УДК 338.1 *DOI 10.46960/74159_2020_2_86*

Ю.Ю. Швец

РОЛЬ ИНФОРМАЦИОННЫХ РИСКОВ В СИСТЕМЕ НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ В КОНТЕКСТЕ ПАНДЕМИИ

Институт проблем управления им. В.А. Трапезникова РАН, Москва

Работа посвящена исследованию информационных рисков в системе национальной безопасности. Сегодняшняя биологическая угроза заставляет искать новые взаимосвязи между отраслями для повышения качества жизни и снижения информационных угроз. Представленные информационные угрозы требуют идентификации и нивелирования в будущем при возникновении подобных внешних ограничений. Это дает возможность быстро адаптироваться к повышению уровня внешний опасности для экономически активных агентов. К сожалению, работа по нивелированию подобного вида угроз сегодня не проводится. В стране проводится сопоставление информационных запросов и информационной повестки для того, чтобы показать белые пятна информационных рисков, на которые необходимо реагировать. Имеющая реакция позволяет расширить негативное внешнее влияние и повысить уровень угрозы путем фишинговых атак на экономически активное население. В статье приводится схема работы по созданию принципов и основ минимизации издержек при борьбе с информационными рисками.

Ключевые слова: информационный риск, экономическая безопасность, пандемия, фишинговая атака, корреляция экономического взаимодействия, информационная повестка.

Введение

Экономические подходы, связанные с обеспечением национальной безопасности, имеют множество институциональных ограничений, которые в рамках внешних факторов, таких как пандемия, играют положительную роль для повышения эффективности отдельных систем. Система здравоохранения, начиная с марта 2020 года, проявила себя встроенной в систему национальной безопасности и, начиная с этого периода, в связи с внешней угрозой, показала себя не как агентом, а как принципалом в системе государственного управления. Целью статьи является выявление уровня экономических угроз в разрезе проведения борьбы с COVID-19 на национальном уровне в России. Задачей работы является определение принципов и задач информационной безопасности в контексте информационных потоков.

Проведение подобного исследования требует определения понятий параэкономических терминов и понятий, которые имеют место в процессе движения от сугубо медицинских фактов в экономическую реальность. Различное понимание понятий и терминов привело к тому, что некоторые страны ввели ограничения относительно поздно, и вполне возможно, это привело к увеличенному количеству заболевших COVID-19. Одним из классов средств, позволяющих обеспечить безопасность систем любого уровня и набора устройств, являются системы управления информацией и событиями безопасности (Security Informational and Event Management SIEM).[1]

В контексте приоритета предупредительным мер в целях обеспечения безопасности[2] под пандемией понимается ситуация с заболеванием выявленном более чем у 5% населения страны и/или распространение нового заболевания в мировом масштабе[3]. Самое же формула «COVID-19» понимается как определение, данное Всемирной организацией здравоохранения 11 февраля 2020 года как одна из вариаций внешних эффектов, приводящих к повышенному биологическому риску населения. Говорить о том, что человечество не знакомо с причинами и последствиями коронавирусных инфекций также нельзя, поскольку эффект SARS (острый тяжелый респираторный синдром) и MERS (ближневосточный респираторный синдром) знакомы регионам Юго-Восточной Азии с 2002 года[4]. В данном контексте интересной представляется и ситуация в Российской Федерации на конец 2019 года, когда Роспотребнадзор начал фиксировать увеличение количества заболевших пневмонией, то есть за несколько месяцев до официального объявления пандемии[5].

Обработка данных

Обработка данных представляет собой систематизированную последовательность операций, совершаемых с данными, с целью извлечения новой конструктивной и полезной информации посредством вычислений, пересмотра и анализа имеющейся информации, а также представления ее в качественно новой форме. При этом постоянно увеличивается количество

[1] Kotenko I.V., Chechulin A.A. A Cyber Attack Modeling and Impact Assessment Framework // Proceedings of 5th International Conference on Cyber Conflict 2013 (CyCon 2013). 2013. pp. 119–142.

