Информация о публикациях кафедры систем информационной безопасности

1. Ostapenko, A.G. Denial of service in components of information telecommunication systems through the example of “network storm” attacks / A.G. Ostapenko, S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak, L.G. Popova // World Applied Sciences Journal. – 2013. – 25 (3). – P. 404-409.
2. Ostapenko, A.G. The usefulness and viability of systems: Assessment methodology taking into account possible damages / A.G. Ostapenko, E.F. Ivankin, V.S. Zarubin, A.V. Zaryaev // World Applied Sciences Journal. – 2013. – 25 (4). – P. 675-679.
3. Ostapenko, G.A. Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y Makarov, N.M. Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 416-420.
4. Ostapenko, G.A. Analytical models of information-psychological impact of social information networks on users / G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 410-415.
5. Kalashnikov, A.O. Ensuring the security of critically important objects and trends in the development of information technology / A.O. Kalashnikov, Y.V. Yermilov, O.N. Choporov, K.A. Razinkin, N.I. Barannikov // World Applied Sciences Journal. – 2013. - № 25 (3). – P. 399-403.
6. Ermakov, S.A. Optimization of expert methods used to analyze information security risk in modern wireless networks / S.A. Ermakov, A.S. Zavorykin, N.S. Kolenbet, A.G. Ostapenko, A.O Kalashnikov // Life Science Journal. – 2014. – № 11(10s). – P. 511-514.
7. Butuzov, V.V. Email-flooder attacks: The estimation and regulation of damage / V.V. Butuzov, A.G. Ostapenko, P.A. Parinov, G.A. Ostapenko // Life Science Journal. – 2014. – 11 (7s). – P. 213-218.
8. Radko, N.M. Assessment of the system’s EPI-resistance under conditions of information epidemic expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, D.V. Gusev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (3). – P. 1781-1784.
9. Radko, N.M. Peak risk assessing the process of information epidemics expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 251-255.
10. Ostapenko, A.G. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 173-176.
11. Islamgulova, V.V. Discreet risk-models of the process of the development of virus epidemics in non-uniform networks / V.V. Islamgulova, A.G. Ostapenko,,N.M. Radko, R.K. Babadzhanov, O.A. Ostapenko // Journal of Theoretical and Applied Information Technology. – 2016. – Vol. 86. – No.2. – P. 306-315.
12. Sokolova, E.S. Algorithm of Generation of Scale-Free Network at Realization Virus Attacks on Model Chiang Lu. / E.S. Sokolova, N.I. Barannikov, I.L. Bataronov, V.I.Belonozhkin, Research Journal of Pharmaceutical, Biological and Chemical Sciences. – 2016. – Vol. 7. – No.4. – P. 2438-2447.
13. Shvartskopf, E.A. Modeling of layering growth virus epidemic and spread of harmful content on Poisson networks / E.A. Shvartskopf, A.V. Zaryaev, L.V. Parinova, L.G. Popova. / Research Journal of Pharmaceutical, Biological and Chemical Sciences. – 2016. – Vol. 7. – No.4. – P. 2321-2331.
14. Ponomarenko, E.N. Discrete risk models of the process of viral epidemics development in homogenous information and telecommunication networks / E.N. Ponomarenko, V.N. Kostrova, R.K. Babadzhanov, Y.N. Guzev, V.S. Zarubin // Journal of Theoretical and Applied Information Technology. – 2016. – Vol. 92. – No.2. – P. 235-252.

15. Ostapenko, A.G. Denial of service in components of information telecommunication systems through the example of “network storm” attacks / A.G. Ostapenko, S.S. Kulikov, N.N. Tolstykh, Y.G. Pasternak, L.G. Popova // World Applied Sciences Journal. – 2013. – 25 (3). – P. 404-409.

16. Ostapenko, A.G. The usefulness and viability of systems: Assessment methodology taking into account possible damages / A.G. Ostapenko, E.F. Ivankin, V.S. Zarubin, A.V. Zaryaev // World Applied Sciences Journal. – 2013. – 25 (4). – P. 675-679.

17. Ostapenko, G.A. Analytical estimation of the component viability of distribution automated information data system / G.A. Ostapenko, D.G. Plotnicov, O.Y Makarov, N.M. Tikhomirov, V.G. Yurasov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 416-420.

18. Ostapenko, G.A. Analytical models of information-psychological impact of social information networks on users / G.A. Ostapenko, L.V. Parinova, V.I. Belonozhkin, I.L. Bataronov, K.V. Simonov // World Applied Sciences Journal. – 2013. – 25 (3). – P. 410-415.

19. Butuzov, V.V. Email-flooder attacks: The estimation and regulation of damage / V.V. Butuzov, A.G. Ostapenko, P.A. Parinov, G.A. Ostapenko // Life Science Journal. – 2014. – 11 (7s). – P. 213-218.

20. Radko, N.M. Assessment of the system’s EPI-resistance under conditions of information epidemic expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, D.V. Gusev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (3). – P. 1781-1784.

21. Radko, N.M. Peak risk assessing the process of information epidemics expansion / N.M. Radko, A.G. Ostapenko, S.V. Mashin, O.A. Ostapenko, A.S. Avdeev // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 251-255.

22. Ostapenko, A.G. Flood-attacks within the hypertext information transfer protocol: damage assessment and management / A.G. Ostapenko, M.V. Bursa, G.A. Ostapenko, D.O. Butrik // Biosciences Biotechnology Research Asia. – 2014. – Vol. 11 (Spl.End). – P. 173-176.

23. Islamgulova, V.V. Discreet risk-models of the process of the development of virus epidemics in non-uniform networks / V.V. Islamgulova, A.G. Ostapenko,,N.M. Radko, R.K. Babadzhanov, O.A. Ostapenko // Journal of Theoretical and Applied Information Technology. – 2016. – Vol. 86. – No.2. – P. 306-315.