УДК 339.137.2 **DOI: 10.14529/iimj170303**

СОВРЕМЕННОЕ СОСТОЯНИЕ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В АСПЕКТЕ БЕЗОПАСНОСТИ

БОГАТЕНКОВ С.А.
Южно-Уральский государственный университет, г. Челябинск
ЯКОВЛЕВ Г.К.
Уральский институт управления, филиал Российской академии народного хозяйства и государственной службы при президенте Российской Федерации, г. Челябинск

Аннотация. На основе обзора современного состояния развития информационных технологий в статье обосновывается необходимость учета комплексного влияния рисков на успешность проектов предприятий и организаций в области внедрения информационных технологий. В первой части обзора рассмотрены ущербы в результате развития кибертерроризма, расширения сектора интеллектуальных систем управления и применения зарубежного программного обеспечения на предприятиях России. Во второй части обзора рассмотрено влияние психологических, социальных, дидактических и экологических рисков на развитие информационных технологий.

Ключевые слова: информационные технологии, безопасность, риски

Введение

Современное информационное общество отличается широким использованием средств информационных технологий (ИТ). Например, мировая индустрия электронного обучения на начало текущего века составила $48 млрд. [1].

Российская аудитория интернета – крупнейшая в Европе, превышает 80 миллионов пользователей, из них 62 миллиона человек выходят в онлайн ежедневно. Динамично растёт коммерческий сегмент сети. Объём рынков, которые связаны с интернетом, составляет 16 процентов ВВП. Технология удалённого доступа активно используется при оказании государственных и муниципальных услуг, в 2014 году больше трети из этих муниципальных и государственных услуг были предоставлены в автоматизированном режиме. Интернет широко используется для формирования новой технологической основы отечественной экономики, в социальных отраслях, в образовании, в здравоохранении [2].

К основным целям, которые заложены в программу развития цифровой экономики в России до 2024 года, относятся: обеспечение быстрого доступа в интернет для каждого россиянина, включая жителей отдаленных населенных пунктов; замена вузовских дипломов и трудовых книжек на траектории развития, "умные города" и даже автоматизированная система принятия государственных решений [3].

Однако бурное развитие информационных технологий в современном обществе сопровождается усилением рисков для безопасности профессиональной деятельности.

В условиях современного информационного общества доминирующим деструктивным фактором является риск для обеспечения информационной безопасности, представляющей собой состояние защищенности информационной среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций и государства. Информационная среда - сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации [4].

Недостаточное обеспечение информационной безопасности может привести к ущербу экономического характера, поэтому представляется целесообразным информационные и экономические риски рассматривать в совокупности.

Информационные и экономические риски

К проблеме обеспечения информационной и экономической безопасности относится рост кибертерроризма. Термин «киберпреступность» подразумевает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде. Известный эксперт Д. Деннинг говорит о кибертерроризме как о «противоправной атаке или угрозе атаки на компьютеры, сети или информацию, находящуюся в них, совершенной с целью принудить органы власти к содействию в достижении политических или социальных целей» [5].

«Исследование потерь от взлома данных в 2016 г.» (2016 Cost of Data Breach Study), которое провели IBM и Ponemon Institute, по итогам 2015 г. дало следующие результаты [6]:

1. Средние потери 383 обследованных компаний от взлома данных выросли с 3,79 млн. долл. до 4 млн. долл.

2. Средняя сумма, уплаченная за каждую утраченную или украденную запись, содержащую секретную и конфиденциальную информацию, увеличились с 154 долл. до 158 долл.

3. Все обследованные организации пережили хищения данных в объеме от 3 тыс. до 101,5 тыс. взломанных записей. Большинство утечек было вызвано атаками с использованием вредоносного кода. Как и в случае с преступлениями многих других типов, затраты на очистку от него могут значительно превышать добычу хакера.

Хищения данных — не единственные потери бизнеса от онлайновых преступников. По расчетам ФБР, махинации с электронными сообщениями от имени генеральных директоров, в которых мошенники выступают от имени руководителей компаний и убеждают финансовых менеджеров перевести крупные суммы на фиктивные банковские счета, затронули десятки тысяч компаний и с января 2015 г. обошлись им более чем в 3,1 млрд. долл.

