ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И ИНФОРМАТИКА
COMPUTER ENGINEERING AND INFORMATICS

Научная статья
УДК 004.896
https://doi.org/10.25686/2306-2819.2022.3.37

Программно-аппаратный стенд для оценки кибернетической защиты автоматизированной системы управления технологическим процессом

С. О. Иванов[1], Т. Н. Копышева[1]✉, М. В. Никандров[2]
[1] Чувашский государственный университет им. И.Н. Ульянова,
Российская Федерация, 428000, Чебоксары, Московский пр., 15
[2] ООО «Интеллектуальные сети»,
Российская Федерация, 428000, Чебоксары, ул. Пристанционная, д. 1, корп.9, офис 26
tn_pavlova@mail.ru✉

Аннотация. *В данной статье анализируется спроектированный экспериментальный стенд промышленной автоматизации, который может быть использован для моделирования различных режимов работы автоматизированной системы управления технологическим процессом, а также для обучения учащихся навыкам эксплуатации и защиты промышленных систем. Стенд построен по трёхуровневому принципу: верхний уровень – сервер SCADA и клиенты (операторы, диспетчеры), средний уровень – программируемые логические контроллеры (IED), нижний уровень не представлен в стенде, работу датчиков и исполнительных устройств эмулирует программное обеспечение IED. На стенде можно эмулировать как нормальный режим технологического процесса, так и имитацию сбоев в технологическом процессе из-за аварии или действий злоумышленников. В статье предложены способы дополнения методов генерации сетевых атак, необходимые для анализа сетевого трафика с помощью методов машинного обучения, а также перечислены необходимые статистические признаки сетевого трафика. Спроектированный стенд позволяет гибко и с минимальными затратами эмулировать различные автоматизированные системы управления технологическим процессом, имитировать их работу в достаточной степени, чтобы генерировать данные, которые можно использовать для машинного обучения.*

Ключевые слова: *программно-аппаратный стенд; АСУТП; искусственный интеллект; кибернетическая защита; сетевые атаки*

Введение. Для защиты промышленного сегмента сети промышленного предприятия методами машинного обучения требуется сбор данных о штатных, аварийных и аномальных режимах её работы. Использовать для сбора этих данных действующее производственное оборудование возможно, но связано с большими ограничениями.

В настоящее время накоплен опыт создания учебных и экспериментальных стендов [1–3] в различных областях. Стенды используются для проверки теоретических исследований, отладки и доводки

Для цитирования: Иванов С. О., Копышева Т. Н., Никандров М. В. Программно-аппаратный стенд для оценки кибернетической защиты автоматизированной системы управления технологическим процессом // Вестник Поволжского государственного технологического университета. Сер.: Радиотехнические и инфокоммуникационные системы. 2022. № 3 (55). С. 37-46. DOI: https://doi.org/10.25686/2306-2819.2022.3.37

опытных образцов, а также получения практического и исследовательского опыта в условиях, приближённых к реальности [4].

Целью работы является анализ различных аспектов спроектированного экспериментального стенда промышленной автоматизации, который может быть использован для моделирования различных режимов работы автоматизированной системы управления технологическим процессом (АСУТП) для анализа трафика и выявления аномалий с помощью методов машинного обучения, а также для обучения учащихся навыкам эксплуатации и защиты промышленных систем.

Стенд может использоваться для сбора данных о работе АСУТП, для машинного обучения моделей, исследования промышленных систем защиты. Стенд позволит практиковать навыки администрирования промышленных систем, проводить их настройку и отладку контроллеров, АСУТП, промышленных протоколов.

Описание стенда. Типичные АСУТП строятся по трёхуровневому принципу [4]: нижний уровень, состоящий из датчиков и исполнительных устройств, средний уровень – программируемые логические контроллеры (IED), верхний уровень – сервер SCADA и клиенты (операторы, диспетчеры). Концептуальная схема стенда представлена на рис 1.

1. Для лабораторных исследований в качестве нижнего слоя ряд авторов используют различные схемы энергосистем: три балансировочные зоны с различными датчиками, соединённые между собой соединительными линиями [5], схема дистанционной защиты, реализованная на цифровом симуляторе реального времени (RTDS) [6], имитация шведских линий электропередач KTH-Nordic32 [7], модель типичной цифровой подстанции на 500 кВ, используя реальные IED, переключатели и системы мониторинга [8]; IEEE 30-шинная система [9].

В отличие от этих стендов, описываемый стенд не имеет нижний уровень. Работу датчиков и исполнительных устройств эмулирует ПО IED. Для датчиков можно использовать генераторы случайных чисел или заданные списки событий, а для исполнительных устройств – код, вычисляющий состояние технологического процесса. Возможно применение различных промышленных протоколов [8]: DNP3.0, MMS, modbus, и т. п.

Весь сетевой трафик взаимодействия компонентов АСУТП (SCADA, диспетчер, IED) собирается и передаётся узлу ML для хранения и анализа.

Узел «Hacker» используется для выполнения сетевых атак на АСУТП. Атаки могут быть как внешние, так и изнутри.

