Литература

1. IoT Security Guidelines Overview Document // GSM Association, 31 March 2019.
2. Эталонная архитектура безопасности интернета вещей // https://www.anti-malware.ru/practice/solutions/iot-the-reference-security-architecture-part-1.

УДК 007 **Information Control Systems and Technologies, pp. 75-77**

Д.т.н. Бурлов В.Г., Петров С.В., Грозмани Е.С.

ПРИМЕНЕНИЕ АЛГОРИТМА ГРАДИЕНТНОГО БУСТИНГА НАД РЕШАЮЩИМИ ДЕРЕВЬЯМИ ДЛЯ ВЫЯВЛЕНИЯ СЕТЕВЫХ АТАК

Dr.Sci. Burlov V.G., Petrov S.V., Grozmani E.S.

APPLICATION OF THE ALGORITHM OF GRADIENT BUSTING OVER DECISIVE TREES FOR DETECTING NETWORK ATTACKS

В основе любой деятельности лежат решения лица, ей управляющего (далее – лицо, принимающее решения (ЛПР). Человек осуществляет анализ обстановки и выбор плана действий на основе модели решения.

Таким образом, для построения системы обеспечения информационной безопасности и эффективного управления ею, требуется обладать математической моделью решения ЛПР.

В свою очередь формирование условий, гарантирующих достижение целей деятельности, осуществляется с помощью применения естественно-научного подхода, реализуемого научно-педагогической школой «Системная интеграция процессов государственного управления» [1-3].

Сложность и гетерогенность современных телекоммуникационных систем, а также высокая динамика изменения требований к ним, порождает большое число угроз информационной безопасности.

Для борьбы с данным видом угроз предназначены системы обнаружения (и предотвращения) вторжений (СОВ, Intrusion Detection

System (IDS)). Наиболее перспективными являются СОВ, базирующиеся на обнаружении аномалий.

Они могут выявлять не только уже известные вредоносные сигнатуры, но и новые атаки. Это обусловлено применением методов машинного обучения, дающих возможность системам защиты совершенствоваться в процессе работы, улучшая качество решения поставленных перед ними задач по мере накопления «опыта» [4].

Методы идентификации аномалий также подразделяются на четыре категории в зависимости от того, на решении каких классов задач машинного обучения строится их работа [5].

В результате анализа обобщенных архитектур сетевых СОВ, базирующихся на основных категориях методов обнаружения аномалий, установлено, что для обнаружения сетевых аномалий наиболее целесообразным является применение алгоритмов машинного обучения с учителем.

В результате оценки основных алгоритмов контролируемого машинного обучения было установлено, что решающие деревья, а также ансамбли, построенные на их базе, позволяют эффективно решать задачи классификации, не требуя, при этом, сложной предварительной подготовки данных [6].

Деревья решений являются очень быстрым методом, предлагающим легкость интерпретации полученных результатов и практически не требующий предварительной обработки входных данных. Основной проблемой является склонность к переобучению и, как следствие, низкая обобщающая способность. Недостатки данного метода, при сохранении всех преимуществ, нейтрализуются либо минимизируются посредством использования ансамблей: *случайные леса* или *градиентный бустинг*.

Таким образом, деревья решений и построенные на основе них ансамбли являются наилучшим алгоритмом для решения задачи классификации сетевых аномалий.

Литература

1. Бурлов В.Г. Основы моделирования социально-экономических и политических процессов (Методология. Методы) СПб: Факультет Комплексной Безопасности, СПБГПУ.2007г.-265 с.

2. Бурлов В.Г. Математические методы моделирования в экономике. Часть 1, – СПб. СПбГПУ, Факультет безопасности, НП «Стратегия будущего», 2007. – 330с.

3. Бурлов В.Г. О концепции гарантированного управления устойчивым развитием арктической зоны на основе решения обратной задачи. Информационные технологии и системы: управление, экономика, транспорт, право. 2015. № 2 (16). С. 99-111.

4. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. — СПб.: Питер, 2018. — 480 с.

5. Gogoi, P., Bhattacharyya D., Borah B., Kalita, J. A Survey of Outlier Detection Methods in Network Anomaly Identification // The Computer Journal. – 2011. – V. 54. – № 4. – С. 570–588.

6. Freeman D., Chio C. Machine Learning and Security // O'Reilly Media, Inc. – 2018. – 367 с.

УДК 621.317 **Information Control Systems and Technologies, pp. 77-79**

Д.т.н. Якимов В.Н., Волков Н.А.

ПОМЕХОУСТОЙЧИВАЯ ПЕРЕДАЧА ДАННЫХ НА ОСНОВЕ БИНАРНОГО КОДИРОВАНИЯ С ПРИМЕНЕНИЕМ ВИРТУАЛЬНОЙ МАШИНЫ

Dr.Sci. Yakimov V.N., Volkov N.A.

DATA TRANSFER NOISE RESISTANCE BASED ON BINARY CODING WITH THE USE OF A VIRTUAL MACHINE

Проблема помехоустойчивости при передаче данных является актуальной проблемой в современном мире. Источники помех могут быть внешними, либо они могут возникать из-за внутренних особенностей канала передачи данных. Даже слабые шумы могут вызывать искажения передаваемой информации.

Можно выделить два основных подхода, применяемых для распознавания помех по каналам связи [1]:

1) распознавание помех с помощью кодирования;

2) распознавание помех посредством обеспечения электромагнитной совместимости технических средств.

В настоящей статье предлагается обеспечить помехоустойчивость передачи данных на основе бинарного кодирования с применением виртуальной машины. Передача данных производится при помощи двухуровневого кодирования [2].