию инцидентов наименее «травматичным» для бизнеса способом (например, обследование компьютеров в ночное время).
Превентивные меры технического характера могут включать:

✔ Контроль трафика в локальной сети (маршрутизация с помощью управляемого коммутатора, использование системы обнаружения атак).

✔ Контроль интернет-трафика (использование межсетевых экранов с протоколированием соединений, а также хостовых DLP-систем). Собранная с их помощью информация в большинстве случаев дает возможность детального восстановления развития инцидента.

✔ Контроль активности пользователей (кейлоггеры, агентские DLP-системы).
Использование данных средств существенно упрощает расследование инцидентов, вызванных недобросовестными действиями бизнес-пользователей.

✔ Контроль обхода периметра (средства защиты от несанкционированного доступа, регулярный аудит лог-файлов). Выявляются попытки доступа бизнес-пользователей к внешним сервисам в обход защищенного корпоративного канала.

✔ Особый контроль критически важных рабочих мест (например, платежные подсистемы). Минимизируется возможность успешной атаки на платежную подсистему, и обеспечивается быстрое выявление злоумышленника.

✔ Организация юридически надежного хранения лог-файлов с целью обеспечения использования их в качестве доказательств в гражданском или уголовном процессе. Для этого могут быть использованы удостоверение собранных лог-файлов квалифицированной электронной подписью, хранение резервных копий у третьей стороны (например, у нотариуса), специализированное программное обеспечение и т. д.

✔ Подготовка специальных автоматизированных рабочих мест сбора и анализа доказательств. Если принято решение отказаться от услуг сторонних подрядчиков, то для сбора и анализа данных при расследовании инцидента целесообразно заранее приобрести специальные программно-аппаратные комплексы для компьютерной криминалистики (форензики). При этом работники подразделения информационной безопасности, а в отдельных случаях и подразделения информационных технологий должны пройти обучение работе с такими комплексами. Разумеется, такая мера экономически оправданна лишь для крупных компаний с большим числом филиалов.

В целом для успеха расследования инцидентов информационной безопасности применяемые технические меры должны обеспечивать сбор наиболее полной информации о сетевом трафике, действиях пользователей корпоративной информационной системы «поведения» оборудования. Организационно-административные меры обеспечивают законность применяемых технических решений, доказательственную ценность собранной с их помощью информации, а также правовую и практическую возможность компенсации нанесенного компании ущерба.