Научно-исследовательский журнал «Modern Economy Success»
https://mes-journal.ru
2025, № 4 / 2025, Iss. 4 https://mes-journal.ru/archives/category/publications
Научная статья / Original article
Шифр научной специальности: 5.2.3. Региональная и отраслевая экономика (экономические науки)
УДК 338.14

[1] Болгова А.М., [1] Куконкова А.М.,
[1] Российский государственный университет нефти и газа имени И.М. Губкина

Инструменты OSINT как компонент системы управления рисками

Аннотация: *целью* исследования является анализ инструментов OSINT как компонентов системы управления цифровыми рисками.

Методы: информационную базу исследования составили информационно-аналитические обзоры по киберугрозам в компаниях малого и среднего бизнеса, экспертное мнение специалистов по информационной безопасности и учебно-методические материалы по разведке по открытым источникам. В работе использованы следующие методы исследования: сравнение, обобщение, абстрагирование, классификация, систематизация, синтез и системный подход.

Результаты (Findings): в условиях стремительного развития киберугроз и роста объемов открытых данных инструменты OSINT (разведка на основе открытых источников) становятся неотъемлемой частью системы управления рисками. В статье анализируется потенциал OSINT для выявления уязвимостей, прогнозирования инцидентов и минимизации угроз в корпоративной среде. Рассматриваются методы сбора, обработки и интерпретации данных из открытых источников, а также их интеграция в автоматизированные системы оценки рисков. Особое внимание уделено практическому применению OSINT в кибербезопасности, выявлению утечек конфиденциальной информации и мониторингу теневых сегментов сети. В результате исследования предложены подходы к повышению эффективности OSINT в управлении рисками, обеспечивающие превентивное выявление угроз и снижение потенциального ущерба.

Выводы: доказано, что рост цифровизации экономики РФ сопровождается значительным увеличением киберугроз, при этом наиболее опасными являются вредоносное ПО, фишинг и DDoS-атаки, а средние убытки от утечек данных достигают $4,88 млн. Применение инструментов OSINT и внедрение систем управления рисками позволяют эффективно выявлять угрозы на ранних этапах, минимизировать финансовые потери и сокращать время реагирования на инциденты.

Ключевые слова: разведка по открытым источникам, OSINT, цифровая трансформация, информационная безопасность, информационные риски, кибератаки, меры минимизации

Для цитирования: Болгова А.М., Куконкова А.М. Инструменты OSINT как компонент системы управления рисками // Modern Economy Success. 2025. № 4. С. 234 – 239.

Поступила в редакцию: 26 марта 2025 г.; Одобрена после рецензирования: 24 мая 2025 г.; Принята к публикации: 11 июля 2025 г.

[1] Bolgova A.M., [1] Kukonkova A.M.,
[1] Gubkin Russian State University of Oil and Gas

OSINT tools as a component of the risk management system

Abstract: *the purpose* of the research is to analyze OSINT tools as components of a digital risk management system.

Methods: the information base of the study included information and analytical reviews of cyber threats in small and medium-sized businesses, expert opinions of information security specialists, and educational and methodolog-

ical materials on open source intelligence. The following research methods were used in the work: comparison, generalization, abstraction, classification, systematization, synthesis, and a systems approach.

Findings: with the rapid development of cyber threats and the growing volume of open data, OSINT (open source intelligence) tools are becoming an integral part of the risk management system. The article analyzes the potential of OSINT to identify vulnerabilities, predict incidents, and minimize threats in the corporate environment. Methods of collecting, processing and interpreting data from open sources, as well as their integration into automated risk assessment systems, are considered. Special attention is paid to the practical application of OSINT in cybersecurity, detection of confidential information leaks and monitoring of shadow network segments. As a result of the research, approaches to improving OSINT's effectiveness in risk management are proposed, ensuring the preventive detection of threats and reducing potential damage.

Conclusions: it has been proven that the growth of digitalization of the Russian economy is accompanied by a significant increase in cyber threats, with malware, phishing and DDoS attacks being the most dangerous, and average losses from data leaks reaching $4.88 million. The use of OSINT tools and the implementation of risk management systems make it possible to effectively identify threats at an early stage, minimize financial losses and reduce incident response time.

Keywords: open source intelligence, OSINT, digital transformation, information security, information risks, cyber-attacks, minimization measures

For citation: Bolgova A.M., Kukonkova A.M. OSINT tools as a component of the risk management system. Modern Economy Success. 2025. 4. P. 234 – 239.

The article was submitted: March 26, 2025; Approved after reviewing: May 24, 2025; Accepted for publication: July 11, 2025.

