УДК 519.876

Н.М. Бобович

ОБ ОЦЕНКЕ ЭФФЕКТИВНОСТИ ЗАЩИТЫ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

Основными задачами исследования путей повышения устойчивости функционирования критически важных объектов информатизации (КВОИ) является: выявление всех возможных способов и средств снижения потерь и сохранения работоспособности (производительности) КВОИ, оценка их эффективности и разработка рекомендаций по практическому использованию с учетом конкретных условий размещения и деятельности КВОИ и его структурных подразделений.

Совокупность всех возможных путей (способов, мероприятий), принципиально способных изменять устойчивость функционирования, будем называть областью управления устойчивостью функционирования. Систему мероприятий, проводимых для повышения устойчивости функционирования, в дальнейшем будем называть системой защиты.

Для оценки эффективности защиты целесообразно использовать два обобщенных критерия, соответствующие двум показателям устойчивости:

1. Приращение сохраняемой производительности за счет осуществления защиты:

$$Э_I = \Delta I = I^з_{\max}(B^з) - I_{\max}(B).$$

2. Приращение деструктивного воздействия, необходимого для обеспечения заданного снижения производительности:

$$Э_B = \Delta B = B^з(I_з) - B(I_з).$$

Верхним индексом (з) обозначены параметры, соответствующие их значениям при осуществлении защиты.

Помимо обобщенных критериев могут использоваться частные критерии, соответствующие конкретным направлениям повышения устойчивости, например, снижение вероятности деструктивного воздействия, уменьшение потерь КВОИ и т. д. Частные и обобщенные критерии связаны между собой функциональными зависимостями.

Для оценки экономической эффективности защиты целесообразно использовать три категории оценок:

реальная деятельность КВОИ за счет сохраняемых защитой возможностей КВОИ;

реальный экономический эффект, выражающийся в снижении бюджета на повышение эффективности использования КВОИ;

условный экономический эффект, определяемый по прогнозу на рассматриваемый период времени, как экономия информационного ресурса КВОИ и перерасход деструктивных средств злоумышленником для исключения эффекта защиты.

Третья категория оценки является основной на этапе исследования, вторая может возникнуть при совершенствовании первоначальных решений и корректировки планов, первая возможна после выполнения хозяйственных восстановительных работ.

Экономия информационного ресурса определяется через сохраняемую защитой производительность ΔI и себестоимость работ *(c)*:

$$\Delta C_I = \int_0^\infty c\Delta I(t)dt.$$

Перерасход средств для исключения эффекта защиты может быть принят в первом приближении равным стоимости дополнительного числа активных деструктивных средств и мощностей, необходимых для поражения структурных элементов КВОИ:

$$\Delta C_B = C\left(B^3\right) - C\left(B\right).$$

Условный экономический эффект с учетом расходов на защиту Сз необходимо принимать равным его минимальному значению при всех возможных вариациях деструктивных воздействий:

$$Эс = \min(B)\{\Delta C_I + \Delta C_B - C_з\}.$$

Предлагаемый подход оценки экономической эффективности защиты может быть использован в процессе проектирования и модернизации сложных систем, к которым относится система защиты КВОИ, когда не удается заранее исследовать, промоделировать и рассчитать основные характеристики и логику функционирования КВОИ адекватно реально протекающим процессам.

УДК 519.876

Н.М. Бобович, Д.А. Петрович

О ПРОГНОЗИРОВАНИИ ЗАЩИЩЕННОСТИ ОБЪЕКТА ИНФОРМАТИЗАЦИИ

При разработке системы мероприятий защиты объектов информатизации (ОИ) от деструктивных воздействий возникает задача прогнозирования результатов воздействий противоборствующей стороны

по ОИ, который подлежит защите. В настоящее время эта задача для объектов со сравнительно простыми функциональными связями между технологическими звеньями (элементами в звеньях) решается с использованием методов, разработанных применительно к выбору совокупности средств для воздействия по объектам противоборствующей стороны.

