DOI: 10.37791/2687-0649-2022-17-1-83-96

Исследование результатов применения программного тренажера по реагированию на факты реализации компьютерных угроз в АСУ ТП

М. В. Тумбинская[1]*, ***А. Р. Абзалов***[1]
[1] *Казанский национальный исследовательский технический университет им. А. Н. Туполева, Казань, Россия*
** tumbinskaya@inbox.ru*

Аннотация. Обеспечение информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) – задача сложная, и ее решение требует комплексного подхода. Необходимо рассматривать различные компьютерные угрозы, которые могут носить внешний, внутренний, случайный или преднамеренный характер. Мировой рост киберпреступлений и постоянное совершенствование кибератак требуют повышения уровня защищенности АСУ ТП, веб-ресурсов, информационных систем и т. д. Целью данного исследования является повышение уровня защищенности АСУ ТП. Достижение поставленной цели возможно путем решения главной задачи – обучения пользователей реагированию на факты реализации компьютерных угроз при эксплуатации АСУ ТП, т. е. инциденты информационной безопасности. В статье описано программное обеспечение, которое позволит получить пользователям промышленной автоматизированной системы практические навыки для адекватного реагирования на инциденты, повысить уровень знаний пользователей в области защиты информации. В работе представлен анализ информационной безопасности АСУ ТП, который показал, что в среднем в 89,5% случаев злоумышленники для несанкционированного получения доступа к информации используют вредоносное программное обеспечение, в среднем в 83% случаев – методы социальной инженерии. Для исследования выбрана промышленная автоматизированная система крупного предприятия машиностроительной отрасли Республики Татарстан. Результаты исследования показали, что после применения тренажера пользователи более адекватно реагируют на возникающие инциденты информационной безопасности. В среднем количество атак в анализируемых периодах в целом сократилось на 28%: число атак, реализуемых с помощью методов социальной инженерии, – на 51,75%, количество атак с использованием вредоносного программного обеспечения – на 40,25%, количество атак типа DoS – на 11,75%, количество атак подбора учетных данных – на 7,5%.

Ключевые слова: защита информации, программное обеспечение, информационная система, уязвимость, атака, злоумышленник, угроза

Для цитирования: *Тумбинская М. В., Абзалов А. Р.* Исследование результатов применения программного тренажера по реагированию на факты реализации компьютерных угроз в АСУ ТП // Прикладная информатика. 2022. Т. 17. № 1. С. 83–96. DOI: 10.37791/2687-0649-2022-17-1-83-96

Investigation of the results of using a software simulator for responding to the facts of the implementation of computer threats in an automated process control system

M. Tumbinskaya[1*]***, A. Abzalov***[1]
[1] *Kazan National Research Technical University named after A. N. Tupolev, Kazan, Russia*
** tumbinskaya@inbox.ru*

Abstract. Ensuring information security of automated process control systems (IACS) is a difficult task and its solution requires an integrated approach. Various computer threats need to be considered, which may be external, internal, accidental or deliberate. With the global growth of cybercrimes and the constant improvement of cyberattacks, it is necessary to increase the level of security of IACS, web resources, information systems, etc. Achieving the goal of increasing the level of security is possible by solving the problem of training users to respond to the facts of the implementation of computer threats during the operation of the IACS, i. e. information security incidents. The article describes software, the main task of which is to provide users of an industrial automated system with practical skills for an adequate response to incidents, which will increase the level of users' knowledge in the field of information security. The paper presents an analysis of the information security of an automated process control system, which showed that, on average, in 89.5% of cases, attackers use malicious software to gain access to information unauthorizedly, and on average, in 83% of cases, they use social engineering methods. An industrial automated system of a large enterprise in the machine-building industry of the Republic of Tatarstan was selected for the study. The results of the study and experimental data showed that as a result of training and after it, users more correctly and adequately respond to emerging information security incidents due to the fact that most situations were considered and analyzed during the training period using software. On average, the number of attacks in the analyzed periods as a whole decreased by 28%: the number of attacks carried out using social engineering methods decreased by 51.75%, the number of attacks using malicious software by 40.25%, the number of DoS-type attacks – by 11.75%, the number of credential brute-force attacks – by 7.5%.

Keywords: information protection, software, information system, vulnerability, attack, intruder, threat

For citation: Tumbinskaya M., Abzalov A. Investigation of the results of using a software simulator for responding to the facts of the implementation of computer threats in an automated process control system. *Prikladnaya informatika*=Journal of Applied Informatics, 2022, vol.17, no.1, pp.83-96 (in Russian). DOI: 10.37791/2687-0649-2022-17-1-83-96

Введение

Обеспечение информационной безопасности АСУ ТП – задача сложная, и ее решение требует комплексного подхода. Необходимо рассматривать разнородные угрозы, которые могут быть внешними и внутренними, случайными и преднамеренными. Причем какая бы классификация ни была рассмотрена, в любой из них так или иначе имеет место человеческий фактор. В связи с этим при формировании перечня мер противодействия угрозам безопасности в него всегда включается пункт «обучение персонала». Однако когда речь идет об информационной безопасности, повы-