ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
ҰЛТТЫҚ ҒЫЛЫМ АКАДЕМИЯСЫ

әл-Фараби атындағы Қазақ ұлттық университетінің

ХАБАРЛАРЫ

ИЗВЕСТИЯ

НАЦИОНАЛЬНОЙ АКАДЕМИИ
НАУК РЕСПУБЛИКИ КАЗАХСТАН
Казахский национальный
университет имени аль-Фараби

N E W S

OF THE ACADEMY OF SCIENCES
OF THE REPUBLIC OF
KAZAKHSTAN
al-Farabi Kazakh National University

PHYSICO-MATHEMATICAL SERIES

4 (344)

OCTOBER – DECEMBER 2022

PUBLISHED SINCE JANUARY 1963

PUBLISHED 4 TIMES A YEAR

ALMATY, NAS RK

«ҚР ҰҒА Хабарлары. Физика-математикалық сериясы».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Меншіктеуші: «Қазақстан Республикасының Ұлттық ғылым академиясы» РҚБ (Алматы қ.). Қазақстан Республикасының Ақпарат және қоғамдық даму министрлігінің Ақпарат комитетінде 14.02.2018 ж. берілген **No 16906-Ж** мерзімдік басылым тіркеуіне қойылу туралы куәлік.
Тақырыптық бағыты: *физика-математикалық сериясы».*
Қазіргі уақытта: *«ақпараттық технологиялар»бағыты бойынша ҚР БҒМ БҒСБК ұсынған журналдар тізіміне енді.*
Мерзімділігі: *жылына 4 рет.*
Тиражы: *300 дана.*
Редакцияның мекен-жайы: *050010, Алматы қ., Шевченко көш., 28, 219 бөл., тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Типографияның мекен-жайы: «Аруна» ЖК, Алматы қ., Мұратбаев көш., 75.

«Известия НАН РК. Серия физико-математическая».
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Собственник: *Республиканское общественное объединение «Национальная академия наук Республики Казахстан» (г. Алматы).*
Свидетельство о постановке на учет периодического печатного издания в Комитете информации Министерства информации и общественного развития Республики Казахстан **No 16906-Ж** выданное 14.02.2018 г.
Тематическая направленность: *серия физика-математическая.*
В настоящее время: *вошел в список журналов, рекомендованных ККСОН МОН РК по направлению «информационные коммуникационные технологии».*
Периодичность: *4 раз в год.*
Тираж: *300 экземпляров.*
Адрес редакции: *050010, г. Алматы, ул. Шевченко, 28, оф. 219, тел.: 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Адрес типографии: ИП «Аруна», г. Алматы, ул. Муратбаева, 75.

News of the National Academy of Sciences of the Republic of Kazakhstan.
Physico-matematical series.
ISSN 2518-1726 (Online),
ISSN 1991-346X (Print)

Owner: RPA «National Academy of Sciences of the Republic of Kazakhstan» (Almaty). The certificate of registration of a periodical printed publication in the Committee of information of the Ministry of Information and Social Development of the Republic of Kazakhstan **No. 16906-Ж,** issued 14.02.2018
Thematic scope: *physical-mathematical series.*
Currently: *included in the list of journals recommended by the CCSES MES RK in the direction of «information and communication technologies».*
Periodicity: *4 times a year.*
Circulation: *300 copies.*
Editorial address: *28, Shevchenko str., of. 219, Almaty, 050010, tel. 272-13-19*
http://www.physico-mathematical.kz/index.php/en/

Address of printing house: ST «Aruna», 75, Muratbayev str, Almaty.

NEWS OF THE NATIONAL ACADEMY OF SCIENCES
OF THE REPUBLIC OF KAZAKHSTAN
PHYSICO-MATHEMATICAL SERIES
ISSN 1991-346X
Volume 4, Namber 344 (2022), 68-80
https://doi.org/10.32014/2022.2518-1726.157

МРНТИ81.93.29
УДК 004.056.5

С.Т. Мамбетов[1*], Е.Е. Бегимбаева[1,2], С.К. Джолдасбаев[3], Б.О. Куламбаев[3], Г.Н. Казбекова[4]

[1]Казахский национальный университет им. аль-Фараби, Алматы, Казахстан;
[2]Казахский национальный исследовательский технический университет имени К.И. Сатпаева, Алматы, Казахстан;
[3]Международный университет информационных технологий, Алматы, Казахстан;
[4]Международный казахско-турецкий университет имени Ходжи Ахмеда Ясави, Туркестан, Казахстан.
E-mail: *mambetov.saken@gmail.com*