[2] Статья 2 Федерального закона «О безопасности» №390-ФЗ от 28.12.2010. Законодательная база «Гарант». [Электронный ресурс]. – URL: http://www.consultant.ru /document/cons_doc_LAW_108546/247e2ca8fe0f9d1d821eae037dd70806804b0d3c/

[3] Всемирная организация здравоохранения. [Электронный ресурс]. – URL: https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/ru/

[4] About Severe Acute Respiratory Syndrome. U.S. Centers for Disease Control and Prevention. [Электронный ресурс]. – URL: https://www.cdc.gov/sars/about/index.html

[5] Газета РБК. Росстат зафиксировал рост заболеваемости пневмонией в Москве. [Электронный ресурс]. – URL: https://www.rbc.ru/society/13/03/2020/5e62695e9a794761618f1a7b

источников информации о текущем состоянии защищенности, усложняя администраторам информационной безопасности задачу контроля над общей картиной происходящего. Суть процесса обработки данных мониторинга заключается в обнаружении необходимых на практике знаний в большом количестве необработанного материала, который делает эти знания неочевидными[6]. Обеспечение поставленной цели обработки данных мониторинга ресурсов сети достигается путем выполнения следующих прикладных задач[7]: оценка качества собранных данных; ввод данных в различные информационные системы; интеллектуальный анализ данных; представление данных; хранение накопленных данных; доступ к данным.

Формирование информационных рисков можно отследить по запросам сервиса подбора слов Яндекс, который позволяет отслеживать статистику запросов по различным параметрам[8]. В этом случае необходимо выработать понятие защищенной информации, которая в целом будет стремиться к минимизации рисков и защиты информации от внешних эффектов. Соответственно с увеличением спроса на безопасную информацию необходимо определить общий список информационных подкастов, связанных с качеством жизни в новом статусе, которые в подобные периоды будут пользоваться наибольшим спросом, а, следовательно, требуют дополнительной защиты.

В частности, издание NewsGuard[9] показало завышение уровня заболеваемости некоторыми СМИ, в связи с тем, что на одной площадке находятся люди с различным социальном поведением. Это создает повышенные риск изменения социального поведения и социального доступа, но также открывает новые возможности для фишинговых атак, таких, как электронные письма с вредоносным вложением; предложение по установке заведомо вредоносных вложений (например, отслеживание социальных контактов)[10]; ложных информационных порталов с генерациями кодов

[6] Цветков А.А. Задачи обработки данных мониторинга ресурсов распределения вычислительной сети // Науковедение. Выпуск 4(23). 2014. [Электронные ресурс]. – URL: https://naukovedenie.ru/PDF/81TVN414.pdf

[7] Там же.

[8] Информационные ресурс статистики поиска слов wordstat.yandex.ru. Электронные ресурс] – URL: https://wordstat.yandex.ru/#!/history?words=%D0%BF%D0%B0%D0%BD%D0%B4%D0%B5%D0%BC%D0%B8%D1%8F

[9] Coronavirus misinformation spreading fast: Fake news on COVID-19 shared far more than CDC, WHO reports. [Электронный ресурс]. – URL: https://www.zdnet.com/article/coronavirus- misinformation-is-increasing-newsguard-finds.

[10] Managing the information security impact of Covid-19. Газета KPMG. [Электронный ресурс]. – URL: https://home.kpmg/xx/en/home/insights/2020/04/managing-the-information-security-impact-of-covid-19.html

доступа к условно закрытой информации[11]; доступ к удаленным фазам видеоконференции (skype, teams, zoom и т.д.)[12].