Основной исходной предпосылкой этих методов является предположение о полной определенности сведений относительно средств воздействия и недостаточной достоверности сведений о цели воздействия. При решении обратной задачи исходные предпосылки и в равной степени и задачи расчета коренным образом меняются. Прежде всего метод решения этой задачи должен быть чувствителен к размещению объектов на местности, их устойчивости к поражающему деструктивному воздействию, функциональным связям между элементами объекта и т. д. Отсюда следует, что основные сведения о цели должны быть известны и введены в алгоритм расчета. В то же время данные о внешнем воздействии на цель, а также ряд данных о цели (случайные отклонения от прочностных характеристик элементов цели, их ориентация относительно деструктивного воздействия и т. д.) не могут быть предсказаны точно.

Производительность объекта информатизации, определяемая оператором сопряжения последовательно-параллельной модели, будет представлять собой функцию, содержащую операции «сумма» и «выбор минимума».

При случайной вариации производительности элементов и подсистем статистические характеристики производительности объекта информатизации I = Ф(Ii) определяются методами расчета статистических характеристик функций случайных аргументов в рамках классической теории вероятностей.

Задача сводится к определению статистических характеристик вида

$$I_i = \sum_{j=1}^{m_i} I_{ij} \left(j = \overline{1, m_i} \right) \qquad (1)$$

$$I = \min_{(i)} \{ I_i \} \left(i = \overline{1, n} \right), \qquad (2)$$

где n – число технологических звеньев в системе;

m_i – число элементов, выполняющих (обеспечивающих выполнение) i -той технологической операции.

Математическое ожидание и дисперсия функций распределения «сложение» (1) и «минимум» (2) (для системы, состоящей их двух групп элементов) для случая нормального распределения определяются соотношениями, приведенным в (1).

Задача сводится к определению числовых характеристик производительностей, входящих в систему групп элементов и соответствующих корреляционных моментов.

УДК 343.8

П.Л. Боровик, В.А. Самойло

АКТУАЛЬНЫЕ МЕТОДОЛОГИЧЕСКИЕ ПОДХОДЫ К ДЕАНОНИМИЗАЦИИ ЛИЦ, СОВЕРШАЮЩИХ ПРЕСТУПЛЕНИЯ С ИСПОЛЬЗОВАНИЕМ КРИПТОВАЛЮТ

Анализ оперативно-следственной и судебной практики по делам о преступлениях, связанных с использованием криптовалют, свидетельствует, что одной из насущных проблем выявления и расследования соответствующих криминальных деяний является установление личности (идентификация) владельца публичного биткоин-адреса, с которого либо на который осуществлялась транзакция. Поскольку процесс создания криптокошелька в основном анонимен, а переводы с одного биткоин-адреса на другой не верифицируются, установить персональные сведения о лицах (IP-адрес, географическое местоположение, Ф.И.О. и пр.), участвующих в транзакции, традиционными средствами не представляется возможным.

В ходе изучения и обобщения специальной литературы, посвященной рассматриваемой проблематике [1–4], было установлено, что в основу практической деятельности по деанонимизации лиц, совершающих преступления с использованием криптовалют, может быть положен процесс привязки публичного биткоин-адреса к цифровому идентификатору пользователя или его IP-адресу. Исследование показало, что этот процесс может осуществляться с применением так называемых интерактивных, активных и пассивных методов (данное деление в некоторой степени условно, оно лишь демонстрирует степень активности субъекта оперативно-розыскной деятельности по отношению к объекту исследования).

Так, интерактивные методы деанонимизации владельца публичного биткоин-адреса могут быть реализованы с использованием социальной инженерии, позволяющей установить непосредственный контакт с владельцем с целью совершения им определенных действий или разглашения соответствующей информации. Такие методы подходят в основном для деанонимизации частично неизвестных владельцев биткоин-адресов в условной цепочке биткоин-транзакций.