Интеллектуальная система информационной безопасности

А. А. СТЕПАНЕНКО, директор по развитию бизнеса компании «Информзащита»

Интеллектуальная система управления информационной безопасностью (ИСУИБ) повысит надежность функционирования информационных систем ОАО «РЖД», позволит эффективно контролировать их защищенность, своевременно выявлять нарушения, оперативно реагировать на инциденты, в кратчайшие сроки устраняя их последствия.

Любая информационная система не застрахована от возникновения инцидентов информационной безопасности (ИБ), приводящих к сбоям в работе, компрометации корпоративных IT-ресурсов и пр. Степень ущерба и время восстановления информационных систем напрямую зависят от скорости реагирования.

Важнейшими задачами службы ИБ являются своевременное выявление инцидентов, адекватное реагирование на них, обеспечение снижения ущерба за счет локализации инцидентов и исключение их повторения. Для этого сотрудники служб ИБ обрабатывают огромный массив информации, поступающей от систем ИБ, управления базами данных, операционных систем, сетевого оборудования, бизнес-приложений и т. п. Важные события, требующие внимания и немедленного вмешательства, не всегда своевременно выявляются из общего информационного потока. Более того, из-за отсутствия заранее проработанных процедур реагирования на инциденты задерживается устранение их негативных последствий.

Эта ситуация отражена в отчете «2012 Data Breach Investigations Report» компании Verizon Business. Эксперты Verizon Business RISK Team на основе изучения истории возникновения, расследования и устранения последствий 875 инцидентов, зафиксированных в 2011 г., установили, что:

- 85 % действий, приведших к инциденту, совершены менее чем за один час;
- 2 % инцидентов выявлены в течение одного дня, а 85 % — не ранее чем через одну неделю после их совершения;
- 10 % обнаруженных инцидентов обработаны в течение одного дня; реагирование на 70 % инцидентов начиналось в срок от нескольких дней до нескольких недель (см. *рис.*).

Изучение и обобщение успешного опыта решения данной задачи позволяет создать систему ИБ, способную оперативно реагировать на события и адаптироваться к изменяющимся условиям.

Такая система позволяет увеличивать интеллектуальность корпоративной системы обеспечения ИБ, а именно:

- автоматизировать всю черновую работу по контролю над состоянием информационной системы и выявлению инцидентов;
- максимально автоматизировать реагирование на известные угрозы и типовые инциденты;
- обеспечить предоставление необходимой информации для быстрого принятия решений, связанных с «нетипичными» инцидентами и новыми угрозами.

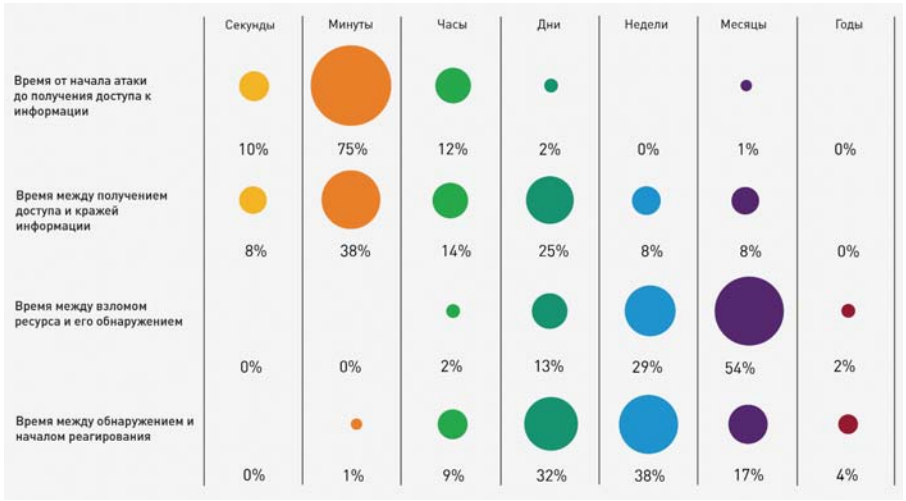
Также система дает возможность совершенствовать процессы управления систем ИБ и выстраивать взаимодействие всех заинтересованных сторон.

Инициированные департаментом безопасности ОАО «РЖД» работы по проектированию и внедрению интеллектуальной системы управления информационной безопасностью направлены на использование лучшего мирового опыта в этой области.

В ближайшей перспективе выполнение этих проектов обеспечит:

- возможность непрерывного контроля защищенности всех информационных систем ОАО «РЖД»;
- способность выявлять инциденты в реальном времени;
- качественный анализ выявленных инцидентов и своевременное реагирование на них;
- снижение размера ущерба и времени восстановления информационной системы после инцидентов;
- повышение надежности функционирования информационной системы за счет мер по предотвращению инцидентов.

В дальнейшем ИСУИБ может применяться для интеграции с используемыми приложениями с целью оперативного выявления инцидентов в бизнес-процессах (АСУ «Экспресс», ЭТРАН, АСУФР и др.) и со специализированными АСУ ТП ОАО «РЖД» для обнаружения попыток вмешательства в их работу, а также для подключения средств контроля подозрительных транзакций, чтобы оперативно выявлять мошенничество при продаже железнодорожных билетов.



Длительность периодов между этапами инцидента (доля от общего числа расследованных инцидентов, связанных с утечкой данных)