3. Kravets A. G., Fomenkov S. A., Kravets A. D. Component-Based Approach to Multi-Agent System Generation. *Knowledge-Based Software Engineering: Proceedings of 11th Joint Conference, JCKBSE 2014 (Volgograd, Russia, September 17–20, 2014)*, Springer International Publishing Publ., 2014, pp. 483–490.

4. Kravets A. G., Shevchenko S. V., Kravets A. D. Generator agentov multiagentnoy sistemy sbora dannykh o perspektivnykh tekhnologiyakh [Agent generator for multi-agent system of gathering data on forecast technologies]. *Vestnik Kharkovskogo politekhnicheskogo institute* [Bulletin of the Kharkov Polytechnic Institute], 2012, no. 29, pp. 92–97.

5. Kravets A. D. Razrabotka metodov generatsii intellektualnykh multiagentnykh system [Development of intellectual multi-agent system generation methods]. *Izvestiya Volgogradskogo gosudarstvennogo tekhnicheskogo universiteta. Ser. Aktualnye problemy upravleniya, vychislitelnoy tekhniki i informatiki v tekhnicheskikh sistemakh* [Izvestia of Volgograd State Technical University. Ser. Actual Problems of Management, Computer Science and Informatics in Technical Systems], 2014, vol. 22, no. 25 (152), pp. 145–150.

6. Krylov I. B. Matematicheskie metody i multiagentnyy podkhod, primenyaemye pri razrabotke intellektualnoy obuchayushchey sistemy tekhnicheskoy discipliny [Mathematical methods and multiagent approach used in the development of intelligent tutoring system of technical disciplines]. *Universitetskiy kompleks kak regionalnyy tsentr obrazovaniya, nauki i kultury* [The University Complex as a Regional Center of Education, Science and Culture], 2014, pp. 333–336.

7. Petrova I., Kravets A. D. Method of Multi-agent System Design Based on Generation Algorithm. *Creativity in Intelligent Technologies and Data Science. CIT&DS 2015. Proceedings First Conference (Volgograd, Russia, September 15–17, 2015)*, Switzerland, Springer International Publishing Publ., 2015, pp. 169–178.

8. Tarasov V. B. *Ot mnogoagentnykh sistem k intellektualnym organizatsiyam: filosofiya, psikhologiya, informatika* [From multi-agent systems to intellectual organizations: philosophy, psychology, computer science], Moscow, Editorial Publ., 2002. 352 p.

9. Shcherbakov M. V., Chin T. Kh., May N. T., Kamaev V. A. Multiagentnyy metod upravleniya energopotokami v gibridnoy energosisteme s istochnikami vozobnovlyaemoy energii [Multi-agent method of management energy flows in hybrid power systems with renewable energy sources]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2013, no. 2 (22), pp. 30–41.

10. Adelinde M. *Uhrmacher, Danny Weyns, Multi-Agent Systems: Simulation and Applications*, CRC Press, 2009.

11. Arcangeli J.-P., Noël V., Migeon F. Software Architectures and Multiagent Systems. *Software Architecture 2*, 2014, pp. 171–207.

12. Kravets A. G., Kravets. A. D., Korotkov A. A. Intelligent multi-agent systems generation. *World applied sciences journal*, 2013, vol. 24, no. 24, pp. 98–104.

13. Kravets A. G., Kravets A. D., Fomenkov S. A., Kamaev V. A. Multi-agent systems component-based generator: development approach. *Applied Computing 2013. Proceedings of the IADIS International Conference (Fort Worth, Texas, USA, October 23–25, 2013)*, Texas, 2013, pp. 178–182.

004.056:[624.01+624.9]

АНАЛИЗ РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИЙ, СВЯЗАННЫХ С РАСПОЛОЖЕНИЕМ, КОНСТРУКЦИЯМИ И ОСОБЕННОСТЯМИ ЭКСПЛУАТАЦИИ ЗДАНИЙ[1]

Статья поступила в редакцию 05.09.2015, в окончательном варианте 03.11.2015г.

Брумштейн Юрий Моисеевич, кандидат технических наук, доцент, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: brum2003@mail.ru

Дюдиков Иван Андреевич, аспирант, Астраханский государственный университет, 414056, Российская Федерация, г. Астрахань, ул. Татищева, 20а, e-mail: shtorman@mail.ru

[1] Исследование выполнено при финансовой поддержке РФФИ. Грант № 14-06-00279 «Разработка методов исследования и моделирования объемов / структуры интеллектуальных ресурсов в регионах России».

С позиций информационной безопасности (ИБ) рассмотрен состав взаимосвязанных средств (компонент), обеспечивающих эффективность использования в организациях информационных технологий: здания и помещения в них; компьютерное оборудование; программное обеспечение; техническое оснащение зданий; каналы связи; инженерные коммуникации энерго-, тепло- и водоснабжения; персонал; информационные ресурсы; организационно-административные решения; финансово-экономических ресурсы и пр. Обоснована актуальность анализа номенклатуры и величин рисков ИБ организаций, определяемых особенностями расположения зданий на местности, их конструкциями, степенью изношенности. Указаны возможные варианты выбора для организаций зданий, уже существующих или тех, которые еще только предстоит спроектировать и построить. Проанализированы принципы принятия решений при выборе с учетом факторов ИБ, состав учитываемых ограничений. Показано, что такой выбор осуществляется в нечетких условиях, в том числе из-за неполноты и неточности информации о существующей ситуации и ее изменениях в будущий период. Исследованы вопросы обеспечения ИБ при проектировании новых зданий, реконструкции существующих, обустройстве прилегающих территорий. В связи с этим рассмотрены такие факторы: природно-климатические особенности возможных мест размещения; политика зонирования территорий в населенных пунктах; рельеф местности; характеристики грунтов; особенности режимов грунтовых вод; видовой состав и другие особенности растительности; наличие промышленных объектов и транспортных магистралей вблизи мест расположения зданий; возможности осуществления терактов и пр. Кратко проанализированы также вопросы ИБ, связанные с процессами строительства и реконструкции зданий, прокладки в них кабелей, проведения перепланировки помещений, выполнения их текущих ремонтов, перемещения организаций в новые здания.

Ключевые слова: информационная безопасность, информационные технологии, структура рисков, здания организаций, места расположения зданий, принципы выбора, нечеткие решения, характеристики зданий, проектирование зданий, строительство зданий, реконструкция зданий

RISK ANALYSIS OF INFORMATION SECURITY FOR ORGANIZATIONS, CONNECTED WITH BUILDINGS ARRANGEMENTS, DESIGNS AND OPERATION FEATURES

Brumshteyn Yuriy M., Ph.D. (Engineering), Associate Professor, Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation, e-mail: brum2003@mail.ru

Dyudikov Ivan A., post-graduate student, Astrakhan State University, 20a Tatishchev St., Astrakhan, 414056, Russian Federation, e-mail: shtorman@mail.ru

From positions of information security (IS) authors considered the structure of interconnected means (components), providing efficiency of information technologies usage in organizations: buildings and placements in them; computer equipment; software; technical equipment of buildings; communication channels; engineering communications of power-, warm- and water supply; personnel; information resources; organizational and administrative decisions; financial and economic resources and so forth. In article is proved analysis relevance for organizations of nomenclature and sizes for IS risks, determined by buildings arrangement features at the district, buildings designs, their wear degree. Authors are specified possible options of choice – taking into account IS risks, connected with buildings locations (already existing buildings or those, which only should be designed and constructed). Also are analyzed the principles of decisions adoption at such choice, concerned with IS factors; structure of considered restrictions. In article is shown, that such choice is carried out in indistinct conditions – because of incompleteness and inaccuracy of information about existing situation and its development in future period. Authors are investigated questions of IS providing in design process of new buildings, the reconstruction of existing buildings, arrangement of adjacent territories. In this regard such factors are considered: climatic features of possible locations; policy of territories zoning in settlements; land relief; characteristics of soil; features of ground waters modes; specific structure and other features of vegetation; existence of industrial objects and thoroughfares near buildings locations; possibilities of terrorist acts implementation and so forth. Also are briefly analyzed IS questions, connected with proc-

esses of construction and reconstruction of buildings, laying cables in them, carrying out re-planning of placements, performance of their maintenance, moving of organizations to new buildings.

Keywords: information security, information technologies, structure of risks, buildings for organizations, buildings locations, principles of choice, indistinct decisions, buildings characteristics, buildings design, buildings construction, buildings reconstruction

Введение. Процессы информатизации деятельности организаций играют важнейшую роль в повышении эффективности их работы, рациональности использования их интеллектуальных ресурсов. С развитием информатизации деятельности организаций для них меняется и структура угроз информационной безопасности (ИБ) [1], методы анализа угроз ИБ [28], подходы к защите от них [8, 29], включая системные подходы [30, 33]. Однако, несмотря на большое количество работ, посвященных различным видам угроз ИБ в условиях информатизации организаций, некоторые направления этой тематики остаются раскрытыми недостаточно полно. Одно из этих направлений – роль зданий в обеспечении ИБ организаций при работе с информационными ресурсами (ИР), в т.ч. с использованием информационных технологий (ИТ). Поэтому цель настоящей статьи – комплексное исследование этой проблематики.

Необходимые условия эффективности работы организаций с информационными ресурсами. Ниже мы рассмотрим условия, указанные в заголовке раздела, с учетом развития ИТ и диверсификации видов угроз ИБ организаций.

