ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Профессор У.А. ТУКЕЕВТІҢ 75 жылдық мерейтойына арналған ақпараттық технологиялар саласындағы Халықаралық ғылыми конференция МАТЕРИАЛДАРЫ

МАТЕРИАЛЫ Международной научной конференции в области информационных технологий, посвященной 75-летию профессора У.А. ТУКЕЕВА

PROCEEDINGS of the International scientific conference in the field of Information technologies dedicated to the 75th anniversary of professor U. TUKEYEV

ӘЛ-ФАРАБИ АТЫНДАҒЫ ҚАЗАҚ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Профессор У.А. ТУКЕЕВТІҢ 75 жылдық мерейтойына арналған ақпараттық технологиялар саласындағы Халықаралық ғылыми конференция МАТЕРИАЛДАРЫ

8 қазан 2021 жыл

МАТЕРИАЛЫ Международной научной конференции в области информационных технологий, посвященной 75-летию профессора У.А. ТУКЕЕВА

8 октября 2021 года

PROCEEDINGS of the International scientific conference in the field of Information technologies dedicated to the 75th anniversary of professor U. TUKEYEV

8 October, 2021

Алматы
«Қазақ университеті»
2021

Материалы Международной научной конференции в области информационных технологий, посвященной 75-летию профессора У.А. Тукеева. Алматы, 8 октября 2021 года: – Алматы: Қазақ университеті, 2021. – 149 с.

ISBN 978-601-04-5672-3

ISBN 978-601-04-5672-3

Пайдаланылған дереккөздер тізімі

1. Alanjary, M., Cano-Prieto, C., Gross, H. & Medema, M. H. Computer-aided re-engineering of nonribosomal peptide and polyketide biosynthetic assembly lines. Nat. Prod. Rep. 36, 1249–1261 (2019).
2. Montalbán-López, M. et al. New developments in RiPP discovery, enzymology and engineering. Nat. Prod. Rep. 38, 130–239 (2020).
3. Hannigan, G. D. et al. A deep learning genome-mining strategy for biosynthetic gene cluster prediction. Nucleic Acids Res. 47, e110 (2019).
4. Frontino, G., Meschi, F., Bonfanti, R., Rigamonti, A., Battaglino, R., Favalli, V., Bonura, C., Ferro, G., & Chiumello, G. (2013). Future perspectives in glucose monitoring sensors. European Endocrinology, 9(1), 6- 11.
5. Villena Gonzales, W., Mobashsher, A. T., & Abbosh, A. (2019). The Progress of Glucose Monitoring-A Review of Invasive to Minimally and Non-Invasive Techniques, Devices and Sensors. Sensors (Basel, Switzerland), 19(4), 800. https://doi.org/10.3390/s19040800
6. Facchinetti A. (2016). Continuous Glucose Monitoring Sensors: Past, Present and Future Algorithmic Challenges. Sensors (Basel, Switzerland), 16(12), 2093. https://doi.org/10.3390/s16122093.
7. Salam, N. A., W. H. M. Saad, Z. Manap and F. Salehuddin. “The Evolution of Non-invasive Blood Glucose Monitoring System for Personal Application.” Journal of Telecommunication, Electronic and Computer Engineering 8 (2016): 59-65.
8. Kumar, P. M., Lokesh, S., Varatharajan, R., Babu, G. C., & Parthasarathy, P. (2018). Cloud and IoT based disease prediction and diagnosis system for healthcare using Fuzzy neural classifier. FutureGeneration Computer Systems, 86, 527-534
9. Narkhede, P., Dhalwar, S. and Karthikeyan, B. (2016). NIR Based Non-Invasive Blood Glucose Measurement. Indian Journal of Science and Technology, 9(41). DOI:10.17485/ijst/2016/v9i41/98996]
10. Н.А. Жолдас, М.Е. Мансурова. Информационные технологии для мониторинга юных пациентов с сахарным диабетом. Автоматика и программная инженерия. 2021, №1(35). Стр. 11-20

