Научно-методический аппарат обеспечения протокольной защиты информационно-телекоммуникационной сети

Дементьев Владислав Евгеньевич,
докторант, Военная академия связи им. С.М. Буденного,
подполковник

Проблема обеспечения информационной безопасности (ИБ) стоит в ряду первостепенных задач при проектировании информационно-телекоммуникационных сетей (ИТКС). Поскольку ИТКС является результатом конвергенции компьютерных и телекоммуникационных сетей, ее функционирование осуществляется в условиях воздействия некоторой совокупности информационных угроз, направленных на ее элементы и тем самым негативно влияющих на ее эффективность. В связи с этим важной задачей является обеспечение достаточной степени защищенности ИТКС в условиях проявления информационных угроз, для чего в свою очередь необходимо наличие адекватного аппарата, позволяющего оценить возможные методы и способы воздействия на ИТКС.

В ряду наиболее актуальных угроз, существенно влияющих на общий уровень защищенности ИТКС, стоят различные информационные воздействия (ИВ). По своей сути эти воздействия сводятся к эксплуатации общеизвестных принципов и способов обработки данных, т. е. протокольного взаимодействия между различными элементами сети. В общем виде протокол — это совокупность процедур, определяющих взаимодействие и обмен данными между устройствами, абонентами и уровнями ИТКС. Тогда протокольное воздействие — это заранее спланированное целенаправленное воздействие на протоколы информационного обмена, обмена данными, функционального и другого назначения через установление соединения или попытки установления соединения на уровнях эталонной модели взаимодействия открытых систем или других известных моделей Интернета с объектом данного воздействия.

Цель протокольного воздействия — организация канала утечки информации, модификация, уничтожение информационных ресурсов, блокирование (перевод во внештатный режим работы) системы защиты информации, а также изменение штатного функционирования ИТКС, приводящее к нарушению или блокированию информационного обмена.

В данном случае, когда речь идет о протокольной защищенности, мы говорим не о состоянии ИТКС, которое влияет на уровень ее защиты, а о некоторой совокупности признаков, наличие которых позволяет говорить о возможных ИВ на ИТКС. Наличие или отсутствие подобных ИВ определяется совокупностью информационных признаков, характерных для того или иного протокола ИТКС. Каждый из признаков обладает определенным уровнем информативности, по которому определяется степень опасности протокола для ИТКС. Таким образом, на первом этапе определяется совокупность критически важных информационных признаков и их степень информативности.

Кроме того, немаловажное значение имеет уровень ИТКС (в соответствии с уровнем ЭМВОС) и набор протоколов соответствующего уровня. Для определения априорной и апостериорной иерархичности ИВ в рамках методологического подхода проводится оценка важности уровней ИТКС и протоколов, соответствующих определенным уровням, что в дальнейшем позволит получить исходные данные для прогнозирования вероятностей воздействия на протоколы ИТКС.

В итоге полученные исходные данные используются для оценки протокольной защищенности ИТКС путем определения коэффициентов надежности и стойкости каждого протокола, участвующего в информационном обмене ИТКС, и формирования матриц защищенности, позволяющих спрогнозировать общий уровень защищенности ИТКС от протокольных воздействий.

В рамках разработанного научно-методического аппарата обеспечения протокольной защиты ИТКС рассматривается подход по определению вероятностей воздействия на ИТКС, который включает:

1. методику оценки информативности признаков ИТКС;
2. методику оценки комплексного информационного воздействия на протоколы ИТКС;
3. методику оценки протокольной защищенности ИТКС;
4. алгоритм модификации и идентификации признаков протокольных воздействий на ИТКС;
5. устройство программного изменения параметров протокола.

Каждая последующая методика использует исходные данные, полученные в результате расчетов по предыдущей методике. В общем виде научно-методический аппарат обеспечения протокольной защиты представлен на рис. 1.