(С1) Здания организаций и помещения в них, а также примыкающие к зданиям участки территорий, должны обеспечивать потенциально благоприятные условия для размещения и использования аппаратных и программных средств ИТ; безопасность хранения и работы с ИР в бумажной и электронной формах; физическую безопасность и комфортность условий деятельности персонала; безопасность их личного имущества и т.д. Планирование затрат и фактические расходы на проектирование, строительство, реконструкцию, эксплуатацию зданий и помещений в них должны увязываться с размещением, размерами, техническим состоянием зданий [4]; располагаемыми финансовыми ресурсами организаций [11], необходимыми сроками достижения поставленных целей и пр. Для решения этих задач целесообразно использование методологии управления проектами и соответствующих программных средств – в т.ч. распространяемых по модели SaaS [14].

(С2) Номенклатура помещений в зданиях и возможности перемещений сотрудников между ними должны с одной стороны обеспечивать необходимое деловое общение, а с другой – исключать ненужные контакты, снижать возможности несанкционированного доступа к ИР, вероятности их повреждения, уничтожения, хищения. Специально отметим также необходимость исключения несанкционированного ввода информации в компьютерные базы данных и вноса «бумажных документов» в архивы, хранилища.

(С3) Эффективность использования систем охраны зданий и прилагающих к ним территорий во многом зависит от протяженности периметра зданий; количества входов в них; высоты первых этажей над уровнем земли и пр. Увеличение размеров контролируемых территорий вокруг зданий потенциально позволяет снизить возможности несанкционированного доступа (НСД) к информации с использованием визуального наблюдения, перехвата электромагнитных излучений [3, 17, 22], дистанционного прослушивания помещений с применением остронаправленных микрофонов (но не лазерных лучей, отражающихся от стекол зданий). Снижение возможностей НСД путем визуального наблюдения может обеспечиваться также за счет «рядов деревьев», однако это расширяет возможности маскировки злоумышленников.

Системы видеонаблюдения для контроля окружающих территорий, въездов на территорию, входов в здания, лестниц, коридоров, некоторых внутренних помещений сейчас используются уже повсеместно (в том числе и с инфракрасной подсветкой в ночное время

суток). Однако при большом числе изображений, выведенных на монитор «мозаикой», их непрерывная оценка персоналом службы охраны затруднена – особенно в дневное время, когда в зданиях много людей. Автоматизация анализа (оценки) таких изображений в реальном масштабе времени пока наталкивается на значительные алгоритмические трудности. При возникновении в зданиях пожаров может быть автоматически отдан приоритет [26] отображению на мониторах соответствующих помещений.

Особенно большое значение имеют системы контроля доступа физических лиц на территорию и непосредственно в здания через «пропускные пункты». Для этой цели помимо визуального наблюдения и обычных пропусков могут использоваться также системы биометрического контроля.

(С4) Системы пожарной и охранной сигнализации предназначены для обеспечения контроля помещений в том числе тех, где расположено компьютерное оборудование, большие количества бумажных документов и пр. Создание таких систем в уже построенных зданиях иногда вызывает технические трудности из-за необходимости прокладки большого количества кабелей.

(С5) Системы отопления и кондиционирования воздуха проектируются исходя из климатических условий территории, конструкций зданий, их расположения на местности. Такие системы должны поддерживать температурно-влажностные режимы в помещениях, необходимые для устойчивой работы технических средств информатизации (ТСИ); безопасного хранения ИР в бумажной форме; комфортности условий деятельности персонала. Качество и надежность работы таких систем во многом зависят от конструкций зданий, номенклатуры и расположения помещений, применяемых средств обеспечения энергоэффективности и энергобезопасности [23, 36].

(С6) Системы естественного и искусственного освещения в зданиях должны обеспечивать удобные условия работы персонала; снижать возможности НСД к ИР; их хищений в вещественной форме, копирования в электронной форме. Однако при этом должны минимизироваться негативные воздействия на бумажные документы (особенно, солнечного света, в т.ч. отраженных лучей). Это особенно важно для архивов. Отметим, что при проектировании размещения зданий и расположения комнат в них нужно учитывать обязательные нормы инсоляции – не только для новых зданий, но и для уже возведенных, которые могут «затеняться» (загораживаться) от света.

(С7) Освещение в темное время суток зданий и прилегающих территорий должно решать не только задачи минимизации криминальных рисков [27], но и архитектурно-эстетические [12], быть энергоэффективным [36].

(С8) «Лифтовое хозяйство» зданий должно обеспечивать удобство вертикальных перемещений персонала, технического оборудования (включая компьютерное), больших объемов ИР в бумажной форме. Отметим, что по действующим нормативам проектирования лифты могут не использоваться только в малоэтажных зданиях. Патерностеры в России практически не применяются – из-за их б*о*льшей опасности для людей по сравнению с лифтами. Эскалаторы используются лишь в крупных торговых центрах.

(С9) В процессе эксплуатации зданий кабели сигнализации, компьютерных сетей и энергокоммуникаций нуждаются в защите от повреждений. Такую защиту обеспечивает, в частности, размещение кабелей внутри кабель-каналов (в т.ч. «структурированных», т.е. использующих различные секции для кабелей разного назначения), а также над «фальш-потолками». Трубы тепло- и водоснабжения нуждаются в периодическом техническом обслуживании и замене (обычно срок службы металлических труб горячего и холодного водоснабжения, канализации значительно меньше, чем расчетный период эксплуатации зданий [4]). При этом конструкции зданий должны обеспечивать возможности таких замен. В настоящее

время начинают применяться долговечные полипропиленовые трубы, в т.ч. и для замены металлических. Своевременная замена труб снижает риски возникновения утечек из них и, как следствие, повреждений компьютерного оборудования, кабелей, носителей ИР в электронной и бумажных формах. Кроме того, пластмассовые трубы проводят звук хуже металлических – это снижает риски несанкционированного прослушивания «чужих» помещений с использованием таких труб в качестве звукопроводов [3]. Собственно съем колебаний, вызванных звуковыми воздействиями в комнатах на трубы, может осуществляться с использованием накладных акселерометрических датчиков.

(С10) Системы мониторинга технического состояния зданий [24], выявления повреждений в них (а также в оборудовании [31], обеспечивающем функционирование зданий), должны быть достаточно надежными. Системы автоматизации управления зданиями [9, 13, 23, 26] должны иметь защиту от компьютерных атак [35], в т.ч. и в отношении так называемых «промышленных вирусов».

Таким образом, особенности зданий, в которых размещаются (или предполагаются к размещению) организации, значительно влияют на состав и эффективность решений, связанных с различными компонентами, обеспечивающими работу с ИР в организациях. Планирование и согласованную по времени реализацию необходимых мероприятий целесообразно осуществлять с использованием методологии управления проектами [14].

Подходы к выбору зданий для размещения организаций. При принятии решений, связанных со зданиями для размещения организаций, целесообразно учитывать такие основные факторы: места расположения зданий [19] – в т.ч. в отношении возможностей привлечения клиентуры, возникновения больших скоплений людей, транспортных пробок; текущий «статус» зданий в отношении вещественного воплощения; функциональное назначение (характер использования) здания; условия получения зданий или помещений во владение/пользование; финансовые ресурсы, которыми располагает организация; необходимые сроки размещения организаций в зданиях (помещениях); риски, связанные с перемещением организаций на новые места расположения. Таким образом, в общем случае выбор является многокритериальным и обычно осуществляется в нечетких условиях. При этом могут быть использованы методы «структурирования альтернатив» [18], иные специальные методы теории принятия решений.

Размещение зданий в достаточно крупных населенных пунктах дает значительные преимущества: возможности использования уже существующей инфраструктуры этих пунктов (сетей тепло-, водо-, энергоснабжения, связи, канализации, транспортной структуры, услуг широкополосного доступа к Интернет на альтернативной основе и пр.): легче обеспечить организации квалифицированным персоналом с нужными специализациями деятельности. В тоже время в большинстве крупных населенных пунктов России, сейчас наблюдается дефицит доступных площадок для строительства. Это имеет такие последствия: для проектирования и застройки вынужденно используются «неудобные» участки [19], в т.ч. с повышенными рисками деформаций оснований сооружений; в ряде случаев необходим предварительный снос сооружений, расположенных на участках, планируемых для застройки, иногда – расселение жильцов; площади вокруг зданий, которые могут быть использованы их владельцами (в т.ч. для озеленения, организации парковок, в будущем – для размещения пристроек и пр.) часто оказываются минимальными; вблизи доступных для застройки участков нередко находятся транспортные магистрали с интенсивным движением, иногда – производства, значительно загрязняющие атмосферный воздух; для застройки нередко приходится использовать участки вблизи водоемов (это может увеличивать риски затопления и подтопления зданий грунтовыми водами; появления в зданиях комаров; для непроточных водоемов – ухудшать экологические условия при «цветении» воды); дефицит площадей приводит к росту этажности зданий и необходимости использования лифтов, снижающих энергоэффектив-

ность сооружений [36]. По действующим нормативам при проектировании новых общественных зданий лифты должны предусматриваться уже при высоте пола верхнего этажа по отношению к полу нижнего равной 9,9 м. На практике это обычно означает, что уже новые четырехэтажные здания должны быть оборудованы лифтами. При надстройке только мансардных этажей зданий это правило может не соблюдаться. В иных случаях (например, надстройка дополнительного этажа + мансарды) лифты необходимы. Они могут размещаться в специально возводимых пристройках, т.к. оборудование лифтовых шахт в уже эксплуатируемых зданиях обычно труднореализуемо.

В некоторых случаях свободных площадок для строительства в нужных районах может просто не быть. Тогда возможен лишь выбор из числа существующих – в т.ч. при условии реконструкции или сноса уже существующих сооружений, строительства новых зданий [15].