Введение

Согласно Указу Президента Российской Федерации от 7 мая 2024 года № 309 «О национальных целях развития Российской Федерации на период до 2030 года и на перспективу до 2036 года» одним из приоритетных направлений является цифровая трансформация экономики, поэтому можно наблюдать внедрение цифровых технологий во все сферы жизни. Как следствие цифровизации увеличивается объем данных в информационной среде, и в связи с этим непременно растёт количество киберугроз.

Так, например, за 2024 год было выявлено более 30 тыс. новых уязвимостей, что на 17% больше, чем в предыдущем году. По данным «Отчета о глобальных рисках 2024» Всемирного экономического форума, кибербезопасность останется постоянной проблемой, и в 2025 году сохранится риск атак на технологические ресурсы и услуги, включая финансовые системы и коммуникационную инфраструктуру [1, 3].

Актуальность исследования обусловлена тем, что 48% всех предприятий малого и среднего бизнеса подвергались кибератакам, а 43% из них не могут понять, какие именно меры безопасности им необходимы, согласно данным опубликованным в отчете Sage Group «Кибербезопасность для предприятий малого и среднего бизнеса: преодоление сложностей и построение устойчивости».

Материалы и методы исследований

Информационные риски в компаниях представляют собой опасность возникновения убытков или ущерба в результате обработки, хранении и передачи информации с помощью автоматизированных информационных систем, а также сбоев в работе этих систем. Как правило, все виды информационных рисков взаимосвязаны и оказывают влияния на деятельность предприятия. При этом изменение одного вида риска может вызывать изменение большинства остальных. В методических пособиях приводят различные классификации информационных рисков [2].

По характеру последствий выделяют допустимые и критические риски. Допустимый риск – это риск, при наступлении которого, организации понесут потери, не превышающие величину ожидаемой прибыли от деятельности предприятия и его деятельность, продолжает быть целесообразной. Критический риск – это риск, в результате наступления которого, предприятию грозят потери, превышающие предполагаемую прибыль от деятельности предприятия, и могут привести к потере всех средств, вложенных в реализацию проекта [5, 7].

Результаты и обсуждения

Реализация цифрового риска влечет за собой нарушение защищенности информационной системы организации, которая представляет собой

функцию взаимодействия основных параметров защиты информации:

- доступности;
- целостности;
- конфиденциальности.

Оказывая влияние на основные составляющие информационной безопасности, цифровые риски также делятся по типу воздействия на объекты информационной системы:

- кибератаки на системы управления производством. Могут произойти атаки с целью получения контроля над управляемыми объектами, изменения производственного процесса, выключения оборудования и т.д.;
- утечки информации. Взломы баз данных с конфиденциальной информацией о производстве, клиентах, поставщиках;
- социальная инженерия. Атака на слабости человеческого фактора и сбор информации о системах, паролях, аккаунтах;
- рассылка вредоносных программ через электронную почту или социальные сети. Могут нанести ущерб управляемым объектам, системам управления, базам данных;
- DDoS-атаки. Намеренное перегрузка систем лишними запросами, что приводит ко временной неработоспособности систем и к технологическим сбоям;
- использование уязвимостей в программном обеспечении. При отсутствии обновлений и защиты в систему могут попасть вредоносные программы;
- проникновение в систему через беспроводные сети. Уязвимые точки доступа могут использоваться для взлома систем;
- внутренние угрозы от сотрудников компании. Несанкционированный доступ или технические ошибки могут привести к утечкам информации или неправомерному управлению производственным процессом. [6]

Одним из методов предотвращения вышеперечисленных киберугроз является система управления рисками (СУР), которая представляет собой комплексный подход к выявлению, анализу и минимизации потенциальных угроз, способных повлиять на безопасность и стабильность организации. Важнейшим этапом управления рисками является выявление всех возможных угроз и уязвимостей, которые могут повлиять на безопасность организации. Это может включать анализ внутренних процессов, изучение внешних факторов и выявление потенциальных источников угроз [2].

В современных условиях значительную роль в этом процессе играет разведка на основе открытых источников (OSINT), которая позволяет собирать и анализировать информацию из различных источников для прогнозирования рисков и принятия решений. [4] Рассмотрим применение инструментов OSINT на первом этапе управления рисками [8, 9, 10].

