Тип работы: Курсовая работа

Предмет: Информационные системы и процессы

Интеграция интеллектуальных устройств и технологий с различными отраслями деятельности значительно трансформировала всю технологиче-скую инфраструктуру. Автоматизированные системы управления техноло-гическими процессами (АСУ ТП) в большинстве случаев продолжают кон-тролироваться человеком, однако роль человека в них сводится к мини-муму.
Интеграция информационных технологий с АСУ ТП и их доступ-ность из сети Интернет делает промышленные системы привлекательным объектом деструктивных кибервоздействий для злоумышленников. Стати-стика атак за последние несколько лет демонстрирует рост числа кибе-ратак на АСУ ТП, при этом, в большинстве случаев, целью злоумышлен-ников является получение контроля над подсистемой управления. Наибо-лее критичной является задача сохранения способности АСУ ТП к кор-ректному функционированию даже в условиях деструктивных информа-ционных воздействий, поскольку успешная реализация кибератак на такие системы способна повлечь за собой негативные финансовые последствия, экологические катастрофы и привести к гибели людей.
Для обеспечения корректного функционирования АСУ ТП в услови-ях кибератак необходимо своевременно обнаруживать аномалии в работе системы, вызванные попытками злоумышленников реализовать деструк-тивные кибервоздействия на систему. Подход к обнаружению аномалий должен быть инвариантен к типу кибератак и обеспечивать получение чис-ленной характеристики, значение которой будет свидетельствовать о нали-чии/отсутствии аномалии.
Вышеизложенное обусловило актуальность выбранной темы.
Целью курсовой работы является изучение особенностей выявления аномалий в информационных системах.
В соответствии с поставленной целью необходимо решить ряд задач, таких как:
- рассмотреть понятие и классификацию информационных систем;
- охарактеризовать понятие аномалий в информационных системах;
- изложить основы выявления аномалий в работе информационных систем с помощью машинного обучения;
- проанализировать систему обнаружения аномалий нового поколе-ния CyberThymus.

Объектом исследования являются аномалии в информационных си-стемах, предметом – особенности их выявления и устранения.
Структура работы обусловлена целью и задачами исследования. Курсовая работа состоит из введения, двух глав, заключения и списка ис-пользованных источников.

1 Теоретические аспекты выявления аномалий в информационных системах

1.1 Понятие и классификация информационных систем

Под информационной системой обычно понимается прикладная про-граммная подсистема, ориентированная на сбор, хранение, поиск и обра-ботку текстовой и/или фактографической информации. Подавляющее большинство информационных систем работает в ре-жиме диалога с пользователем.
Свойства информационных систем:
- любая ИС может быть подвергнута анализу, построена и управля-ема на основе общих принципов

построения сложных систем;
- при построении ИС необходимо использовать системный подход;
- ИС является динамичной и развивающейся системой;
- ИС следует воспринимать как систему обработки информации, со-стоящую из компьютерных и телекоммуникационных устройств, реализо-ванную на базе современных технологий;
- выходной продукцией ИС является информация, на основе которой принимаются решения или производится автоматическое выполнение ру-тинных операций;
- участие человека зависит от сложности системы, типов и наборов данных, степени формализации решаемых задач.
Процессы в информационной системе:
 ввод информации из внешних и внутренних источников;
 обработка входящей информации;
 хранение информации для последующего ее использования; вывод информации в удобном для пользователя виде;
 обратная связь, т.е. представление информации, переработанной в данной организации, для корректировки входящей информации.
С учетом сферы применения выделяют:
 технические ИС,
 экономические ИС,
 ИС в гуманитарных областях и т.д.
Классификация ИС
1. По областям применения.
Информационных системы в экономике (АСЭ – автоматизированные системы в экономике). В образовании (АСО). В научных исследованиях (АСНИ) и т.д.
2. По характеру информации, которой оперирует ИС. Фактографи-ческие или документальные
3. По роли, которую ИС играют в профессиональной деятельности.
1. Системы управления. АСУ (автоматизированная система управле-ния), САУ (система автоматического управления - без участия человека).
2. Вычислительные информационные системы.
3. Поисково-справочные информационные системы.
4. Системы принятия решения.
5. Информационные обучающие системы.
4. По техническим средствам:
Один компьютер / Локальная сеть / Глобальная сеть.

1.2 Понятие аномалий в информационных системах
Кибератаки представляют собой наиболее эффективный способ воз-действия на АСУ ТП, поскольку они позволяют злоумышленникам оказы-вать скрытное влияние на систему на любом расстоянии. Следует отметить, что целью реализации кибератак на такие системы является не получение информации, а получение контроля над системой, которое позволит не только вывести ее из строя, но и осуществлять гибкое, незаметное измене-ние параметров ее функционирования, заставляя систему работать нуж-ным образом.

1. Strategies for Building and Growing Strong Cybersecurity Teams, (ISC)2 cybersecurity workforce study, 2019
2. Sterritt, R. Autonomic computing. Innovations Syst Softw Eng 1, 79–88 (2005). DOI: 10.1007/s11334-005-0001-5.
3. ГОСТ Р ИСО/МЭК 27001-2006 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента ин-формационной безопасности. Требования.
4. Mohiuddin Ahmed, Abdun Naser Mahmood, Jiankun Hu “A survey of network anomaly detection techniques”, Journal of Network and Computer Applications, Volume 60, January 2016, Pages 19-31, DOI:10.1016/j.jnca.2015.11.016.
5. Dmitri Bekerman, Bracha Shapira, Lior Rokach, Ariel Bar “Unknown Malware Detection Using Network Traffic Classification”, 2015 IEEE Confer-ence on Communications and Network Security (CNS), Florence, Italy, 28-30 Sept. 2015, pp. 134-142, DOI: 10.1109/CNS.2015.7346821.
6. Rui Li, Xi Xiao, Shiguang Ni, Haitao Zheng, Shutao Xia “Byte Seg-ment Neural Network for Network Traffic Classification”, 2018 IEEE/ACM 26th International Symposium on Quality of Service (IWQoS), Banff, AB, Canada, 4-6

June 2018, DOI: 10.1109/IWQoS.2018.8624128.
7. Antônio J.Pinheiro, Jeandrode M. Bezerra, Caio A.P.Burgardt, Divan-ilson R.Campelo “Identifying IoT devices and events based on packet length from encrypted traffic”, Computer Communications, Volume 144, 15 August 2019, Pages 8-17, DOI: 10.1016/j.comcom.2019.05.012
8. А.И. Аветисян, А.И. Гетьман. Восстановление структуры бинар-ных данных по трассам программ. . Труды Института системного про-граммирования РАН, том 22, 2012, стр. 95-118. DOI: 10.15514/ISPRAS-2012-22-7.
9. Fanghui Sun Shen Wang, Chunrui Zhang, Hongli Zhang “Unsuper-vised field segmentation of unknown protocol messages”, Computer Commu-nications, Volume 146, 15 October 2019, Pages 121-130, DOI: 10.1016/j.comcom.2019.06.013.
10. Л. Фогель, А. Оуэнс, М. Уолш «Искусственный интеллект и эволюционное моделирование», М.: Издательство «МИР», 1969.
11. Самообучающиеся автоматические системы. Сборник. – М.: Издательство «Наука», 1966.