НАУКА XXI ВЕКА: АКТУАЛЬНЫЕ ВОПРОСЫ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ (SCIENCE OF THE XXI CENTURY: CURRENT ISSUES, PROBLEMS AND PROSPECTS)

Материалы Международной научно-практической конференции 20 декабря 2019 года (г. Душанбе, Таджикистан)

Научно-издательский центр «Мир науки»
Nəşriyyat **«Vüsət»**
Материалы Международной (заочной) научно-практической конференции
под общей редакцией **А.И. Вострецова**

НАУКА XXI ВЕКА: АКТУАЛЬНЫЕ ВОПРОСЫ, ПРОБЛЕМЫ И ПЕРСПЕКТИВЫ (SCIENCE OF THE XXI CENTURY: CURRENT ISSUES, PROBLEMS AND PROSPECTS)

научное (непериодическое) электронное издание

Наука XXI века: актуальные вопросы, проблемы и перспективы [Электронный ресурс] / Nəşriyyat «Vüsət», Научно-издательский центр «Мир науки». – Электрон. текст. данн. (2,16 Мб.). – Нефтекамск: Научно-издательский центр «Мир науки», 2019. – 1 оптический компакт-диск (CD-ROM). – Систем. требования: PC с процессором не ниже 233 МГц., Microsoft Windows Server 2003/XP/Vista/7/8, не менее 128 МБ оперативной памяти; Adobe Acrobat Reader 10.1 или выше; дисковод CD-ROM 8x или выше; клавиатура, мышь. – Загл. с тит. экрана. – Электрон. текст подготовлен НИЦ «Мир науки».

СВЕДЕНИЯ ОБ ИЗДАНИИ

Классификационные индексы:
УДК 001
ББК 72
Н124

Составители: Научно-издательский центр «Мир науки»
А.И. Вострецов – гл. ред., отв. за выпуск

Аннотация: В сборнике представлены материалы Международной (заочной) научно-практической конференции «Наука XXI века: актуальные вопросы, проблемы и перспективы», где нашли свое отражение доклады студентов, магистрантов, аспирантов, преподавателей и научных сотрудников вузов Российской Федерации и Казахстана по техническим, экономическим, педагогическим, юридическим и другим наукам. Материалы сборника представляют интерес для всех интересующихся указанной проблематикой и могут быть использованы при выполнении научных работ и преподавании соответствующих дисциплин.

Сведения об издании по природе основной информации: текстовое электронное издание.

Системные требования: PC с процессором не ниже 233 МГц., Microsoft Windows Server 2003/XP/Vista/7/8, не менее 128 МБ оперативной памяти; Adobe Acrobat Reader 10.1 или выше; дисковод CD-ROM 8x или выше; клавиатура, мышь.

ПРОИЗВОДСТВЕННО-ТЕХНИЧЕСКИЕ СВЕДЕНИЯ

НАДВЫПУСКНЫЕ ДАННЫЕ:

Сведения о программном обеспечении, которое использовано при создании электронного издания: Adobe Acrobat Reader 10.1, Microsoft Office 2003.

Сведения о технической подготовке материалов для электронного издания: материалы электронного издания были предварительно вычитаны филологами и обработаны программными средствами Adobe Acrobat Reader 10.1 и Microsoft Office 2003.

Сведения о лицах, осуществлявших техническую обработку и подготовку материалов:
А.И. Вострецов.

ВЫПУСКНЫЕ ДАННЫЕ:

Дата подписания к использованию: 20 декабря 2019 года.

Объем издания: 2,16 Мб.

Комплектация издания: 1 пластиковая коробка, 1 оптический компакт диск.

Наименование и контактные данные юридического лица, осуществившего запись на материальный носитель: Научно-издательский центр «Мир науки»
Адрес: Республика Башкортостан, г. Нефтекамск, улица Дорожная 15/294
Телефон: 8-937-333-86-86

СОДЕРЖАНИЕ

БИОЛОГИЧЕСКИЕ НАУКИ

П.А. Малютина Биоэлементы в рационах детей 8

ТЕХНИЧЕСКИЕ НАУКИ

Л.С. Агапитова, Д.П. Шайхутдинова Искусственный интеллект в маркетинге 12
А. Есенгельдинов, М.К. Кожахметов Гигиеническая оценка безопасности мясных продуктов 16
Р.О. Карпиков, А.А. Рябыкин, Е.М. Минаева, А.О. Мамичев Как правильно пользоваться автоматической коробкой 21
Т.В. Кшукина, С.А. Паузин Станции снеготаяния в Нижнем Новгороде 25
A.A. Solovyova Analysis of existing methods of monitoring isolation of overhead power transmission lines and open distribution devices 29
Н.В. Тюлюпа Методы и средства защиты информации 32
Р.М. Хисматуллин Водопотребление промышленных предприятий и источники его удовлетворения 36
Д.П. Шайхутдинова, Л.С. Агапитова Информационная безопасность банковской системы и ее защита 40