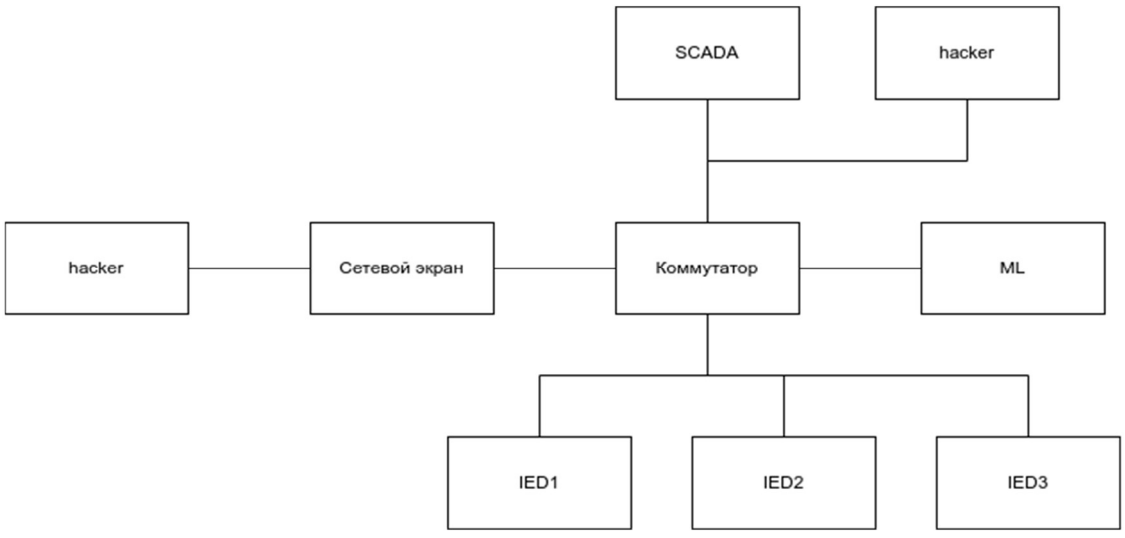

Рис. 1. Концептуальная схема стенда
Fig. 1. Conceptual scheme of the facility

Описание оборудования стенда представлено в таблице. В стенде используются промышленные версии коммутатора, сетевого экрана и сервера. В качестве IED – одноплатные компьютеры с эмуляторами ПЛК. Для администрирования, взаимодействия с АСУТП, а также для атакующих узлов используются мобильные ноутбуки.

С учётом имеющегося оборудования детализируем схему с рис. 1 и получим сетевую схему стенда (рис. 2).

Для роли узла «Admin» и «Engineer» используется один ноутбук. Так же и для внешнего и внутреннего источника атак.

UserGate C100 – аппаратный межсетевой экран с функциями безопасности: система обнаружения вторжений, потоковый антивирус, анализ и выгрузка информации об инцидентах безопасности, контроль приложений L7.

Промышленный коммутатор Ruggedcom RSG2100 оптимизирован для работы в промышленном окружении, поддерживает расширенные функции кибербезопасности: SSH/SSL (128/256-bit encryption), отключение портов, безопасность по порту 802.1X, VLAN (802.1Q), аутентификация и шифрование SNMPv3.

D400 (SWM0066) – это защищённая, высокопроизводительная платформа, которая собирает метрики, статусы, события и отчёты от IED. Она поддерживает последовательные порты (RS-232), оптоволокно.

Для разделения среднего и верхнего уровня используется мини-роутер Weidmuller IE-ARM-U-OSPF. В нём интегрирован сетевой экран, а также реализованы Stateful Packet Inspection firewall (SPI), Integrated Security Data Sheet (SDS), SNMP.

Оборудование стенда
Equipment of the facility

Название	Количество	Характеристики
Сетевой экран	1	UserGate C100
Промышленный коммутатор	2	Ruggedcom RSG2100
Промышленный сервер	2	D400 (SWM0066)
Промышленный сетевой экран	1	Weidmuller IE-ARM-U-OSPF
Стойка телекоммуникационная	1	
Комплект одноплатного компьютера	5	Raspberry Pi 4
Ноутбук	2	HP Laptop