О МОНИТОРИНГЕ УГРОЗ И УЯЗВИМОСТЕЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Аннотация. Стремительная информатизация в разных сферах деятельности общества имеет радикальное влияние на доступ и обработку информации. В буквальном смысле за последние два десятилетия появились новые формы транслирования и передачи данных и совершенно новые виды деятельности внутри мировой Интернет-паутины, связанные с последними новшествами. Широко распространилось понятие «социальная сеть», в котором люди без всяких страхов и не имея представления о риске афишируют свои данные на публику. Сейчас крайне редко можно встретить человека, который не пользуется ни одним приложением социальной сети, и чаще всего верно утверждение, что один человек пользуется несколькими разными приложениями. Кроме того, в ходе работы используются Интернет-сервисы, поисковые системы, электронная почта. Соответственно, возрастают и появляются новые, ранее неизвестные виды разного рода угроз и уязвимости информационных систем. С развитием Интернета атаки хакеров также были сосредоточены на тех же уязвимостях и новых типах угроз. Система мониторинга помогает выявлять эти уязвимости и угрозы. В свою очередь, мониторинг ситуации с

информационной безопасностью создает возможность контролировать работу ИТ-ресурсов, сетевых программ, устройств и веб-сервисов любой компании в автоматическом режиме. Благодаря постоянному мониторингу (контролю) можно вовремя выявить уязвимости и угрозы информационной системы и остановить их работу. Своевременный мониторинг снижает размер ущерба, причиняемого информационной системе. В данной статье мы приводим анализ по направлению исследования мониторинга угроз и уязвимостей информационной системы, методов защиты от угроз с приоритетом, основанных на анализе данных тематических Интернет-ресурсов. Кроме того, будет сделан обзор предыдущих статей авторов.

Ключевые слова: мониторинг; Интернет-угрозы; уязвимости; кибербезопасность.

С.Т. Мамбетов[1*], Е.Е. Бегимбаева[1,2], С.К. Джолдасбаев[3], Б.О. Куламбаев[3], Г.Н. Казбекова[4]

[1]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан;
[2]Қ.И. Сәтбаев атындағы Қазақ ұлттық техникалық зерттеу университеті, Алматы, Қазақстан;
[3]Халықаралық Ақпараттық технологиялар университеті, Алматы, Қазақстан;
[4]Қожа Ахмет Яссауи атындағы Халықаралық Қазақ-Түрік университеті, Түркістан, Қазақстан.
E-mail: *mambetov.saken@gmail.com*

АҚПАРАТТЫҚ ЖҮЙЕНІҢ ҚАУІПТЕРІ МЕН ОСАЛ ТҰСТАРЫНЫҢ МОНИТОРИНГІ ТУРАЛЫ

Аннотация. Қоғамның әртүрлі салаларындағы жедел ақпараттандыру ақпаратқа қол жеткізу мен өңдеуге түбегейлі әсер етеді. Соңғы екі онжылдықта инновациялармен байланысты ғаламдық интернет желісінде хабар тарату мен деректерді берудің жаңа нысандары және жаңа қызмет түрлері пайда болды. Әлеуметтік желі ұғымы кең тарап, онда адамдар қорқынышсыз, қауіп туралы ешқандай түсініксіз өз деректерін көпшілікке жариялап отырады. Қазір ешқандай әлеуметтік желі қосымшасын пайдаланбайтын адам өте сирек кездеседі және көбінесе бір адам бірнеше түрлі қосымшаларды пайдаланады деген мәлімдеме шындыққа сәйкес келеді. Оған қоса жұмыс барысында интернет сервистерді, іздеу жүйелерін, электронды пошталарды қолданады. Сәйкесінше, ақпараттық жүйелердің жаңа, бұрын белгісіз, әртүрлі қауіптер мен осал түрлері көбейіп, пайда болуда. Ғаламтор желісінің дамуымен хакерлердің де шабуылдары сол осалдықтар мен жаңа қауіп түрлеріне бағытталды. Осы осалдықтар мен төнетін қауіптерді анықтауға мониторинг жүйесі көмектеседі. Өз кезегінде ақпараттық қауіпсіздік жағдайының мониторингі кез-келген

компанияның IT-ресурстарының, желілік бағдарламаларының, құрылғылар мен веб-сервисінің автоматты режимде жұмысын бақылауға мүмкіндік туғызады. Сондай тұрақты мониторинг (бақылау) арқасында ақпараттық жүйенің осалдықтары мен қауіптерін дер кезінде анықтап, олардың жұмысын тежеуге мүмкіндік береді. Уақытылы бақылау жүргізілген кезде ақпараттық жүйеге келтірілетін шығын көлемін азайтады. Бұл мақалада біз тақырыптық интернет-ресурстар деректерін талдау негізінде ақпараттық жүйенің қауіп-қатерлері мен осал тұстарының мониторингін, қауіптерден басымдықпен қорғау әдістерін зерттеу бағыты бойынша талдауды ұсынамыз. Соған қоса алдыңғы авторлардың мақалаларына шолу жасалады.

Түйін сөздер: мониторинг; интернет қауіптер; осалдықтар; киберқауіпсіздік.

