ПОСОЛЬСТВО РЕСПУБЛИКИ БЕНИН В РОССИИ
ПОСОЛЬСТВО РЕСПУБЛИКИ ГВИНЕЯ В РОССИИ
ТОРГОВО-ПРОМЫШЛЕННАЯ ПАЛАТА РОССИЙСКОЙ ФЕДЕРАЦИИ
УПРАВЛЕНИЕ ФЕДЕРАЛЬНОЙ СЛУЖБЫ ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
ПО ЦЕНТРАЛЬНОМУ ФЕДЕРАЛЬНОМУ ОКРУГУ
ПРАВИТЕЛЬСТВО РЯЗАНСКОЙ ОБЛАСТИ
СОВЕТ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЪЕДИНЕНИЯ ВУЗОВ РОССИЙСКОЙ ФЕДЕРАЦИИ ПО ОБРАЗОВАНИЮ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
КОЛЛЕГИЯ МЕДИАТОРОВ ЯРОСЛАВСКОЙ ОБЛАСТИ
МЕЖРЕГИОНАЛЬНАЯ ОБЩЕСТВЕННАЯ ОРГАНИЗАЦИЯ АУДИТОРЫ КОРПОРАТИВНОЙ БЕЗОПАСНОСТИ

ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ: ПРОБЛЕМЫ И РЕШЕНИЯ

СБОРНИК ТЕЗИСОВ ДОКЛАДОВ
IV МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ

Рязань, Россия
2015 г.

УДК 65.012.8
ББК 65.05
О - 136

Рецензент: кафедра «Корпоративной безопасности» Рязанского государственного радиотехнического университета (зав. кафедрой, к.э.н., доц., фед. эксперт (св-во №11313707.4668 в федеральном реестре экспертов ФГУ НИИ РИНКЦЭ) А.В. Янкевский).

Авторская редакция и стилистические особенности публикаций полностью сохранены.

О - 136 Обеспечение комплексной безопасности предприятий: проблемы и решения: Сборник тезисов докладов IV международной научно-практической конференции (г. Рязань, 9-11 июня 2015г.) – Рязань: Изд-во Рязан. радиотех. ун-та, 2015г. – 148 с.

В сборник вошли доклады и научные труды участников IV Международной научно-практической конференции «Обеспечение комплексной безопасности предприятия: проблемы и решения».

Тематика сборника затрагивает совокупность таких подсистем как: экономическая безопасность, информационная безопасность, кадровая безопасность, психологическая безопасность, инженерно-техническая безопасность и правовая безопасность.

Материалы и тезисы конференции могут быть интересны собственникам предприятий, руководителям высшего и среднего звена, субъектам предпринимательства различных форм собственности, специалистам служб безопасности, юридических, кадровых и ИТ-департаментов, студентам всех факультетов ВУЗов, слушателям программ МВА, Президентской программы подготовки управленческих кадров для организаций народного хозяйства РФ. А также программ, в рамках которых предусмотрено изучение вопросов и задач, связанных с недобросовестной конкуренцией, случаями недружественного поглощения (рейд), коррупцией, промышленным шпионажем, недостаточной профессионально-психологической надежностью персонала и иными аспектами по обеспечению комплексной безопасности предприятий и организаций.

УДК 65.012.8
ББК 65.05
О - 136

ОГЛАВЛЕНИЕ

ПРИВЕТСТВЕННЫЕ СЛОВА

Виктор
Сергевич
ГУРОВ,

д.т.н., профессор
Ректор Рязанского
государственоого
радиотехнического
университета (РГРТУ)

Уважаемые гости и участники конференции,
преподаватели и студенты Университета!

Традиционно в первую декаду июня мы собираемся в стенах Университета чтобы обсудить насущные вопросы и проблемы, обменяться мнениями по широкому спектру различных вопросов, связанных с обеспечением корпоративной безопасности предприятий и организаций различного размера (от крупнейших холдингов, до малых и средних) из различных секторов экономики Российской Федерации.

В связи с вступлением в силу ряда санкционных мероприятий, особую важность занимают обширный пул вопросов по обеспечению устойчивого развития российской экономики, поддержка и развитие наукоемких и инновационных предприятий.

Мне приятно приветствовать коллег, как новых гостей, так и уже ставших постоянными партнерами и участниками нашего мероприятия.

Отдельно хочу приветствовать присоединившихся в этом году коллег из Торгово-Промышленной Палаты Российской Федерации, специалистов из Коллегии медиаторов Ярославской области, что позволит делегатам Конференции получить реальный практический опыт и знания.

Мы продолжим начатые ранее дискуссии по традиционным направлениям: инженерно-технической безопасности и экологии, защиты интеллектуальной собственности и ноу-хау, правовой безопасности предприятий, информационной безопасности и защите конфиденциальной информации, а также финансово-экономической и имущественной безопасности субъектов экономической деятельности РФ.

Желаю гостям и участниками конференции плодотворной работы, направленной на решение вопросов и задач обеспечения комплексной безопасности предприятий и организаций не только на территории России, но и на международном уровне!

Александр
Сергеевич
АЛПАТОВ,

Главный эксперт
Торгово-
промышленной палаты
Российской Федерации

Уважаемые участники конференции!

В последнее время мировое сообщество всё больше обращает внимание и продвигает проекты государственно-частного партнёрства в противодействии коррупции.

