Автоматизация в промышленности 2021. №10
www.avtprom.ru

DOI: 10.25728/avtprom.2021.10.10

Н.П. Васильев (РТУ МИРЭА), А.В. Фефилов (АО «Перспективный мониторинг»)

Проблемы выявления и отражения кибератак на информационные системы

Рассмотрена проблема обнаружения и обезвреживания кибератак на информационные системы (ИС), в том числе в реальном времени. Приводятся современные системы обнаружения и предотвращения вторжений (атак) в ИС, включая системы интеллектуального анализа угроз. Описываются некоторые аспекты по обучению специалистов в области информационной безопасности (ИБ), включая on-line-тренинги с использованием инновационного киберполигона Ampire. Система позволяет участникам тренинга как выявлять инциденты информационной безопасности, так и оперативно реагировать на них, закрывая уязвимости в ИС.

Ключевые слова: обнаружение и обезвреживание кибератак, информационные системы, интеллектуальный анализ угроз, киберполигон, обучение.

Васильев Николай Петрович *- канд. техн. наук, доцент, доцент кафедры КБ-1 «Защита информации» МИРЭА – Российского технологического университета (РТУ МИРЭА),*
Фефилов Александр Валерьевич *– старший специалист информационной безопасности АО «Перспективный мониторинг».*

Список литературы

1. *Steve Morgan*. Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021 [Электронный ресурс]. https://www.csoonline.com/article/3200024/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html
2. Актуальные киберугрозы: итоги 2019 г. https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019
3. *Lance Spitzner*. Honeypots: Tracking Hackers. Addison Wesley, 2002.
4. Honeypots Solutions. https://web.archive.org/web/20090308063216/http://www.tracking-hackers.com/solutions/

Vasiliev N.P., Fefilov A.V. The problems of detection and repulsion of cyberattacks against information systems

The problems of detecting and repulsing cyberattacks against information systems, in particular, in real time is discussed. State-of-the-art detection and repulsion system including intelligent threat analysis systems are presented. Some aspects of cyber security specialist training are outlined, including on-line trainings with innovative Ampire Cyber Polygon. The system enables the detection of cyber incidents and timely response to them for neutralizing security vulnerabilities.

Keywords: cyberattack detection and repulsion, information systems, intelligent threat analysis, Cyber Polygon, training.