Д.К. Мухаев[1], Г.С. Байрбекова[1], А.Т. Мазакова[1,2], М.С. Әлиасқар[1]
[1]КазНУ им. аль-Фараби, Алматы, Казахстан
[2]Институт информационных и вычислительных технологий, Алматы, Казахстан
e-mail: daryn.mukhayev@gmail.com

ВЫЯВЛЕНИЕ УГРОЗ И УЯЗВИМОСТЕЙ НАРУШЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Аннотация*. В статье рассматриваются вопросы выявления угроз и уязвимостей нарушения информационной безопасности. Для защиты информации необходимо создание систем обнаружения компьютерных атак. Были даны разъяснения по понятию кибератак и затронуты их виды. Ни одна организация в настоящее время недостаточно защищена от кибератак. Все организации должны разработать специальный план по борьбе с киберпреступниками. Специальный план позволяет подготовиться к чрезвычайным ситуациям, противостоять возникающим угрозам и быстро восстановить эффект атаки. Подчеркивается необходимость знать угрожающие факторы и понимать их тактику, методы и процедуры для защиты от кибератак. Процесс защиты информации должен быть комплексным и непрерывным, осуществляемым на всех этапах создания и использования автоматизированных средств обработки данных. Приведены основные методы защиты информации.*

Ключевые слова. *Информационная безопасность, кибератака, киберпреступность, защита информации, угрозы, уязвимость.*

Аңдатпа. *Мақалада ақпараттық қауіпсіздікті бұзу қаупі мен осалдығын анықтау мәселелері талқыланады. Ақпаратты қорғау үшін компьютерлік шабуылдарды анықтайтын жүйелерді құру қажет. Кибершабуылдар туралы түсінік берілді және олардың түрлері қозғалды. Қазіргі уақытта ешбір ұйым кибершабуылдан жеткілікті түрде қорғалмаған. Барлық ұйымдар киберқылмыскерлермен күресудің арнайы жоспарын әзірлеуі керек. Арнайы жоспар төтенше жағдайларға дайын болуға, туындаған қатерлерге қарсы тұруға және шабуылдан тез қалпына келуге көмектеседі. Қауіп -қатерлерді білу және олардың кибершабуылдардан қорғану тактикасын, әдістері мен процедураларын түсіну қажеттілігі айтылады. Ақпаратты қорғау процесі ақпаратты өңдеудің автоматтандырылған құралдарын жасау мен қолданудың барлық кезеңдерінде жүргізілетін кешенді және үздіксіз болуы керек. Ақпаратты қорғаудың негізгі әдістері келтірілген.*

Түйін сөздер. *Ақпараттық қауіпсіздік, кибер шабуыл, киберқылмыс, ақпаратты қорғау, қатерлер, осалдық.*

Abstract. *The article discusses the issues of identifying threats and vulnerabilities in information security breaches. To protect information, it is necessary to create systems for detecting computer attacks. Clarifications were given on the concept of cyberattacks and their types were touched upon. No organization is currently inadequately protected from cyberattacks. All organizations must develop a dedicated plan to combat cybercriminals. A dedicated plan helps you prepare for emergencies, confront emerging threats, and quickly recover from an attack. The need to know threats and understand their tactics, methods and procedures to defend against cyberattacks is emphasized. The information protection process should be comprehensive and continuous, carried out at all stages of the creation and use of automated data processing tools. The main methods of information protection are given.*

Keywords. *Information security, cyber attack, cyber crime, information protection, threats, vulnerability.*

В связи с бурным развитием науки и техники усиливается влияние мировых информационных технологий на все сферы производства. В связи с этим в обществе формируются новые социальные группы, существенно меняется нормальный образ жизни людей. Вопросы информационной безопасности, связанные с осуществляемой в настоящее время активной информатизацией, имеют первостепенное значение. Многие из них направлены на создание единого информационного пространства с целью оптимизации обработки больших объемов информации, в том числе обеспечения ее надежного хранения и доступности для обмена информацией.

Основными задачами, поставленными для реализации данной цели, являются выявление, анализ и классификация угроз информационной безопасности, которые могут привести к несанкционированному получению информации или нарушению нормального функционирования информационных систем, определение основных мер, применяемых для противодействия угрозам и устранения уязвимостей, разработка критериев и механизмов безопасности, а также соответствующей законодательной и нормативно-правовой базы.

