В результате анализа атаки фишинга при авторизации пользователей публичного Wi-Fi следует учесть, что данный способ может быть использован практически в любых публичных сетях. Предложены комбинированные способы противодействия, включающие ограничительные меры и обучение населения основам информационной безопасности и цифровой гигиены.

DOI: 10.25728/iccss.2023.99.51.041

Фомин Н.А.

Уязвимости кибер-физических систем. Метод управления и оценивания защищенности кибер-физической системы водоснабжения

Аннотация: Рассмотрены особенности уязвимостей кибер-физических систем водоснабжения (КФСВ). Сформулированы определения – угроза безопасности, уязвимость и риск КФС. Описан метод управления и оценивания защищенности КФСВ.

Ключевые слова: кибербезопасность, кибер-физические системы, методы оценки безопасности, уязвимости, управление системами

Метод управления и оценивания защищенности кибер-физические системы водоснабжения (КФСВ) является элементом создаваемой модели безопасности социально-экономической системы цифрового водоканала. Метод M_1 входит в перечень мероприятий и механизмов формирования политики обеспечения кибербезопасности системы управления рассматриваемого объекта. Метод M_1 отличается от существующих выявлением и классификацией потенциальных уязвимостей, угроз и рисков функционирования КФСВ Умного города. На основе проведенного международного анализа проблем управления [1], сформируем требования к входам и выходам проектируемой модели [2]. На входе модели M_1 международные проблемы безопасности управления, стандарты, сведения о ресурсах, лучшие практики управления водными ресурсами. На выходе – классифицированный перечень потенциальных уязвимостей, угроз и рисков КФСВ (рисунок 1).

Рисунок 1 – Модель метода управления и оценивания защищенности КФСВ (M_1)

В последние годы угроза критической инфраструктуре водных систем возросла. Превентивные механизмы безопасности часто недостаточны для того, чтобы выявить и нейтрализовать действия злоумышленников. Обеспечение безопасности функционирования кибер-физических систем (КФС) «Умного города» является комплексной задачей [3, 4]. Проанализировав существующие тенденции функционирования КФС современных городов, можно выявить перечень актуальных уязвимостей и угроз безопасности управления [5, 6]. Сформулируем основные термины безопасности КФС [7].

Угроза безопасности кибер-физической системы – совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности функционирования КФС.

Уязвимость кибер-физической системы – недостаток (слабость) инфраструктурного, программного (программно-технического), программно-аппаратного уровней и влияние человеческого фактора на функционирование КФС в целом, который (которая) может быть использована для реализации угроз безопасности.

Риск безопасности кибер-физической системы – произведение степени вероятности возникновения угрозы функционирования КФС на размер (величину) потенциальных последствий.

Кибер-физические атаки на инфраструктуру водоснабжения возросли с увеличением количества подключенного оборудования и автоматизации водоснабжения – трансформации в управление «умной водой». Выявление и нейтрализация потенциальных уязвимостей важный процесс, позволяющий безопасно и эффективно использовать преимущества от цифрового оборудования в отрасли водоснабжения и водной безопасности

«Умных городов» [8, 9] и создания КФС поддержки и принятия решений [10, 11]. Одним из способов является совершенствование алгоритмов обнаружения кибер-физических атак управления водными сетями. Важным аспектом является процедура обнаружения атаки на КФСВ. Существуют различные механизмы комплексной оценки состояния систем, в том числе осуществление устойчивого и безопасного дистанционного мониторинга [12].

Совокупность мер оценки состояния системы на каждом временном шаге, в том числе с помощью искусственного интеллекта, способствует своевременному обнаружению определенных атак [13]. В научной работе [14] создан численно эффективный алгоритм достижения устойчивости и обнаружения атак на системы дистанционного мониторинга. На основе проведенных ранее исследований [15] и введенного термина уязвимости КФС, сгруппируем уязвимости КФСВ (рисунок 2).

Рисунок 2 – Группировка уязвимостей КФСВ

Расчет рисков (СтР_i) осуществлен для двух типов КФСВ – аналогового (АВ) и цифрового (ЦВ). Расчет состоит из нескольких подэтапов – первично требуется для каждой уязвимости (Уяз_i) рассчитать степень риска (СтР_i) указать вероятность (Вер_i) и потенциальные последствия реализации уязвимости (Посл_i) по формуле (1):

$$СтР_i = Вер_i * Посл_i. \quad (1)$$

Суммарные значения представлены в таблице 1, подробные расчеты отражены в таблице 2.

