процесу прийняття рішення, виражені коефіцієнтами кореляції, можуть бути використані в рамках розробки інтелектуальних систем оцінки професійної діяльності як базові фактори відповідних робочих правил бази знань [10].

Отримані результати досліджень не вступають в протиріччя з існуючими знаннями теорії прийняття рішення, яка базується на процесному підході, та описує взаємні зв'язки якісними характеристиками, а навпаки підтверджують введені гіпотези щодо впливу елементів моделі та доповнюють їх кількісними оцінками, даючи науковцям потужний апарат для розширення теорії шляхом нових досліджень.

Література

1. Мильнер, Б. З. Теория организации [Текст]: учебник / Б. З. Мильнер. — 5-е изд., перераб. и доп. — М.: ИНФРА-М, 2005. — 720 с.
2. Драчева, Е. Л. Менеджмент [Текст] / Е. Л. Драчева, Л. И. Юликов. — М.: Мастерство, 2002. — 564 с.
3. Ямпольская, Д. Менеджмент [Текст] / Д. Ямпольская, М. Зонис. — М.: Центр креативных технологий, 2007. — 675 с.
4. Лаукс, Г. Основы организации: управление принятием решений [Текст]: пер. с нем. / Гельмут Лаукс, Феликс Лирманн. — 4-е изд. — М.: Дело и Сервис, 2006. — 600 с.
5. Заріцький, О. В. Теоретичні основи побудови функціональних моделей професійної діяльності людини [Текст]: теорет. і наук.-практ. часоп. / О. В. Заріцький // Вісник Інженерної академії України. — 2015. — № 2. — С. 233–236.
6. Заріцький, О. В. Функціональне моделювання базових елементів професійної діяльності в межах моделі «Сутність — зв'язок» [Текст]: зб. наук. пр. / О. В. Заріцький // Проблеми інформатизації та управління. — 2015. — № 2(50). — С. 70–75.
7. Заріцький, О. В. Інформаційне моделювання процесу прийняття рішення [Текст]: зб. наук. пр. / О. В. Заріцький // Інженерія програмного забезпечення. — 2015. — № 1(21). — С. 56–61.
8. Заріцький, О. В. Класифікація сучасних інформаційних систем моделювання та управління людськими ресурсами [Текст]: зб. наук. пр. / О. В. Заріцький, В. В. Судік // Вісник Чернігівського державного технологічного університету. Серія «Технічні науки». — 2015. — № 1(77). — С. 98–108.
9. Заріцький, О. В. Аналітичний огляд методологій та інформаційних систем моделювання та оцінки професійної діяльності людини [Текст]: зб. наук. пр. / О. В. Заріцький // Проблеми інформатизації та управління. — 2015. — № 1(49). — С. 32–36.
10. Заріцький, О. В. Теоретичні основи побудови експертних систем аналізу та оцінки професійної діяльності [Текст]: зб. наук. пр. / О. В. Заріцький // Електроніка та системи управління. — 2015. — № 2(44). — С. 103–106.

ОЦЕНКА ВЗАИМНОГО ВЛИЯНИЯ ЭЛЕМЕНТОВ ИНФОРМАЦИОННОЙ МОДЕЛИ ПРИНЯТИЯ РЕШЕНИЯ

Представлены результаты структурного анализа информационной модели процесса принятия решения. Выявлены связи между элементами (сущностями, атрибутами) модели и сделана оценка их силы путем расчета коэффициентов конкордации и корреляции. Отдельно рассмотрен элемент процесса принятия решения «Модель решения», как наиболее сложный с точки зрения системного анализа его атрибутов.

Ключевые слова: модель принятия решения, структурный анализ, информационная технология, оценка профессиональной деятельности.

Заріцький Олег Володимирович, *кандидат технічних наук, докторант, кафедра засобів захисту інформації, Національний авіаційний університет, Київ, Україна,*
e-mail: oleg.zaritskyi@gmail.com.

Зарицкий Олег Владимирович, *кандидат технических наук, докторант, кафедра средств защиты информации, Национальный авиационный университет, Киев, Украина.*

Zaritskyi Oleg, *National Aviation University, Kyiv, Ukraine,*
e-mail: oleg.zaritskyi@gmail.com

УДК 004.056.5:005(303.732.4:006.88)
DOI: 10.15587/2312-8372.2015.51111

Янченко В. Н.,
Ивченко А. В.,
Залога В. А.,
Дынник О. Д.