Научные исследования, посвященные выявлению и анализу угроз информационной безопасности, проводились многими российскими и зарубежными учеными, среди которых Я.Н. Алгулиев, И.Л. Алферов, А.А. Захаров, С.Л. Зефирова, Д.О. Карпеева, А.Г. Кащенко, А.А. Кононова, А.О. Сидорова, М.В. Тимонина и др.

Результаты исследований показывают, что ущерб от преступлений в сфере информации оценивается в миллиарды долларов в год. В настоящее время темпы развития компьютерных технологий значительно опережают процесс создания средств информационной безопасности. Кроме того, не сформирована единая теория безопасных информационных систем, применимых к различным предметным областям.

Одним из средств решения указанных задач являются системы обнаружения компьютерных атак, которые уже давно используются для защиты информации. Большинство современных систем работают с использованием методов обнаружения компьютерных атак, коррекции сетевых отклонений и анализа сигнатур. Эти методы имеют недостатки, связанные с вычислительными затратами на их реализацию, а также низкую эффективность в поиске новых видов компьютерных атак.

Основой обеспечения информационной безопасности являются специальные базы данных и интернет-ресурсы, созданные зарубежными и отечественными коммерческими или государственными органами. Заполнение базы данных осуществляется экспертным способом с участием авторитетных научных центров. Однако приведенные в базе данных списки информационных угроз и уязвимостей не являются исчерпывающими. Дискуссия, касающаяся событий, происходящих в определенных тематических зонах, становится все более распространенной среди пользователей Интернет-платформ. На основе тематического анализа появляется возможность прогнозировать возникновение угроз и уязвимостей информационной безопасности.

В связи с вышеизложенным, неотложной задачей является выявление общедоступных информационных ресурсов, содержащих данные об уязвимостях, компьютерных атаках и вирусах, а также результаты специализированных исследований по выявлению угроз информационной безопасности. Специалист по информационной безопасности, получая результаты прогнозирования возникновения опасности или уязвимости, может оценить степень опасности для защищаемых информационных ресурсов, правильность действующей модели угроз информационной безопасности и принять меры по нейтрализации уязвимостей.

Кибератака – это вредоносная, осуществляемая сознательно попытка человека или организации проникнуть в информационную систему другого человека или организации. Как правило, нарушая работу сети жертвы, хакер стремится получить выгоду.

Вредоносная программа – компьютерная программа или переносной код, предназначенный для реализации угроз информации, хранящейся в компьютерной системе, либо для скрытого нецелевого

использования ресурсов системы, либо иного воздействия, препятствующего нормальному функционированию компьютерной системы.

Сфокусированный фишинг-это более продвинутый тип фишинговых атак, ориентированных только на тех, кто имеет преимущество, таких как системные организаторы и руководители. Более 71% целевых атак включают сфокусированный фишинг.

Атака «человек посередине» (Man-in-the-Middle) – это форма кибератаки, при которой для перехвата данных используются методы, позволяющие внедриться в существующее подключение или процесс связи. Злоумышленник может быть пассивным слушателем в вашем разговоре, незаметно крадущим какие-то сведения, или активным участником, изменяя содержание ваших сообщений или выдавая себя за человека или систему, с которыми вы, по вашему мнению, разговариваете.

SQL инъекция – это один из самых доступных способов взлома сайта. Суть таких инъекций – внедрение в данные передаваемые через GET, POST запросы или значения Cookie произвольного SQL кода. Если сайт уязвим и выполняет такие инъекции, то по сути есть возможность творить с БД (чаще всего это MySQL) что угодно.

Программы-вымогатели – это относительно новая форма вредоносного ПО, которое шифрует файлы на устройстве пользователя, а затем требует совершить анонимный онлайн-платеж для восстановления доступа. По прогнозам, такие атаки принесут убытки мировым организациям в 2021 году в размере 20 миллиардов долларов.

DNS-спуфинг, также известный как отравление кэша DNS, является одной из форм взлома компьютерных сетей, в котором данные кэша доменных имен изменяются злоумышленником, с целью возврата ложного IP-адреса. Это приводит к атаке посредника на компьютер злоумышленника или любой другой компьютер. Средняя стоимость атаки DNS в 2020 году составила 9 924,000 $.