Таблица 1 – Сводный расчет $\sum Вер_i$ и $\sum Посл_i$ для АВ, ЦВ

Уязвимость ($Уяз_i$)	**Вероятность ($\sum Вер_i$)**		**Последствия ($\sum Посл_i$)**	
	АВ	**ЦВ**	**АВ**	**ЦВ**
Группа 1– Инфраструктурный уровень (системы водоснабжения, оборудование, источники водоснабжения)	0,78	0,17	0,78	0,70
Группа 2 – Программный уровень	0,60	0,69	0,68	0,73
Группа 3 – Аппаратный уровень (цифровое оборудование)	0,62	0,62	0,80	0,79
Группа 4 – Человеческий фактор (влияние человека на систему)	0,46	0,36	0,69	0,75

Таблица 2 –Детальный расчет $\sum Вер_i$ и $\sum Посл_i$ для *АВ*, *ЦВ* (группы 1 и 2)

	Уязвимость ($Уяз_i$)	**Вероятность ($\sum Вер_i$)**		**Последствия ($\sum Посл_i$)**	
		АВ	**ЦВ**	**АВ**	**ЦВ**
Группа 1 –Инфраструктурный уровень (системы водоснабжения, оборудование, источники водоснабжения)		0,78	0,17	0,78	0,70
1	Применение устаревших технологий по выявлению степени загрязнения воды ($Уяз_{1.1}$)	0,91	0,12	0,64	0,38
2	Высокий уровень износа инфраструктуры водоснабжения ($Уяз_{1.2}$)	0,79	0,37	0,72	0,46
3	Отсутствие резервных источников	0,62	0,09	0,87	0,87

	водоснабжения ($Уяз_{1.3}$)				
4	Отсутствие хранилищ пресной воды ($Уяз_{1.4}$)	0,64	0,21	0,72	0,72
5	Отсутствие систем мониторинга состояния сетей ($Уяз_{1.5}$)	0,85	0,05	0,87	0,87
6	Отсутствие магистральных систем мониторинга состояния воды, поставляемой потребителю ($Уяз_{1.6}$)	0,89	0,17	0,88	0,88
Группа 2 – Программный уровень		0,60	0,69	0,68	0,73
7	Программный код, НДВ ($Уяз_{2.1}$)	0,58	0,63	0,53	0,74
8	Программные инъекции ($Уяз_{2.2}$)	0,47	0,75	0,68	0,68
9	Доступность извне (потенциальное вторжение хакеров) ($Уяз_{2.3}$)	0,49	0,53	0,63	0,63
10	Бэкдоры импортного программного обеспечения ($Уяз_{2.4}$)	0,85	0,85	0,87	0,87

Представим наглядно полученные значения для каждой из уязвимостей ($Уяз_i$) АВ и ЦВ (рисунок 3, 4).

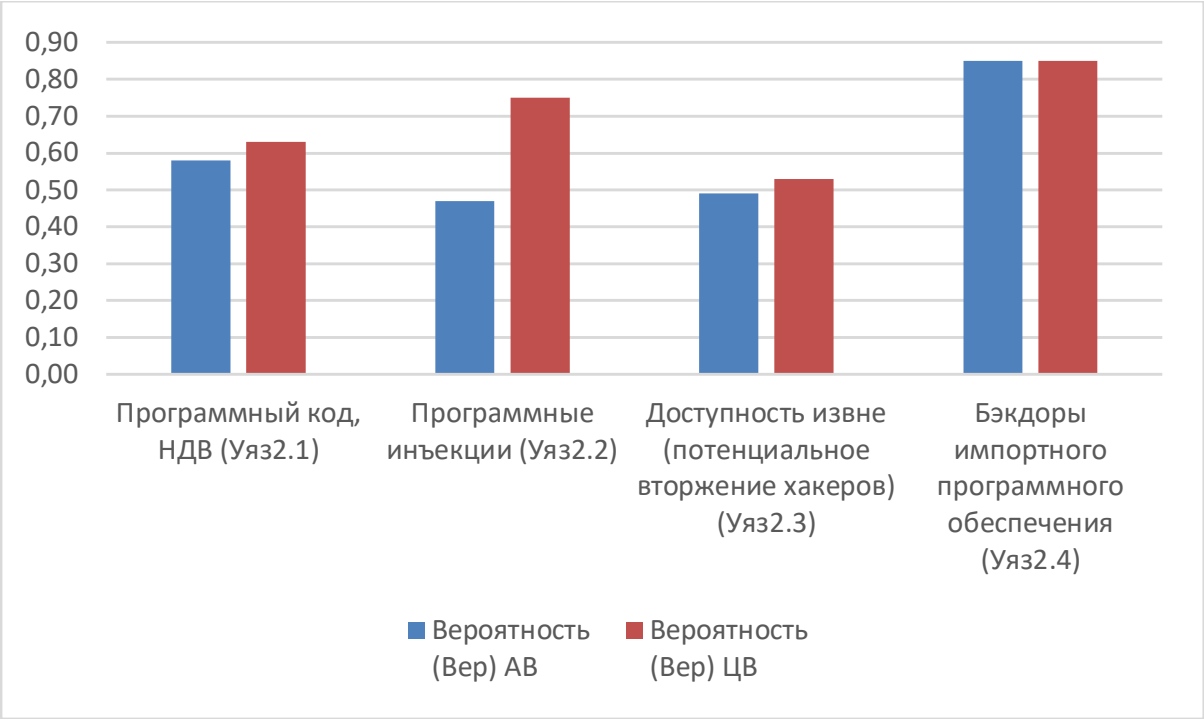

Рисунок 3 – Сравнение $Вер_i$ для АВ и ЦВ для $Уяз_i$ (группа 2 – Программный уровень)