Необходимо обратить внимание, что многокомпонентная сфера использует входные данные из результатов деятельности предыдущих блоков, что не всегда является строго определенным. Более полезным являлось бы использование циклических операций между модулями / участника системы[13], а сами участники модулей могли бы выравниваться в правах и обязанностях, исходя из своей экономической роли. В частности, говоря о последнем сервисе и отходя от социальной инженерии, можно привести пример из биржевого опыта, когда резкий рост спроса на сервисы дистанционного общения, в частности zoom, привел к скачку спроса инвесторов на акции данной компании, при том инвесторы вместо Zoom Video Communication купили акции Zoom Technologies, повысив капитализацию компании на 47000%[14].

В отечественной информационной системе наблюдался рост потребления государственных информационных ресурсов, которые в марте-апреле 2020 года показывали сбои (например, mail.ru), а некоторые коммуникационные сервисы решились на блокирование видео высокой четкости[15]. В этом случае можно говорить о корреляции уровня биологической и информационной безопасности.

В этом случае вопрос об информационной безопасности, который затрагивается в Государственной программе «Информационное общество», видится в новом ключе, что требует институционального вмешательства и корректировки для создания и поддержания баланса информационной безопасности во время биологических угроз.

В частности, сравнение появления предписывающих (запретительных) актов с информационной повесткой дня[16], позволило сделать вывод, что последняя остается незакрытой. Следовательно, запросы общества по обеспечению экономической безопасности в этом аспекте не соблюдаются, то есть запросы общества шире, чем разъяснительные документы.

---

[11] Technology information secutiry. [Электронный ресурс]. URL: https://www.ey.com/en_gl/covid-19/technology-information-security

[12] Covid-19 hygiene for conferencing. Газета KPMG. [Электронный ресурс]. URL: https://home.kpmg/xx/en/home/insights/2020/04/covid-19-hygiene-for-conferencing.html

[13] Федорченко, А. В., Левшун, Д. С., Чечулин, А. А., & Котенко, И. В. (2016). Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. *Труды СПИИРАН*, *4*(47), 5-27.

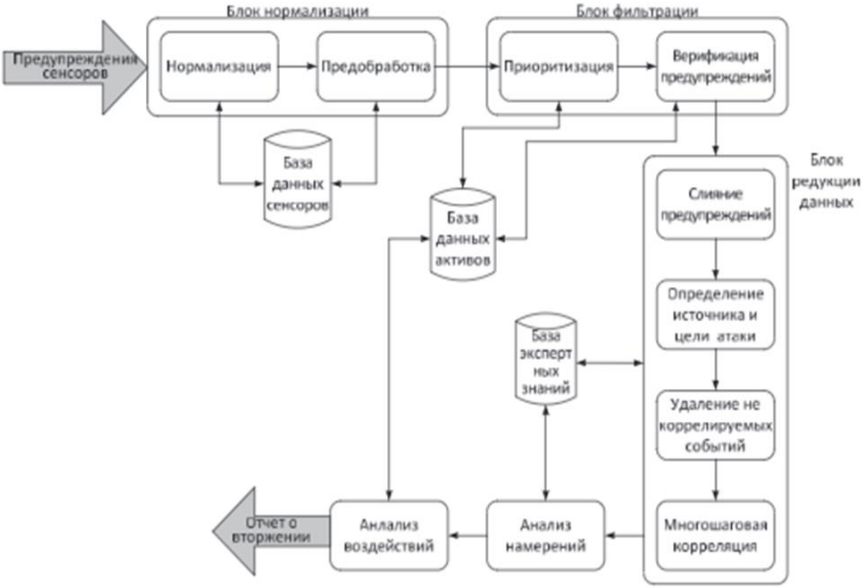
[14] Инвесторы по ошибке купили акции Zoom Technologies вместо стартапа Zoom и подняли их цену на 47 000%. [Электронный ресурс]. URL: https://vc.ru/finance/65037-investory-po-oshibke-kupili-akcii-zoom-technologies-vmesto-startapa-zoom-i-podnyali-ih-cenu-na-47-000

[15] Your internet may be getting slower as coronavirus outbreak causes huge surge in daytime traffic. [Электронный ресурс]. URL: https://www.thesun.co.uk/tech/11208549/vodafone-talktalk-internet-traffic-uk-coronavirus/

[16] Проведено автором на основании законодательных актов и сервиса wordstat.yandex.ru

Таким образом, экономическая деятельность агентов малого бизнеса не была подготовлена, и не было предложено путей по информационной стабилизации ситуации, о чем свидетельствуют пиковые информационные запросы в различные периоды пандемии.