S.T. Mambetov[1*], Ye.Ye. Begimbayeva[1,2], S. Joldasbayev[3], B.O. Kulambayev[3], G.N. Kazbekova[4]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan;
[2]Satbayev University, Almaty, Kazakhstan;
[3]International University of Information Technologies, Almaty, Kazakhstan;
[4]Akhmet Yassawi International Kazakh-Turkish University,
Turkestan, Kazakhstan.
E-mail: *mambetov.saken@gmail.com*

ABOUT MONITORING THREATS AND VULNERABILITIES OF THE INFORMATION SYSTEM

Abstract. The rapid informatization in various areas of society has a radical impact on the access and processing of information. In the literal sense, over the past two decades, new forms of broadcasting and data transmission have appeared and completely new types of activities within the global Internet network associated with the latest innovations. The concept of the Social Network has spread widely, in which people, without any fears and without any idea of the risk, advertise their data to the public. Now it is extremely rare to find a person who does not use any social network application, and most often the statement is true that one person uses several different applications. In addition, Internet services, search engines, and e-mail are used in the course of work. Accordingly, new, previously unknown, types of various threats and vulnerabilities of information systems are increasing and appearing. With the development of the Internet, hacker attacks have also focused on the same vulnerabilities and new types of threats. The monitoring system helps to identify these vulnerabilities and threats. In turn, monitoring the information security situation makes it possible to monitor the operation of IT resources, network programs, devices and web services of any company in automatic mode. Thanks to

constant monitoring (control), it is possible to identify vulnerabilities and threats of the information system in time and stop their work. Timely monitoring reduces the amount of damage caused to the information system. In this article, we provide an analysis in the direction of the study of monitoring threats and vulnerabilities of the information system, methods of protection against threats with priority, based on the analysis of data from thematic Internet resources. In addition, a review of the authors' previous articles will be made.

Key words: monitoring, Internet threats, vulnerabilities, cybersecurity.

Введение. Сегодня глобальное развитие проходит эру цифровизации, и если одни сообщества, регионы и даже целые страны уже полностью перешли на новый уровень, в котором большинство услуг производятся в цифровом пространстве, то некоторые группы только переходят к этому направлению. Никому не секрет, что цифровые технологии являются передовыми в эпоху, которую мы переживаем, и данное внедрение положительно сказывается в первую очередь на экономическом росте, обеспечивая высокую производительность, хранение, обработку и транспортировку цифровых ресурсов. В Республике Казахстан, с целью ускорения темпов развития экономики, улучшения качества жизни населения за счет цифровых технологий, также реализуется программа «Цифровой Казахстан» (Государственная програма «Цифровой Казахстан», 2018), где одним из важных пунктов указано обеспечение информационной безопасности в сфере IT. Еще одним катализатором послужил факт распространения COVID-19, когда практически более 80% (Gurova, 2020) офисных работников крупных корпораций перешли к дистанционной форме и после ослабления карантинных мер в целях безопасности долгое время оставались на удаленной работе. В любом случае после таких глобальных изменений мир уже не будет прежним.

Соответственно, при оптимизации процессов обработки различного рода данных необходимо обеспечить надежное хранение и оперативный доступ для участников информационного обмена, где существуют риски утечки, нарушения целостности и другие подобные уязвимости. Следует также брать во внимание, что с количеством роста пользователей также растет и количество уязвимости информационного пространства, так как это расширяет возможности злоумышленников, повышает вероятность непредвиденных случаев и рассеивает возможности их предотвращения устоявшимися методами. В данной работе проводится анализ типов угроз и уязвимостей, анализ методов и программных реализации предотвращения и борьбы с угрозами и уязвимостями информационной системы. При анализе информационной безопасности информационной системы организаций и предприятий проводится рассмотрение нескольких способов при работе пользователей общей системы с данными, таких как сбор и обработка данных из открытых источников, мониторинг распределения ресурсов и способы повышения безопасности.

Материалы и методы исследования. Обнаружение уязвимостей информационной системы дает преимущество для предотвращения разного рода действий злоумышленников. Чтобы бороться с проблемой, для начала нужно определить характер проблемы. Обычно программисты создают большое количество разного рода методы, алгоритмы, программы и даже целые системы защиты от взлома, тем не менее они происходят. Злоумышленник планирует атаку подобно шахматной игре, предполагая вопросы, которые цель атаки может задать, так что у него могут быть готовы подходящие ответы (Mitnick et al., 2002). Мы не стали описывать причины действий злоумышленников в данной работе, хотя, как известно, в большинстве случаев мотив раскрывает характер действий, тем не менее, мы попытались определить виды угроз, которые распространены в сети и те, которые приносят большие убытки.

По данным исследовательского центра Data Pro Research (США), в 62% причинами утечки или утраты информации служит человеческий фактор, среди которого 16% – повреждение софта, 16% – хищение персональной информации, 12% – подмена и фальсификация информации, 54% – финансовые махинации разного рода: переводы или кража с электронного счета, оплата услуг за чужой счет и т.д. Также прогнозируется, что если количество киберугроз будет расти и дальше, то объем расходов на решения в области кибербезопасности к 2022 году достигнет 133,7 миллиардов долларов США (Data Pro Research, 2022).