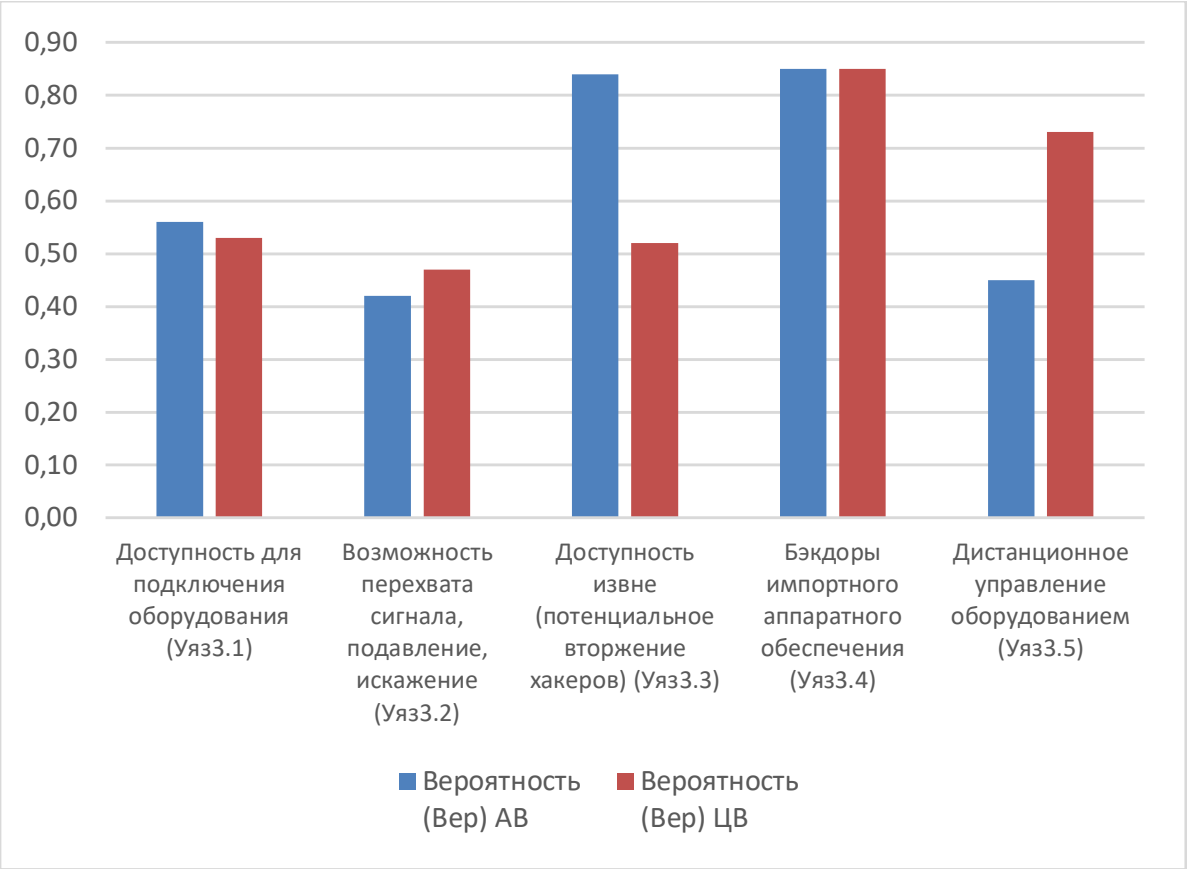

Рисунок 4 – Сравнение $Вер_i$ для АВ и ЦВ для $Уяз_i$ (группа 3 – Аппаратный уровень (цифровое оборудование))

Благодаря методу управления и оценивания защищенности КФСВ удалось осуществить классификацию перечня потенциальных уязвимостей, угроз КФСВ. На основе расчета рисков КФСВ можно сделать вывод о высоких рисках эксплуатации АВ, ЦВ КФСВ, которые необходимо учесть для повышения уровня безопасности КФСВ.