Проработка сценариев действий бизнеса во время биологических угроз, или же корреляции информационных потоков, может стать дополнением для Государственных программ с целью недопущения резкого снижения количества зарегистрированных субъектов малого и среднего бизнеса[17]. Подобные модели, показанные на рисунке далее, корреляции прорабатываются для обеспечения информационной безопасности в сугубо узких целях.



Модель процесса корреляции событий безопасности

Источник: Elshoushand H.T., Osman I.M. An improved framework for in trusion alert correlation // Proceedings of World Congre ss on Engineering 2012 (WCE 2012) . 2012. vol. 1. pp. 518–524.

Такой информационной повесткой обеспечения информационной безопасности экономически активных субъектов может стать:

[17] Федеральная налоговая служба. [Электронный ресурс]. – URL: Режим доступа https://www.nalog.ru/rn77//related_activities/statistics_and_analytics/forms/9558929/

1) разработка сценариев работы субъектов малого и среднего бизнеса при наличии внешних угроз (биологических, информационных, природных и т.д.). Например, необходимо определить возможность работы предприятия при изменении внешних условий, связанных с изменением вида деятельности и создания актуальных запросов по перепрофилированию производству. Так, предприятия производящие текстильные изделия могут в течение производственного цикла переквалифицироваться для производства медицинских изделий (масок, халатов и т.д.). Места общественного питания могут обеспечить продуктами питания людей и расширить свой ассортимент;

2) разработка курсов повышения квалификации для кадров для изменения вида деятельности;

3) разработка текущих версий программного обеспечения для обеспечения экономической безопасности граждан по обеспечения информации и субъектов МСП по обеспечению этой информацией.

4) включение в борьбу с фишингом и электронным, банковским мошенничеством компаний, которые обладают достаточными информационными, неиспользованным ресурсами (например, крупные банковские учреждения);

5) разработка доступности информационных потоков для МСП, населения для снижения экономических рисков для указанных субъектов с целью недопущения повышения рисков потери финансовых ресурсов путем систематизации информации как доступной и проверенной, так и информации из открытых источников, что покажет повышенный риск их использования для конечного пользователя.

Заключение

Указанные мероприятия должны привести к снижению информационных рисков в системе национальной безопасности в текущей биологической угрозе. Турбулентное пространство, связанное с реализацией внешних угроз, требует, в целях обеспечения национальное безопасности, отработки информационных потоков с целью недопущения снижения качества жизни населения и экономической активности. В дальнейшем это позволит настраивать корреляцию для информационных потоков для снижения уровня информационного риска и экономической безопасности в периоды наступления внешних угроз. Фактическая редукция – уменьшение общего количества событий до достаточного уровня – позволит нормализовать работу любой системы после вмешательства в ее деятельность.

© Швец Ю.Ю., 2020.

Библиографический список

[1] Kotenko I.V., Chechulin A.A. A Cyber Attack Modeling and Impact Assessment Framework // Proceedings of 5th International Conference on Cyber Conflict 2013 (CyCon 2013). 2013. pp. 119–142.

[2] Статья 2 Федерального закона «О безопасности» №390-ФЗ от 28.12.2010. Законодательная база «Гарант» Электронный ресурс. Режим доступа http://www.consultant.ru/document/cons_doc_LAW_108546/247e2ca8fe0f9d1d821eae037dd70806804b0d3c/ (дата доступа 10.06.2020).