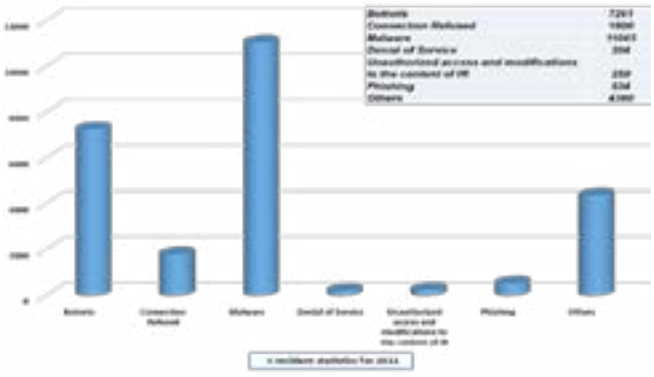

Рисунок 1. Статистика инцидентов киберугроз на территории РК за 2021 год

Казахстан 2017 году в рейтинге 194 стран по уровню кибербезопасности Global Cybersecurity Index был на 82 месте, а в 2021 году занял 31 место из 182 возможных (Clobal Cybersecurity Index, 2021), что показывает рост интереса к кибербезопасности в стране и актуальность исследований в этой области. Потому что информационная безопасность является задачей, которая требует регулярного процесса мониторинга уязвимостей и не имеет конечного решения еще со времен появления первых компьютерных сетей. На рисунке-1 приведена статистика, взятая из сайта о кибератаках, совершенных в Казахстане за 2021 год.

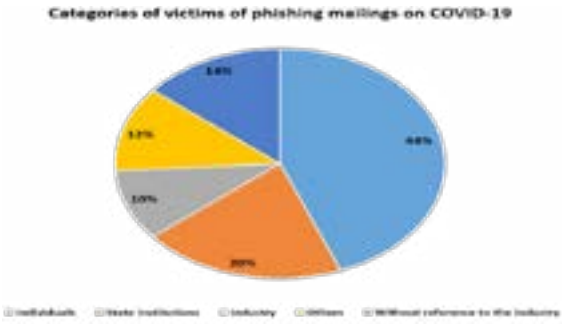

Рисунок 2. Категории жертв фишинговых рассылок на тему COVID-19

Следует взять за внимание и тот факт, что мошенничество не всегда осуществляется в физическом мире, существуют разновидность онлайн-форм, где приманки включают в себя привлекательную рекламу, которая ведет на вредоносные сайты или побуждает пользователей загрузить приложение, зараженное вредоносным ПО. Так, на примере в 2020 году злоумышленники подхватили тему всеобщего беспокойства по поводу COVID-19 и стали использовать ее для фишинговых писем (рисунок 2).

В (Миков, 2014) анализируются возможности методов и средств оценки рисков информационной безопасности применительно к различным этапам процесса оценки и построена схема процесса в виде вложенных алгоритмов с указанием взаимосвязей между всеми этапами, также рассмотрены наиболее эффективные способы реализации этих этапов. Автор предлагает при оценке рисков информационной безопасности использовать не один универсальный метод, а комбинировать методы и средства на разных этапах процесса: DFD или IDEF0 – на этапе анализа потоков данных в информационной системе, экспертный опрос с методами Дельфи, конкордации или симплекс-методом – на этапе оценки факторов риска, методы искусственного интеллекта, среди них гибридные модели – на этапе оценки риска, соответствующие математические методы – на этапе экономической оценки защиты информации и минимизация, принятие, передача или уклонение от риска – на этапе реализации управления рисками.

В (Киселева и др., 2017) определено понятие информационного риска, рассмотрены методы для оценки уровня текущего состояния информационной безопасности предприятия, для получения точных удовлетворительных результатов оценки предложено использовать комплексный подход к оценке рисков на основе существующих методик. Также в работе (Аникин и др., 2015) рассмотрены основные методы качественной и количественной оценки рисков информационной безопасности в корпоративных информационных сетях и поднята актуальность применения теории нечетких множеств при оценке рисков информационной безопасности. Значимым для нас считается, что здесь приведены методы, разработанные IT специалистами разных агентств разных стран.

В (Xiong et al., 2019) представлен обзор моделирования угроз на основе систематических запросов в четырех ведущих научных базах данных, и было оценено 176 статей, разделенных три отдельных кластера: (1) работы, вносящие вклад в моделирование угроз, (2) статьи, использующие существующий подход к моделированию угроз, и (3) вводные статьи, представляющие работу, связанную с процессом моделирования угроз. Авторы верно подметили, что большая часть работы по моделированию угроз по-прежнему выполняется вручную, и существует ограниченная уверенность в их валидации.