Потенциально возможны следующие варианты выбора мест расположения зданий. (В1) Глобальный – это актуально, в основном, для транснациональных корпораций. Выбор страны обуславливает ряд т.н. «страновых рисков» (в т.ч. и для ИБ), включая политическую и/или экономическую нестабильность; нетипичные условия (ограничения) по работе с ИР в стране, по доступу к Интернет-ресурсам; особые требования по соотношению лояльности персонала к корпорациям и государству и пр. (В2) В пределах России. Это важно, в основном, для крупных компаний. Выбор региона расположения организации может обуславливать некоторые региональные риски ИБ, в т.ч. связанные с природно-климатическими условиями (диапазоны колебаний температур, изменения влажностей воздуха, уровни его запыленности и пр.); сейсмической опасностью; дефицитом квалифицированного персонала; неразвитостью коммуникационных сетей; повышенными криминальными и / или вандальными рисками и пр. (В3) В пределах определенного региона. При этом выбор населенного пункта может обуславливать риски отсутствия приемлемых участков для строительства зданий или значительных расходов на получение таких участков; больших длительностей проектирования зданий и высокой вероятности «не утверждения» проектов различными контролирующими/согласующими организациями, градостроительными советами; высокие уровни криминальных рисков, приводящие к снижению эффективности работы персонала и пр. (В4) Населенный пункт (или даже район населенного пункта) заранее предопределены. Такой вариант на практике встречается наиболее часто. При этом в общем случае на выбранном участке может возводиться не только одно здание, но и их группа – при этом охраняемый периметр для них является общим. Состав рисков в основном аналогичен пункту «В3», но дополнительно можно указать возможность высокой запыленности воздуха. (В5) Место расположения организации является безальтернативным. Однако если речь идет о новом здании, то для него при проектировании обычно можно выбрать разную ориентацию по отношению к частям света в пределах строительной площадки, а также предусмотреть в проектах некоторые меры ИБ, обеспечения комфортности работы сотрудников. (В6) Если организация относительно небольшая и для ее размещения необходимо лишь ограниченное количество комнат, то в пределах конкретных зданий нередко возможен выбор места этой группы помещений. При этом в типичных случаях на нижних этажах (как более доступных для посетителей) стоимость аренды площадей обычно выше, чем на верхних. Однако для таких этажей выше уровни внешних «вандальных угроз» для находящихся в помещениях ИР, технических средств информатизации (ТСИ).

В свою очередь в пределах площадей, занимаемых организацией, обычно возможен выбор помещений для установки ТСИ; размещения персонала, занимающегося информатизацией, работой с ИР в бумажной форме и пр. При этом для отдельных помещений возможности принятия мер по повышению ИБ существуют, но достаточно ограничены.

В отношении «статуса» зданий возможны такие варианты.

(V1) Здания, из числа которых осуществляется выбор для размещения организации или ее подразделений, уже существуют (построены). Подварианты: еще не эксплуатируемые здания; здания, находящееся (или находившееся ранее) в эксплуатации. Возможности реконструкции таких зданий обычно ограничены недопустимостью снижения прочности несущих конструкций при перепланировке помещений; запретами на изменение внешнего вида и внутренней планировки зданий, имеющих особый статус («памятники архитектуры» и пр.). Отметим, что ограничения на реконструкцию зданий, установки на их крышах громоздких антенн дальней радиосвязи могут возникать и в период их эксплуатации – если они попадают в охранные зоны сооружений, получающих статус «памятников архитектуры». При получении в пользование здания может быть создана / изменена система видеонаблюдения (в т.ч. по периметру здания и на территории); по контуру территории может быть установлен (реконструирован) забор, в т.ч. с применением непрозрачных элементов (например, железобетонных или пластиковых плит).

На практике основные риски ИБ, относящиеся к эксплуатации зданий, обычно связаны с перерывами в подаче электроэнергии из внешних источников (обычно порядка нескольких часов), а также отключений электроэнергии при выполнении сервисных операций в зданиях, замене распределительных устройств и пр. Подключение зданий к «двум независимым источникам электроэнергии» по действующим нормативам предусматривается лишь для ограниченного круга «социально значимых» объектов, включая больницы [13].

В тоже время выбор источников бесперебойного питания (ИБП) для ПЭВМ обычно осуществляется исходя из продолжительности их работы порядка 10 мин., а серверов – как правило, не более часа. Поэтому в «ответственных случаях могут создаваться «зеркальные сервера», размещенные на других площадках – они должны брать на себя функции основных при отключении электропитания. Альтернативным решением в отношении размещения сайтов организаций (но, обычно, не корпоративных баз данных) может быть использование услуг хостинга специализированных фирм.

Коммутационные устройства локальных компьютерных сетей (концентраторы, маршрутизаторы) часто не подключаются к ИБП – поэтому сетевые соединения при отключении электроэнергии разрываются сразу. Подчеркнем, что в большинстве случаев в проектах зданий для городов не закладываются возможности использования аварийных дизель-генераторов для питания электросетей зданий в целом и / или отдельных электросетей для питания ТСИ. Для некоторых категорий помещений (например, операционных в больницах) [13] при проектировании должен предусматриваться третий источник энергоснабжения – однако подключение к нему систем видеорегистрации операций обычно не предусматривается. На практике в некоторых случаях (особенно провайдерами услуг доступа к Интернету) применяются маломощные электрогенераторы на сжиженном газе, которых достаточно для поддержки работы серверов при отключении электроэнергии.

Существенные сложности могут также возникать в связи с необходимостью установки в ранее построенных зданиях систем кондиционирования воздуха. (H1) Такие системы значительно увеличивают энергопотребление и это может потребовать замены кабелей, распределительных шкафов в зданиях, редко – реконструкции трансформаторных подстанций. (H2) Для уже существующих зданий часто невозможно или сильно затруднено размещение «чилеров» (систем централизованного управления температурно-влажностным режимом в помещениях) на крышах зданий и / или создание системы труб для централизованной подачи охлажденного воздуха. (H3) В тоже время установка многочисленных внешних блоков сплит-систем на фасадах зданий значительно искажает их архитектурный облик [10]; при некоторых видах неисправностей может создавать электромагнитные помехи для ТСИ и иного оборудования. (H4) Включение-выключение сплит-систем приводит к броскам на-

пряжения. Они могут отрицательно влиять на компьютерное оборудование, снижать надежность хранения ИР в электронной форме даже при использовании ИБП.

Отметим, что в условиях жаркого климата [21] отказы систем кондиционирования воздуха, а также прекращение их электропитания, могут значительно ухудшать условия работы ИТ-оборудования, концентрацию вниманиия персонала – в т.ч. технического и медицинского [14].

Само по себе проведение ремонтов и особенно реконструкций зданий (помещений) также несет дополнительные риски ИБ организаций, т.к. ремонтные операции осуществляют посторонние лица. Их контроль если и осуществляется, то преимущественно для исключения выноса «материальных ценностей» из зданий, но не вноса средств НСД к информации, средств ее копирования (включая закладки, электронные носители информации и пр.).

(V2) Здания, рассматриваемые как варианты для размещения организации или ее подразделений, находятся в процессе строительства. При этом иногда возможны изменения проектов строительства по требованию новых будущих владельцев зданий. Однако это обычно вызывает необходимость повторных согласований измененных проектов, задержки строительства.

Строительные организации могут допускать ограниченные отступления от проектов [15] (в основном, в отношении замены строительных материалов) – иногда это может влиять и на уровни ИБ – например, из-за увеличения «звукопроводности» перегородок.

С позиций ИБ важным риском в процессе строительства является возможность установки «закладок», которые затем будут передавать информацию по радиоканалу [3] – в том числе (как вариант) и с использованием металлических конструкций зданий в качестве антенн. Эти конструкции могут использоваться и для волновой накачки аккумуляторов (устройств энергопитания) закладок. Последние могут устанавливаться как непосредственно на стройплощадках, так и на заводах (в строительные изделия). Наиболее известны случаи установки таких закладок в здания посольств. Информация, относящаяся к обнаружению закладок в зданиях корпоративных структур, возможно, просто не предается огласке.

По сравнению с уже эксплуатируемыми зданиями охрана строительных площадок осуществляется, как правило, значительно слабее. При этом преследуются, в основном, цели исключения хищения строительных изделий, сантехники и пр. [15], но не снижения вероятности установки закладок и иных средств НСД к информации. На заводах железобетонных изделий соответствующий контроль, как правило, не ведется – в т.ч. и на площадках, где готовые изделия хранятся до набора ими «отпускной прочности».

В ходе возведения зданий качество строительства контролируется [5] как ГосАрхСтройнадзором, так и в рамках «авторского надзора» проектировщиков за ходом строительства [10]. Однако эти организации не ведут специального контроля соблюдения условий, связанных с обеспечением ИБ. Привлечение для такого контроля сторонних организаций требует наличия в них квалифицированного персонала; специального согласования со строительными организациями, т.к. это будет затруднять их работу. Перспективным является использование видеоконтроля строительства [34], в т.ч. с применением управляемых видеокамер.

(V3) Здания спроектированы, но строительство еще не начато. При этом проекты могут быть изменены до начала строительства – с учетом интересов нового владельца и важности факторов ИБ для него. Изменения в проекты должны оплачиваться новыми владельцами зданий по договорам с проектными организациями. Отметим, что такие изменения, как правило, требуют повторных согласований проектов.

(V4) Уже ведется процесс проектирования приобретаемого здания вместе с участком. В этом случае договор с проектной организацией должен заключить новый будущий владелец здания и (при необходимости) оплатить дополнительные расходы на изменение уже выполненной части проекта – с учетом своих интересов.