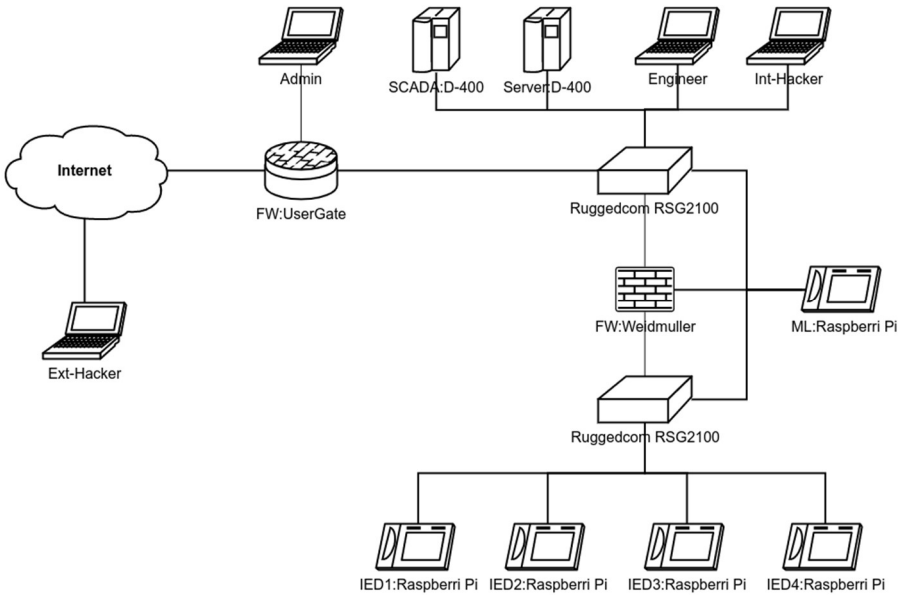

Рис. 2. Сетевая схема стенда
Fig. 2. Network scheme of the facility

Рис. 3. Фотография стенда
Fig. 3. The view of the facility

Для реализации IED используется Raspberry Pi 4, который обеспечивает производительность настольного компьютера, поддерживает беспроводную локальную сеть 2,4 / 5,0 ГГц, Bluetooth 5.0, Gigabit Ethernet, USB 3.0.

Для настройки стенда и для проведения атак используются ноутбуки, которые можно подключить к любому сегменту или устройству

Собранный стенд представлен на рис. 3.

Генерация трафика. На узлах IED и SCADA реализован обмен трафиком по следующим протоколам: IEC 60870-5-104, OPC UA, IEC 60870. Также для мониторинга состояния оборудования используется протокол SNMP.

Трафик нормального режима работы показан на рис. 4.

Промышленные протоколы, использующиеся в компьютерных сетях, обладают теми же недостатками, что и традиционные сетевые протоколы. Типичные атаки: спуффинг, человек-посредине, перехват трафика, ложные запросы, флуд, повтор трафика.

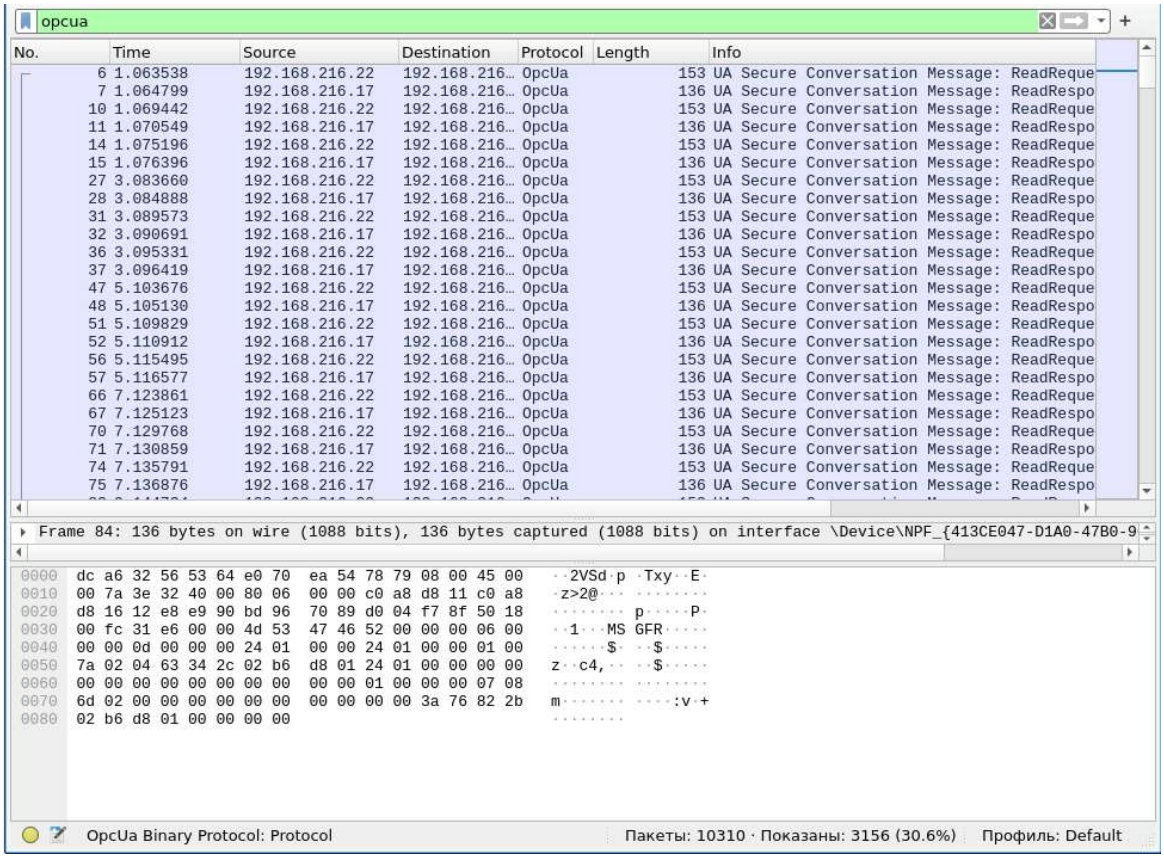

Рис. 4. Нормальный режим работы АСУ ТП
Fig. 4. Normal mode of operation of the industrial control system (ICS)