В (Russo et al., 2019) была разработана CYber Risk Vulnerability Management (CYRVM) – для упрощения и улучшения автоматизации и непрерывности оценки кибербезопасности. Основными нововведениями CYRVM являются сочетание в единой и простой в использовании программной веб-платформе онлайн-инструмента оценки уязвимостей в рамках структуры анализа рисков в соответствии с NIST 800-30 Risk Management руководящие принципы и интеграция прогнозных решений, способных предложить пользователю рейтинг и классификацию риска.

В (Chhajed et al., 2014) приводится обзор некоторых алгоритмов и методов обнаружения межсайтового скриптинга (XSS), а также сниффинга (sniffing) контента, когда в ход вступает изменение данных в содержимом текстовых, pdf-файлов и изображений.

В работе (Ajmal et all, 2021) хорошо описано положение, когда злоумышленники стремятся скомпрометировать организации и их данные с помощью передовых скрытых методов, используя законные инструменты, а также предлагается метод по определению системе незнакомых угроз, на новом подходе к моделированию имитации противника (отображение каждой соответствующей фазы) внутри подхода поиска угроз с минимальными ресурсами. Предлагаемый подход может быть использован для разработки атакующей среды, ориентированной на безопасность, в которой организации могут выявлять расширенные механизмы атак и проверять их способность обнаруживать атаки. Еще одна работа, на которую следует обратить внимание (Bakić et al., 2021), где был оценен прогресс в области кибербезопасности за последние 10 лет, спровоцированная в свою очередь в результате атаки Stuxnet в 2010 году. Авторы предлагают реактивные и упреждающие меры для снижения вездесущих рисков кибербезопасности.

В (Laković et al., 2021) рассматриваются вопросы кибербезопасности: существующие модели кибербезопасности и их усовершенствования, предлагается методология семантического расширения и улучшения моделей кибербезопасности. В работе (Velickovic et al., 2021) рассматривается проблема инфодемии – переизбыток информации о проблеме, обычно ложной и непроверенной, вызванная объявлением пандемии COVID-19. Был сформирован список веб-сервисов, которые предоставляют достоверные данные о пандемии из соответствующих источников и как таковые могут использоваться в борьбе с COVID-19 инфодемией, описаны данные COVID-19 службы

Freemium Web API с набором методов GET. На основании полученных результатов был предложен способ использования данного веб-сервиса в борьбе с инфодемией COVID-19.

В (Болатбек, т.б., 2022) этой работе поднимается проблема кибербезопасности, которая в настоящее время очень важна из-за некоторых угроз безопасности и кибератак. Дается определение кибербезопасности и приводятся наиболее распространенные виды атак на сегодняшний день. Кроме того, было показано, что некоторые проблемы кибербезопасности можно решить с помощью методов NLP обработки естественного языка, и был проведен систематический литературный обзор текущих работ.

Также следует дать описание экспертным системам, которые предназначены для решения классификационных задач в определенной области на основе базовых знаний, полученных путем опроса квалифицированных и представленных правилами системы классификации. В системах безопасности информационных технологий экспертные системы используются в интеллектуальных системах защиты информации на основе стенографической модели и содержат, как правило, неявные операторы преобразования в командный код каждого приложения отдельно, где имеются конкретные файловые системы и прикладные программное обеспечения отдельно. Возможность брать за основу опыт экспертов и информационную безопасность в виде правил являются преимуществами таких систем, и процесс аналогичен работе человеческой логики. Процесс описания последовательности правил определения реализовывается путем прямого и обратных операций (рисунок 4).

Рисунок 3. Архитектура простой экспертной системы мониторинга угроз и уязвимостей

Говоря об экспертной системе, стоит упомянуть, что для больших объемов данных и при частом обновлении контента обычно предлагается парсинговый метод – метод синтаксического анализа. Алгоритм действий такой программы приведен на рисунке-4.

Недостатком систем является требование больших вычислительных мощностей готовых правил без обоснования необходимости для конкретной цели. Учитывая необходимость обеспечения скрытой и своевременной передачи данных в современных экспертных системах, можно предположить,

что использование технологии самомодификации файлов, а именно программы скрытой перекодировки, важно для разработки технологий в области искусственного интеллекта (Shterenberg et al., 2016).

Рисунок 4. Алгоритм действий парсинговой программы

Использование машинного обучения в качестве решения также пользуется большим успехом. Они подразумеваются в двух видах в зависимости управления: контролируемые, неконтролируемые.

Результаты исследования. Таким образом, был выявлен ряд решений отслеживания угроз, которые применимы в информационных системах. Как показывает практика, системы мониторинга угроз условно можно разделить на категории:

1. Системы анализа в реальном времени;
2. Системы сбора данных действий пользователей;
3. Системы детекции аномалии действий пользователей;
4. Системы контроля внутренних операции;
5. Системы поиска и выявления угроз, ориентированные на улучшение системы безопасности.

Системы анализа в реальном времени позволяют выполнять обработку поступающих через канал данных и анализировать каждое сообщение по мере его получения. Также анализ в реальном времени преобразует определенные данных, геозон и обнаружения произошедших инцидентов и по завершению создаются набор выходных данных, которые будут храниться в векторном слое и также отправляться в виде оповещений.