Сами по себе проекты зданий (в бумажной и электронной формах) в некоторых случаях могут представлять значительный интерес для злоумышленников с точки зрения планирования их действий. Такие проекты или их фрагменты потенциально могут быть доступны в различных типах организаций: проектных, в т.ч. при архивном хранении; контролирующих (согласующих); выполняющих профильную экспертизу; в ряде случаев – осуществляющих энерго- и теплоснабжение зданий; у владельцев зданий (действующих и прежних). Фрагменты проектов (особенно в электронной форме) также могут сохраняться в личных архивах отдельных специалистов – в т.ч. и уволившихся из проектных или эксплуатационных организаций. При этом существенно, что непосредственно в проектах зданий может быть отражено размещение ТСИ, средств пожарно-охранной сигнализации, прохождение коммуникационных кабелей (в т.ч. компьютерных сетей) и пр.

С позиций ИБ риск может представлять также утрата планов размещения кабельного хозяйства компьютерных сетей в зданиях, прокладки инженерных коммуникаций на территориях организаций и пр.

(V5) Площадка для строительства выбрана, но проектирование еще не начато. Риски проектирования и согласования проектов включают в себя следующее: возможности профессиональных ошибок проектировщиков, в т.ч. и в отношении обеспечения ИБ (такие ошибки могут снижать и экономическую безопасность проектных организаций – если не осуществляется страхование рисков); неполный учет при проектировании факторов ИБ, т.к. в числе строительных норм и правил, относящихся к гражданскому строительству, нет специального документа, отражающего требования ИБ; отрицательные заключения госэкспертизы на разработанные проекты – это может вызвать либо исключение возможности строительства здания вообще, либо дополнительные затраты времени и сил на изменение проекта и, как следствие, задержку начала строительства; «не прохождение» процедуры согласования проекта в контролирующих организациях; проект здания (группы зданий) может также не пройти согласование в «градостроительном совете» населенного пункта – в том числе по причине «несогласованности» его архитектурного облика с расположенными рядом зданиями / сооружениями, несоответствия проекта планам перспективного развития населенного пункта.

Использование ранее апробированных проектов (т.е. тех, на основе которых уже построены здания) имеет для заказчиков строительства такие положительные эффекты: снижаются риски не выявленных своевременно недочетов проектирования в отношении ИБ; уменьшается стоимость проектирования (необходима лишь «привязка» готовых проектов к новым местоположениям зданий); унифицируются внутрикорпоративные процедуры контроля зданий в отношении соблюдения норм ИБ; потенциально облегчается внутрикопоративная мобильность сотрудников, т.к. снижается вероятность их ошибок, связанных с адаптацией к новым условиям труда (во всех зданиях такие условия будут сходными).

Отметим, что с позиций защиты (охраны) периметра предпочтительны здания с минимальным количеством входов и с прямоугольной в горизонтальном сечении формой – так легче организовать видеонаблюдение.

В отношении направлений использования зданий, в которых предполагается разместить (или уже находится) организация, типичными являются такие варианты. (И1) Здание преимущественно «офисного назначения», которое целиком принадлежит (или будет принадлежать) организации – коммерческой или бюджетной (включая органы государственного и муниципального управления). При этом прилегающая территория в определенных пределах закреплена за «владельцем здания» и он может ограничивать доступ на нее автотранспорта, людей, прокладку через нее различных кабелей, трубопроводов и пр. (И2) Здание «офисного назначения», в котором располагаются различные организации «непроизводственного характера», в т.ч. и в рамках аренды помещений. (И3) Другие здания непроизводственного назначения, включая те, в которых размещаются организации образования и здра-

воохранения. (И4) Здания преимущественно складского назначения, в которых необходимо размещение ТСИ. (И5) Здания преимущественно промышленного назначения. В последних двух случаях в отношении ИР возникают риски, связанные с воздействиями производственного оборудования на носители ИР в электронной и бумажной формах, компьютерное оборудование (вибрации, электромагнитные излучения, промышленная пыль и пр.).

В отношении условий получения зданий в пользование возможны следующие варианты. (U1) Приобретение готового здания – риски ИБ могут быть связаны с не выявленной своевременно высокой изношенностью здания и инженерных коммуникаций в нем; неблагоприятных воздействий со стороны организаций/предприятий, размещенных в соседних зданиях; возможностями визуального просмотра внутренних помещений из рядом стоящих зданий и пр. (U2) Приобретение строящегося здания. Риски ИБ могут быть связаны с тем, что архитектурно-планировочные и конструктивные решения зданий не полностью отвечают требованиям организации, в т.ч. и в отношении условий обеспечения ИБ. (U3) Приобретение уже утвержденного проекта, прошедшего все стадии согласования и привязки к конкретному местоположению. Однако такая привязка может быть связана с обязательствами по сносу сооружений, фактически находящихся на месте строительства; расселения жильцов из них – а это может затрудняться несогласием жильцов, выдвижением ими труднореализуемых требований. (U4) Получение зданий целиком или части их помещений в аренду на определенный срок. Риски могут быть связаны с изменением арендодателя и желанием нового владельца досрочно прекратить аренду. Отметим, что в случае аренды (особенно краткосрочной) затраты на реконструкцию и ремонт помещений, обеспечение ИБ обычно носят ограниченный характер.

Риски ИБ резко возрастают при размещении в зданиях нескольких организаций. При этом обычно затруднен контроль входящих и выходящих из зданий лиц; умышленного или неумышленного появления посторонних лиц в районах расположения помещений организаций и пр.; несанкционированного выноса злоумышленниками оборудования и носителей с ИР; размещения (в том числе временного) в зданиях / помещениях средств НСД к информации и пр. Кроме того, больше и риски реализации террористических угроз, в т.ч. путем подрыва зданий с помощью взрывчатки доставленной во внутренние помещения (например, при завозе мебели въезжающей организацией).

Объемы финансовых ресурсов, которыми располагают организации, могут значительно ограничивать выбор решений в отношении зданий. При этом необходим учет затрат не только на покупку существующих зданий (или их проектирование и строительство), но и эксплуатационных расходов – включая средства, связанные с обеспечением ИБ организаций.

Предельные сроки, в которые организации должны быть размещены в зданиях, также могут ограничивать номенклатуру допустимых решений. При этом аренда помещений может рассматриваться как временный (промежуточный) вариант перед приобретением или строительством зданий.

Риски, связанные с перемещением организаций на новое место расположения, включают в себя следующее: временную утрату доступности ИР различных типов в процессе переезда; физическую утрату или повреждения носителей ИР при их транспортировке; повреждения ТСИ при демонтаже, транспортировке и монтаже на новом месте; потерю доступности в отношении ИР в бумажной форме, т.к. они оказываются в непривычных местах; увольнение сотрудников, для которых новое место расположения оказывается неудобным по тем или иным причинам (при этом уволившиеся сотрудники могут быть носителями ИР, представляющих угрозу для ИБ организаций); временное снижение эффективности служб охраны зданий, т.к. им также необходим период времени для адаптации к изменившимся условиям.

Риски ИБ организаций, определяемые особенностями расположения зданий на местности, их конструкциями, степенью изношенности. В отношении расположения зданий на местности целесообразно учитывать ряд рисков, прямо или косвенно влияющих на ИБ организаций.

(Р1) В случае развитого рельефа при расположении зданий в «низинах» увеличиваются такие риски. (Р1а) Несанкционированного дистанционного съема информации – за счет визуального наблюдения, анализа электромагнитных излучений ТСИ в здании [3, 17] или применения лазерных лучей для считывания вибраций со стекол [3]. В этом случае верхние этажи зданий не дают дополнительную защиту по сравнению с нижними. (Р1б) Развития на прилегающих возвышенных участках оползней [37], которые могут повредить здания. (Р1в) Затопления подвальных помещений талыми водами и ливневыми осадками, стекающими с близлежащих возвышенностей. При этом может повреждаться в основном техническое оборудование, входящее в системы инженерного обеспечения зданий, т.к. размещение в подвалах компьютерного оборудования не характерно. (Р1г) Вероятности затопления подвалов зданий паводковыми водами в крупных населенных пунктах относительно невелики - особенно если были своевременно выполнены берегоукрепительные работы (т.е. дамбы поддерживаются в нормальном состоянии). В тоже время для небольших населенных пунктов, прежде квсего расположенных по берегам крупных рек, такие риски существуют. (Р1д) Подъемов уровней грунтовых вод при прохождении волны паводка (это существенно, в основном, для зданий, расположенных вблизи водотоков и только для некоторых регионов – включая Астраханскую область).

(Р2) При размещении зданий вблизи оврагов (и иных естественных углублений рельефа) возрастают риски, связанные с влиянием оползней [37] – причем не только для самих зданий, но и для заглубленных в грунт инженерных коммуникаций (включая кабели связи). Эти риски не всегда могут быть устранены укреплением стенок оврагов, цементированием грунтов, устройством подпорных стенок. Факторы, увеличивающие риски оползней: наличие вибраций грунта (например, от прохождения тяжелого транспорта [6], работы метрополитена и пр.); высокая влажность грунта – в том числе и из-за обильных осадков, утечек из водонесущих коммуникаций.

(Р3) Если здания расположены вблизи берегов морей (океанов), то потенциальным фактором риска являются цунами. Высота их волн может превышать расчетные значения, используемые при проектировании для штормов. Последние могут негативно влиять на здания за счет соленых брызг, переносимых ветром – они вызывают ускоренную коррозию металлических частей; могут проникать в помещения и воздействовать на компьютерное оборудование, бумажные документы. Риск могут представлять также «ветровые нагоны» водных масс, характерные, например, для побережья Каспия.