В дополнение к этим атакам промышленные протоколы реализуют логику управления технологическим процессом, вмешательство в которую позволяет выполнить различные атаки. Выделяют следующие категории атак на системы электроснабжения в зависимости от уровня [4]:

- на физическое оборудование: отключение устройств, несанкционированное изменение параметров,
- на коммуникационные каналы: обрыв линии связи,
- на приложения: отказ в обслуживании, эксплуатация уязвимости ПО,
- на данные: ложные данные (False Data Injection Attacks), перераспределения нагрузки [9, 10, 11].

Ложные данные включают в себя отправку ложных сигналов [12], а также изменение контролируемых значений [5]: масштабирование (scale), увеличение или уменьшение значений (ramp), кратковременные вбросы (pulse), случайные значения (random).

Для генерации атак можно использовать стандартные утилиты для пентеста: scapy, ettercap, nmap, metasploit, arpspoof и т. п.

2. Для реализации способа обучения с учителем необходимо сопоставить генерируемый трафик с трафиком, перехваченным анализаторами (сенсорами). Можно предложить несколько подходов к решению этой проблемы. Первый: сохранять время генерации пакетов, чтобы сопоставить его с временным штампом перехваченных пакетов. Второй: использовать системы обнаружения вторжений для выявления времени атак в захваченном сетевом трафике. Третий: помечать генерируемые пакеты, используя поле options IP-пакетов.

На рис. 5 показана атака ICMP-флуд и её влияние на обычный трафик АСУТП.

Как видно на рис. 5, после начала атаки ICMP-флуд трафик промышленного протокола подавляется.

Для анализа с помощью методов машинного обучения, например методом опорных векторов (SVM) [13], методом случайного леса [14], ИНС, необходимо выявить дискретизированные статистические признаки потоков сетевого трафика. Сетевой трафик будет разбит на интервалы от 1 до 3 секунд. В каждом интервале будут вычислены следующие метрики – статистическая характеристика потока:

- количество пакетов разных протоколов: IP, ICMP, TCP, UDP, ARP, HTTP, SMTP, DHCP;
- количество ошибочных пакетов;

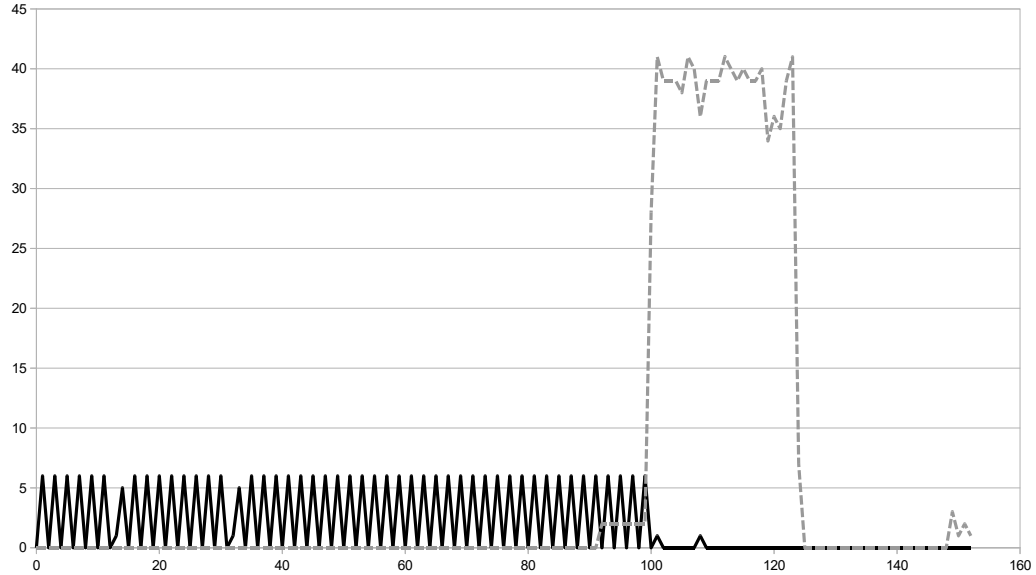

Рис. 5. Атака ICMP-флудом(серая пунктирная линия) на трафик АСУ ТП (сплошная черная)
Fig. 5. ICMP flood attack (gray dotted line) on ICS traffic (solid black)

- количество пакетов IP с флагом X (DF, MF);
- количество пакетов TCP с флагом X (SYN,ACK,CLOSE);
- количество различных адресов, портов;
- количество переданных байт;
- количество переданных данных;
- средний размер пакета;
- стандартное отклонение размера пакета;
- отношение объёма данных прикладного уровня к объёму данных сетевого с транспортным;
- средний интервал между пакетами;
- стандартное отклонение интервала между пакетами;
- среднее время появления пакетов.