Защита от атак тоже дорого обходится бизнесу. Согласно аналитической фирме Gartner, мировые расходы на продукты и сервисы безопасности увеличатся в этом году до 81,6 млрд. долл. (62,8 млрд. ф. ст.), или на 8% по сравнению с прошлым годом из-за все более изощренных угроз и нехватки специалистов по кибербезопасности [7].

Крупнейшее в мире исследование в сфере киберпреступлений в отношении пользователей (Norton Cybercrime Report 2012), в котором приняло участие более 13 тысяч человек из 24 стран мира, было выполнено с целью определить общую осведомленность пользователей о киберугрозах в сети, наиболее популярные типы кибератак а также влияние новых технологий на информационную безопасность пользователей. По результатам исследования ущерб от киберпреступности за 2012 год оценивается в $2 миллиарда в год в России и $110 миллиардов во всём мире [8].

В современных условиях изменился характер киберпреступности:

− 15 % пользователей социальных сетей сообщили о взломе своего персонального аккаунта и действиях от их имени;

− 1 из 10 пользователей социальных сетей говорил, что стал жертвой мошенничества или несуществующей ссылки;

− в то время как 75 % полагают, что киберпреступники нацелены на социальные сети, менее половины (44 %) используют решения для защиты от киберугроз в социальных сетях;

− почти одна треть (31 %) пользователей мобильных устройств получали текстовое сообщение от неизвестного адресанта с просьбой перейти по предложенной ссылке или набрать неизвестный номер для получения голосового сообщения.

Расширение сектора интеллектуальных систем управления в энергетической сфере, включая «интеллектуальные» сети − smart grid, информационные технологии поддержки принятия управленческих решений, создаваемые на основе средств и методов искусственного интеллекта, повышает риски управленческих решений, связанные с авариями и сбоями в работе таких систем [9].

Ущерб от техногенных катастроф, аварий соизмерим с ежегодным ростом ВВП [10].

Об усилении информационных и экономических рисков свидетельствует увеличение случаев крупномасштабных аварий в мире [11].

Например, 14 августа 2003 г. в США произошла авария с каскадным развитием, когда выход одного элемента энергосистемы привел к прекращению ее работы из-за перегрузок и повреждения других ее элементов. В итоге массовыми отключениями электроэнергии были охвачены крупнейшие города в северо-восточной части США и Канады. Общая потеря нагрузки составила 61800 Мвт [12]. В результате этой аварии 50 млн. потребителей не получали электроэнергию в среднем около 4 суток. Ущерб только в США составил около 10 млрд. дол., а в Канаде – более 2 млрд. канадских дол.

Другой пример, катастрофический пожар и мощные взрывы в марте 2004 г. на крупном американском нефтеперерабатывающем заводе компании British Petrolium в г. Техас Сити. Это событие привело к многочисленным человеческим жертвам и резкому росту биржевых цен на топливо. Благодаря следственным экспериментам появилась возможность подтвердить замаскированное дистанционное изменение параметров электроснабжения и технологических температурных режимов ректификационного оборудования по сети Интернет [13].

Объяснением ситуации видится отсутствие адекватной интеллектуальной системы управления и поддержки решений, которая по совокупности динамик текущих и ретроспективных значений отдельных параметров ситуации (политических, природных, технических, мотивационных, экономических, социальных и пр.) способна была бы упредить наступление катастрофических событий. Здесь могли бы помочь нейронные технологии либо системы управления знаниями (экспертные системы), обучаемые с подключением сетевых экспертных процедур [14].

Такое положение объясняется рядом причин.

Во-первых, энергетическое оборудование, коммуникации и средства измерения энергетических потоков в энергосистемах имеют достаточно большой срок эксплуатации, что приводит к необходимости увеличения количества энергосберегающих мероприятий, направленных на поддержку режима эксплуатации в заданных пределах надежности. При этом возникает необходимость в частом отключении отдельных участков энергетических потоков для проведения планово-предупредительных ремонтов оборудования, коммуникаций и замены средств измерения. Кроме того, при выполнении указанных мероприятий увеличивается время нахождения персонала в зонах возможного поражения электрическим током или от действия энергоносителей или вибрации, что увеличивает угрозу для его безопасности.