Чтобы эффективно реагировать на кибератаки, необходимо знать угрожающие факторы и понимать их тактику, методы и процедуры.

Пандемия коронавируса стала самой большой проблемой для бизнеса и ИТ-организаций в 2020 году. В условиях пандемии киберугрозы и нарушения данных стали более сложными и масштабными, а количество нарушений выросло на 273% в первом квартале по сравнению с 2019 годом. Microsoft заявила, что число фишинговых и социальных инженерных атак увеличилось до 30 000 в день только в США.

Киберпреступники продолжали использовать пандемию коронавируса и связанные с ней темы в качестве темы для своих фишинговых и социальных инженерных кампаний. Их атаки часто совпадают с важными событиями, такими как внезапная вспышка случаев COVID-19 или сообщение о новой вакцине. Злоумышленники призывают пользователей нажать на вредоносную ссылку или приложение, которое покрывает название легальных тем COVID-19.

Когда многие компании переходят в облако, чтобы облегчить удаленную работу и непрерывность бизнеса, киберпреступники следуют той же тенденции и нацеливаются на облако. Угроза облачной безопасности, включая неправильную конфигурацию облака, неполное удаление данных и уязвимые облачные приложения, будут общими источниками кибератак.

В условиях пандемии почти все предприятия начали работать из дома, чтобы обеспечить непрерывность бизнеса. Связисты используют такие устройства, как смартфоны и планшеты, с безопасными незащищенными, не покрытыми патчем или не управляемыми отделом ИТ-безопасности. К сожалению, они вызывают некоторые особые угрозы и уязвимости безопасности ИТ, которые создают угрозу кибератак на организации.

В современную цифровую эпоху ни одна организация не защищена от кибератак. Таким образом, организации всех масштабов должны разработать эффективный план противодействия инцидентам для борьбы с киберпреступниками. Это позволяет предприятиям быть готовыми к чрезвычайным ситуациям, противостоять возникающим угрозам и быстро восстанавливать последствия атаки

Регулярное резервное копирование данных может помочь снизить риск кражи данных. Вы должны регулярно и последовательно создавать резервные копии Веб-сайта, приложений, баз данных, электронной почты, приложений, файлов, календарей и т.д.

Анализ существующих угроз и уязвимостей информационной безопасности показывает, что достижение целей и задач защиты информации, а также обеспечение высокого уровня безопасности требует комплексного применения доступных методов и средств защиты. По этой причине одним из основных принципов, основанных на разработке концепций информационной безопасности и конкретных средств информационной безопасности, является комплексность.

Процесс обеспечения защиты информации должен быть комплексным и непрерывным, осуществляемым на всех этапах создания и использования автоматизированных средств обработки

данных. Реализация процесса информационной безопасности в этих условиях основывается на производственных концептуальных подходах и производстве техники безопасности. Как правило, для создания защитных механизмов, обеспечения их надежной и эффективной работы привлекаются высококвалифицированные специалисты по информационной безопасности.

Основная цель защиты информации – выявление и устранение или нейтрализация источников негативного воздействия на информацию, а также их причин и условий. Указанные источники информации представляют угрозу безопасности информации. К основным методам защиты информации относятся:

– предупреждение известных угроз путем принятия активных мер по обеспечению информационной безопасности для нейтрализации возможности их возникновения;

– выявление угроз в результате конкретных несанкционированных действий злоумышленников в отношении защищаемой информации;

– выявление новых угроз в ходе непрерывного анализа и контроля за возникновением реальных или возможных угроз, а также своевременное принятие активных мер.

Информация об угрозе – это заранее проанализированная информация о нападениях, которые могут угрожать организации. Анализ угроз помогает организациям понять потенциальные или текущие киберугрозы. Чем больше персонала информационной безопасности о субъектах риска, их возможностях, инфраструктуре и мотивации, тем больше они могут защитить свои организации.

Системы анализа рисков обычно используются в сочетании с другими средствами безопасности. В большинстве случаев анализ помогает автоматически блокировать угрозы – например, определенные IP-адреса могут быть отправлены в брандмауэр для автоматической блокировки трафика с взломанных серверов.