Кроме данных, собираемых из трафика, возможно использовать протоколы сетевого контроля (SNMP), которые покажут внутреннее состояние устройств. Для анализа соединений для каждого контролируемого узла рассчитываются следующие метрики:

- количество входящего/исходящего трафика;
- отношение объёма переданных/полученных данных;
- отношение количества переданных/полученных пакетов.

Для контролируемых протоколов в рамках каждого соединения определяются следующие метрики:

- количество сообщений;
- общее время обмена сообщений;
- размер первой порции данных;
- размер второй порции данных;
- количество сообщений типа T.

Сбор, обработка и анализ трафика происходит в узле ML, на который «зеркалирован» сетевой трафик и направлены протоколы сетевого контроля.

Заключение. Описанный и собранный стенд позволяет имитировать работу АСУТП в достаточной степени, чтобы генерировать данные, которые можно использовать для машинного обучения [15, 16]. В общем случае для этой задачи необходимо одновременно определение плохих данных, оценка состояния SCADA, слежение за значениями системы глобальных измерений (WAMS) [17].

Применение оборудования, поддерживающее протоколы сетевого контроля (SNMP), позволяет осуществлять мониторинг оборудования не только по их внешней активности, но и по внутреннему статусу [18, 19].

Использование микрокомпьютеров вместо IED и нижнего уровня позволяет сократить расходы на создание стенда, а также имитировать различные конфигурации и устройства, не ограничиваясь конкретным производителем. При анализе различных технологических процессов достаточно изменить количество и сконфигурировать IED для имитации работы аппаратных компонентов нижнего уровня и программного обеспечения цифровых устройств защиты и управления. Стоит отметить, что по производительности один IED может имитировать несколько цифровых устройств.

Недостатком данного подхода является ограниченность атак на физические устройства и их датчики.

Кроме генерации трафика для машинного обучения стенд позволяет учащимся получить опыт разработки, настройки и эксплуатации АСУТП [4]. Также возможна отработка навыков защиты АСУТП от атак, проверка оборудования и нового ПО на уязвимости, соответствия требованиям и анализа защищённости [4], разработка новых систем защиты.

Таким образом, показано, что спроектированная архитектура стенда позволяет гибко и с минимальными затратами эмулировать различные АСУТП, полностью контролируя сетевой трафик в различных условиях и ситуациях. Также показано, что для исследования описанных сетевых атак машинными методами обучения необходимо дополнить методы их генерации способами фиксации времени.

Список источников

1. *Плешков В.В.* Методика организации занятий производственного обучения (инновационный подход) // Вестник науки. 2020. № 7 (28). С. 27-30. URL: https://cyberleninka.ru/article/n/metodika-organizatsii-zanyatiy-proizvodstvennogo-obucheniya-innovatsionnyy-podhod (дата обращения: 18.08.2022).

2. *Плужник Е. В., Никульчев Е. В., Паяин С. В.* Лабораторный экспериментальный стенд облачных и сетевых технологий // Cloud of science. 2014. № 1. С. 78-87. URL: https://cyberleninka.ru/article/n/-laboratornyy-eksperimentalnyy-stend-oblachnyh-i-setevyh-tehnologiy (дата обращения: 14.08.2022).

3.Управляющая измерительно-информационная система экспериментального стенда / А. Н. Цветков, В. Ю. Корнилов, А. Р. Сафин и др. // Известия вузов. Проблемы энергетики. 2020. № 4. С. 88-98. URL: https://cyberleninka.ru/article/n/upravlyayuschaya-izmeritelno-informatsionnaya-sistema-eksperimentalnogo-stenda (дата обращения: 14.08.2022).

4. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid / Liu Ren, Vellaithurai Ceeman, Biswas Saugata et al. // IEEE Transactions on Smart Grid. 2015. Vol. 6. Pp. 1-1. DOI:10.1109/TSG.2015.2432013.

5. *Sridhar S., Govindarasu M.* Model-Based Attack Detection and Mitigation for Automatic Generation Control // IEEE Transactions on Smart Grid. 2014. Vol. 5, no. 2. Pp. 580-591. DOI:10.1109/TSG.2014.2298195.

6. *Pan Shengyi, Morris Thomas, Adhikari Uttam.* Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems // IEEE Transactions on Smart Grid. 2015. Vol. 6. DOI:10.1109/TSG.2015.2409775.

7. *Ashrafi A., Shahrtash S.M.* Dynamic Wide Area Voltage Control Strategy Based on Organized Multi-Agent System // IEEE Transactions on Power Systems. 2014. Vol. 29, no. 6. Pp. 2590-2601. DOI:10.1109/TPWRS.2014.2313607.

8. Multidimensional Intrusion Detection System for IEC 61850 based SCADA Networks / Yang Yi, Gao Lei, Yuan Yu-Bo et al. // IEEE Transactions on Power Delivery. 2016. Vol. 32. DOI: 10.1109/TPWRD.2016.2603339.

9. *Chu Zhigang, Kosut Oliver, Sankar Lalitha*. Detecting Load Redistribution Attacks via Support Vector Models // IET Smart Grid. 2020. Vol. 3. DOI:10.1049/iet-stg.2020.0030.