Во-вторых, погрешность измерения электроэнергии и энергоносителей в традиционных условиях представляет собой достаточно большую величину, зависящую от субъективной составляющей, связанной с особенностями работы персонала. Кроме того, достаточно сложно определить экономически обоснованное значение пиковой мощности. Поэтому на практике из

соображений надежности заявляют ее завышенное значение.

В-третьих, сбои и повреждения в измерительной системе могут искажать коммерческие измерения энергоресурсов и приводить к финансовым рискам энергоснабжающих организаций. Кроме того, ошибки в измерениях могут быть связаны с умышленным искажением измерений для уменьшения платы за использование энергоресурсов со стороны потребителя, что приводит к появлению коммерческих потерь энергоресурса [15].

Такая ситуация создает энергетический барьер экономического роста, связанный с необходимостью привлечения дополнительных средств для реализации мероприятий, направленных на энергобезопасность и энергосбережение.

Основной проблемой, решению которой способствует «Государственная программа энергосбережения и повышения энергетической эффективности на период до 2020 года», является преодоление энергетических барьеров экономического роста, в т.ч. за счет экономии средств, высвобождаемых в результате реализации энергосберегающих мероприятий, с соответствующей корректировкой объемов вводов дорогостоящих энергетических мощностей. Одним из основных целевых ориентиров долгосрочного социально-экономического развития Российской Федерации на период до 2020 года обозначена безопасность граждан и общества [16].

К другой проблеме обеспечения информационной безопасности относится усиление угрозы для безопасного применения зарубежного программного обеспечения на предприятиях России. Начало текущего века в России ознаменовалось бурным развитием для производителей компьютерных программ. Бизнес многих из них увеличился в разы, а наша страна превратилась в один из ключевых рынков для гигантов софтверной индустрии. Но конец 2013 и весь 2014 год отмечены спадом у ряда иностранных компаний. В статье Александра Страха, опубликованной в новостях экспертного центра электронного государства, раскрыты следующие причины такого положения [17]:

1. Сворачивание усилий государства по защите авторских прав на программы.

2. Озабоченность, вызванная тотальной слежкой американских спецслужб за пользователями Интернета.

3. Попытки российских государственных органов представить собственную стратегию в области интеллектуальной собственности.

4. Американские санкции в связи с Украиной.

Американские IT-корпорации, такие как Microsoft, Oracle, Symantec и Hewlett-Packard (HP), присоединились к санкциям в отношении ряда российских банков и компаний. Специалисты говорят об ускоренном переходе на отечественное программное обеспечение и оценивают влияние происходящего на другие отрасли экономики. Одним из путей развития отечественного программного обеспечение является применение унифицированных проектных решений [18].

Проблема обеспечения техногенной энергобезопасности на 70 % связана с человеческим фактором [10].

Поэтому недостаточное обеспечение психологической, социальной, экологической и дидактической безопасности может также привести к ущербу экономического характера.

Психологические, социальные, дидактические и экологические риски

В настоящее время уровень развития информационных технологий стер границы между государствами в информационном пространстве и создал беспрецедентные возможности для подавления противника без использования традиционных средств поражения. Все это давно осознали в Пентагоне, и в 1998 г. МО США была разработана новая «Объединенная доктрина информационных операций». В ней впервые вводится термин «стратегическое

информационное противоборство». Целями воздействия в нем являются объекты противника, выбираемые по принципу «пяти колец» (по мере убывания важности): 1) политическое и военное руководство страны; 2) системы жизнеобеспечения; 3) инфраструктура; 4) население; 5) вооруженные силы [19].

Поскольку воздействие на указанные объекты осуществляется с помощью сетевых технологий и методов, такое противоборство получило название «информационно-сетевая война». Основой ее является массированное воздействие на морально-психологическое состояние руководство и население страны-противника, что свидетельствует о возрастании угроз психологической безопасности. Причем, зачастую даже сам факт такого воздействия заблаговременно не может быть выявлен ее спецслужбами.