Для этого вспомогательными методами выступают следующие инструменты OSINT:

- Поиск уязвимых систем в открытом доступе – инструменты, такие как Shodan, theHarvester позволяют выявлять устройства и сервисы, подключенные к интернету, которые могут представлять угрозу для компании. Например, обнаружение открытых портов SCADA-систем на объектах может указывать на потенциальные уязвимости.
- Анализ утечек данных – сервисы, такие как Have I Been Pwned, DeHashed, помогают выявлять случаи компрометации учетных записей сотрудников, что может привести к несанкционированному доступу к корпоративным системам.
- Мониторинг даркнета и теневых форумов – использование инструментов Intelligence X, Dark Web Monitor помогает выявлять обсуждения, касающиеся атак на определенную компанию, утечек корпоративной информации и данных о проданных уязвимостях.
- Разведка о потенциальных злоумышленниках – сервисы Social Links, Pipl, Sherlock позволяют собирать данные о киберпреступниках и возможных инициаторах атак, а также анализировать их активность.
- Корреляция данных из различных источников – инструменты, такие как Maltego, SpiderFoot, позволяют анализировать взаимосвязи между обнаруженными объектами, такими как IP-адреса, домены, email-адреса и социальные профили. Это помогает выявлять потенциальные атаки, связанные с социальной инженерией.

По результатам данного этапа можем получить список информационных рисков. Так, например, при анализе нескольких компаний малого и среднего предпринимательства с помощью прописанных выше инструментов были определены следующие распространённые информационные риски: атаки на персонал и фишинг, вредоносное ПО, DDoS и Dos атаки, атаки на системы управления промышленным оборудованием, атаки через устройства Интернет вещей, атаки на облачные инфраструктуры, сбои и отказы программных средств и сетевого оборудования и др.

Далее после выявления рисков был проведён анализ и оценка уровня потенциального воздействия. Этот процесс включает в себя

определение вероятности наступления угрозы и её последствий. Для определения особо опасных воспользуемся качественной оценкой рисков, а именно методом экспертной оценки. В табл. 1 представлены результаты, основанные на оценке пяти специалистов в области информационной безопасности.

Таблица 1

Метод экспертной оценки рисков.

Table 1

The method of expert risk assessment.

№ риска	Наименование риска	Среднее значение опасности	Среднее значение вероятности	Среднее значение важности
1	Вредоносное ПО	4,67	0,83	**3,88**
2	Атаки на персонал и фишинг	4,42	0,71	**3,1**
3	DDoS и Dos атаки	4,33	0,70	**3,03**
4	Атаки на системы управления промышленным оборудованием	4,1	0,62	**2,5**
5	Атаки через устройства Интернет вещей	4,0	0,50	2,0
6	Атаки на облачные инфраструктуры	3,9	0,50	1,95
7	Сбои и отказы программных средств	3,9	0,45	1,75
8	Сбои и отказы сетевого оборудования	3,9	0,45	1,75

Визуализация результатов представлена на тепловой карте рисков на рис. 1.

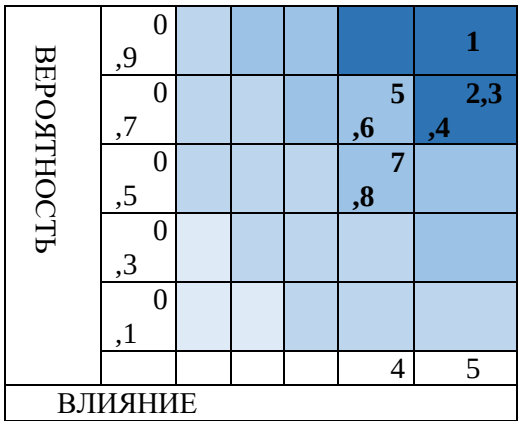

Рис. 1. Тепловая карта рисков.

Fig. 1. Heat map of risks.

По результатам проведенного исследования, особо значимыми информационными рисками являются №1 «Вредоносное ПО», №2 «Атаки на персонал и фишинг», №3 «DDoS и Dos атаки» и №4 «Атаки на системы управления промышленным оборудованием». Одна атака – будь то утечка данных, вредоносное ПО, программа-вымогатель или DDoS-атака – может иметь значительные последствия. Так, в « Отчете о киберготовности Hiscox 2024» показано, что 43% организаций потеряли существующих клиентов из-за кибератак, а согласно отчету IBM и Ponemon Institute, средняя общая стоимость утечек данных в 2024 году составила $4,88 млн. Одними из самых дорогостоящих утечек данных стали реализованные риски в сфере финансовых услуг – $6,08 млн.

На выявление и устранение утечки данных в среднем необходимо 258 дней, а если риск связан с кражей учетных данных, то количество дней увеличивается до 292 по данным отчета «Cost of a

Data Breach Report 2024», опубликованного IBM и Ponemon Institute.

Выводы

Таким образом, с помощью инструментов разведки данных по открытым источникам можно собирать информацию о новых уязвимостях в программном обеспечении и системах, что позволяет своевременно применять необходимые меры минимизации реализации информационных рисков и обновлению компонентов информационной безопасности предприятия. Инструменты позволяют находить, систематизировать информацию, размещенную в открытых источниках и превращать ее в полезные аналитические данные, что сокращает затрачиваемое время и денежные средства на устранения последствий киберугроз.