В ходе исследования были рассмотрены некоторые системы анализа в реальном времени. Одним из таких систем является информативно-аналитический Интернет-сервис Mindscan, который имеет графический интерфейс в качестве Web-браузера, развертывается в облаке SaaS, и в основном занимается мониторингом и анализом социального Медиа.

Данный программный сервис ориентирован на крупные и средние организации и доступна не каждому пользователю, так как имеет плату за оказание услуг. Еще одним широко распространенным продуктом является система онлайн-мониторинга Katyusha. Данная система подходит как для среднего персонального компьютера, так и для смартфонов iOS и Android, с возможностями показа новостей в режиме реального времени, информативной аналитики и систематического выявления информативных атак и оценки эффективности. Также данная система выполняет поиск необходимой информации. Облачная система позволяет оценивать степень распространения той или иной определенной информации и перепубликаций одного источника. Система комплексного управления с анализом новостей для СМИ и социальных сетях в режиме реального времени SCAN, которая является профессиональным инструментом специалистов связи с общественностью. Данная система имеет возможность сбора данных более чем из 20 000 источников информации, в числе которых Facebook, VK, Twitter и многие другие более распространенные социальные сети. Существуют также большинство других не менее распространенных систем мониторинга и анализа информативных сред, таких как SemanticForce, Cision, Awario, PressIndex, YouScan, Seldon.News, Mediascope, Mention и множество других (Базенков и др., 2013).

Что касается сбора данных действий пользователей браузер пользователя передает в систему аналитики информацию о действиях, выполняемых им на сайте. Сайт в свою очередь, также может передавать данные как напрямую в систему аналитики, так и в интегрированную CRM-систему. CRM, используя полученные от сайта данные, может передавать их сразу в систему аналитики или же после их предварительной обработки. Несмотря на множество источников, из которых данные могут поступать в систему аналитики, наиболее исчерпывающими являются те данные, которые передаются в систему непосредственно браузером, поскольку не были подвержены модификации. Для сбора пользовательских данных при открытии сайта на страницу встраивается код, который непосредственно выполняет сбор данных. С помощью этого можно отслеживать передвижения клиента по вашему сайту и строить граф переходов, определять наиболее частые действия того или иного пользователя (Gubanov, 2020).

Системы детекции аномалии действий пользователей было определено в списке как отдельный пункт, так как бывают ситуации, когда эффект действия будет распознан позже, чем само действие. К примеру, была произведена определенная операция пользователем, а обработка и ответ из сервера проходит через большое количество времени. Таким образом, при возобновлении операции браузер клиента отключен и возможно даже сайт заблокирован и нет возможности определить информацию об успешном завершении действий. Для данных о трафике веб-сайта эти риски не редкость, но они могут нанести полноценный ущерб. Потеря некоторой полезной информации

может привести к ложным обвинениям и, следовательно, к неэффективным неденежным решениям.

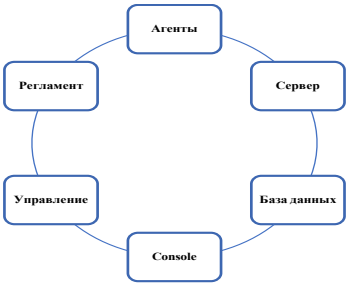

Рисунок 5. Основные компоненты для систем безопасностей

Также были определены основные компоненты для систем безопасностей (рисунок 5), где каждому компоненту определена своя роль: программные агенты собирают данные из различных источников, выше мы уже указывали программные продукты поддерживающие данный компонент; сервер анализирует поступающую информацию с заданными политикой и правилами; база данных консолидируют все события, сохраняет и производит быстрое развертывания необходимых данных в нужный момент; консоль управляет параметрами обработки и производит поправки в системе; управление производится системным администратором (или несколькими администраторами), которые работают с системой; и регламенты работы по мониторингу, выставляемые заказчиками.

Дискуссия. Поскольку 21 век – век информации, компьютерная индустрия получила широкое развитие. В частности, увеличилось количество пользователей Интернета. Однако увеличилось количество источников угроз из той же сети, а также увеличились уязвимости информационных систем. Мы убеждены в необходимости мониторинга в целях предотвращения уязвимостей информационной системы и угроз системе. Система мониторинга позволит выявить и оценить слабые места информационной системы. Оценивание уязвимости позволяет нормально, без угроз работать системе. Жизненный цикл системы мониторинга состоит из 4 этапов.

- Выявление и профилактика активных поломок;
- Выявление и устранение потенциальных уязвимостей;
- Оценка риска угроз и уязвимостей информационной системы;
- Исправление уязвимостей и угроз информационных систем.