Информационно-сетевая война предусматривает проведение комплекса мероприятий в отношении противника:

- создание атмосферы бездуховности и безнравственности, что автоматически создает благоприятную атмосферу для нагнетания конфликтной обстановки внутри страны-противника и падению авторитета государственной власти;
- манипулирование общественным мнением и политической ориентацией социальных групп с целью создания обстановки политической напряженности и хаоса;
- дестабилизация политических отношений между партиями, объединениями и движениями с целью провокации конфликтов, разжигания атмосферы недоверия и подозрительности;
- обострение политической борьбы, провоцирование репрессий против оппозиции;
- развязывание в обществе гражданской войны;
- снижение уровня информационного обеспечения органов власти и управления с целью затруднения принятия важных решений;
- дезинформация населения о работе государственных органов, подрыв их авторитета, дискредитация органов управления;
- провоцирование социальных, политических, национальных и религиозных столкновений;
- инициирование массовых протестных акций, забастовок, массовых беспорядков;
- подрыв международного авторитета государства;
- нанесение ущерба жизненно важным интересам государства в политической, экономической, оборонной и других сферах [19].

Развитие электронного обучения и внедрение дистанционных образовательных технологий приводит к уменьшению времени общения студентов с преподавателями, что оказывает отрицательное влияние на результаты обучения и воспитания, являющиеся предметом дидактики, т.е. усиливаются угрозы дидактической безопасности. Для минимизации угрозы дидактической безопасности необходимо пересмотреть содержание обучения и воспитания в условиях электронного обучения, исследовать процесс мышления учащихся в новых условиях, чтобы дать ответы на вопросы: «чему учить?» и «как учить?».

Реалии современного информационного общества таковы, что недостаточное внимание к уровню использовании информационных технологий сопровождается потерями вследствие снижения конкурентоспособности. В образовании и науке отсутствие интернет-технологий приводит к опасности, связанной с недостатком актуальной информации. На энергоемких предприятиях в отсутствие информационно-измерительных систем возникает опасность, связанная с большой погрешностью измерения расходов электроэнергии и энергоносителей. На машиностроительных предприятиях в отсутствие автоматизированных систем проектирования возникает опасность

длительной и неэффективной подготовки производства.

Приведенные факты свидетельствуют о необходимости включения предприятия или организации в процесс внедрения информационных технологий в профессиональную деятельность. После осознания такой необходимости встает вопрос об эффективном выполнении данного процесса, в первую очередь о подготовке кадров для работы с автоматизированными средствами, которая в настоящее время оставляет желать лучшего.

Серьезной угрозой безопасности является современное состояние педагогического образования в России. В концепции поддержки развития педагогического образования опубликованы результаты мониторинга деятельности государственных вузов и их филиалов, проведенного в 2012 году Министерством образования и науки РФ, которые показали, что 30 из 42 педагогических вузов (71,43%) и 29 из 37 их филиалов (78,38%) признаны имеющими признаки неэффективности. Немаловажную роль в сложившейся ситуации играет проблема неудовлетворительного качества подготовки выпускников, обусловленная устаревшими методами и технологиями, отсутствием связи учебных дисциплин и реальных потребностей работодателей [20].

О недостаточном уровне информационной подготовки кадров отмечалось, например, в докладе Д.Медведева на заседании президиума Госсовета «О реализации стратегии развития информационного общества в Российской Федерации»: «…Я вообще хотел бы сказать, что чиновник, не владеющий элементарными навыками пользования компьютером, не может эффективно работать. А стало быть, должен искать себе иное место приложения труда. Или учись, или, что называется «до свидания». Мы же не принимаем на работу людей, которые не умеют читать и писать. Владение компьютером сегодня – это то же самое» [21, с.5].

О ситуации в области электронного обучения в образовательных организациях России свидетельствуют следующие факты:

1. Образовательные программы не адаптированы для дистанционных образовательных технологий (ДОТ);
2. ДОТ применяется к «не лучшим» обучающимся;
3. Электронный образовательный контент не отличается высоким качеством;
4. Электронные образовательные ресурсы и курсы являются закрытыми внутри образовательных учреждений;
5. Разработанные электронные ресурсы не всегда своевременно обновляются;
6. Ведущие «классические» университеты зачастую остаются в стороне от ДОТ;
7. Несовершенная нормативная база.