Список источников

1. 35 cybersecurity statistics to lose sleep over in 2025 // TechTagret URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 (дата обращения: 02.02.2025)

2. Harvard Business Review (HBR) // Управление рисками URL: https://upravlenie-riskami.ru/luchshie-knigi-po-upravleniyu-riskami/ (дата обращения: 05.02.2025)

3. The global risks report 2024 // World economiv forum URL: chrome-exten-si-on://efaidnbmnnnibpcajpcglclefindmkaj/https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (дата обращения: 02.02.2025)

4. Григорьев В.К. Управление рисками информационных технологий: учебное пособие. Москва: РТУ МИРЭА, 2023. 97 с.

5. Кононов Д.Ю. Оценка и учет инвестиционных рисков при прогнозных исследованиях развития ТЭК // Проблемы анализа риска. 2018. № 2. С. 72 – 77.

6. Вострецова Е.В. Основы информационной безопасности. Екатеринбург, 2019. 202 с.

7. Петренко С.А., Симонов С.В. Управление информационными рисками. Москва: Информационные технологии для инженеров, 2019. 386 с.

8. Шармае, В.И., Андреева Я.А., Василевский К.А. Обеспечение информационной безопасности с помощью разведки по открытым источникам (OSINT) // Вопросы защиты информации. 2022. № 2 (137). С. 45 – 50. DOI 10.52190/2073-2600_2022_2_45

9. Бикмаева А.А. OSINT в сфере информационной безопасности: методы и инструменты, используемые в разведке по открытым источникам // Актуальные вопросы научного познания молодого ученого: Материалы Всероссийской научно-практической конференции, Уфа, 20 июня 2024 года. Уфа: Уфимский юридический институт МВД РФ, 2024. С. 61 – 65.

10. Добросельская Е.С., Ешенко Р.А. Инструменты и методы разведки по открытым источникам // Информационные технологии в науке и образовании: Материалы Всероссийской научно-практической конференции, Хабаровск, 30-31 октября 2024 года. Хабаровск: Дальневосточный государственный университет путей сообщения, 2024. С. 300 – 305.

References

1. 35 cybersecurity statistics to lose sleep over in 2025. TechTagret URL: https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020 (date accessed: 02.02.2025)

2. Harvard Business Review (HBR). Risk Management URL: https://upravlenie-riskami.ru/luchshie-knigi-po-upravleniyu-riskami/ (date accessed: 05.02.2025)

3. The global risks report 2024. World economiv forum URL: chrome-exten-si-on://efaidnbmnnnibpcajpcglclefindmkaj/https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (date accessed: 05.02.2025)

4. The global risks report 2024. World economiv forum URL: chrome-exten-si-on://efaidnbmnnnibpcajpcglclefindmkaj/https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (date accessed: 05.02.2025) accessed: 02.02.2025)

4. Grigoriev V.K. Information Technology Risk Management: a tutorial. Moscow: RTU MIREA, 2023. 97 p.

5. Kononov D.Yu. Assessment and accounting of investment risks in predictive studies of the development of the fuel and energy complex. Problems of risk analysis. 2018. No. 2. P. 72 – 77.

6. Vostretsova E.V. Fundamentals of information security. Yekaterinburg, 2019. 202 p.

7. Petrenko S.A., Simonov S.V. Information Risk Management. Moscow: Information Technologies for Engineers, 2019. 386 p.

8. Sharmae, V.I., Andreeva Ya.A., Vasilevsky K.A. Ensuring information security using open source intelligence (OSINT). Information Security Issues. 2022. No. 2 (137). P. 45 – 50. DOI 10.52190/2073-2600_2022_2_45

9. Bikmaeva A.A. OSINT in the field of information security: methods and tools used in open source intelligence. Actual issues of scientific knowledge of a young scientist: Proceedings of the All-Russian scientific and practical conference, Ufa, June 20, 2024. Ufa: Ufa Law Institute of the Ministry of Internal Affairs of the Russian Federation, 2024. P. 61 – 65.

10. Dobroselskaya E.S., Yeshchenko R.A. Tools and methods of open source intelligence. Information technologies in science and education: Proceedings of the All-Russian scientific and practical conference, Khabarovsk, October 30-31, 2024. Khabarovsk: Far Eastern State Transport University, 2024. P. 300 – 305.

Информация об авторах

Болгова А.М., Российский государственный университет нефти и газа имени И.М. Губкина

Куконкова А.М., ассистент, Российский государственный университет нефти и газа имени И.М. Губкина

© Болгова А.М., Куконкова А.М., 2025