СЕЛЬСКОХОЗЯЙСТВЕННЫЕ НАУКИ

В.В. Камнева Влияние норм высева на урожайность и качество семян подсолнечника в условиях Костанайской области 45
П.Е. Черник, А.С. Тераевич Кормление КРС по кластерам 50

ИСТОРИЧЕСКИЕ НАУКИ И АРХЕОЛОГИЯ

А.Г. Трошева Морально-нравственное влияние православия на местное население Русской Америки 55

ТЕХНИЧЕСКИЕ НАУКИ

Л.С. Агапитова,
студент 4 курса напр. «Прикладная информатика в экономике»,
e-mail: ***lubovaga@gmail.com,***
Д.П. Шайхутдинова,
студент 4 курса напр. «Прикладная информатика в экономике»,
e-mail: ***dsh.007@mail.ru,***
науч. рук.: ***А.В. Каляшина,***
к.э.н., доц.,
КГЭУ,
г. Казань

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В МАРКЕТИНГЕ

Аннотация: в данной статье рассмотрено взаимодействие современных алгоритмов в рекламе с человеком, формирование спроса у пользователя с помощью этих алгоритмов, персонифицированные коммуникации, манипуляция людьми с помощью рекомендательных систем, а также способы борьбы с нею.

Ключевые слова: искусственный интеллект, маркетинг, анализ данных, персонифицированные коммуникации, нарушение прав.

Маркетинг – отрасль, где технологии анализа больших данных наиболее часто используется. Последние года все, что окружает нас в рекламных коммуникациях завязано именно на анализе данных и на том, что можно назвать искусственным интеллектом.

Сейчас информационные технологии стремятся к получению знаний без коммуникации с пользователем. Человек хочет нажать одну кнопку и получить то, что ему нужно. Задача заключается в том, чтобы понять, что это за человек и как с ним коммуницировать еще до того, как он пришел на на тот или иной ресурс. Появились технологии, которые пытаются решить

эту задачу.

Данные – новая нефть. Но люди научились собирать их уже достаточно давно, а вот извлечение знаний из этих данных – это именно та задача, которую пытается решить искусственный интеллект в маркетинге.

Есть три этапа взаимодействия современных алгоритмов в рекламе с человеком:

1) понимание клиента (получение дополнительных знаний о нем);

2) персональный подход;

3) формирование спроса.

Чтобы понять, что человеку нужно и как сформировать спрос вокруг него, нужно проанализировать цифровой след – совокупность информации о посещениях и вкладе пользователя в сети Интернет [3]. Это могут быть личные профили и учетные записи в социальных сетях, история посещений сайтов, личные сообщения, комментарии, видео, фотографии. Весь этот огромный набор данных можно идентифицировать и разделить на 3 уровня:

30% – собственные данные компании (история покупок, транзакции, то, как человек взаимодействовал с интерфейсом);

40% – открытые источники (личные профили в социальных сетях);

30% – друзья и окружение.

Персонифицированные коммуникации – это система, которая следит за вашими предпочтениями и показывает вам именно ту рекламу, которая вам интересна, которая может зацепить и привести к покупке. То есть на одной и той же информационной площадке разные люди видят разный креатив. Ни одно современное СМИ или видеоресурс не показывает вам какие-то новости просто так. Заходя туда, загружается огромное количество алгоритмов, которые идентифицируют вас, понимают всю вашу предыдущую активность и затем выдают актуальную, тщательно подобранную информацию. Кроме того, рекомендательные системы сейчас совершенно другого уровня, нежели были раньше, когда алгоритмы были очень простыми: смотрите категорию "политика", в следствие чего вам и показываются новости категории "политика". Сейчас система

анализирует на каком абзаце вы остановили мышку, что скопировали, как взаимодействовали со страницей, а потом предлагаются подходящие конкретно этому пользователю новости. Это все создано для того, чтобы удержать человека на ресурсе посредством предоставления интересной юзеру информации.