Исследования в области внедрения электронного обучения свидетельствуют о наличии проблемы безопасности, включающей в себя, кроме информационной составляющей, дополнительно экономический, дидактический, экологический, социальный и психологический компоненты. При проектировании информационной подготовки имеют место следующие угрозы безопасности:

1) угроза дидактической безопасности связана с использованием учебных материалов, не отражающих или отражающих не в полной мере требования федеральных государственных образовательных стандартов и иных нормативных документов, основанных на применении компетентностного подхода, требований информационного общества и эффективных способов контроля приобретенных компетенций;

2) угроза экономической безопасности имеет место в связи с многовариантностью способов проектирования содержания дисциплин, отличающихся отношением цены к качеству;

3) угроза информационной безопасности усиливается в результате

сокращения сроков актуальности информации, а также увеличения доли электронных ресурсов науки и образования, имеющих вид «неопубликованные документы», т.е. возникает необходимость оценки документов на соответствие требованиям новизны и приоритетности;

4) угрозы психологической, социальной и экологической безопасности, возникающие в результате перехода на дистанционное обучение, связаны с уменьшением времени общения преподавателя со студентом и недостаточной надежностью средств и методов обмена информацией, а также с отсутствием мотивации персонала для применения ИКТ; в этом отношении возрастает роль представления учебной информации с точки зрения ее восприятия, усвоения и контроля, а также создание условий для социальной и здоровьесберегающей безопасности [22, с. 129−131].

Можно утверждать, что информационно-коммуникационные технологии воздействуют на сознание, образ жизни людей, их образование, содержание их деятельности, а также на содержание и формы взаимодействия правительства и гражданского общества. Учитывая усиление угроз безопасности в информационном обществе, представляется целесообразным управлять процессом безопасности с целью минимизации угроз информационной, экономической, экологической, психологической и дидактической безопасности.

Различные риски, оказывающие деструктивное воздействие на профессиональную деятельность находятся в тесной взаимосвязи и во взаимодействии друг с другом. В ходе этого взаимодействия возникает результирующий комплекс угроз, который не является простой их совокупностью. Например, вопросы объединения студентов различных направлений в потоки для проведения лекций по сходным дисциплинам, учета взаимосвязи базового и получаемого образования традиционно решаются на основе использования знаний и интуиции специалистов. При таком подходе возможны два варианта. При первом варианте для проведения лекций группы не объединяются в потоки, при втором – объединяются. При первом варианте могут быть экономические риски, т.к. образовательная организация оплачивает работу преподавателю за время для проведения лекций пропорционально количеству групп. При втором варианте могут быть дидактические риски, т.к. при обеспечении требований к формированию знаний студентов одного направления аналогичные требования для студентов других направлений не обеспечиваются. Согласно исследованиям в области профессионально-педагогического образования наблюдается высокий процент погрешности в планировании подготовки кадров [3], что требует учета взаимосвязи компетенций при проектировании подготовки кадров, который, в свою очередь, приведет к минимизации экономических и дидактических рисков.

Таким образом, обеспечить эффективное противодействие существующим и потенциальным угрозам можно только при учете особенностей каждой из них, а также специфики их проявления в единой системе деструктивных факторов. Эти особенности дают основание рассматривать процесс развития информационных технологий в профессиональной деятельности как сложную информационно-аналитическую систему, функционирующую в условиях неопределенности и усиления рисков.

Литература:

1. EC (2000). Communication from the Commission: E-Learning – Designing «Tejas at Niit» tomorrow’s education. Brussels: European Commission