Методика оценки комплексного информационного воздействия на протоколы ИТКС предназначе-

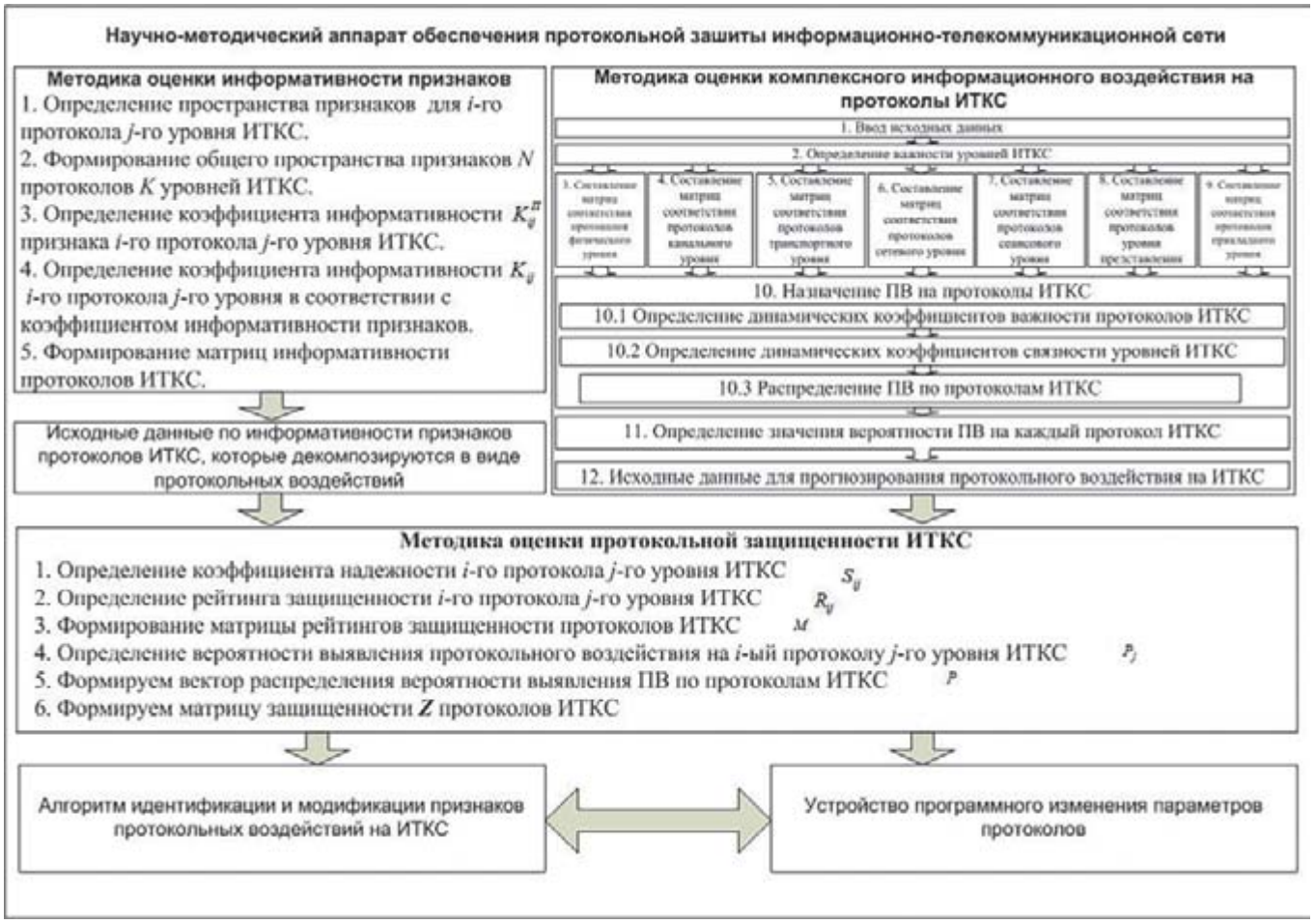

Рис. 1. Научно-методический аппарат обеспечения протокольной защиты ИТКС

на для прогнозирования распределения воздействий на протоколы ИТКС с учётом места и роли этих протоколов в информационном обмене, определения очерёдности воздействия на них и формирования исходных данных для обоснования мер защиты элементов и ИТКС в целом.

В основе данной методики лежит метод анализа иерархии и распределения ресурса защиты ИТКС [1, 2], которые используются для получения итоговых значений распределения вероятностей воздействия на протоколы ИТКС. В результате применения данной методики решена задача определения наиболее критичных протокольных воздействий (ПВ) для каждого протокола ИТКС.