Информация об опасности обычно передается в виде каналов. Существуют бесплатные каналы информации об угрозах, предоставляемые организациями, изучающими коммерческую безопасность, и многое другое. Некоторые разработчики приложений предлагают множество платформ для разведки угроз, чтобы помочь им управлять и интегрировать информацию об угрозах с другими системами безопасности.

Результатом алгоритма, направленного на реализацию данной цели, являются отчеты об обнаруженных угрозах и уязвимостях информационной безопасности, которые могут содержать информацию, отражающую результаты анализа потока текстовых сообщений, на основании которых делается вывод о возникновении уязвимостей. Такая информация может быть следующее:

– частота создания сообщений, относящихся к анализируемому периоду угроз и информационной безопасности на тематических интернет – ресурсах;

– средний рейтинг авторов сообщений, относящихся к тематической сфере информационной безопасности и угрозам за анализируемый период времени;

– частотные характеристики угроз и уязвимостей информационной безопасности, встречающихся в сообщениях тематических интернет – ресурсов в анализируемый период;

– выбор текстов сообщений тематических интернет – ресурсов, созданных в анализируемом периоде и содержащих условия угроз и уязвимостей информационной безопасности;

– перечень онтологий угроз и уязвимостей информационной безопасности, встречающихся в сообщениях, что позволяет классифицировать предполагаемые угрозы и уязвимости.

Количественная оценка риска применяется в тех случаях, когда исследуемые риски сопоставимы с конечными числовыми значениями, выраженными в деньгах, процентах, времени, человеческих ресурсах и т. Метод позволяет получить конкретные значения объектов оценки рисков при осуществлении угроз информационной безопасности. При количественном подходе всем элементам оценки риска присваиваются конкретные числовые значения. Алгоритм получения этих значений должен быть четким и понятным. Объектом оценки могут быть денежное значение актива, вероятность осуществления угрозы, ущерб от угрозы, стоимость защитных мероприятий и другие.

Качественный метод позволяет быстрее оценить риски, но оценка и результаты являются субъективными и не дают четкого представления о вреде, потерях и выгодах от внедрения систем информационной безопасности. Выбор метода зависит от специфики конкретной компании и поставленных перед специалистом задач.

Заключение. В статье проанализированы существующие угрозы и уязвимости информационной безопасности. В рамках будущих исследований планируется рассмотреть возможности улучшения качества прогноза об угрозах и уязвимости информационной безопасности.

Работа выполнена за счет средств программы целевого финансирования на 2021-2022 годы «Developing the concept and mechanisms of balanced territorial development of the economy and society of Kazakhstan».

Список использованных источников

1. Кирсанов К.А. Информационная безопасность: Учеб. пособие К.А. Кирсанов, А.В. Малявина, Н.В. Попов // Моск. акад. экономики и права. – М.: МАЭП, 2000. – 230 с.
2. Конеев И.Р. Информационная безопасность предприятия: [Информ. безопасность. Классификация атак. Методика упр. рисками. Криптограф. средства и механизмы] Искандер Конеев, Андрей Беляев. – СПб.: БХВ-Петербург, 2003. – С. 68-90.
3. Мельников В.В. Защита информации в компьютерных системах. – М.: Финансы и статистика. Электроинформ, 2004. – С. 258-269.
4. Шаковец А.Н. Основы защиты компьютерной информации и информационная безопасность // Лекция А.Н. Шаковец, Н.В. Рымарева; М-во внутрен. дел России, Дальневосточ. юрид. ин-т. – Хабаровск: Дальневосточ. юрид. ин-т МВД РФ, 2003. – С. 28-45.
5. Смагин А.А., Полетаев В.С. Алгоритм прогнозирования угроз информационной безопасности // Инфокоммуникационные технологии. 2018. – Т. 16. – №2. – С. 192–198.
6. Yazan Alshboul, Kevin Streff. Analyzing Information Security Model for Small-Medium Sized Businesses: Twenty-first Americas Conference on Information Systems, Puerto Rico, 2015. DOI: https://core.ac.uk/download/pdf/301365935.pdf
7. Julian Jang-Jaccard, Surya Nepal. A survey of emerging threats in cybersecurity. Journal of Computer and System Sciences. – Vol.80. – Issue 5. August 2014. – Pp. 973-993. https://doi.org/10.1016/j.jcss.2014.02.005
8. Top cybersecurity threats on enterprise networks: https://www.ptsecurity.com/ww-en/analytics/network-traffic-analysis-2020/
9. Eran Toch, Claudio Bettini, Erez Shmueli, Laura Radaelli, Andrea Lanzi, Daniele Riboni, and Bruno Lepri.2018. The Privacy Implications of Cyber Security Systems: A Technological Survey. ACM Comput. Surv.51,2, Article 36 (February 2018), 27 p. https://doi.org/10.1145/3172869
10. B. A. Obotivere, A. O. Nwaezeigwe. Cyber Security Threats on the Internet and Possible Solutions, September 2020, IJARCCE 9(9): 92-97. DOI: 10.17148/IJARCCE.2020.9913