СИСТЕМАТИЗАЦИЯ ФАКТОРОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ОРГАНИЗАЦИИ

Предложена универсальная многоуровневая система факторов информационной безопасности организаций (предприятий). Позволяет: группировать факторы по однородным признакам; разграничивать угрозы организации в сфере информационной безопасности по внешнему и внутреннему контексту; определять природу угроз. Система может быть использована как инструментарий в процессе оценки и/или снижения информационных рисков организаций различных типов, видов и форм управления.

Ключевые слова: *информационная безопасность, система факторов, внешний и внутренний контекст, риск.*

1. Введение

Деятельность любой организации связана с получением и передачей информации. Информация в настоящее время является стратегически важным товаром, несанкционированное раскрытие конфиденциальности, которой, как правило, наносит предприятию значительный ущерб и даже может привести к банкротству [1], что требует от организации (предприятия) серьезно заниматься своей информационной безопасностью (ИБ). Под ИБ понимают состояние защищенности используемых информации и информационной среды от случайных

или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений [1].

Анализ тенденций по обеспечению и управлению качеством производства продукции или предоставлению услуг, показывает широкое использование новых терминов и требований к управлению ИБ. Например, в проекте новой версии стандарта ISO 9001:2015 предложено введение нового термина «Знания организации» и требования, которые являются результатом эволюции требования в отношении управления компетентностью персонала в версии этого стандарта 2008 года (ISO 9001:2008). Данный термин подразумевает определение, накопление и поддержание в рабочем, т. е. доступном для организации состоянии знаний, полученных для обеспечения соответствия требованиям поставляемых продуктов и оказываемых услуг. Распределение доли знаний, хранимых компетентным персоналом организации, и доли знаний, хранимых на других носителях, осуществляется самой организацией [2]. Другими словами, современное промышленное производство практически невозможно представить без применения современных информационных технологий (ИТ), что делает многие виды деятельности организации (предприятия) в значительной мере «прозрачными» и относительно доступными в информационном смысле этого понятия. Поэтому в настоящее время, с одной стороны, преимущества от эффективного использования данных технологий в деятельности организации и формировании ее имиджа переоценить сложно, но, с другой — их использование имеет и ряд недостатков, наиболее существенный из которых относится к ее ИБ. Это приводит к осознанию организациями потребности не только в обеспечении своего имиджа, но и обеспечения защиты от несанкционированного разглашения информации как собственной, так и потребителей их продукции (услуг) [3].

Таким образом, в настоящее время становится актуальным и своевременным решение научно-практической задачи, направленной на развитие методологических основ разработки и внедрения систем менеджмента информационной безопасности (СМИБ) на основе создания принципов их нормативного обеспечения путем внедрения механизмов реализации данных принципов в реальных производственных условиях деятельности организаций (предприятий) различных отраслей экономики.

2. Анализ литературных данных и постановка проблемы

Проведенный анализ научных работ показал, что в связи со значительным расширением в настоящее время практического использования ИТ, вопросам развития методологических основ создания систем управления ИБ организации уделяется все большее и большее внимание. Например, В. А. Галатенко [4] разработал для обеспечения ИБ организации (предприятия) 2-х уровневую систему факторов (угроз), обуславливающих требуемую степень ее ИБ, которая основывается на трех компонентах: административном, процедурном, программно-техническом. В. В. Андрианов [5] угрозы информационной безопасности предприятий условно разделил на две группы:

1) традиционные угрозы безопасности информации, к которым можно отнести нарушение конфиденциальности или неправомерное использование информации, реализуемые через новые механизмы, возникшие при использовании уже имеющихся в организации информационных систем;

2) новые угрозы, порождаемые специфическими особенностями современных информационных систем — вирусы, сетевые атаки, нарушения функционирования и отказы разного рода, — влияние которых на ИБ существенно усиливается при разного рода нарушениях персоналом установленных регламентов, инструкций и предписаний по эксплуатации и обслуживанию информационных систем.

В работах И. М. Ажмухамедова [6, 7] предложена 4-х уровневая система факторов ИБ: 1) непреднамеренные субъективные угрозы; 2) преднамеренные субъективные угрозы; 3) техногенные угрозы; 4) стихийные угрозы.