2. Российский форум Интернет Экономика 2015 [Электронный ресурс]. – 2015. – Режим доступа: http://ie.iri.center (дата обращения: 29.12.2016).
3. Умные люди, умные города: что надо знать о программе развития цифровой экономики [Электронный ресурс]. – 2017. – Режим доступа: http://tass.ru/ekonomika/4306382 (дата обращения: 01.08.2017).
4. Понятие безопасности информационных систем. URL: http://life-prog.ru/1_21271_ponyatie-bezopasnosti-informatsionnih-sistem.html
5. Кибертерроризм. URL: http://elcomrevue.ru/kiberterrorizm
6. 2016 Cost of Data Breach Study: United States. URL: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=sel03094usen
7. Кибербезопасность: группы, которые за вами охотятся. URL: https://www.itweek.ru/security/article/detail.php?ID=196454
8. Norton Cybercrime Report 2012. URL: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
9. Интеллектуальная электроэнергетика: стратегический тренд международной конкурентоспособности России в XXI веке / Т.В. Иванов, С.Н. Иванов, Е.Л. Логинов, Э.Б. Наумов. М.: Спутник+, 2012
10. Толмачев В.Д. О кадровом обеспечении современной энергетики / / Энергобезопасность и энергосбережение. − 2011. − №1. − С. 37−38.
11. Логинов, Е.Л. Сетевые информационные атаки на системы управления энергетическими объектами критической инфраструктуры / Е.Л. Логинов, А.Н. Райков // Теплоэнергетика. – 2015. – №4. – С. 3-9.
12. Рахманов, М.И. Аварии энергосистем парализуют мир / М.И. Рахманов // – Режим доступа: http://www.Cnews.ru (дата обращения: 29.05.2017)
13. Oil Hits New Hiw after Refinery Blast // Reuters. 2004. August 13
14. Modern Collective Intelligence / D. Gubanov, N. Korgin, D. Novikov, A.Raikov // E-Expertise. Series: Studies in Computational Intelligence. Springer, 2014. V558.
15. Паздерин, А.В. Математический метод контроля достоверности измерительной информации о потоках энергетических ресурсов на основе теории оценивания состояния / А.В. Паздерин, В.В. Софьин, В.О. Самойленко // Теплоэнергетика. − 2015. − №11. − С. − 26−31.
16. Государственная программа энергосбережения и повышения энергетической эффективности на период до 2020 года. URL: http://www.ceskom.ru/files/normativ/energosafe/energysafe_program.pdf
17. Иностранное программное обеспечение в России не бойся, ещё хуже будет // Экспертный центр электронного государства [Электронный ресурс]. – Режим доступа: http://d-russia.ru/inostrannoe-programmnoe-obespechenie-v-rossii-ne-bojsya-eshhyo-xuzhe-budet.html
18. Babkin V.V., Gelrud Ya.D., Loginovsky O.V. Development of information and computing sys-tems of enterprises and organizations based on unified design decisions. Investment and innovation management journal. – 2017. – No. 2. Pp. 137 – 144. DOI: 10.14529/iimj170222
19. Информационные войны [Электронный ресурс]. – Режим доступа: http://www.infwar.ru.
20. Концепция поддержки развития педагогического образования [Электронный ресурс]. – Режим доступа: http://www.mpgu.edu/documents/concepciya-podderzhki-ped-obrazovaniya.pdf
22. Богатенков, С.А. Формирование информационной компетентности в уровневом профессионально-педагогическом образовании: моногр. – Челябинск: Изд-во Челяб. гос. пед. ун-та , 2012. – 185 с.
23. Богатенков, С.А. Система формирования информационной и коммуникационной компетентности: учеб. пособие. – Челябинск: Изд-во Челяб. гос. пед. ун-та, 2014. – 297 с.

Богатенков Сергей Александрович – канд. тех. наук, доцент кафедры информационных технологий в экономике, Южно-Уральский государственный университет, г. Челябинск; e-mail: ser-bogatenkov@yandex.ru.

Яковлев Георгий Константинович – студент Уральского института управления, филиала Российской академии народного хозяйства и государственной службы при президенте Российской Федерации; e-mail: rai9296@yandex.ru.

Дата поступления 20 августа 2017 г.

DOI: 10.14529/iimj170303

THE CURRENT STATE OF DEVELOPMENT OF INFORMATION TECHNOLOGIES IN THE ASPECT OF SECURITY

BOGATENKOV S.A.
South Ural State University, Chelyabinsk, Russia
YAKOVLEV G.K.
Ural Institute of administration-branch of Russian presidential Academy of national economy and public administration under the President of the Russian Federation, Chelyabinsk, Russia

Abstract. Based on the review of the current state of development of information technologies the article substantiates the necessity of taking into account the comprehensive impact of risks on the success of projects of enterprises and organizations in the field of information technology. In the first part of the review considers the damages as a result of development of cyberterrorism, the expansion of intellectual systems of management and use of foreign software in Russia. In the second part of the review considers the influence of psychological, social, educational and environmental risks in the development of information technology.

Keywords: information technologies, safety, risk

References

1. EC (2000). Communication from the Commission: E-Learning - Designing "Tejas at Niit" tomorrow's education. Brussels: European Commission

2. Russian Forum Internet Economy 2015 [Electronic resource]. - 2015. - Access mode: http://ie.iri.center (reference date: 29.12.2016).

