шифроблоков. Для последующих шифроблоков в той же датаграмме счетчик увеличивается на 1 для каждого последующего. Такая организация счетчиков приводит к тому, что значение счетчика никогда не повторяется два раза. 46-ти битное значение блока криптосчетчика управляет 128 битами AES последовательности по следующему алгоритму: 46 бит повторяются 3 раза, в итоге получается 138-битная последовательность, 10 первых бит которой отбрасываются. Полученные 128 бит информации подвергаются обработке AES алгоритма, в результате чего получается случайная шифропоследовательность, которая потом взаимодействует с блоками данных.

Использование стандарта шифрования AES позволяет повысить безопасность личной информации конечных пользователей. Стандарт AES использует 128-битовые ключи и имеет высокую скорость работы, кодируя за один цикл 128-битный блок.

Литература

1. Эксперт: Телекоммуникации вчера, сегодня, завтра. [Электронный ресурс]. — Режим доступа: http://rfcmd.ru/book_07/h5_5. — Дата доступа: 13.05.2016.

МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ПОИСКА АНОМАЛИЙ В ЗАДАЧАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

А.А. Левчук

Методы анализа, используемые в большинстве современных систем детектирования вторжений, направлены на обнаружение известных и формально описанных типов воздействий, но зачастую оказываются не в состоянии обнаружить модификации или новые типы аномалий, что делает их использование не всегда эффективным.

В работе была поставлена задача: на основе изучения алгоритмов поиска аномалий, спроектировать и реализовать отдельные элементы интеллектуальной системы на основе нейронных сетей для применения в задачах обнаружения вторжений.

Для решения задачи был предложены архитектурные решения обнаружения аномалий с использованием нейросетевых моделей. В исследованиях были получены 4 варианта нейросетей, спроектированных путём комбинирования рециркуляционных нейронных сетей и многослойных персептронов.

Чтобы оценить эффективность предложенного подхода обнаружения вторжений, был проведён ряд экспериментов. База данных KDD Cup 99 использовалась для обучения и тестирования нейросетевых моделей. В базе KDD-99 представлены 22 типа атак, разделенных на четыре основных категории: DoS, U2R, R2L и Probe. Наилучший результат распознавания аномалий разработанной системой был достигнут для атак класса DoS и Probe, несколько хуже определяются U2R и R2L.

Таким образом, в работе подтверждено, что модели нейронных сетей могут успешно применяться в задачах обнаружения вторжений. В ходе эксперимента проведён сравнительный анализ спроектированных систем на основе нейронных сетей. Для сравнения были использованы такие показатели эффективности, как доля обнаруженных атак, доля распознанных атак по каждому классу и число ложных срабатываний.

РЕШЕНИЕ ЗАДАЧИ ЦЕЛЕРАСПРЕДЕЛЕНИЯ В ИНФОРМАЦИОННОЙ ПОДСИСТЕМЕ КОМПЛЕКСА СРЕДСТВ АВТОМАТИЗАЦИИ ЗЕНИТНОЙ РАКЕТНОЙ БРИГАДЫ С УЧЕТОМ КЛАССА ЦЕЛЕЙ

А.Ю. Липлянин, Е.И. Михненок, Е.И. Хижняк

В основе эффективного управления боевыми средствами системы войск противовоздушной обороны лежит качественное управление огневыми средствами, решаемое в управляемой подсистеме комплексов средств автоматизации. Одним из факторов успешного функционирования управляющей подсистемы является эффективное решение задачи целераспределения. В настоящее время в комплексах средств автоматизации зенитной ракетной бригады имеется совокупность решаемых задач, в которые входят задачи боевого управления. Одним из типов таких задач является задача распределения усилий между группами зенитных ракетных дивизионов и целераспределение между зенитными ракетными дивизионами. На сегодняшний день эффективность зенитной ракетной бригады оценивается математическим ожиданием количества уничтоженных целей, которая в свою очередь обладает достаточно низкой коррелированностью с действительными результатами боевых действий [1]. Поскольку целью зенитной ракетной бригады при отражении удара воздушного противника является минимизировать ущерб объекту обороны, то и в качестве показателя