М. Туртаева, У.А. Тукеев
Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
marzhan.zt@gmail.com, ualsher.tukeyev@gmail.com

ЕЖЕЛГІ ҚЫПШАҚ ТІЛІНІҢ ЖАЛҒАУЛАРЫНЫҢ ТОЛЫҚ ЖИЫНТЫҒЫ МЕН МОРФОЛОГИЯЛЫҚ МОДЕЛІ

Аңдатпа: *Мақалада ежелгі қыпшақ тілі үшін агглютинативті тілдерді өңдеуге арналған CSE (Complete End of End) технологиясының қолданылуы ұсынылған. Қыпшақ тілінің аяқталуының толық жүйесі жасалды, қыпшақ тілінің септік сөздері мен стоп сөздері жасалды. Қыпшақ тіліндегі сөздердің стеммингі бойынша эксперименттер агглютинативті тілдерді өңдеуге арналған CSE технологияларының әмбебап бағдарламаларын қолдану арқылы жүргізілді.*
Түйінді сөздер: *қыпшақ тілі, морфологиялық сегментация, морфология, модель*

Аннотация: *В статье представлено использование технологии CSE (Complete Set of Endings) технологии обработки агглютинативных языков для древнекыпчакского языка. Разработана полная система окончаний кыпчакского языка, разработаны словари стемов и стоп-слов кыпчакского языка. Проведены эксперименты по стеммингу слов кыпчаксого языка с использованием универсальных программ CSE технологии обработки агглютинативных языков.*
Ключевые слова: *кыпчакский язык, морфологическая сегментация, морфология, модель.*

Abstract: *The article presents the use of CSE (Complete Set of Endings) technology for processing agglutinative languages for the ancient Kypchak language. A complete system of endings of the Kypchak language has been developed, dictionaries of stems and stop words of the Kypchak language have been developed. Experiments on stemming of words of the Kypchak language were carried out using universal programs CSE technologies for processing agglutinative languages.*
Keywords*: қыпшақ тілі, морфологиялық сегментация, морфология, модель. Кыпчакский язык, морфологическая сегментация, морфология, модель. Kypchak language, morphological segmentation, morphology, model.*

Содержание

Ғылыми басылым

ПРОФЕССОР У.А. ТУКЕЕВТІҢ 75 ЖЫЛДЫҚ МЕРЕЙ ТОЙЫНА АРНАЛҒАН АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР САЛАСЫНДАҒЫ ХАЛЫҚАРАЛЫҚ ҒЫЛЫМИ КОНФЕРЕНЦИЯ МАТЕРИАЛДАРЫ

8 ҚАЗАН 2021 ЖЫЛ

ИБ № 14969
Басуға 07.10.2021 жылы қол қойылды. Формат 70х100 1/12.
Көлемі 12,4 б.т. Тапсырыс № 9174. Таралымы 30 дана.
Әл-Фараби атындағы Қазақ ұлттық университетінің
«Қазақ университеті» баспа үйі.
Алматы қаласы, әл-Фараби даңғылы, 71.
«Қазақ университеті» баспа үйі баспаханасында басылды.