[3] Всемирная организация здравоохранения. [Электронный ресурс]. – URL: https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/ru/

[4] About Severe Acute Respiratory Syndrome. U.S. Centers for Disease Control and Prevention. [Электронный ресурс]. URL: https://www.cdc.gov/sars/about/index.html

[5] Газета РБК. Росстат зафиксировал рост заболеваемости пневмонией в Москве. [Электронный ресурс]. – URL: https://www.rbc.ru/society/13/03/2020/5e62695e9a794761618f1a7b

[6] Цветков А.А. Задачи обработки данных мониторинга ресурсов распределения вычислительной сети // Науковедение. Выпуск 4(23). 2014. [Электронные ресурс]. URL: https://naukovedenie.ru/PDF/81TVN414.pdf

[7] Информационные ресурс статистики поиска слов wordstat.yandex.ru. [Электронный ресурс]. – URL: https://wordstat.yandex.ru/#!/history?words=%D0%BF%D0%B0%D0%BD%D0%B4%D0%B5%D0%BC%D0%B8%D1%8F

[8] Coronavirus misinformation spreading fast: Fake news on COVID-19 shared far more than CDC, WHO reports. [Электронный ресурс]. – URL: https://www.zdnet.com/article/coronavirus-misinformation-is-increasing-newsguard-finds.

[9] Managing the information security impact of Covid-19. Газета KPMG. [Электронный ресурс]. – URL: https://home.kpmg/xx/en/home/insights/2020/04/managing-the-information-security-impact-of-covid-19.html

[10] Technology information secutiry. [Электронный ресурс]. – URL: https://www.ey.com/en_gl/covid-19/technology-information-security

[11] Covid-19 hygiene for conferencing. Газета KPMG. [Электронный ресурс]. – URL: https://home.kpmg/xx/en/home/insights/2020/04/covid-19-hygiene-for-conferencing.html

[12] Федорченко, А. В., Левшун, Д. С., Чечулин, А. А., & Котенко, И. В. (2016). Анализ методов корреляции событий безопасности в SIEM-системах. Часть 1. Труды СПИИРАН, 4(47), 5-27.

[13] Инвесторы по ошибке купили акции Zoom Technologies вместо стартапа Zoom и подняли их цену на 47 000%. [Электронный ресурс]. – URL: https://vc.ru/finance/65037-investory-po-oshibke-kupili-akcii-zoom-technologies-vmesto-startapa-zoom-i-podnyali-ih-cenu-na-47-000

[14] Your internet may be getting slower as coronavirus outbreak causes huge surge in daytime traffic. [Электронный ресурс]. – URL:

https://www.thesun.co.uk/tech/11208549/vodafone-talktalk-internet-traffic-uk-coronavirus/

[15] Федеральная налоговая служба. [Электронный ресурс]. URL: https://www.nalog.ru/rn77//related_activities/statistics_and_analytics/forms/9558929/

[16] Elshoushand H.T., Osman I.M. An improved framework for in trusion alert correlation // Proceedings of World Congre ss on Engineering 2012 (WCE 2012) . 2012. vol. 1. pp. 518–524.

Yu.Yu. Shvets

THE ROLE OF INFORMATION RISKS IN THE NATIONAL SECURITY SYSTEM IN THE CONTEXT OF THE PANDEMIC

Institute of Control Sciences of V.A. Trapeznikov of RAS, Moscow

Abstract. The work is devoted to the study of information risks in the system of national security. Today's biological threat forces us to look for new interconnections between industries to improve the quality of life and reduce information threats. The presented information threats require identification and leveling in the future in the event of such external restrictions. This makes it possible to quickly adapt to the increased level of external danger for economically active agents. Unfortunately, work on leveling this type of threat is not carried out today. Comparison of information requests and information agenda is made in order to show white spots of information risks that need to be responded to. Having a reaction allows us to expand negative external influence and increase the level of threat by phishing attacks on the economically active population. The article provides a scheme of work on creation of principles and foundations for minimizing costs in the fight against information risks.