И тут возникает вопрос: угождаем ли мы потребностям людей или же мы их создаем? Изначально рекомендательные системы создавались, чтобы подсказывать, что вам нужно, но они перескочили этот рубеж и начали формировать спрос. Максимально релевантный контент для вас – на самом деле то, что нужно продать. Людьми начинают манипулировать.

Проходя регистрацию на сайтах, мы даем разрешение на обработку личных данных и передачу их третьим лицам, не подозревая, как это будет использоваться в дальнейшем. Под особый риск попадают дети и подростки, не придающие значения этому действию. Таким образом, с каждого пользователя кропотливо собирается информация, которая позже используется для продвижения товаров и услуг.

В Европе для борьбы с этим существует GDPR. Документ предоставляет возможность управлять персональными данными: спрашивать про цели обработки, место их хранения, а в случае необходимости удалить. В Российской Федерации защита персональных данных граждан основана на Конституции РФ, международных договорах РФ, Федеральном законе № 152 – ФЗ от 27.07.2006 «О персональных данных» [2]. Для самостоятельной защиты личной информации рекомендуется вести закрытые профили в социальных сетях, вводить двойную аутентификацию и устанавливать расширение для безопасного и приватного сёрфинга в браузере. А главное, при регистрации на интернет-сайтах пользователь всегда должен быть внимательнее и помнить о безопасности и защите своих персональных данных.

Литература и примечания:

[1] Жигайло В.А. Защита персональных данных в сети Интернет // Научное сообщество студентов: Междисциплинарные исследования: сб. ст. по мат. XXXVII

междунар. студ. науч. – практ. конф. № 2(37). [Электронный ресурс]. URL: https://sibac.info/archive/meghdis/2(37).pdf (дата обращения: 20.10.2019)

[2] Кутейникова О. «Игнорировать GDPR будет сложно всем»: что нужно знать о новом регламенте // Rusbase [Электронный ресурс]. URL: https://rb.ru/opinion/gdpr-questions (дата обращения: 20.10.2019)

[3] Цифровой след. Wikipedia. Wikipedia Foundation, Inc.. Web [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D0%BE%D0%B9_%D1%81%D0%BB%D0%B5%D0%B4 (дата обращения: 20.10.2019)

Д.П. Шайхутдинова,
студент 4 курса напр. «Прикладная информатика в экономике»,
e-mail: ***dsh.007@mail.ru,***
Л.С. Агапитова,
студент 4 курса напр. «Прикладная информатика в экономике»,
e-mail: ***lubovaga@gmail.com,***
науч. рук.: ***А.В. Каляшина,***
к.э.н., доц.,
КГЭУ,
г. Казань

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БАНКОВСКОЙ СИСТЕМЫ И ЕЕ ЗАЩИТА

Аннотация: в статье рассмотрено понятие информационной безопасности банковской системы. Выявлены общие характеристики банковской системы и возможные угрозы. Предложены возможные пути повышения безопасности банковских систем.

Ключевые слова: информационная безопасность, база данных, банковская система, информационная защита, хакеры, кибератака, угроза.

Становясь информативным, современное общество столкнулось с проблемой защиты личности, самого себя, а также государства. Это обусловлено тем, что сохранность информации становиться все более уязвимой. Одним из самых актуальных вопросов на сегодняшний день это информационная защита данных банков России. Предотвращение различных угроз, защита от кибератак, разглашение и утечка конфиденциальной информации, нарушение работоспособности технических средств, именно это является главными целями обеспечения безопасности системы банка.

Что все-таки значит безопасность для банка.? Самое главное это уверенность в следующем дне, неуязвимость, обеспеченность и стабильность! Прежде всего, безопасность

банковской системы подразумевает обеспечение охраны: территории банка, проводимых операций, материальных и денежных ресурсов, безопасность данных персонала и клиентов.

В современном мире стоимость и значимость банковской информации возросли в разы, что повлияло на рост нездорового интереса к ней. Переход к веку компьютеризации дает возможность совершать многочисленные банковские операции через локальную сеть Интернет, это является одной из причин стремительного возрастания угроз. Использование различных онлайн-систем не дает быть полностью закрытыми. При использовании таких банковских электронных систем первостепенной задачей является сохранение данных. [2]

Существуют определенные цели создания Политики информационной безопасности банка:

- антивирусная защита;
- обеспечение аутентификации;
- шифрование данных криптографическими средствами;
- охрана от несанкционированного вмешательства;
- создание механизма для обнаружения всевозможных угроз;
- предугадывание кибератаки с учетом изменений информационной среды банка. [1]

Охраняемые сведения в банковской системе, как правило, подразделяются на группы в зависимости от уровня их конфиденциальности, а также значимости. Обязательно определяются уровни банковского персонала для каждой группы, и проводится ранжирование групп. Выделяются такие типы:

- банковская тайна;
- коммерческая тайна;
- персональные данные;
- не конфиденциальная информация.