Для нейтрализации опасных протокольных воздействий необходим их мониторинг, основу которого составляет Методика оценки информативности признаков протоколов ИТКС, предназначенная для формирования совокупного пространства признаков протокольных воздействий на ИТКС, распределения признаков в соответствии с уровнем их информативности, а также формирования матриц информативности протоколов в соответствии с признаками протокольных воздействий [3].

В основе данной методики лежит способ определения индивидуальных и типовых признаков протоколов ИТКС. В качестве примера рассмотрены некоторые признаки, полученные в результате анализа протоколов ИТКС и определены значения информативности индивидуальных и типовых признаков.

Для разработки мер защищенности ИТКС необходимо оценить ущерб от ПВ, для чего предлагается Методика оценки протокольной защищенности ИТКС, предназначенная для формирования промежуточных рейтингов стойкости и защищенности протоколов ИТКС и определения итогового рейтинга защищенности ИТКС от протокольных воздействий. Представленная методика использует в качестве исходных данных результаты расчетов, полученные по предыдущим методикам. Результаты расчета информативности признаков протоколов и защищенности ИТКС, полученные для исходных данных (рис. 2 и 3) и для случая, когда информативность признаков протоколов приведена к единому уровню, т. е. отсутствуют индивидуальные признаки и получен итоговый уровень защищенности ИТКС (рис. 4 и 5).

Для реализации на практике предлагаемого подхода был разработан алгоритм модификации идентификационных признаков протокольных воздействий на ИТКС, который реализован в рамках разработанного устройства программного изменения параметров протокола. Предполагается, что данное устройство будет размещено на всех элементах ИТКС, что позволит ор-