В работе [8] выделяются следующие основные факторы, влияющие на информационную безопасность предприятия: 1) расширение сотрудничества предприятия с партнерами; 2) автоматизация бизнес-процессов на предприятии; 3) расширение кооперации исполнителей при построении и развитии информационной инфраструктуры предприятия; 4) рост объемов информации предприятия, передаваемой по открытым каналам связи; 5) рост компьютерных преступлений.

Коллектив авторов работы [9] на уровне государства предлагают выделять следующие факторы ИБ: 1) угрозы конституционным правам и свободам информационной деятельности человека и гражданина, а также духовному возрождению и индивидуальному, групповому и общественному сознанию; 2) угрозы информационному обеспечению государственной политики; 3) угрозы развитию национальной информационной индустрии, включая индустрию средств информатизации, телекоммуникации и связи; 4) угрозы обеспечению потребностей внутреннего рынка и выходу этой продукции на мировой рынок; 5) угрозы обеспечению накопления, сохранности и эффективного использования национальных информационных ресурсов; 6) угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых в государстве.

В нормативном документе [10] введено понятие «фактор, воздействующий на защищаемую информацию» — явление, действие или процесс, результатом которых могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней. В данном документе предложено выделить два класса факторов, воздействующих на защищаемую информацию и подлежащих учету при организации защиты информации, по признаку отношения к природе возникновения: объективные и субъективные; и два класса факторов воздействующих на защищаемую информацию, по отношению к объекту информатизации: внутренние и внешние.

Таким образом, анализ работ, в которых представлены результаты исследований в области систематизации и выделения факторов ИБ для различных организаций, показал достаточно широкое применение при построении данных систем различных классификационных признаков. В основу этих признаков положен, как правило, только анализ и минимизация угроз, связанных с потерей информации или раскрытия ее конфиденциальности. В то же время, решение проблемы ИБ

организаций связано не только с минимизацией угроз в данной области, но и с реализацией различных требований (законодательные акты, нормативные документы, контракты и т. п.), которые могут создать дополнительные преимущества по повышению конкурентоспособности организаций. Поэтому разработка универсальной структуры системы классификации факторов (угроз) позволит организациям более эффективно осуществлять работы не только в области обеспечения надлежащего уровня их ИБ, но и управления ими.

3. Объект, цель и задачи исследования

Объект исследования — состояние информационной безопасности организации.

Целью данной работы является систематизация факторов, оказывающих влияние на состояние ИБ в организации на основе теории квалиметрии и причинно-следственного анализа путем обобщения современного опыта в области ИБ и требований нормативных документов национального и международного уровней к обеспечению защиты информации.

Для реализации поставленной цели необходимо было решить основные задачи:

1. Провести тщательный анализ законодательной и нормативной базы различных государств, а так же научных работ в сфере обеспечения информационной безопасности, для того, что бы определить основные тенденции развития и управления данных процессом.
2. Выбрать инструменты для реализации поставленной цели.

4. Разработка системы факторов, оказывающих влияние на информационную безопасность организации (предприятия)

Для разработки универсальной системы классификации факторов ИБ организаций будем использовать:

1) метод оценки рисков «Причинно-следственный анализ», исходя из положения о том, что «...воздействие может иметь несколько влияющих факторов, которые могут быть сгруппированы в различные категории. Влияющие факторы часто идентифицируют во время проведения мозгового штурма и отображают в форме древовидной структуры или рыбьего скелета...» [11];

2) основы теории квалиметрии, исходя из положения о том, что «...свойства, формирующие качество объекта, представляют из себя не просто совокупность, а совокупность, по определенным правилам упорядоченную в некоторую иерархическую структуру, — дерево свойств...» [12].

Система классификации факторов ИБ организаций наиболее рационально представить в виде дерева свойств, в котором для каждого сложного свойства (фактора первого уровня), соответствует группа менее сложных свойств в совокупности составляющих факторы второго уровня и т. д. В общем виде структура первого уровня (факторы первого уровня) представлена на рис. 1.

К факторам первого уровня относятся факторы, непосредственная разработка которых и принятие их во внимание или пренебрежение ими, напрямую влияет на уровень обеспечения ИБ в организации. Их в соответствии с параметрами факторов, которые необходимо брать во внимание (учитывать) условно можно разбить на две группы: внешний и внутренний контексты.