Но сортировка производится, учитывая от сущности сделок, сумму, наличие государственной тайны или кредитуемые связанные с ней проекты.

Для защиты информационной безопасности данных в банковских системах, которые хранятся и передаются техническим оборудованием, используется:

– IPsec;
– аутентификация;
– регламентирование доступа к объектам.
– шифрующая система файлов;
– безопасные соединения;

Можно рассмотреть каждый элемент по отдельности.

IPsec – это совокупность протоколов для обеспечения информационной безопасности данных, которые передаются по протоколу IP.

С одним из элементов информационной защиты, как логин и пароль, встречаются все пользователи операционных систем. Аутентификация – распространённый способ для того, чтобы обеспечить безопасность своим данным, информационные сообщения, которые хранятся на персональном компьютере или сервере.

Также, на аутентификации может строится регламентирование доступа к объектам, к различным файлам и папкам, хранящимся в системе. Но чаще всего используются другие алгоритмы. К соучастникам системы присваивают права и привилегии, где им можно либо только знакомиться с объектами, либо вносить в них изменения, а то и удалять.

Еще одной составляющей информационной безопасности осуществляется системой EFS при помощи определенного ключа является шифрование файлов.

Также в банковском деле широко применяется способ безопасного соединения используют информационные каналы типа «клиент-сервер» или же «клиент-клиент». [4]

Данный вопрос особенно актуален в нашей стране. В отличие от зарубежных банков, где программное обеспечение разработано конкретно под определенный. Когда в России в свою очередь распространяют однотипные банковские пакеты, где информация известна большому кругу IT-работников банков. Это облегчает несанкционированный доступ в банковские информационные системы.

Есть главные пути решения проблем. Как правило, совершают такие действия:

– сотрудники, ответственные за сохранение информационной защиты, должны знать стандарты работы с

безопасностью данных;

– предоставляется каждому сотруднику минимальные необходимые полномочия по доступу к информации;

– применяются технические и программные средства, которые обеспечивают непрерывную работу, и качество системы;

– контролируются деятельность сотрудников, связанных с информационными ресурсами;

– в строгом порядке ведется учет всех документов, всех серверов и каналов связей. [3]

Для исправления неблагоприятных последствий проникновения в банковскую систему, банкам необходимо достаточно хорошо обеспечить свою систему информационной защитой, и желательно чтобы оно сохранялось в течение многих лет.

Исходя из вышесказанного можно отметить, что обеспечение банков информационной защитой является обязательным условием. Информация, которая находится в банковских базах данных предоставляет материальную стоимость, требования к обработке и хранению этих данных всегда будут высокими.

Следует отметить, что, все чаще нарастают угрозы в связи с политической обстановкой в мире, такие как кибератаки, перехваты, искажение информации и многое другое. Всем банкам необходимо выполнять определенные требования кибербезопасности, указанные в нормативных документах Банка России. Кроме тщательного отбора персонала, надежные специализированные программы, надежное специализированное ПО и надежные специализированные сотрудники, также необходимо обновлять программные продукты и электронные системы. Ведь главным моментов в разработке программного обеспечения является анализ угроз. Именно анализ позволяет осведомить сотрудников и руководство о сильных и слабых сторонах программы, тем самым способствует оптимизации системы безопасности.

Литература и примечания:

[1] Внуков А.А. «Защита информации в банковских

системах»: учебное пособие для бакалавриата и магистратуры / А.А. Внуков. – 2-е изд., испр. и доп. – Москва: Издательство Юрайт, 2018. – 246 с.

[2] Золотарюк, В.А. Федотовская, Е.А. Кретова / ЦНС «Интерактив плюс», 2016. – С. 147-149. – ISSN 2413-3957.

[3] Воронцова С.В. Обеспечение информационной безопасности в банковской сфере. Монография / Издательство: Кнорус, 2015 г.

[4] Политика информационной безопасности банка [Электронный ресурс]. URL: https://searchinform.ru/products/kib/politiki-informatsionnoj-bezopasnosti/politika-informacionnoj-bezopasnosti-banka/ (дата обращения: 15.12.2019)