Литература:

1. *Nikolai A. Fomin, Roman V. Meshcheryakov.* Features of controlling the large-scale cyber-physical water supply systems in cities of different countries / Proceedings of the 13th International Conference "Management of Large-Scale System Development" (MLSD). – Moscow: IEEE, 2020. – P. 1-4. – DOI: 10.1109/MLSD49919.2020.9247813.

2. *Силич М.П.* Основы теории систем и системного анализа. – Томск: ТУСУР, 2013. – 342 с.

3. *Hadi Habibzadeh, Brian H. Nussbaum, Fazel Anjomshoa, Burak Kantarci, Tolga Soyata.* A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities // Sustainable Cities and Society. – 2019. – Volume 50. – 101660.

4. *Estévez A.T.* The fifth element: biodigital & genetics // Environmental Management of Air, Water, Agriculture, and Energy. – 2020. – P. 195-212. – DOI: 10.1201/9780429196607.

5. *Фомин Н.А., Самошина А.И., Евсютин О.О., Домуховский Н.А., Комаров Д.Е.* Повышение уровня стратегической безопасности объектов критической информационной инфраструктуры // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2020. – № 7. – С. 161-166.

6. Актуальные киберугрозы: итоги 2022 года. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения 10.10.2023).

7. *Fomin N., Meshcheryakov R.* Modelling Smart City Cyber-Physical Water Supply Systems: Vulnerabilities, Threats and Risks / In: Singh P.K., Veselov G., Vyatkin V., Pljonkin A., Dodero J.M., Kumar Y. (eds) Futuristic Trends in Network and Communication Technologies. FTNCT 2020. Communications in Computer and Information Science. Vol. 1395. – DOI: 10.1007/978-981-16-1480-4_15.

8. *Yang L., Elisa N., Eliot N.* Privacy and security aspects of E-government in smart cities / Smart cities cybersecurity and privacy. – Elsevier, 2019. – P. 89-102. – DOI: B978-0-12-815032-0.00007-X.

9. *Su Y., Gao W., Guan D.* Achieving urban water security: a review of water management approach from technology perspective // Water Resources Management. – 2020. – Vol. 34. – P. 1-17. – DOI: 10.1007/s11269-020-02663-9.

10. Shcherbakov M.V., Glotov A.V., Cheremisinov S.V. Proactive and predictive maintenance of cyber-physical systems / Kravets A., Bolshakov A., Shcherbakov M. (eds) Cyber-Physical Systems: Advances in Design & Modelling. Studies in Systems, Decision and Control. – Springer, Cham, 2020 – Vol. 259. – DOI: 10.1007/978-3-030-32579-4_21.

11. *Cao R., Hao L., Gao Q., Deng J., Chen J.* Modeling and Decision-Making Methods for a Class of Cyber–Physical Systems Based on Modified Hybrid Stochastic Timed Petri Net // IEEE Systems Journal

– 2020. – Vol. 14. Issue: 4. – P. 4684-4693. – DOI: 10.1109/JSYST.2020.2970748.

12. *Iskhakov A., Meshcheryakov R.* Intelligent System of Environment Monitoring on the Basis of a Set of IOT-Sensors / International Siberian Conference on Control and Communications (SIBCON). – Tomsk, 2019. – P. 1-5. – DOI: 10.1109/SIBCON.2019.8729628.

13. *Zeadally S., Adi, E., Baig Z., Khan I.A.* Harnessing artificial intelligence capabilities to improve cybersecurity // IEEE Access. – 2020. – Vol. 8. – Article 8963730. – P. 23817-23837. – DOI: 10.1109/ACCESS.2020.2968045.

14. *Ge X.H., Han Q.L., Zhang X.M., Ding D.., & Yang F.W.* Resilient and secure remote monitoring for a class of cyber-physical systems against attacks // Information Sciences. – 2020. – Volume 512. – P. 1592-1605. – DOI: 10.1016/j.ins.2019.10.057.

15. *Nikolai Fomin, Roman V. Meshcheryakov*. Digital Twin Security of the Cyber-Physical Water Supply System / Handbook of Digital Twins. – CRC Press, 2024. – 1040 p. (in print).

DOI: 10.25728/iccss.2023.65.26.042

Черняев М.Д.

Сравнение методов оценки риска ФСТЭК и EBIOS

Аннотация: Целью данной работы является сравнение двух методов оценки риска: EBIOS и ФСТЭК. EBIOS публикуется Национальным агентством кибербезопасности Франции (ANSSI), а ФСТЭК был разработан в России. Оба метода используются относительно локально, но уже доказали свою эффективность во Франции и России соответственно. В данной работе приводится краткое описание этих методов и их сравнение. Приведенное ниже исследование носит субъективный характер, и автор сравнивает эти методы, исходя из своих личных предпочтений, поскольку других подобных сравнений ранее не производилось. В ходе исследования дается краткое описание и сравнение обоих методов, поскольку оба имеют свои плюсы и минусы, и могут оказаться более