Примечание. Контекст — среда, в которой существует объект. Установление контекста — определение внешних и внутренних параметров, в которых следует принять во внимание время управления рисками, а также установление области и критериев риска для политики менеджмента [13].

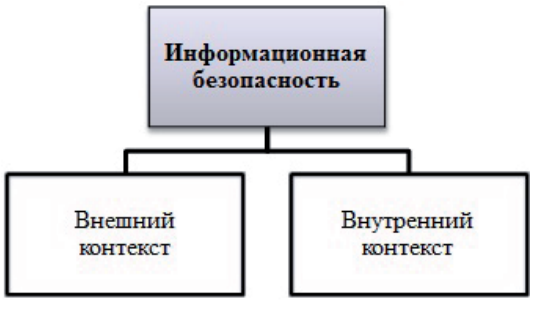

Рис. 1. Факторы первого уровня

Внешний контекст — внешняя среда, в которой организация стремится достигнуть своих целей. Внешний контекст может включать:

— среды — культурную, социальную, политическую правовую, регулятивную, финансовую, технологическую, экономическую, природную и конкурентную, либо среды — международную, национальную, региональную или локальную;

— ключевые движущие силы и тренды, влияющие на цели организации;

— отношения с внешними заинтересованными сторонами, их восприятие и оценка.

Внутренний контекст — внутренняя среда, в которой организация стремится достигнуть своих целей. Внутренний контекст может включать факторы:

— управление, организационную структуру, роли и ответственность;

— политики, цели, стратегии, которые используются для достижения целей;

— возможности, понимание в рамках ресурсов организации и накопленных знаний;

— восприятие и оценку внутренних заинтересованных сторон;

— информационные системы, информационные потоки, а также процессы принятия решений;

— отношения с внутренними заинтересованными сторонами, их восприятие и оценка;

— культуру организации;

— стандарты, руководства и модели, официально принятые организацией;

— формы и объемы договорных отношений.

В свою очередь, каждый из выделенных факторов первого уровня (внешний или внутренний контекст) делится на систему компонентов, которые можно определить как факторы второго уровня (рис. 2), принятие во внимание которых так же необходимо и является неотъемлемой частью обеспечения высокого уровня ИБ.

Рис. 2. Факторы второго уровня ИБ

Законодательные требования являются важными факторами для обеспечения ИБ. Большинство людей не совершают противоправных действий не потому, что это технически невозможно, а, главным образом, потому что это осуждается обществом и/или наказывается с помощью правоохранительных органов, потому, что так поступать не принято/запрещено.

Одним из самых важных и, вероятно, самых трудных моментов является создание на законодательном уровне механизма, позволяющего согласовать процесс разработки законов с действующими в настоящее время реалиями и неизбежным прогрессом в области используемых обществом информационных технологий. Законы, связанные с обеспечением ИБ, не могут опережать жизнь, но очень важно, чтобы отставание не было слишком большим, так как на практике, помимо прочих отрицательных моментов, это ведет к снижению ИБ, что в большинстве случаев ведет к потере конкурентоспособности не только для конкретной организации, но и отрасли в целом. На рис. 3 представлены факторы третьего уровня, которые в комплексе формируют законодательную базу, определяющую политику государства в сфере обеспечения ИБ.

Рис. 3. Факторы ИБ третьего уровня — законодательные требования

Требования рынка. В современном обществе для того, что бы успешно осуществлять разные виды деятельности, необходимо, по меньшей мере, быть конкурентоспособным предприятием (организацией). Рыночные отношения диктуют ряд своеобразных (специфических) условий. Одним из основных таких условий является наличие на предприятии сертификата(ов), подтверждающего(их) достаточно высокий уровень организованности и качества предоставляемых организацией товаров/услуг. Поэтому очевидна потребность в применении единого набора факторов (рис. 4) как для поставщиков средств защиты, так и для компаний, являющихся системными интеграторами, и для организаций, выступающих в качестве заказчиков систем безопасности для своих корпоративных сетей и систем. Этот набор факторов может регламентироваться с помощью соответствующих стандартов, образующих понятийный базис, на котором строятся все работы по обеспечению ИБ, и определяющих критерии, которым должно следовать управление безопасностью. Эти стандарты являются необходимой основой, обеспечивающей совместимость продуктов разных производителей, что чрезвычайно важно при создании систем сетевой безопасности в гетерогенных средах.