3. Smart people, smart cities: what you need to know about the program for the development of the digital economy [Electronic resource]. - 2017. - Access mode: http://tass.ru/ekonomika/4306382 (date of circulation: August 1, 2017).

4. The concept of information systems security. URL: http://life-prog.ru/1_21271_ponyatie-bezopasnosti-informatsionnih-sistem.html

5. Cyberterrorism. URL: http://elcomrevue.ru/kiberterrorizm

6. 2016 Cost of Data Breach Study: United States. URL: http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=sel03094usen

7. Cybersecurity: the groups that you hunt. URL: https://www.itweek.com/security/article/detail.php?ID=196454

8. Norton Cybercrime Report 2012. URL: http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

9. T.B. Ivanov, S.N. Ivanov, E.L. Loginov, E.B. Naumov. Intellectual Electricity: Strategic Trend of Russia's International Competitiveness in the 21st Century / M .: Sputnik +, 2012.

10. Tolmachev V.D. On the staffing of modern energy / Energy security and energy saving. - 2011. - №1. - P. 37-38.

11. E.L. Loginov, A.N. Raikov. Network Information Attacks on Energy Objects Management Systems for Critical Infrastructure / Thermal power engineering. - 2015. - № 4. - P. 3-9.

12. Rakhmanov M.I. Power system failures paralyze the world. - Access mode: http://www.Cnews.ru (reference date: May 29, 2017)

13. Oil Hits New Hiw after Refinery Blast // Reuters. 2004. August 13

14. Modern Collective Intelligence / D. Gubanov, N. Korgin, D. Novikov, A. Raikov // E-Expertise. Series: Studies in Computational Intelligence. Springer, 2014. V558.

15. A.V. Pasedin, V.V. Sofyin, V.O. Samoilenko. A mathematical method for monitoring the reliability of measurement information about energy resource flows based on the theory of state estimation / Heat power engineering. - 2015. - № 11. - P. 26-31.

16. State program of energy saving and energy efficiency improvement for the period until 2020. URL: http://www.ceskom.ru/files/normativ/energosafe/energysafe_program.pdf

17. Foreign software in Russia is not afraid, it will be even worse // Expert center of the electronic state [Electronic resource]. - Access mode: http://d-russia.ru/inostrannoe-programmnoe-obespechenie-v-rossii-ne-bojsya-eshhyo-xuzhe-budet.html

18. Babkin V.V., Gelrud Ya.D., Loginovsky O.V. Development of information and computing systems of enterprises and organizations based on unified design decisions / Investment and innovation management journal. - 2017. - No. 2. Pp. 137-144. DOI: 10.14529 / iimj170222

19. Information wars [Electronic resource]. - Access mode: http://www.infwar.ru.

20. The concept of supporting the development of teacher education [Electronic resource]. - Access mode: http://www.mpgu.edu/documents/concepciya-podderzhki-ped-obrazovaniya.pdf

22. Bogatenkov S.A. Formation of information competence in level professional-pedagogical education: monogr. / - Chelyabinsk: Publishing house of Chelyab. state. ped. University, 2012. - 185 with.

23. Bogatenkov S.A. System for the formation of information and communication competence: Textbook. allowance. / - Chelyabinsk: Publishing house of Chelyab. state. ped. University, 2014. - 297 p.

Bogatenkov Sergei Aleksandrovich – Cand. technical Sciences, associate Professor, Department of information technology in the economy, South Ural state University, Chelyabinsk; e-mail: ser-bogatenkov@yandex.ru

Yakovlev Georgy – the student of the Ural Institute of administration-branch of Russian presidential Academy of national economy and public administration under the President of the Russian Federation; e-mail: rai9296@yandex.ru

Received 20 August 2017

ОБРАЗЕЦ ЦИТИРОВАНИЯ

Богатенков, С.А. Современное состояние развития информационных технологий в аспекте безопасности / С.А. Богатенков, Г.Л. Яковлев // *Журнал управление инвестициями и инновациями.* – 2017. – №3. Стр. 31 – 40.
DOI: 10.14529/iimj170303

FOR CITATION

Bogatenkov S.A., Yakovlev G.K. The current state of development of information technologies in the aspect of security. *Investment and innovation management journal.* – 2017. – No. 3. Pp. 31 – 40.
DOI: 10.14529/iimj170303