эффективности решения вышеуказанных задач определим значение предотвращенного ущерба [2]. При расчете данного показателя учитывается важность цели, которая в настоящий момент задается оператором вручную. Однако, не вызывает сомнения тот факт, что важность цели неразрывно связана с ее классом и задачей выполняемой в налете. Таким образом автоматическое определение классов воздушных объектов позволит достоверно определить важность цели, а, следовательно, и величину предотвращенного ущерба при решении задач распределения усилий и целераспределения. Результаты решения научной и практических задач диссертационной работы позволят выявить недостатки существующих методов распознавания целей, выработать последовательность и этапы решения задачи распознавания целей. Это позволит решать задачи распределения усилий и целераспределения более эффективно.

Литература

1. Скорик А.Б., Воронин В.В., Зверев А.А., Галицкий О.Ф. // Сб. науч. тр. Харьковского университета Воздушных Сил. 2010. № 3. С. 8–14.

2. Кругликов С.В. // Доклады БГУИР. 2013. № 5. С. 93–99.

СВОЙСТВА СИНДРОМОВ ОШИБОК ПРИМИТИВНЫХ БЧХ-КОДОВ

В.А. Липницкий, Н.В. Спичекова

В современных цифровых телекоммуникационных системах (ТКС), за исключением волоконно-оптических, для обнаружения и исправления ошибок, возникающих при передаче информации по каналу связи, используются помехоустойчивые коды. На практике широкое применение получили БЧХ-коды.

На сегодняшний день самый массовый вид ТКС — системы мобильной связи — обеспечивают исправление двойных ошибок на блок передаваемой информации. Практические потребности увеличения скоростей информационных потоков требуют исправления ошибок кратности, большей двух.

Процедура декодирования БЧХ-кода начинается с вычислени синдрома. Неравенство синдрома нулю является единственным свидетельством наличия ошибки в принятом блоке-сообщении. В примитичном БЧХ-коде C_9 длиной $n = 2^m - 1$ и конструктивным расстоянием 9 синдромы всех ошибок весом w, $1 \le w \le 4$, попарно различны. Данный факт является основой синдромных методов коррекции ошибок. Первым шагом в применении синдромных методов на практике является определение веса возникшей ошибки.

Авторами были исследованы свойства синдромов ошибок весом 1–4 в примитивных БЧХ-кодах C_9, сформулирована методика определения кратности ошибки по ее синдрому, установлена связь между предлагаемой методикой и методом определителей Блейхута нахождения веса ошибки БЧХ-кода на основании ее синдрома.

КЛАССИФИКАЦИЯ DDOS-АТАК В ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЯХ

В.В. Маликов, И.И. Лившиц

В настоящее время DDoS-атаки получили широкое распространение среди киберпреступников как один из эффективных и экономически доступных инструментов, позволяющих удаленно нарушить режим устойчивого функционирования сетевого сервиса/ресурса за счет эксплуатации уязвимостей, направленных на исчерпание пропускной способности каналов связи и/или вычислительной емкости атакуемого объекта.

Авторами на основе данных из открытых источников проведен анализ методов/технологий проведения DDoS-атак и предложена классификация таких атак с привязкой к уровням модели OSI. Дополнительно предложена классификация DDoS-атак по уровню сложности их технической реализации, учитывающая количественные параметры: векторов атаки, хостов атаки, скорости атаки, времени атаки, использования метода усиления (амплификатора).

По результатам проведенного анализа методов/технологий, используемых для проведения DDoS-атак, можно сделать следующие выводы:

1. Как правило, в качестве основного ресурса для проведения DDoS-атак злоумышленниками используются ранее атакованные и зараженные вредоносным кодом устройства/системы легитимных пользователей, которые потом объединяются в управляемые бот-сети. При этом показатели