Рис. 4. Классификация факторов ИБ третьего уровня — рыночные требования

В сфере подтверждения высокого уровня обеспечения ИБ одним из лучших являются требования международного стандарта ISO 27001 [14]. Он определяет процессы, представляющие возможность организации устанавливать, применять, пересматривать, контролировать и поддерживать эффективную систему менеджмента ИБ. Кроме того, он устанавливает требования к разработке, внедрению, функционированию, мониторингу, анализу, поддержке и совершенствованию документированной системы менеджмента ИБ в контексте существующих бизнес рисков организации.

Административно-организационные меры. К административно-организационным мерам можно отнести как действия общего характера, предпринимаемые руководством организации, так и конкретные меры безопасности при информационной работе с персоналом. Факторы, влияющие на качественное обеспечение информационной безопасности на этом уровне представлены на рис. 5.

Одним из главных и проблемных факторов при утере информации является персонал. Согласно проведенным исследованиям, представленным в [1], более 80 % инцидентов на предприятиях в области ИБ, в которых виноваты сотрудники, происходят в результате их неумышленных действий. Привлечение сотрудников к участию в решении вопросов ИБ и их профессиональная в этих вопросах подготовка (обучение) позволит существенно повысить защищенность активов компании. Компетентность сотрудников в вопросах ИБ, а также их умение применять эти навыки и знания в основной

сфере деятельности значительно повышают доверие со стороны клиентов и партнеров компании, способствует более стабильным взаимоотношениям, что способствует заметному снижению рисков.

Рис. 5. Система факторов ИБ третьего уровня — административно-организационные меры

Комплексное обучение руководителей и специалистов правовым, организационным и практическим вопросам обеспечения ИБ, а также мотивация сотрудников к добросовестному выполнению своих обязанностей, путем проведения всевозможных мероприятий с целью поощрения и формирования у них осознания собственной значимости и чувства востребованности, может обеспечить создание крепкого фундамента для формирования надежного «тыла» в организации. Обученные основным правилам в области ИБ сотрудники предприятия и особенно те, которые используют полученные знания на практике, существенно снижают риск нарушения ИБ и, как следствие, уменьшают возможный ущерб предприятия.

При этом обучение сотрудников в области ИБ при грамотном подходе не требует значительных материальных и временных затрат. В настоящее время существует большое количество различных методов повышения осведомленности сотрудников в области ИБ. Наибольшая же эффективность, достигается при комплексном использовании различных элементов.

Программно-технические средства защиты. К программно-техническим средствам обеспечения защиты относятся: программное и аппаратное обеспечение, а также технические средства (рис. 6).

К программному обеспечению относятся качественно написанные и грамотно подобранные (часто специально разработанные) программы и инструкции по их использованию.

Значительное место в реализации политики безопасности любой организации занимают аппаратные средства, которые могут быть установлены, например, на объекте для защиты помещений при ведении переговоров и важных деловых совещаний, а также для защиты техники обработки информации и соответствующих коммуникаций.

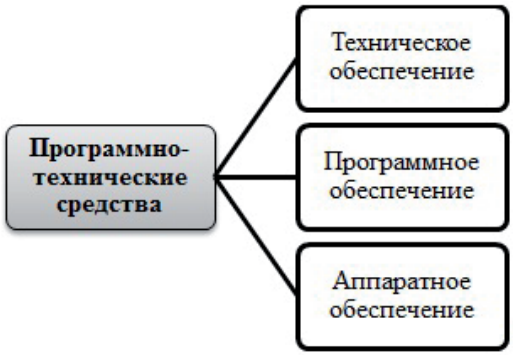

Рис. 6. Факторы третьего уровня ИБ — программно-технические средства обеспечения ИБ

К вопросу выбора аппаратуры, которую необходимо устанавливать в организации, следует подходить очень внимательно. При выборе аппаратуры зашумления, генератора радиопомех, устройств активной защиты телефонных линий и других аппаратных средств защиты необходимо учитывать достаточно большой объем определяющих факторов: их сильные и слабые стороны, их взаимовлияние, доступность и т. п.

К техническим средствам относятся разного рода регистрирующие (например, записывающие), передающие и другие устройства.