Заключение. Таким образом, было определены основные понятия систем анализа и мониторинга информативных интернет-ресурсов, их полезные и уязвимые качества. В работе были описаны эти системы мониторинга и безопасности, а также регламент, поддерживаемый на территории Республики Казахстан. Также был сделан вывод касательно того, что в большинстве случаев атаки злоумышленников на простых потребителей

приводятся в действие при помощи социальной инженерии. Следовательно, с появлением нового вида такой деятельности необходимо постоянно развивать систему мониторинга и применять новые методы защиты от подобных случаев, которые позволят улучшать защищенность информационной системы. Таким образом, в качестве метода защиты будет применен анализ данных по содержанию во избежание ложных данных и предотвращения, а также разработана информационная система с использованием методов искусственного интеллекта, которая повысит уровень безопасности данных, в первую очередь от уязвимостей, непреднамеренно допускаемых простыми пользователями (сотрудниками предприятия).

Благодарность. *Авторы выражают благодарность научному руководителю проекта ГФ AP09259208 «Создание масштабируемой отказоустойчивой информационной системы цифровизации предприятия с использованием технологий Big Data» профессору ф.-м. н. Г.Т. Балакаевой.*

Information about the authors:

Mambetov Saken Tolegenuly – Doctoral student of the Department of Information Systems of the Al-Farabi Kazakh National University, Almaty, Kazakhstan, E-mail: mambetov.saken@gmail.com; *https://orcid.org/0000-0002-7249-5378*;

Begimbayeva Yenlik Ye. – PhD, Associate Professor of the Department of Information Systems, Al-Farabi Kazakh National University, Almaty, Kazakhstan E-mail: *enlik_89@mail.ru*, *https://orcid.org/0000-0002-4907-3345*;

Joldasbayev Serik K. – Senior Lecturer of the Department of Computer Engineering, International IT University, Almaty, Kazakhstan, E-mail: serykjoldasbaev@mail.ru, *https://orcid.org/0000-0002-8689-1822*;

Kulambayev B.O. – Candidate of Technical Sciences, Associate Professor of the Department of Computer Engineering, International IT University, Almaty, Kazakhstan, E-mail: b.kulambayev@iitu.edu.kz, *https://orcid.org/0000-0001-8387- 3736*;

Kazbekova G.N. – Candidate of Technical Sciences, Head of the Department of Computer Engineering, Khoja Akhmet Yassawi International Kazakh-Turkish University, Turkistan, Kazakhstan; E-mail: 3gulnur.kazbekova@ayu.edu.kz, *https://orcid.org/0000-0002-2756-7926*.

REFERENCES

Ajmal A.B., Shah M.A., Maple C., Asghar M.N., Islam S.U. (2021). Offensive Security: Towards Proactive Threat Hunting via Adversary Emulation. in IEEE Access, vol. 9, pp. 126023-126033, 2021, *https://doi.org/10.1109/ACCESS.2021.3104260* (in Eng.).

Anikin I.V., Emaletdinova L.Yu., Kirpichnikov A.P. (2015). Methods of information security risk assessment and management in corporate information networks. Bulletin of Kazan Technological University, 18 (6), 195-197. (in Russ.).

Bakić B., Milić M., Antović I., Savić D., Stojanović T. (2021). 10 years since Stuxnet: What have we learned from this mysterious computer software worm? 2021 25th International Conference on Information Technology, IT 2021, 9390103, *https://doi.org/10.1109/IT51528.2021.9390103* (in Eng.).

Bazenkov N.I., Gubanov D.A. (2013). Information systems for social networks analysis: a survey. Управление большими системами: сборник трудов, (41), 357-394. (in Russ.).

Bolatbek M.A., Bagitova K., & Mussiraliyeva Sh.Zh. (2022). A SYSTEMATIC REVIEW ON CYBERSECURITY ISSUES USING NATURAL LANGUAGE PROCESSING TECHNIQUES. Reports of NAS RK. Physico-Mathematical Series, (3), 52–70. *https://doi.org/10.32014/2022.2518-1726.139*.

Chhajed U., Kumar A. (2014). A Critical Review on Detecting Cross-Site Scripting Vulnerability. International Journal of Innovative Research in Science, Engineering and Technology, Vol. 3, Issue 4, April 2014 (in Eng.).

Data Pro Reseacrch (2021) [Electronic resource] (date of application 01/10/2022) URL: *https://dataproresearch.com/research-cyber-security-2021.html* (in Eng.).

Global Cybersecurity Index 2020, Measuring commitment to cybersecurity (2021). [Electronic resource] (date of application 01/10/2022) URL: *https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf* (in Eng.).

Gubanov I.A. (2020) An approach to simulation of user actions for data collection of analytics system. The electronic scientific journal "Young science of Siberia", no. 3(9). (in Russ.).

Gurova I.M. (2020) Remote Work as a Trend of Time: Results of Mass Testing. MIR (Modernization. Innovation. Research). 11(2):128-147. *https://doi.org/10.18184/2079-4665.2020.11.2.128-147* (in Russ.).

Kiseleva I.A., Iskajyan S.O. (2017). Information risks: methods of estimation and analysis. ITportal, (2 (14)), 10. (in Russ.).