(Р4) Если здания размещаются на возвышенных участках территории, то риски их подтопления грунтовыми водами резко снижаются. Однако увеличиваются другие риски. (Р4а) Ветровых воздействий на сами здания и оборудование (в т.ч. предназначенное для связи), которое размещено на их крышах. (Р4б) Ветровой эрозии грунтов, на которых возведены здания – если не было произведено их «дернование» или покрытие специальными строительными сетками. (Р4в) Оползней грунтов под зданиями после сильных осадков и / или при сейсмических воздействиях – особенно если не были приняты меры по сейсмоизоляции зданий [30], закреплению грунтов, в т.ч. с использованием подпорных стенок и пр. (Р4г) Возрастает вероятность ударов молний в здания, особенно высотные. Даже если здания грамотно защищены молниеотводами [2, 22], кабели локальных сетей могут «срабатывать» как антенны, через которые электромагнитный импульс поступает на сетевые карты и концентраторы (хабы) [25]. Это, как показывает личный опыт одного из авторов, во многих случаях приводит к их выходу из строя. (Р4д) Дистанционного визуального наблюдения того, что

происходит в помещениях зданий – особенно в вечернее время, когда такие помещения подсвечены изнутри.

(Р5) Возможность повреждения заглубленных коммуникаций (включая кабели электроснабжения, коммуникационные оптоволоконные кабели, трубы водоснабжения и пр.) при сдвигах массивов грунта в результате просадок. Обрывы кабелей электроснабжения могут приводить к прекращению функционирования ТСИ, так как продолжительности их работы от ИБП много меньше, чем время восстановления работоспособности кабелей.

(Р6) Утечки из водонесущих коммуникаций в грунт могут приводить к подтоплению зданий (особенно построенных на суглинистых грунтах с низким коэффициентом фильтрации); появлению сырости в подвалах за счет значительной капиллярной каймы над грунтовыми водами (это может исключать использование подвалов для хранения бумажных документов) и пр.

(Р7) Деформации зданий при просадках грунтов оснований (особенно при отсутствии свайных фундаментов), а также провалов грунтов, вызванных суффозионными явлениями техногенного происхождения. Просадки и подъемы уровней грунтовых вод могут вызываться обильными осадками; неумеренными поливами зеленых насаждений – в т.ч. на территориях, примыкающих к зданиям; утечками из водонесущих коммуникаций.

(Р8) Свайные фундаменты обеспечивают возможности строительства зданий на грунтах с низкими естественными «несущими» свойствами. Однако за счет барражных эффектов свайных полей в отношении потоков грунтовых вод, они могут приводить к «самоподтоплению» зданий; повышать уровни грунтовых вод для других близко расположенных объектов.

(Р9) Средства транспорта могут создавать для зданий (и находящихся в них организаций) такие виды рисков. (Р9а) Негативные эффекты от вибрации зданий [6] возможны не только для самих зданий, но и для компьютерного оборудования (включая работающие винчестеры), климатического оборудования с вращающимися частями и пр. Мерами борьбы могут быть, в частности, специальные амортизирующие прокладки над фундаментами зданий [6] – но их создание возможно лишь в процессе строительства. (Р9б) Повреждения пристроек или первых этажей зданий при наезде на них транспорта в случае аварий. При этом негативные последствия обычно больше при значительных площадях остекления первых этажей. (Р9в) Звуковых воздействий на здания, в т.ч. от пролетающих выше или разогревающих двигатели самолетов. В тоже время в отношении автотранспорта эффективным может быть использование специальных звукозащитных стенок; насаждение нескольких рядов деревьев [6] и пр. (Р9г) Повышение загазованности воздуха от проезжающего мимо зданий автотранспорта; от грузовиков, доставляющих товары в магазины, размещенные на первых этажах зданий и пр. (Р9д) Увеличение загазованности воздуха от тепловозов, перемещающихся по близлежащим железнодорожным путям. (Р9е) Разрушения остекления, а иногда и самих прилегающих зданий, при взрывах грузов на железнодорожном и автотранспорте (взрывчатые вещества, горюче-смазочные материалы и пр.) – сейчас такие события уже достаточно редки. (Р9ж) Воздействие электромагнитных помех от «электрических разрядов» на электротранспорте (электричек, троллейбусов, трамваев) на компьютерное и иное оборудование в зданиях [2, 22, 25], носители ИР в электронной форме. (Р9и) Работа трамвайного транспорта при недостаточной эффективности т.н. «фидерных подстанций» приводит к возникновению под землей значительных блуждающих токов. Они, в свою очередь, ускоряют разрушение железобетонных фундаментов; металлических труб; металлических оболочек кабелей и пр.

(Р10) Воздействия от электромагнитных полей линий электропередач, по которым передаются большие мощности [25]; проводов для энергопитания электровозов могут затруднять использование в зданиях локальных беспроводных сетей, ухудшать (или даже исключать) беспроводной доступ к Интернет, неблагоприятно воздействовать на персонал.

Практика показывает, что такие воздействия могут также при определенных условиях блокировать использование пультов дистанционного управления для простых радиоохранных систем автомобилей [20], принадлежащих сотрудникам.

(Р11) При малых размерах окружающих здания территорий владельцы могут провести обустройство окружающих территорий (в т.ч. озеленение, асфальтирование) лишь на ограниченных площадях. При этом риски наличия на прилегающих территориях аллергенных растений (включая лебеду, амброзию и пр.) по крайней мере в южных регионах России достаточно велики. Следствиями воздействия аллергенной пыльцы на сотрудников (особенно при отсутствии кондиционирования воздуха) могут быть снижение концентрации внимания, повышенная рассеянность и пр. Аналогичное влияние оказывает и появление в помещениях организаций комаров, в меньшей степени – высокая запыленность воздуха. В результате возрастают риски неумышленных ошибок при работе с ИР, неадекватных реакций на предупреждающие сообщения антивирусных и антиспамовых программных средств и пр.

(Р12) Малые площади прилегающих территорий вокруг зданий часто не обеспечивают достаточного количества парковочных мест для личного автотранспорта сотрудников. Размещение же такого транспорта в отдалении от зданий, где работает персонал, приводит к тому, что сотрудники часто нервничают в отношении сохранности своих автомобилей. Как следствие, снижается концентрация внимания, могут допускаться неумышленные ошибки при работе с ИР. В определенной степени нервозность сотрудников может быть снята применением современных радиоохранных систем автомобилей [20], обеспечивающих для владельцев расширенные возможности дистанционного получения информации – в т.ч. и по их запросам.

При нехватке парковочных площадей вблизи зданий возможны такие проектные решения: создание корпоративных многоэтажных парковок на территории организации; подземные парковки под зданиями; использование первых этажей зданий под «открытые парковки» (остальные этажи при этом «подняты» на несущих колоннах). Отметим, что последние два варианта более уязвимы к возможностям подрыва зданий при реализации террористических угроз (мировой опыт показывает, что в качестве «взрывчатых веществ» могут применяться даже минеральные удобрения).

Риски, связанные с недостатками в конструкциях зданий.

(Р13) Возникновения вибраций [6] при работе технологического оборудования, перемещениях лифтов и пр. Это особенно существенно для зданий производственного назначения, в том числе «перепрофилированных» под такое использование. Повышенные риски вибраций ограничивают возможности расположения на крышах зданий «чилеров», а в подвалах – мотор-генераторов, предназначенных для стабилизации напряжения питания, защиты электросетей зданий от кратковременных скачков напряжения.

(Р14) Использование плоских (или близких к таковым) крыш зданий увеличивает риски накопления на них в зимний период снежного покрова выше расчетных величин, принятых при проектировании. Это может приводить к разрушению крыш. При таянии снега на крышах (в т.ч. при кратковременных оттепелях) возможно образование сосулек по периметру крыш, просачивание жидкости в чердачные помещения. Такие помещения в офисных зданиях нередко используются провайдерами услуг доступа к Интернету для размещения своих локальных серверов – в том числе и по причине отсутствия арендной платы за эти помещения.

(Р15) Расчетные прочности фундаментов и несущих конструкций зданий могут либо вообще не допускать увеличение в последующем их этажности (создания надстроек), либо допускать в весьма ограниченном размере. В свою очередь это снижает возможности приспособления (адаптации) зданий под новые нужды при их реконструкции (например, надстройки этажей, в которых строго выполнены на определенном уровне требования ИБ).

Ограничения (причем часто весьма существенные) по допустимому весу оборудования обычно есть и для отдельных помещений в зданиях. Поэтому при размещении тяжелого оборудования иногда приходится принимать специальные меры по усилению несущих конструкций.

Конструкции зданий могут также ограничивать возможности возведения пристроек к ним (в т.ч. для размещения ТСИ, установки аварийных дизель-генераторов электропитания и пр.), создания закрытых переходов между зданиями. С позиций ИБ наличие таких переходов позволяет уменьшить количество входов в здания (максимально – до одного). Это в свою очередь облегчает контроль доступа в здания сотрудников и посторонних лиц, уменьшает возможности несанкционированного выноса материальных ценностей, носителей ИР и пр. С другой стороны такие переходы (особенно наземные и расположенные на небольших высотах) также должны контролироваться системами видеонаблюдения в отношении несанкционированного доступа в них.

(Р16) При значительных площадях остекления зданий через стекла в помещениях возможны значительные потери тепла (в холодное время года) и холода (в теплое время). Летом, если не используются светоотражающие пленки или специальные жалюзи, это может приводить к перегреву помещений – особенно тех, в которых расположены ТСИ со значительным тепловыделением. Большие амплитуды периодических колебаний температуры воздуха могут снижать сроки эксплуатации компьютерного оборудования, ускорять разрушение носителей ИР. Кроме того, прямое воздействие солнечных лучей на экраны мониторов ПЭВМ может уменьшать субъективно воспринимаемые яркости изображений – вплоть до потери их различимости.