Предложенная система факторов, оказывающих влияние на степень обеспечения ИБ, является универсальной и может быть применима к организации (предприятию) любого типа, причем факторы третьего уровня, исходя из специфики и требований конкретной организации, можно систематизировать более детально, т. е. выделять факторы четвертого, пятого и других уровней. Например, с учетом того, что активные технические средства защиты занимают достаточно большую часть в общем объеме специальных средств и представлены достаточно широким спектром изделий, можно выделить факторы четвертого, пятого и других уровней, различающиеся как по областям их применения, так и по техническим характеристикам, функциональным принципам применения и т. п.

5. Выводы

1. На основе проведенных исследований современного состояния вопроса обеспечения конкурентоспособности организаций установлено, что в настоящее время становится актуальным и своевременным решение научно-практической проблемы, направленной на развитие методологических основ разработки и внедрения систем менеджмента информационной безопасности организаций, целью которых является минимизация влияния различных факторов на ИБ организации (предприятия).

2. Анализ работ в области систематизации и выделения факторов, обуславливающих требуемую степень (требуемый уровень) ИБ показал, что применяемые в настоящее время классификационные признаки при определении факторов базируются, в основном, на анализе угроз, связанных с потерей информации или раскрытия ее конфиденциальности, как правило, не обладают универсальным характером и являются сугубо специализированными системами, т. е. их можно практически применять только в той организации, для которой они разработаны.

3. Установлено, что полнота и достоверность выявления факторов, воздействующих на ИБ организации, должны быть достигнуты путем рассмотрения полного множества факторов, воздействующих на все элементы ИБ (технические и программные средства обработки информации, средства обеспечения объекта информатизации и т. д.) и на всех этапах обработки информации.

4. Выявление факторов, воздействующих на ИБ, должно быть осуществлено с учетом следующих требований:

— достаточности уровней классификации факторов, воздействующих на защищаемую информацию, позволяющей формировать их необходимое (наиболее полное) множество;

— гибкости классификации, позволяющей расширять множества классифицируемых факторов, группировок и признаков, а также вносить необходимые изменения без нарушения структуры принятой классификации.

5. На основе теории квалиметрии и причинно-следственного анализа путем обобщения современного опыта в области ИБ впервые предложена универсальная многоуровневая система факторов информационной безопасности организаций (предприятий), которая позволяет:

— группировать (систематизировать) факторы, обуславливающие ИБ организации (предприятия), по однородным признакам, что путем их формализации позволит эффективно применять современные информационные системы с целью выявления наиболее сильных угроз, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях;

— разграничивать угрозы организации (предприятия) в сфере ИБ по внутреннему и внешнему контекстам, а также в полной мере учитывать требования законодательных актов, нормативных документов и отдельных контрактов (договоров);

— определять природу какой бы ни было угрозы, предлагать (разрабатывать) и эффективно применять мероприятия, направленные на, в первую очередь, предупреждение возникновения нежелательных последствий — минимизация рисков или их предотвращение;

— обеспечивать разработку методологических основ создания и внедрения систем менеджмента информационной безопасности, базирующихся на интегрированных системах управления.