Laković L., Ognjanović I., Šendelj R., Injac O. (2021). Semantically enhanced cyber security model for industry 4.0: Methodological framework. 2021 25th International Conference on Information Technology, IT 2021 this link is disabled, 2021, 9390120, *https://doi.org/10.1109/IT51528.2021.9390120* (in Eng.).

Mikov D.A. (2014). Analisys of methods and tools which are used in the various stages of information security risk assessment. Cybersecurity issues, (4 (7)), 49-54. (in Russ.).

Mitnick K.D., Simon W.L., Wozniak S. (2003). The Art of Deception: Controlling the Human Element of Security. John Wiley & Sons. (in Eng.).

On the approval of the State Program «Digital Kazakhstan» (2018) (date of application 01/05/2022) [Electronic resource]. URL: *https://adilet.zan.kz/rus/docs/P1700000827* (in Russ.).

Russo P., Caponi A., Leuti M., Bianchi G. (2019). A Web Platform for Integrated Vulnerability Assessment and Cyber Risk Management. Information, 10(7), 242. https://doi.org/10.3390/info10070242 (in Eng.).

Shterenberg S.I., Kaflanov R.I., Druzhin A.S., Marchenko S.S. (2016) Method of use of self-modification files for secure communication in the expert system. H&ES Research. Vol. 8. No. 1. Pp. 71–75 (in Eng.).

Veličković Z.S., Veličković M.Z., Milivojević Z.N. (2021). Application of a Reliable Web API's in the Fight Against COVID-19 Infodemia. 2021 25th International Conference on Information Technology (IT). *https://doi.org/10.1109/IT51528.2021.9390128* (in Eng.).

Xiong W. & Lagerström R. (2019). Threat modeling – A systematic literature review. Computers & Security. *https://doi.org/10.1016/j.cose.2019.03.010* (in Eng.).

МАЗМҰНЫ

СОДЕРЖАНИЕ

CONTENTS

Publication Ethics and Publication Malpracticein the journals of the National Academy of Sciences of the Republic of Kazakhstan

For information on Ethics in publishing and Ethicalguidelines for journal publication see http://www.elsevier.com/publishingethics and http://www.elsevier.com/journal-authors/ethics.

Submission of an article to the National Academy of Sciences of the Republic of Kazakhstan implies that the described work has not been published previously (except in the form of an abstract or as part of a published lecture or academic thesis or as an electronic preprint, see http://www.elsevier.com/postingpolicy), that it is not under consideration for publication elsewhere, that its publication is approved by all authors and tacitly or explicitly by the responsible authorities where the work was carried out, and that, if accepted, it will not be published elsewhere in the same form, in English or in any otherlanguage, including electronically without the written consent of the copyright-holder. In particular, translations into English of papers already published in another language are not accepted.

No other forms of scientific misconduct are allowed, such as plagiarism, falsification, fraudulent data, incorrect interpretation of other works, incorrect citations, etc. The National Academy of Sciences of the Republic of Kazakhstan follows the Code of Conduct of the Committee on Publication Ethics (COPE), and follows the COPE Flowcharts for Resolving Cases of Suspected Misconduct (http://publicationethics.org/files/u2/New_Code.pdf). To verify originality, your article may be checked by the Cross Check originality detection service http://www.elsevier.com/editors/plagdetect.

The authors are obliged to participate in peer review process and be ready to provide corrections, clarifications, retractions and apologies when needed. All authors of a paper should have significantly contributed to the research.

The reviewers should provide objective judgments and should point out relevant published works which are not yet cited. Reviewed articles should be treated confidentially. The reviewers will be chosen in such a way that there is no conflict of interests with respect to the research, the authors and/or the research funders.

The editors have complete responsibility and authority to reject or accept a paper, and they will only accept a paper when reasonably certain. They will preserve anonymity of reviewers and promote publication of corrections, clarifications, retractions and apologies when needed. The acceptance of a paper automatically implies the copyright transfer to the National Academy of Sciences of the Republic of Kazakhstan.

The Editorial Board of the National Academy of Sciences of the Republic of Kazakhstan will monitor and safeguard publishing ethics.

Правила оформления статьи для публикации в журнале смотреть на сайтах:
www:nauka-nanrk.kz
http://physics-mathematics.kz/index.php/en/archive
ISSN2518-1726 (Online),
ISSN 1991-346X (Print)

Директор отдела издания научных журналов НАН РК *А. Ботанқызы*
Заместитель директор отдела издания научных журналов НАН РК *Р. Жәлиқызы*
Редакторы: *М.С. Ахметова, Д.С. Аленов*
Верстка на компьютере *Г.Д.Жадыранова*

Подписано в печать 15.09.2022.
Формат 60х881/8. Бумага офсетная. Печать – ризограф.
10,5 п.л. Тираж 300. Заказ 4.

Национальная академия наук РК
050010, Алматы, ул. Шевченко, 28, т. 272-13-19