Также укажем, что значительные площади остекления увеличивают потенциальные возможности НСИ к работающему компьютерному оборудованию по электромагнитному каналу [3]; наблюдения происходящего в помещениях извне – в т.ч. с использованием легких беспилотных летательных аппаратов и пр.

(Р17) Конструкции уже существующих зданий могут также затруднять размещение на входах в здания сотрудников служб охраны, технических средств защиты – если в проектах не было предусмотрено наличие специальных помещений; нет возможностей установки турникетов и др.

(Р18) Риски возникновения в зданиях и отдельных помещениях пожаров (в том числе при больших объемах документов в бумажной форме) могут быть значительно снижены путем использования при проектировании соответствующих отделочных материалов [7], а при эксплуатации – за счет исключения использования электронагревательного оборудования с целью отопления. Однако необходимо отметить, что в существующих зданиях большая часть строительных материалов и мебели является «сгораемой», при этом в случае горения может выделяться большое количество газообразных токсичных веществ, дыма [16]. Даже при локальных возгораниях дым может оказывать негативное влияние на ТСИ и носители ИР по всему зданию.

(Р19) Особо отметим риски, связанные с использованием в зданиях природного газа, например в котлах, предназначенных для локальных систем горячего водоснабжения, отопления помещений. Не выявленные своевременно утечки газа из газопроводов могут приводить к объемным взрывам (имеющим особую опасность), пожарам и пр.

Изношенность зданий может обуславливать такие виды рисков.

(Р20) Общее снижение механической прочности конструкций зданий и, как следствие, повышение вероятностей их частичного или полного разрушения при интенсивных внешних воздействиях (сейсмические волны, резкие порывы ветра, большая толщина снежного покрова на крышах, вибрации от проходящего транспорта [6] и др.). Кроме того, износ несущих конструкций может менять расчетный спектр собственных частот колебаний конструкций.

(Р21) В случае агрессивных грунтовых вод и / или значительных величин «блуждающих токов» ускоряется разрушение железобетонных свайных фундаментов зданий. При этом их несущая способность может уменьшиться ниже расчетных значений до истечения

плановых сроков эксплуатации [4]. Отметим еще, что при длительной эксплуатации зданий, агрессивность грунтовых вод может значительно увеличиваться по сравнению с той, которая была определена при инженерно-геологических изысканиях перед началом проектирования/возведения сооружений.

(Р22) Для зданий из сборного железобетона в процессе эксплуатации возможно появление протечек на межпанельных стыках, зимой такие стыки могут промерзать. Как следствие меняется температурно-влажностный режим в помещениях, ухудшаются условия работы с ИР. Однако такие протечки даже в достаточно старых зданиях могут эффективно устраняться за счет обработки стыков битумом, специальными мастиками и пр.

(Р23) Срок службы деревянных рам, используемых для остекления ряда старых зданий, достаточно ограниченный. При короблении и других изменениях формы таких рам возникают щели. Они приводят к значительному поступлению в помещения наружного воздуха – особенно при сильном ветре и/или большой разнице температур снаружи и внутри помещений. Это меняет расчетный температурно-влажностный режим в помещениях; может приводить к термоциклированию ТСИ и, как следствие, к сокращению срока их службы. Однако сейчас во многих зданиях офисного и иного назначения уже произведена замена «деревянных» окон на «пластиковые стеклопакеты», более долговечные в эксплуатации.

Итак, сделаем **выводы**. 1. Выбор местоположений зданий для размещения организаций в общем случае может носить многоэтапный характер (страна –> регион –> населенный пункт –> конкретное место–> ориентация зданий). 2. Сам выбор является многокритериальным и достаточно часто осуществляется в нечетких условиях. 3. Выбранное размещение зданий в значительной степени влияет на номенклатуру угроз ИБ, вероятности (частоты) реализации неблагоприятных событий, величины ущербов от их реализации. 4. При проектировании зданий для размещения организаций целесообразен более полный учет факторов ИБ – в т.ч. путем привлечения профильных специалистов; проведения специальных экспертиз. 5. Проекты большинства видов зданий, а также схемы размещения в них ТСИ, охранной и пожарной сигнализации, кабельных сетей в настоящее время являются слишком доступными для потенциальных злоумышленников. 6. Повышение уровней ИБ организаций, занимающих уже существующие здания, во многих случаях существенно ограничивается особенностями использованных при первоначальном проектировании конструктивных решений.

Список литературы

1. Ажмухамедов И. М. Оценка состояния защищенности данных организации в условиях возможности реализации угроз информационной безопасности / И. М. Ажмухамедов, О. М. Князева // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3. – С. 24–39.

2. Акбашев Б. Б. Обеспечение информационной и функциональной безопасности в специальных технических зданиях при электромагнитных воздействиях / Б. Б. Акбашев, Н. В. Балюк, Л. Н. Кечиев // Технологии электромагнитной совместимости. – 2011. – № 2. – С. 3–12.

3. Атаманов Г. А. Технические каналы утечки информации: определение, сущность, классификация / Г. А. Атаманов // Защита информации. Инсайд. – 2010. – № 1 (31). – С. 28–33.

4. Балькин В. М. Безопасность здания и факторы влияния на этапах жизненного цикла / В. М. Балькин //Вестник Самарского государственного архитектурно-строительного университета. Градостроительство и архитектура. – 2012. – № 1 (5). – С. 74–76.

5. Балькин В. М. Строительный контроль и безопасность зданий / В. М. Балькин // Вестник Самарского государственного архитектурно-строительного университета. Градостроительство и архитектура. – 2013. – № 3 (11). – С. 40–41.

6. Балькин В. М. Элементы воздействия транспорта на здания и сооружения. Их защита от транспортного шума и вибраций / В. М. Балькин // Вестник Самарского государственного архитектурно-строительного университета. Градостроительство и архитектура. – 2013. – № 3 (11). – С. 44–45.

7. Баранников Н. И. Подсистема определения категорий помещений, зданий и сооружений по взрывопожарной и пожарной опасности в САПР пожарной безопасности / Н. И. Баранников, М. А. Сергеева // Вестник компьютерных и информационных технологий. – 2013. – № 2 (104). – С. 17–21.

8. Баранов А. П. Современное состояние философии управления информационной безопасностью / А. П. Баранов // Бизнес-информатика. – 2014. – № 2 (28). – С. 7–14.

9. Батырев В. В. Технологии создания структурированных систем мониторинга и управления инженерными системами зданий и сооружений / В. В. Батырев, О. С. Волков, С. А. Качанов, В. В. Батырев, О. С. Волков, С. А. Качанов. – Москва : Всероссийский научно-исследовательский институт по проблемам гражданской обороны и чрезвычайных ситуаций МЧС России (федеральный центр науки и высоких технологий), 2011. – 270 с.

10. Брумштейн Ю. М. Авторский надзор в строительстве как элемент системы защиты прав авторов проектов / Ю. М. Брумштейн, В. В. Гладких, А. М. Сизов // Интеллектуальная собственность. Авторское право. – 2005. – № 3. – С. 12–18.

11. Брумштейн Ю. М. О возможных подходах к оценке вариантов улучшения информационной безопасности организаций / Ю. М. Брумштейн // Информационные технологии моделирования и управления. – 2007. – № 4 (38). – С. 490–494.

12. Брумштейн Ю. М. Освещение архитектурных объектов: синтез творчества и современных технологий / Ю. М. Брумштейн // Интеллектуальная собственность. Авторское право и смежные права. – 2015. – № 2. – С. 14–24.

13. Брумштейн Ю. М. Риски информационной безопасности медучреждений, их специалистов и пациентов / Ю. М. Брумштейн, Д. А. Захаров, В. Г. Акишкин // Информационная безопасность регионов. – 2013. – № 1. – С. 13–21.

14. Брумштейн Ю. М. Сравнительный анализ функциональности программных средств управления проектами, распространяемых по модели SaaS / Ю. М. Брумштейн, И. А. Дюдиков // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 4. – С. 34–51.

15. Дюдиков И. А. Системный анализ структуры строительного кластера региона в условиях развития информационно-коммуникационных технологий / И. А. Дюдиков, А. Б. Кузьмина, М. В. Иванова, Ю. М. Брумштейн, Е. Ю. Васьковский // Инженерно-строительный вестник Прикаспия. – 2014. – № 3 (9). – С. 43–51.

16. Исаков Г. Н. Системный анализ вопросов безопасности применения напольных покрытий и математическая модель процессов их терморазрушения / Г. Н. Исаков, А. Р. Манаева // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 1. – С. 30–43.

17. Казарин О. В. Особенности анализа рисков утечки конфиденциальной информации по техническим каналам при создании радиоэлектронных средств / О. В. Казарин, М. М. Репин // Вопросы кибербезопасности. – 2015. – № 4 (12). – С. 62–69.

18. Кандырин Ю. В.. Многокритериальное структурирование альтернатив в автоматизированных системах выбора / Ю. В. Кандырин, Л. Т. Сазонова, Шкурина Г. Л., Чивилев А. Д. // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 1. – С. 23–33.

19. Кираковский В. В. Анализ возможностей применения нейро-нечетких технологий при разработке проектов застройки территорий в условиях неполноты исходных данных / В. В. Кираковский, А. Н. Пылькин, А. О. Фаддеев // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 1. – С. 74–86.

20. Колганов А. А. Инженерная методика проектирования автомобильных радиоохранных систем / А. А. Колганов // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3. – С. 122–138.

21. Лапина О. А. Строительство в условиях жаркого климата / О. А. Лапина // Научное обозрение. – 2014. – № 7-3. – С. 876–879.