Keywords: information risk, economic security, pandemic, phishing attack, correlation of economic interaction, information agenda

References

[1] Kotenko I.V., Chechulin A.A. (2013). [A Cyber Attack Modeling and Impact Assess-ment Framework]. *Proceedings of the 5th International Conference on Cyber Conflict 2013*. pp. 119-142. (Russian Translation).

[2] Article 2 of the Federal Law "On Security" No. 390-FZ of 28.12.2010. Legislative base "Garant". [Electronic resource]. Available at: http://www.consultant.ru/document/cons_doc_LAW_108546/247e2ca8fe0f9d1d821eae037dd70806804b0d3c/

[3] World Health Organization. [Electronic resource]. Available at: https://www.who.int/csr/disease/swineflu/frequently_asked_questions/pandemic/ru/

[4] About Severe Acute Respiratory Syndrome. U.S. Centers for Disease Control and Prevention. [Electronic resource]. Available at: https://www.cdc.gov/sars/about/index.html

[5] RBC newspaper. Rosstat recorded an increase in the incidence of pneumonia in Moscow. [Electronic resource]. Available at: https://www.rbc.ru/society/13/03/2020/5e62695e9a794761618f1a7b

[6] Tsvetkov, A.A. (2014). [Problems of processing data for monitoring the resources of the distribution of a computer network]. *Naukovedenie* [Science study]. Issue 4 (23). [Electronic resource]. Available at: https://naukovedenie.ru/PDF/81TVN414.pdf

[7] Wordstat.yandex.ru information resource for word search statistics. [Electronic resource]. Available at: https://wordstat.yandex.ru/#!/history?words=%D0%BF%D0%B0%D0%BD%D0%B4%D0%B5%D0%BC%D0%B8%D1% 8F

[8] Coronavirus misinformation spreading fast: Fake news on COVID-19 shared far more than CDC, WHO reports. [Electronic resource]. Available at: https://www.zdnet.com/article/coronavirus-misinformation-is-increasing-newsguard-finds.

[9] Managing the information security impact of Covid-19. KPMG newspaper. [Electronic resource]. Available at: https://home.kpmg/xx/en/home/insights/2020/04/managing-the-information-security-impact-of-covid-19.html

[10] Technology information secutiry. [Electronic resource]. Available at: https://www.ey.com/en_gl/covid-19/technology-information-security

[11] Covid-19 hygiene for conferencing. KPMG newspaper. [Electronic resource]. Available at: https://home.kpmg/xx/en/home/insights/2020/04/covid-19-hygiene-for-conferencing.html

[12] Fedorchenko, A.V., Levshun, D.S., Chechulin, A.A., Kotenko, I.V. (2016). [Analysis of methods for correlating security events in SIEM systems]. *Trudy SPIIRAN* [Proceedings of SPIIRAN]. 4 (47). pp. 5-27. (In Russ.).

[13] Investors mistakenly bought shares of Zoom Technologies instead of the startup Zoom and raised their price by 47,000%. [Electronic resource]. Available at: https://vc.ru/finance/65037-investory-po-oshibke-kupili-akcii-zoom-technologies-vmesto-startapa-zoom-i-podnyali-ih-cenu-na-47-000

[14] Your internet may be getting slower as coronavirus outbreak causes huge surge in daytime traffic. [Electronic resource]. Available at: https://www.thesun.co.uk/tech/11208549/vodafone-talktalk-internet-traffic-uk-coronavirus/

[15] Federal Tax Service. [Electronic resource]. Availble at: https://www.nalog.ru/rn77//related_activities/statistics_and_analytics/forms/9558929/

[16] Elshoushand, H.T., Osman, I.M. (2012). [An improved framework for in trusion alert correction]. *Proceedings of World Congress on Engineering 2012 (WCE 2012).* Vol. 1. pp. 518-524.