10. Power System Reliability Evaluation Considering Load Redistribution Attacks / Xiang Yingmeng, Ding Zhilu, Zhang Yichi et al. // IEEE Transactions on Smart Grid. 2016. Vol. 8. Pp. 1-1. DOI:10.1109/TSG.2016.2569589.

11. *Yuan Y., Li Z., Ren K.* Modeling Load Redistribution Attacks in Power Systems // IEEE Transactions on Smart Grid. 2011. Vol. 2, no. 2. Pp. 382-390. DOI:10.1109/TSG.2011.2123925.

12. A Review of False Data Injection Attacks Against Modern Power Systems / Liang Gaoqi, Zhao Junhua, Luo Fengji et al. // IEEE Transactions on Smart Grid. 2016. Vol. 8. Pp. 1-1. DOI:10.1109/TSG.2015.2495133.

13. *Gowsalya R., Amali S.M.* SVM Based Network Traffic Classification Using Correlation Information // Networking and Communication Engineering. 2014. Vol.6. Pp. 188-192.

14. *Krasnova I.A., Deart V. Yu., Mankov V.A.* Development of a Feature Matrix for Classifying Network Traffic in SDN in Real-Time Based on Machine Learning Algorithms // 2020 International Scientific and Technical Conference Modern Computer Network Technologies (MoNeTeC). Moscow, 2020. Pp. 1-9. doi:10.1109/MoNeTeC49726.2020.9258314

15. *Иванов С.О, Никандров М.В.* Программная реализация нейросети для контроля максимальной токовой защиты // Динамика нелинейных дискретных электротехнических и электронных систем. Материалы XIV Всероссийской научно-технической конференции. Чебоксары: Чувашский государственный университет имени И.Н. Ульянова. 2021. С. 121-124.

16. *Singh V.K., Govindarasu M.* A Cyber-Physical Anomaly Detection for Wide-Area Protection Using Machine Learning // IEEE Transactions on Smart Grid. 2021. Vol. 12, no.4. Pp. 3514-3526. DOI: 10.1109/TSG.2021.3066316.

17. *Kolosok I., Korkina E.* Decomposition of power system state estimation problem as a method to tackle cyber attacks // 2018 IEEE Industrial Cyber-Physical Systems (ICPS). 2018. Pp. 398-403. DOI:10.1109/ICPHYS.2018.8387691.

18. *Кощеев М.И., Ларюхин А.А., Славутский А.Л.* Использование адаптивных нейроалгоритмов для распознавания аномальных режимов систем вторичного оборудования электроэнергетики // Вестник Чувашского университета. 2019. № 1. С. 47-58.

19. Комплекс обеспечения контролируемой деградации системы управления энергообъекта при киберинцидентах / И. Г. Назаров, Д. В. Суслов, М. В. Никандров и др. // Вестник Чувашского университета. 2018. № 1. С. 146-152.

Статья поступила в редакцию 04.08.2022; одобрена после рецензирования 30.08.2022; принята к публикации 12.09.2022

Информация об авторах

ИВАНОВ Сергей Олегович – аспирант кафедры математического и аппаратного обеспечения информационных систем, Чувашский государственный университет им. И.Н. Ульянова. Область научных интересов – кибербезопасность, искусственный интеллект, сети, компьютерное моделирование, методы защиты информации. Автор 57 научных публикаций. ORCID: https://orcid.org/0000-0003-3918-3919.

КОПЫШЕВА Татьяна Николаевна – кандидат физико-математических наук, доцент кафедры математического и аппаратного обеспечения информационных систем, Чувашский государственный университет им.И.Н. Ульянова. Область научных интересов – вычислительная техника, кибербезопасность, искусственный интеллект, сети. Автор 94 научных публикаций. ORCID: https://orcid.org/0000-0003-0935-0384.

НИКАНДРОВ Максим Валерьевич – директор, ООО «Интеллектуальные сети». Область научных интересов – математическое моделирование, кибербезопасность, искусственный интеллект. Автор 30 научных публикаций. ORCID: https://orcid.org/0000-0001-6846-3384.

Вклад авторов:
Иванов С. О. – разработка методики моделирования атак и сбора данных.
Копышева Т. Н. – описание результатов, формулирование основных положений.
Никандров М. В. – концепция экспериментального стенда; консультация по техническим вопросам.

Авторы заявляют об отсутствии конфликта интересов.
Все авторы прочитали и одобрили окончательный вариант рукописи.