22. Любимова Н. С. Электромагнитная безопасность зданий / Н. С. Любимова, А. Б. Волков, В. А. Мартемьянов // Технические науки – от теории к практике. – 2013. – № 28. – С. 158–169.

23. Мальвина А. С. Автоматизация, диспетчеризация и информатизация высокотехнологичных медучреждений как средство повышения эффективности их работы / А. С. Мальвина, Ю. М. Брумштейн, Е. В. Скляренко, А. Б. Кузьмина // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 1. – С. 122–138.

24. Малый И. Н. Автоматизированная станция мониторинга состояния высотных зданий / И. Н. Малый // Ресурсоэнергоэффективные технологии в строительном комплексе региона. – 2012. – № 2. – С. 165–167.

25. Морозов Б. Н. Защита информации от электромагнитных импульсов в интеллектуальных зданиях / Б. Н. Морозов, Е. Г. Соколов // T-Comm: Телекоммуникации и транспорт. – 2012. – Т. 6, № 8. – С. 55–56.

26. Нгуен Суан Мань Подсистема формирования входных данных в системе интеллектуального управления зданием / Нгуен Суан Мань, Г. А. Попов, И. Ю. Кучин // Прикаспийский журнал: управление и высокие технологии. – 2015. – № 3. – С. 142–158.

27. Полянцева Е. Р. Криминогенная безопасность общественных зданий / Е. Р. Полянцева, Ю. С. Янковская // Новые идеи нового века: материалы международной научной конференции ФАД ТОГУ. – 2014. – Т. 3. – С. 363–367.

28. Поморцев А. С. Разработка системы параметров оценки рисков нарушения информационной бехзопасности организаций / А. С. Поморцев, С. Н. Новиков // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 2 (32). – С. 170–174.

29. Попов С. И. Анализ современных методов и алгоритмов оптимизации на этапе формирования структуры и состава комплекса технических средств защиты информации на объекте информатизации / С. И. Попов, Е. А. Рогозин, С. Ю. Рослов // Вестник Воронежского государственного технического университета. – 2009. – Т. 5, № 6. – С. 83–85.

30. Райкова Н. О. Об интеграции систем менеджменты информационной безопасности и качества / Н. О. Райкова // Вопросы кибербезопасности. – 2013. – № 3. – С. 47–53.

31. Савочкин А. Е. Алгоритмизация работы систем мониторинга и контроля для решения задач идентификации степени повреждения технически сложных объектов / А. Е. Савочкин // Прикаспийский журнал: управление и высокие технологии. – 2014. – № 2. – С. 23–35.

32. Смирнов В. И. Сейсмоизоляция – современная антисейсмическая защита зданий в России / В. И. Смирнов // Сейсмостойкое строительство. Безопасность сооружений. – 2013. – № 4. – С. 41–54.

33. Собакин И. Б. Системный подход к управлению рисками информационной безопасности / И. Б. Собакин // Актуальные проблемы современной науки. – 2013. – № 3 (71). – С. 39–40.

34. Соболев В. В. Моделирование и оптимизация условий применения видеорегистрационного контроля качества при строительстве зданий / В. В. Соболев, О. А. Бабкин // Интернет-журнал Науковедение. – 2014. – № 6 (25). – С. 19.

35. Стариковский А. В. Повышение защищенности систем автоматизации управления зданиями от компьютерных атак / А. В. Стариковский, И. Ю. Жуков, Д. М. Михайлов, А. А. Шептунов, А. В. Савчук, А. С. Крымов // Спецтехника и связь. – 2012. – № 4. – С. 2–5.

36. Чеснокова О. Е. Энергоэффективные технологии, используемые при проектировании общественных зданий / О. Е. Чеснокова, В. М. Андреев // Актуальные проблемы современной науки, техники и образования. – 2013. – Т. 2, № 71. – С. 223–225.

37. Шешеня Н. Критерии инженерно-геологического обоснования мероприятий по защите зданий и сооружений от опасных оползневых процессов / Н. Шешеня // Инженерная защита. – 2015. – № 3 (8). – С. 44–55.

References

1. Azhmukhamedov I. M., Knyazeva O. M. Otsenka sostoyaniya zashchishchennosti dannykh organizatsii v usloviyakh vozmozhnosti realizatsii ugroz informatsionnoy bezopasnosti [Evaluation of data security state for organization in the conditions of realization possibility of threats for information security]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2015, no. 3, pp. 24–39.

2. Akbashev B. B., Balyuk N. V., Kechiev L. N. Obespechenie informatsionnoy i funktsionalnoy bezopasnosti v spetsialnykh tekhnicheskikh zdaniyakh pri elektromagnitnykh vozdeystviyakh [Ensuring information and functional security in special technical buildings at electromagnetic influences]. *Tekhnologii elektromagnitnoy sovmestimosti* [Technologies of Electromagnetic Compatibility], 2011, no. 2, pp. 3–12.

3. Atamanov G. A. Tekhnicheskie kanaly utechki informatsii: opredelenie, sushchnost, klassifikatsiya [Technical channels of information leakage: definition, essence, classification]. *Zashchita informatsii. Insayd* [Information Security. Insider], 2010, no. 1 (31), pp. 28–33.

4. Balkin V. M. Bezopasnost zdaniya i faktory vliyaniya na etapakh zhiznennogo tsikla [Security of building and factors influencing at it during stages of life cycle]. *Vestnik Samarskogo gosudarstvennogo arkhitekturno-stroitelnogo universiteta. Gradostroitelstvo i arkhitektura* [Bulletin of the Samara State University of Architecture and Civil Engineering. Town planning and architecture], 2012, no. 1 (5), pp. 74–76.

5. Balkin V. M. Stroitelnyy kontrol i bezopasnost zdaniy [Construction control and safety of buildings]. *Vestnik Samarskogo gosudarstvennogo arkhitekturno-stroitelnogo universiteta. Gradostroitelstvo i arkhitektura* [Bulletin of the Samara State University of Architecture and Civil Engineering. Town planning and architecture], 2013, no. 3 (11), pp. 40–41.

6. Balkin V. M. Elementy vozdeystviya transporta na zdaniya i sooruzheniya. Ikh zashchita ot transportnogo shuma i vibratsiy [Elements of transport impact at buildings and constructions. Their protection against transport noise and vibrations]. *Vestnik Samarskogo gosudarstvennogo arkhitekturno-stroitelnogo universiteta. Gradostroitelstvo i arkhitektura* [Bulletin of the Samara State University of Architecture and Civil Engineering. Town planning and architecture], 2013, no. 3 (11), pp. 44–45.

7. Barannikov N. I., Sergeeva M. A. Podsistema opredeleniya kategoriy pomeshcheniy, zdaniy i sooruzheniy po vzryvopozharnoy i pozharnoy opasnosti v SAPR pozharnoy bezopasnosti [Subsystem for definition of categories for rooms, buildings and constructions on fire and explosion danger in SAPR of fire safety]. *Vestnik kompyuternykh i informatsionnykh tekhnologiy* [Bulletin of the Computer and Information Technologies], 2013, no. 2 (104), pp. 17–21.

8. Baranov A. P. Sovremennoe sostoyanie filosofii upravleniya informatsionnoy bezopasnostyu [Current state of philosophy of information security management]. *Biznes-informatika* [Business Informatics], 2014, no. 2 (28), pp. 7–14.

9. Batyrev V. V., Volkov O. S., Kachanov S. A., Batyrev V. V., Volkov O. S, Kachanov S. A. *Tekhnologii sozdaniya strukturirovannykh sistem monitoringa i upravleniya inzhenernymi sistemami zdaniy i sooruzheniy* [Creation technologies of structured systems for monitoring and management of engineering systems for buildings and constructions] ,Moscow, All-Russian Research Institute for Civil Defense and Emergencies of Russia (Federal Centre for Science and High Technologies) Publ. House, 2011. 270 p.

10. Brumshteyn Yu. M., Gladkikh V. V., Sizov A. M. Avtorskiy nadzor v stroitelstve kak element sistemy zashchity prav avtorov proektov [Architectural supervision in construction as an element of system of protection of the rights of authors of projects]. *Intellektualnaya sobstvennost. Avtorskoe pravo* [Intellectual Property. Copyright], 2005, no. 3, pp. 12–18.

11. Brumshteyn Yu. M. O vozmozhnykh podkhodakh k otsenke variantov uluchsheniya informatsionnoy bezopasnosti organizatsiy [About possible approaches to an assessment of improvement options of organizations information security]. *Informatsionnye tekhnologii modelirovaniya i upravleniya* [Information Technologies of Modeling and Management], 2007, no. 4 (38), pp. 490–494.

12. Brumshteyn Yu. M. Osveshchenie arkhitekturnykh obektov: sintez tvorchestva i sovremennykh tekhnologiy [Illumination of architectural objects: synthesis of creativity and modern technologies]. *Intellektualnaya sobstvennost. Avtorskoe pravo i smezhnye prava* [Intellectual Property. Copyright and Adjacent Rights], 2015, no. 2, pp. 14–24.

13. Brumshteyn Yu. M., Zakharov D. A., Akishkin V. G. Riski informatsionnoy bezopasnosti meduchrezhdeniy, ikh spetsialistov i patsientov [Risks of information security for medical institutions, their specialists and patients]. *Informatsionnaya bezopasnost regionov* [Information Security of Regions], 2013, no. 1, pp. 13–21.

14. Brumshteyn Yu. M., Dyudikov I. A. Sravnitelnyy analiz funktsionalnosti programmnykh sredstv upravleniya proektami, rasprostranyaemykh po modeli SaaS. [The comparative analysis of software functionality for projects management extended by the SaaS model]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2014, no. 4, pp. 34–51.