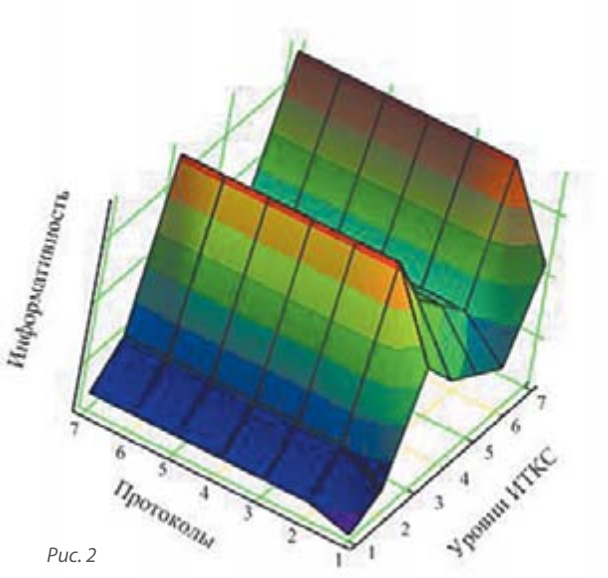

Рис. 2

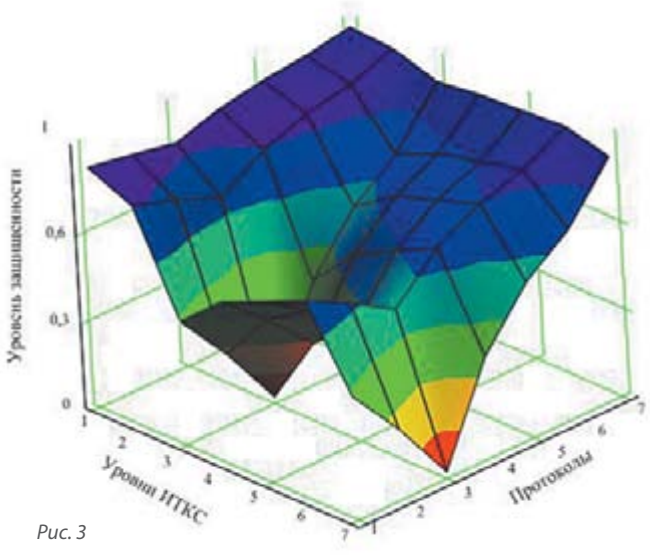

Рис. 3

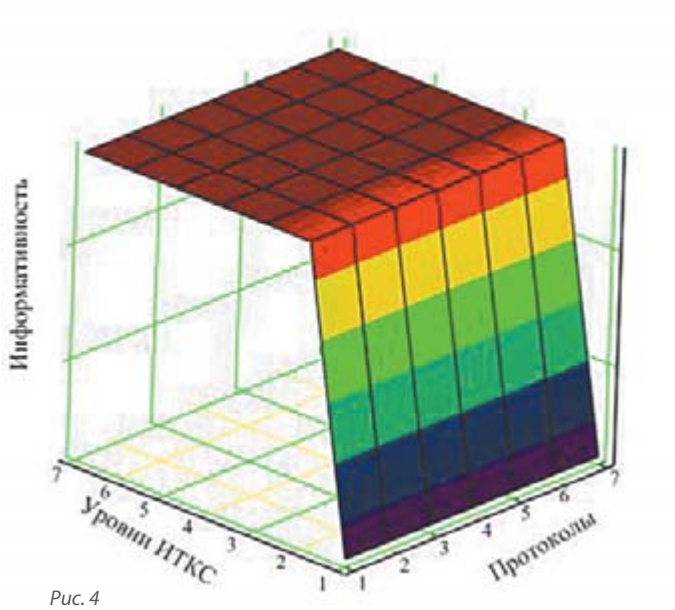

Рис. 4

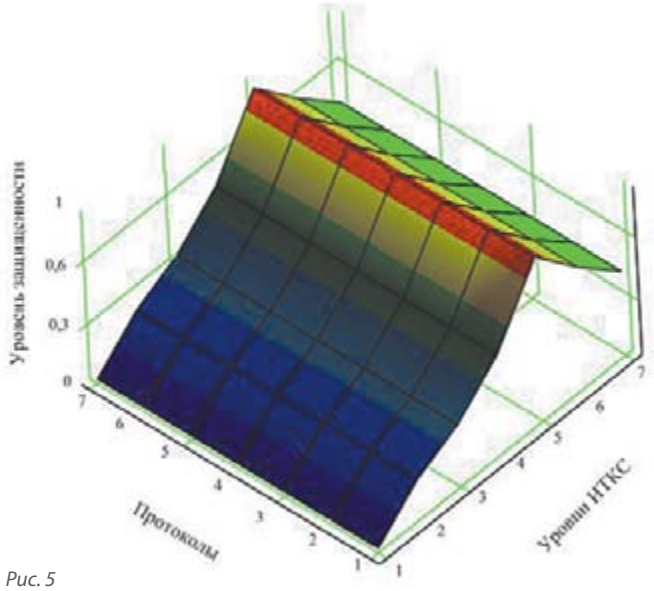

Рис. 5

ганизовать мониторинг параметров (признаков) протоколов ИТКС.

Таким образом, представленная совокупность методик, алгоритма и устройства представляют собой научно-методический аппарат обеспечения протокольной защиты ИТКС в условиях информационного противоборства (ИП). Однако современные системы защиты ИТКС не рассчитаны на внедрение предлагаемых решений.

Результаты анализа современных средств и методов защиты ИТКС показывают, что в них практически не затронуты возможности активного противодействия информационно-техническим воздействиям (ИТВ) в условиях ИП. Большинство известных подходов обнаружения и пресечения ИТВ не учитывают специфику функционирования самой ИТКС и решаемых ею задач. Практически отсутствуют комплексные методы и алгоритмы, на основе которых возможно построение средств обнаружения и пресечения ИТВ и взаимосвязанных процессов, протекающих в ходе ИП. Недостаточно проработаны методы поддержки и принятия решений в ходе разработки замысла, планов и сценариев активного противодействия ИТВ. Применение нового класса систем идентификационного противоборства и активной защиты должно существенно повысить защищенность ИТКС и дать адекватный ответ противнику в ходе ведения ИП.

Литература.

1. Берзин Е. А. Оптимальное распределение ресурсов и элементы синтеза систем. Под ред. Е. В. Золотова, М., «Сов. радио», 1974, 304 с.
2. Саати Т. Принятие решений. Метод анализа иерархий.— М.: Радио и связь, 1993.— 278 с.
3. Коцыняк М. А., Осадчий А. И., Коцыняк М. М., Лаута О. С., Дементьев В. Е., Васюков Д. Ю. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства.— Спб.: ЛО ЦНИИС, 2015.— 126 с.