Scientific article
UDC 004.896
https://doi.org/10.25686/2306-2819.2022.3.37

Software Hardware Facility for Evaluating Cybernetic Protection of the Automated System for Controlling Technological Process

S. O. Ivanov[1], T. N. Kopysheva[1]✉, M. V. Nikandrov[2]
[1]Chuvash State University named after I.N. Ulyanova,
15, Moskovsky Ave, Cheboksary, 428015, Russian Federation
[2]LLC "Intellectual networks",
1, bldg. 9, office 26, Pristationnaya str., Cheboksary, 428000, Russian Federation
tn_pavlova@mail.ru✉

Keywords: *software and hardware training facility; ICS; artificial intelligence; cyber defense; network attacks*

ABSTRACT

Introduction*. Protecting the industrial network segment of an industrial enterprise with the use of machine learning methods requires collecting data on normal, emergency and abnormal modes of its operation. The paper considers experimental facility for industrial automation, which can be used to simulate various modes of operation of industrial control system (ICS), as well as to teach students how to operate and protect industrial systems.* ***Methods****. The facility is built on a three-level principle: the top level is the SCADA server and clients (operators, dispatchers), the middle level is programmable logic controllers (IEDs), the bottom level is not represented in the facility, so the software of IED emulates the operation of sensors and units. The entire network traffic of interaction between the ICS components (SCADA, dispatcher, IED) is collected and transmitted to the ML node for storage and analysis. The Hacker node is used to perform network attacks on the ICS.* ***Results****. Experimental facility allows one to emulate the normal mode of the technological process and the simulation of failures in the technological process due to an accident and an attacker. In addition to typical network attacks, there are special attacks on different levels of industrial systems. The following standard pentest tools can be used to generate attacks: scapy, ettercap, nmap, metasploit, arpspoof, etc. The paper lists the main statistical features of network traffic for analysis with the use of machine learning methods.* ***Conclusions****. The described experimental facility allows one to simulate the operation of ICS to generate data that can be used for machine learning. In addition to generating traffic, the facility can be used for students to gain experience in developing, configuring and operating ICS. Also, it can be used to improve the skills of protecting ICS from attacks, checking equipment and new software for vulnerabilities, checking compliance with requirements, security analysis, and developong new protection systems.*

REFERENCES

1. Pleshkov V.V. Metodika organizacii zanjatij proizvodstvennogo obuchenija [Methodology for organizing industrial training classes]. *Vestnik nauki* [Science Bulletin]. 2020. Vol. 1. No 7 (28). P. 27-30. https://cyberleninka.ru/article/n/metodika-organizatsii-zanyatiy-proizvodstvennogo-obucheniya-innovatsionnyy-podhod (reference date: 18.08.2022). (In Russ.).

2. Pluzhnik E.V., Nikulchev E.V., Payain S.V. Laboratornyj jeksperimental'nyj stend oblachnyh i setevyh tehnologij [Cloud and network laboratory test bench]. *Cloud of science*. 2014. Vol. 1. No 1. Pp. 78-87. URL: https://cyberleninka.ru/article/n/laboratornyy-eksperimentalnyy-stend-oblachnyh-i-setevyh-tehnologiy (reference date: 14.08.2022). (In Russ.).

3. Tsvetkov A.N., Kornilov V.Yu., Safin A.R. et al. Upravljajushhaja izmeritel'no-informacionnaja sistema jeksperimental'nogo stenda [Control measuring and information system of the experimental stand]. *Izvestija vuzov. Problemy jenergetiki* [Power engineering: research, equipment, technology]. 2020. Vol. 22. No 4. Pp. 88-98. URL: https://cyberleninka.ru/article/n/upravlyayuschaya-izmeritelno-informatsionnaya-sistema-eksperimentalnogo-stenda (reference date: 14.08.2022). (In Russ.).

4. Liu Ren, Vel-laithurai Ceeman, Biswas Saugata et al. Analyzing the Cyber-Physical Impact of Cyber Events on the Power Grid. *IEEE Transactions on Smart Grid.* 2015. Vol. 6. Pp. 1-1. DOI:10.1109/TSG.2015.2432013.

5. Sridhar S., Govindarasu M. Model-Based Attack Detection and Mitigation for Automatic Genera-tion Control. *IEEE Transactions on Smart Grid.* 2014. Vol. 5, no. 2. Pp. 580-591. DOI:10.1109/TSG.2014.2298195.

6. Pan Shengyi, Morris Thomas, Adhikari Uttam. Developing a Hybrid Intrusion Detection System Using Data Mining for Power Systems. *IEEE Transactions on Smart Grid.* 2015. Vol. 6. DOI:10.1109/TSG.2015.2409775.

7. Ashrafi A., Shahrtash S.M. Dynamic Wide Area Voltage Control Strategy Based on Organized Multi-Agent System. *IEEE Transactions on Power Systems.* 2014. Vol. 29, no. 6. Pp. 2590-2601. DOI:10.1109/TPWRS.2014.2313607.

8. Yang Yi, Gao Lei, Yuan Yu-Bo et al. Multidimensional Intrusion Detection System for IEC 61850 based SCADA Networks. *IEEE Transactions on Power Delivery.* 2016. Vol. 32. DOI: 10.1109/TPWRD.2016.2603339.

9. Chu Zhigang, Kosut Oliver, Sankar Lalitha. Detecting Load Redistribution Attacks via Support Vector Models. *IET Smart Grid*. 2020. Vol. 3. DOI:10.1049/iet-stg.2020.0030.

10. Xiang Yingmeng, Ding Zhilu, Zhang Yichi et al. Power System Reliability Evaluation Consid-ering Load Redistribution Attacks. *IEEE Transactions on Smart Grid.* 2016. Vol. 8. Pp. 1-1. DOI:10.1109/TSG.2016.2569589.