Литература

1. Романенко, Е. А. Методы обучения персонала по вопросам информационной безопасности [Электронный ресурс] / Е. А. Романенко, Д. С. Тимофеев. — Режим доступа: \www/ URL: http://ir.nmu.org.ua/bitstream/handle/123456789/1667/14.pdf?sequence=1. — 18.01.2015.
2. Smith, L. R. The triple Bottom (Top) Line [Text] / L. R. Smith // Quality Progress. — 2004. — № 37(2). — P. 23.
3. Ивченко, А. В. Современное состояние и пути развития нормативного обеспечения информационной безопасности [Текст]: сб. науч. труд. / А. В. Ивченко, Б. А. Ступин, В. Н. Янченко, Т. Ю. Нагорна // 4-й МНПК «Техника и технологии: пути инновационного развития». — Курск: Юго-Западный государственный университет, 2014. — С. 124–129.
4. Галатенко, В. А. Основы информационной безопасности [Текст] / В. А. Галатенко; под ред. В. Б. Бетелина. — М.: Интернет-университет информационных технологий, 2006. — 208 с.
5. Андрианов, В. В. Обеспечение информационной безопасности бизнеса [Электронный ресурс] / В. В. Андрианов. — Режим доступа: \www/URL: http://bezopasnik.org/article/book/andrianov_infobez_biz_2011.pdf. — 28.02.2015.
6. Ажмухамедов, И. М. Динамическая нечеткая когнитивная модель оценки уровня безопасности информационных активов вуза [Текст] / И. М. Ажмухамедов // Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. — 2012. — № 2. — С. 137–142.
7. Ажмухамедов, И. М. Информационная безопасность корпоративной сети вуза [Текст] / И. М. Ажмухамедов, О. М. Проталинский // Датчики и системы. — 2009. — № 5. — С. 3–7.
8. Концепция обеспечения информационной безопасности предприятия [Электронный ресурс]. — Режим доступа: \www/ URL: http://securitypolicy.ru/index.php/Концепция_обеспечения_информационной_безопасности_предприятия. — 28.02.2015.
9. Арменский, А. Е. Информационная и экономическая безопасность государства [Текст]: учебно-метод. пос. для гос. служащих / А. Е. Арменский, В. С. Гусев, А. Е. Петров, Ю. В. Шленов. — М.: Мобиле, 2003.
10. ГОСТ Р 51275-99. Объект информатизации. Факторы, воздействующие на информацию [Текст]. — Действует с 2000-01-01. — М.: Стандартинформ, 1999. — 12 с.
11. ГОСТ Р ИСО/МЭК 31010-2011. Менеджмент риска. Методы оценки риска (ISO/IEC 31010:2009) [Текст]. — Действует с 2011-12-01. — М.: Стандартинформ, 2012. — 74 с.
12. Азгальдов, Г. Г. Квалиметрия в архитектурно-строительном проектировании [Текст] / Г. Г. Азгальдов. — М.: Стройиздат, 1989.
13. ГОСТ Р ИСО 31000-2010. Менеджмент риска. Принципы и руководство (ISO 31000:2009) [Текст]. — Действует с 2011-09-01. — М.: Стандартинформ, 2012. — 25 с.
14. Раджаб, З. М. Исследование взаимодействия международных универсальных стандартов при создании интегрированных систем менеджмента [Текст]: сб. науч. тр. / З. М. Раджаб, В. А. Залога, А. В. Ивченко // Сучасні технології в машинобудуванні. — 2012. — Вып. 7. — С. 315–332.

СИСТЕМАТИЗАЦІЯ ФАКТОРІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ОРГАНІЗАЦІЇ

Запропоновано універсальну багаторівневу систему факторів інформаційної безпеки організацій (підприємств). Дозволяє: групувати фактори за однорідними ознаками; розмежовувати загрози організації у сфері інформаційної безпеки по зовнішньому і внутрішньому контексту; визначати природу загроз. Система може бути використана як інструментарій у процесі оцінки та/або зниження інформаційних ризиків організацій різних типів, видів і форм управління.

Ключові слова: інформаційна безпека, система факторів, зовнішній і внутрішній контекст, ризик.

Янченко Вадим Николаевич, *аспирант, кафедра технологии машиностроения, станков и инструментов, Сумский государственный университет, Украина,* ***e-mail: ia_vadim@ukr.net****.*
Ивченко Александр Владимирович, *кандидат технических наук, доцент, кафедра технологии машиностроения, станков и инструментов, Сумский государственный университет, Украина.*
Залога Вильям Александрович, *доктор технических наук, профессор, заведующий кафедрой технологии машиностроения, станков и инструментов, Сумский государственный университет, Украина.*
Дынник Оксана Дмитриевна, *кандидат технических наук, доцент, кафедра технологии машиностроения, станков и инструментов, Сумский государственный университет, Украина.*

Янченко Вадим Миколайович, *аспірант, кафедра технології машинобудування, верстатів та інструментів, Сумський державний університет, Україна.*
Івченко Олександр Володимирович, *кандидат технічних наук, доцент, кафедра технології машинобудування, верстатів та інструментів, Сумський державний університет, Україна.*
Залога Вільям Олександрович, *доктор технічних наук, професор, завідувач кафедри технології машинобудування, верстатів та інструментів, Сумський державний університет, Україна.*
Динник Оксана Дмитрівна, *кандидат технічних наук, доцент, кафедра технології машинобудування, верстатів та інструментів, Сумський державний університет, Україна.*

Ianchenko Vadym, *Sumy State University, Ukraine,* ***e-mail: ia_vadim@ukr.net****.*
Ivchenko Aleksandr, *Sumy State University, Ukraine.*
Zaloga Vilyam, *Sumy State University, Ukraine.*
Dunnik Oksana, *Sumy State University, Ukraine*