15. Dyudikov I. A., Kuzmina A. B., Ivanova M. V., Brumshteyn Yu. M., Vaskovskiy Ye. Yu. Sistemnyy analiz struktury stroitelnogo klastera regiona v usloviyakh razvitiya informatsionno-kommunikatsionnykh tekhnologiy [System analysis of regions construction cluster structure in the conditions of information and

communication technologies development]. *Inzhenerno-stroitelnyy vestnik Prikaspiya* [The Caspian Engineering and Construction Bulletin], 2014, no. 3 (9), pp. 43–51.

16. Isakov G. N., Manaeva A. R. Sistemnyy analiz voprosov bezopasnosti primeneniya napolnykh pokrytiy i matematicheskaya model protsessov ikh termorazrusheniya [System analysis of safety issues of application of floor coverings and mathematical model of processes of their thermodestruction]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2015, no. 1, pp. 30–43.

17. Kazarin O. V., Repin M. M. Osobennosti analiza riskov utechki konfidentsialnoy informatsii po tekhnicheskim kanalam pri sozdanii radioelektronnykh sredstv [Features of risk analysis of leakage of confidential information on technical channels at creation of radio-electronic means]. *Voprosy kiberbezopasnosti* [Questions of Cybersafety], 2015, no. 4 (12), pp. 62–69.

18. Kandyrin Yu. V., Sazonova L. T., Shkurina G. L., Chivilev A. D. Mnogokriterialnoe strukturirovanie alternativ v avtomatizirovannykh sistemakh vybora. [Multicriteria structuring alternatives in the automated choice systems]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2014, no. 1, pp. 23–33.

19. Kirakovskiy V. V., Pylkin A. N., Faddeev A. O. Analiz vozmozhnostey primeneniya neyronechetkikh tekhnologiy pri razrabotke proektov zastroyki territoriy v usloviyakh nepolnoty iskhodnykh dannykh [The opportunities analysis of neuro and indistinct technologies application when developing projects of territories building in conditions of basic data incompleteness]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2015, no. 1, pp. 74–86.

20. Kolganov A. A. Inzhenernaya metodika proektirovaniya avtomobilnykh radiookhrannykh sistem [Engineering technique of automobile radio security systems design] *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2015, no. 3, pp. 122–138.

21. Lapina O. A. Stroitelstvo v usloviyakh zharkogo klimata [Construction in the conditions of hot climate]. *Nauchnoe obozrenie* [The Scientific Review], 2014, no. 7-3, pp. 876–879.

22. Lyubimova N. S., Volkov A. B., Martemyanov V. A. Elektromagnitnaya bezopasnost zdaniy [Electromagnetic safety of buildings]. *Tekhnicheskie nauki – ot teorii k praktike* [Technical Science – from Theory to Practice], 2013, no. 28, pp. 158–169.

23. Malvina A. S., Brumshteyn Yu. M., Sklyarenko Ye. V., Kuzmina A. B. Avtomatizatsiya, dispetcherizatsiya i informatizatsiya vysokotekhnologichnykh meduchrezhdeniy kak sredstvo povysheniya effektivnosti ikh raboty [Automation, scheduling and informatization of hi-tech medical institutions as means of their work efficiency increasing]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2014, no. 1, pp. 122–138.

24. Malyy I. N. Avtomatizirovannaya stantsiya monitoringa sostoyaniya vysotnykh zdaniy [The automated station for monitoring condition of high-rise buildings]. *Resursoenergoeffektivnye tekhnologii v stroitelnom komplekse regiona* [Resource and Energy Effective Technologies in Regions Construction Complex], 2012, no. 2, pp. 165–167.

25. Morozov B. N., Sokolov Ye. G. Zashchita informatsii ot elektromagnitnykh impulsov v intellektualnykh zdaniyakh [Information security from electromagnetic impulses in intellectual buildings]. *T-Comm: Telekommunikatsii i transport* [T-Comm: Telecommunications and transport], 2012, vol. 6, no. 8, pp. 55–56.

26. Nguen Suan Man, Popov G. A., Kuchin I. Yu. Podsistema formirovaniya vkhodnykh dannykh v sisteme intellektualnogo upravleniya zdaniem [Subsystem of entrance data formation in intellectual management system of building]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2015, no. 3, pp. 142–158.

27. Polyantseva Ye. R., Yankovskaya Yu. S. Kriminogennaya bezopasnost obshchestvennykh zdaniy [Criminogenic safety of public buildings]. *Novye idei novogo veka: materialy mezhdunarodnoy nauchnoy konferentsii FAD TOGU* [New Ideas of the New Century. Proceedings of the TOGA FAD International Scientific Conference], 2014, vol. 3, pp. 363–367.

28. Pomortsev A. S., Novikov S. N. Razrabotka sistemy parametrov otsenki riskov narusheniya informatsionnoy bekhzopasnosti organizatsiy [System of parameters Development of the for assessment of risks of violation of information security of the organizations]. *Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniya i radioelektroniki* [Proceedings of the Tomsk State University of Control Systems and Radio Electronics], 2014, no. 2 (32), pp. 170–174.

29. Popov S. I., Rogozin Ye. A., Roslov S. Yu. Analiz sovremennykh metodov i algoritmov optimizatsii na etape formirovaniya struktury i sostava kompleksa tekhnicheskikh sredstv zashchity informatsiina obekte informatazatsii [The analysis of modern optimization methods and algorithms at a stage of structure and nomenclature formation of technical means complex for information protection at object of informatization]. *Vestnik Voronezhskogo gosudarstvennogo tekhnicheskogo universiteta* [Bulletin of the Voronezh State Technical University], 2009, vol. 5, no. 6, pp. 83–85.

30. Raykova N. O. Ob integratsii sistem menedzhmenty informatsionnoy bezopasnosti i kachestva [About integration of system management of information security and quality]. *Voprosy kiberbezopasnosti* [Cybersafety Questions], 2013, no. 3, pp. 47–53.

31. Savochkin A. Ye. Algoritmizatsiya raboty sistem monitoringa i kontrolya dlya resheniya zadach identifikatsii stepeni povrezhdeniya tekhnicheski slozhnykh obektov [Algoritmization of monitoring and control systems work for identification problems solution of technically complex objects rate damage]. *Prikaspiyskiy zhurnal: upravlenie i vysokie tekhnologii* [Caspian Journal: Management and High Technologies], 2014, no. 2, pp. 23–35.

32. Smirnov V. I. Seysmoizolyatsiya – sovremennaya antiseysmicheskaya zashchita zdaniy v Rossii [Seismoisolation – modern aseismic protection of buildings in Russia]. *Seysmostoykoe stroitelstvo. Bezopasnost sooruzheniy* [The Seismoresistant Construction. Safety of Constructions], 2013, no. 4, pp. 41–54.

33. Sobakin I. B. Sistemnyy podkhod k upravleniyu riskami informatsionnoy bezopasnosti [System approach to risk management of information security]. *Aktualnye problemy sovremennoy nauki* [Actual Problems of Modern Science], 2013, no. 3 (71), pp. 39–40.

34. Sobolev V. V., Babkin O. A. Modelirovanie i optimizatsiya usloviy primeneniya videoregistratsionnogo kontrolya kachestva pri stroitelstve zdaniy [Modeling and optimization of application conditions of video registration quality control during buildings construction]. *Internet-zhurnal Naukovedenie* [Research of Science. Internet Journal], 2014, no. 6 (25), pp. 19.

35. Starikovskiy A. V., Zhukov I. Yu., Mikhaylov D. M., Sheptunov A. A., Savchuk A. V., Krymov A. S. Povyshenie zashchishchennosti sistem avtomatizatsii upravleniya zdaniyami ot kompyuternykh atak [Increasing security from computer attacks for buildings management automation systems]. *Spetstekhnika i svyaz* [Special Equipment and Communication], 2012, no. 4, pp. 2–5.

36. Chesnokova O. Ye., Andreev V. M. Energoeffektivnye tekhnologii, ispolzuemye pri proektirovanii obshchestvennykh zdaniy [The power effective technologies used for public buildings design]. *Aktualnye problemy sovremennoy nauki, tekhniki i obrazovaniya* [Actual Problems of Modern Science, Equipment and Education], 2013, vol. 2, no. 71, pp. 223–225.

37. Sheshenya N. Kriterii inzhenerno-geologicheskogo obosnovaniya meropriyatiy po zashchite zdaniy i sooruzheniy ot opasnykh opolznevykh protsessov [Criteria of engineering and geological justification of actions for buildings and constructions protection from dangerous landslide processes]. *Inzhenernaya zashchita* [Engineering Protection], 2015, no.3 (8), pp. 44–55.

УДК 004:912

МЕТОД ФОРМАЛИЗАЦИИ НЕЧЁТКИХ КОЛЛОКАЦИЙ ТЕРМОВ В ТЕКСТАХ НА ОСНОВЕ ЛИНГВИСТИЧЕСКИХ ПЕРЕМЕННЫХ[1]

Статья поступила в редакцию 22.10.2015 г., в окончательном варианте 5.11.2015 г.

Поляков Дмитрий Вадимович, кандидат технических наук, старший преподаватель, Тамбовский государственный технический университет, 392000, Российская Федерация, г. Тамбов, ул. Советская, 106, e-mail: dimadress@yandex.ru

Митрофанов Николай Михайлович, магистрант, лаборант кафедры, Тамбовский государственный технический университет, 392000, Российская Федерация, г. Тамбов, ул. Советская, 106, e-mail: n.mitrofanow@gmail.com

[1] Работа выполнена при финансовой поддержке РФФИ (проект 15-41-03143).