11. Yuan Y., Li Z., Ren K. Modeling Load Redis-tribution Attacks in Power Systems. *IEEE Transac-tions on Smart Grid.* 2011. Vol. 2, no. 2. Pp. 382-390. DOI:10.1109/TSG.2011.2123925.

12. Liang Gaoqi, Zhao Junhua, Luo Fengji et al. A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Transactions on Smart Grid.* 2016. Vol. 8. Pp. 1-1. DOI:10.1109/TSG.2015.2495133.

13. Gowsalya R., Amali S.M. SVM Based Network Traffic Classification Using Correlation Information. *Networking and Communication Engineering.* 2014. Vol. 6. Pp. 188-192.

14. Krasnova I.A., Deart V. Yu., Mankov V.A. De-velopment of a Feature Matrix for Classifying Network Traffic in SDN in Real-Time Based on Machine Learning Algorithms. *2020 International Scientific and Technical Conference Modern Computer Net-work Technologies* (*MoNeTeC*). Moscow, 2020. Pp. 1-9. doi:10.1109/MoNeTeC49726.2020.9258314

15. *Ivanov S.O., Nikandrov M.V.* Programmnaja realizacija nejroseti dlja kontrolja maksimal'noj tokovoj zashhity [Software implementation of a neural network to control overcurrent protection]. *Dinamika nelinejnyh diskretnyh jelektrotehnicheskih i jelektronnyh sistem. Materialy XIV Vserossijskoj nauchno-tehnicheskoj konferencii* [Dynamics of non-linear discrete electrical and electronic systems. Proceedings of the XIV All-Russian Scientific and Technical Conference]. Cheboksary: Chuvash State University named after I.N. Ulyanova, 2021. Pp. 121-124. (In Russ.).

16. Singh V.K., Govindarasu M. A Cyber-Physical Anomaly Detection for Wide-Area Protection Using Machine Learning. *IEEE Transactions on Smart Grid.* 2021. Vol. 12, no. 4. Pp. 3514-3526. DOI: 10.1109/TSG.2021.3066316.

17. Kolosok I., Korkina E. Decomposition of power system state estimation problem as a method to tackle cyber attacks. *2018 IEEE Industrial Cyber-Physical Systems (ICPS)*. 2018. Pp. 398-403. DOI:10.1109/ICPHYS.2018.8387691.

18. *Koshcheev M.I., Laryukhin A.A., Slavutsky A.L.* Ispol'zovanie adaptivnyh nejroalgoritmov dlja raspoznavanija anomal'nyh rezhimov sistem vtorichnogo oborudovanija jelektrojenergetiki [Application of adaptive neuro algorithms for recognition of anomalous behaviour of secondary equipment systems in electric power industry]. *Vestnik Chuvashskogo universiteta* [Bulletin of the Chuvash University]. 2019. No 1. Pp. 47-58. (In Russ.).

19. Nazarov I.G., Suslov D.V., Nikandrov M.V., Slavutsky L.A. Kompleks obespechenija kontroliruemoj degradacii sistemy upravlenija jenergoobekta pri kiberincidentah [Complex to provide controlled degradation of electrical facility control system at cyber incidents]. *Vestnik Chuvashskogo universiteta* [Bulletin of the Chuvash University]. 2018. No 1. Pp. 146-152. (In Russ.).

The article was submitted 04.08.2022; approved after reviewing 30.08.2022; accepted for publication 12.09.2022

For citation: Ivanov S. O., Kopysheva T. N., Nikandrov M. V. Software Hardware Facility for Evaluating Cybernetic Protection of the Automated System for Controlling Technological Process. *Vestnik of Volga State University of Technology. Ser.: Radio Engineering and Infocommunication Systems*. 2022. No 3 (55). Pp. 37–46. DOI: https://doi.org/10.25686/2306-2819.2022.3.37

Information about the authors

Sergey O. Ivanov – PhD student at the Department of Mathematical and Hardware Support of Information Systems, Chuvash State University named after I.N. Ulyanova. Research interests – cybersecurity, artificial intelligence, networks, computer modeling, information security methods. The author of 57 scientific publications. ORCID: https://orcid.org/0000-0003-3918-3919.

Tatyana N. Kopisheva – Candidate of Physical and Mathematical Sciences, associate professor at the Department of Mathematical and Hardware Support of Information Systems, Chuvash State University named after I.N. Ulyanova. Research interests – computer technology, cybersecurity, artificial intelligence, networks. The author of 94 scientific publications. ORCID: https://orcid.org/0000-0003-0935-0384.

Maksim V. Nikandrov – CEO at Intelligent Networks LLC. Research interests – mathematical modeling, cybersecurity, artificial intelligence. The author of 30 scientific publications. ORCID: https://orcid.org/0000-0001-6846-3384.

Contribution of authors:
Ivanov S. O. – development of method for attack modeling and data collection.
Kopysheva T. N. – description of the results, formulation of the main outlines.
Nikandrov M. V. – concept of the experimental facility; technical advice.

Authors declare that they have no conflict of interest.
All authors read and approved the final manuscript.