Таким образом, факт выполнения неопределенной операции, являясь большой проблемой систем обнаружения вторжений, может служить событием-триггером, по которому целесообразно проводить переобучение системы обнаружения вторжений. Тогда переобучение системы обнаружения вторжений можно выполнять при следующих условиях:

1) если пользователь выполнил запрещенную политикой безопасности операцию: соответствующую аномальному поведению (система обучалась нормальному поведению) или атаку (система обучалась атакам);

2) если пользователь выполнил неопределенную операцию: неспецифицированную как нормальную операцию политикой безопасности или операцию, разрешенную политикой безопасности, которая может быть выполнена при вторжении.

СПИСОК ЛИТЕРАТУРЫ:

1. *Zegzhda P. D., Kort S. S.* Host-based Intrusion Detection System: model and design features // The Forth International Conference, MMM-ACNS 2007. St. Petersburg, Russia. September 13–15. 2007. Proceedings. Communications in Computer and Information Science (CCIS). Springer. Vladimir Gorodetsky, Igor Kotenko, Victor Skormin (Eds.). Vol. 1. 2007. P. 340–345.

А. Б. Костина

ПРАКТИЧЕСКИЕ АСПЕКТЫ УПРАВЛЕНИЯ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ни одна самая совершенная мера по снижению рисков ИБ не может полностью предотвратить возникновение в информационной среде событий, потенциально несущих угрозу бизнесу организации. Неготовность организации к обработке подобного рода ситуаций может существенно затруднить восстановление нормального функционирования организации и потенциально усилить нанесенный ущерб.

Справиться с данной проблемой может процесс управления инцидентами ИБ. Именно во время работы разных этапов этого процесса проявляются конкретные уязвимости активов организации, обнаруживаются следы атак и вторжений, проверяется работа защитных механизмов, эффективность работы процессов обеспечения ИБ и управления ею.

Внедрение процесса управления инцидентами ИБ на практике может быть связано с рядом проблем, в частности, в организации необходимо наличие четкого определения события и инцидента ИБ. На данный момент существует большое количество международных документов, регламентирующих терминологию данного процесса. Однако, приводимых в них определений этих терминов недостаточно, так как в зависимости от специфики деятельности организации, от ее масштаба, а также от общего уровня зрелости организации по ИБ значения понятий «событие ИБ» и «инцидент ИБ» могут варьироваться.

Важным аспектом успешного внедрения процесса управления инцидентами ИБ является введение классификации инцидентов ИБ. От правильно выбранной классификации зависит то, насколько эффективен будет процесс в целом.

Также особое значение имеет осведомленность пользователей о процессе управления инцидентами ИБ, их вовлеченность в процесс и ответственность в рамках процесса управления инцидентами информационной безопасности.

СПИСОК ЛИТЕРАТУРЫ:

1. ISO/IEC 27001:2005. Information security management system. Requirements. 2005–15–10.
2. ГОСТ Р ИСО/МЭК 27001–2006. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. 2006–27–12.

С. Д. Кулик, А. В. Жижилев

СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВАЛЮТНОГО РЫНКА

Выполненные исследования [1, 2, 3] показывают, что различные некорректные действия в сфере финансов [4, 5, 6, 8] возникают именно там, где сконцентрированы большие денежные средства и есть важная информация, связанная с этими средствами. На рынке FOREX (Foreign Exchange Market) в рамках условий маржинальной торговли участниками торговли реализуются специфические валютные спекулятивные операции с опорой на текущую информацию о рынке, макроэкономический анализ, технический анализ и т. п. На практике такая операция сопровождается актом обмена взаимной информацией (по соответствующим каналам связи), необходимой для принятия решений. В случае если эта информация подвергается искажению при передаче по каналам связи, может искажаться и результат самой коммерческой операции. Выполненные искажения коммерческой операции являются целью злоумышленника и направлены в итоге на разорение одного из участников, получающего искаженную информацию, по которой он принимает свои неправильные решения.

Трейдер при торговле на FOREX для получения (передачи) информации использует специальное программное обеспечение (ПО), например нейросетевое ПО для прогнозирования состояния финансового рынка (ФР). Трейдер, получив необходимую информацию, принимает ответственные торговые решения. Важно отметить, что существуют [8] обучающиеся системы принятия статистически оптимальных торговых решений (СОТР) на ФР.

На практике, принимая решение по искаженной информации, трейдер может потерять вложенные средства. При торговле на рынке FOREX выполняемые трейдером операции далеко не безопасны для его денежных средств. Под безопасной операцией понимается такая операция, которая обеспечивает требуемый уровень получения прибыли. Такая операция является устойчивой (т. е. эффективной) к воздействиям, искажающим информацию, передаваемую между участниками рынка и затем используемую ими для принятия решения [1]. Сами методы защиты информации, обеспечивающие работу алгоритмов с учетом возможных искажений информации, будем назвать эффективными [1]. На рынке FOREX возможны искажения информации, передаваемой по каналам связи [6, 8]. Анализ этих искажений позволил сделать вывод, что все искажения информации, в конечном итоге, направлены на то, чтобы трейдер (т. е. инвестор) в процессе