В этой связи хотел бы отметить, что Торгово-промышленная палата Российской Федерации выступает за постоянный диалог представителей государства и бизнеса и считает крайне необходимым обеспечить выработку стратегии, а также реального механизма партнёрства государства и бизнеса по приоритетным направлениям противодействия коррупции.

Безусловно, меры, которые приняты со стороны Президента и Правительства, Законодательного собрания Российской Федерации, правоохранительных структур и предпринимательских организаций, позитивно влияют на общую обстановку в борьбе с коррупцией, преодоление административных барьеров, поиск благоприятных условий для развития бизнеса. Изложенное вселяет уверенность, что проводимая сейчас антикоррупционная политика государства будет продолжена.

Совершенно естественно, что государство ждет ответных шагов со стороны бизнес-сообщества.

Одним из значимых встречных шагов со стороны предпринимателей в направлении создании системы противодействия коррупции является разработка и внедрение нового механизма в сфере противодействия коррупции ─ Антикоррупционной хартии российского бизнеса.

В 2012 году четыре ведущих отечественных бизнес-объединений (Торгово-промышленная палата Российской Федерации, Российский союз промышленников и предпринимателей, «Деловая Россия», ОПОРА РОССИИ) выступили в качестве инициаторов принятие Хартии и документа о порядке ее реализации в предпринимательской деятельности.

Данный документ был разработан в соответствии с решением Президиума Совета при Президенте Российской Федерации по противодействию коррупции от 4 ноября 2011 г., на котором с участием ТПП РФ рассматривался вопрос «О формировании

комплекса нормативно-правовых мер, направленных на активизацию совместного участия в противодействии коррупции представителей бизнес-сообщества и органов государственного управления».

Следует подчеркнуть отличительную особенность Хартии, которая, по моему глубокому убеждению, представляет собой определенный свод правил для бизнеса, своеобразный «Кодекс чести». Она предполагает внедрение в корпоративную политику компаний антикоррупционных программ, мониторинг и оценку их реализации, эффективный финансовый контроль, принцип публичности антикоррупционных мер, отказ участников Хартии от незаконного получения преимуществ, участие в тендерах на основе принципов прозрачности и конкуренции, информационное противодействие коррупции, сотрудничество с государством, содействие осуществлению правосудия и другие меры.

В настоящее время ТПП РФ, территориальные палаты проводят работу по разъяснению положений Хартии и активному привлечению предпринимательства к ее реализации. Организация этой работы строилась на принципе публичности.

В ряде регионов процедуры присоединения к Хартии были приурочены к мероприятиям, имеющим международный, всероссийский или межрегиональный характер.

Что дает присоединение предпринимателей к Хартии

В условиях интеграции российских деловых кругов в мировое экономическое пространство, сведения о присоединении к Хартии способствует развитию международных контактов, формированию и развитию доверия, уверенности в добросовестности российских компаний.

Палата, а также объединенный Комитет ведут Реестр Антикоррупционной хартии, который уже активно используется в установлении деловых связей с зарубежными предприятиями, как подтверждение надежности в выполнении контрактов и договоров. При этом Палата не только подтверждает статус предприятия, но и берет на себя обязательства в оказании соответствующей помощи.

Хартия открыта для любого предпринимателя, компании или, объединения вне зависимости от формы собственности, организационно-правовой формы, масштаба и профиля деятельности. Поэтому мы приветствуем инициативу предпринимательских объединений, предприятий которые планирует заявить на данном мероприятии о решении стать участниками Хартии, соблюдать ее положения и осуществлять разъяснительную работе среди других организаций по ее реализации.

Яо Никез АДУ,

к.ю.н.,
Президент Ассоциации
Иностранных
Студентов России

Уважаемый Виктор Сергеевич!
Уважаемые коллеги и дорогие гости!

Позвольте мне, прежде всего, поблагодарить Руководство университета за многолетнее сотрудничество. Как вы знаете, Ассоциация иностранных студентов России входит в состав организаторов данного мероприятия.

Ежегодное проведение подобных Международных Конференций подтверждает высокое качество полученного в стенах РГРТУ уровня образования. Это служит основанием к сотрудничеству АИС с РГРТУ и присутствию большого количества контингента иностранных студентов. В связи с этим я хочу поблагодарить Руководство РГРТУ и России за предоставленную возможность сотням тысяч иностранных студентов получать это неоценимое и качественное образование.

Ассоциация Иностранных Студентов со своей стороны и в дальнейшем будет поддерживать подобную инициативу и всячески способствовать развитию данного вида сотрудничества.

Что касается сегодняшнего мероприятия, надо сказать, что тематика конференции: «Обеспечение безопасности на предприятиях: проблемы и решения» очень объемна, комплексна и интересна, потому что любой специалист (юрист, экономист, инженер и др.) может найти для себя что-то новое и интересное в рамках рассматриваемых вопросов и задач. Уверен, что будут очень интересные дискуссии и в различны секциях, мастер-классах и в кулуарах мероприятия.

Желаю участникам Конференции плодотворной работы и успехов!

Владимир
Павлович
ЛОСЬ,

д.воен.н., профессор,
лауреат премии
Правительства РФ в
области образования,
председатель Совета
регионального
отделения УМО ИБ
по ЦФО.

Уважаемые участники конференции!

События последних лет заставляют совершенно по-другому взглянуть на проблему обеспечения информационной безопасности. Если раньше, скорее всего по умолчанию, мы предполагали участие в этом процессе равноправных сторон, сейчас ситуация коренным образом изменилась. Это изменение, прежде всего, связано с отступлением, а фактически игнорированием США тех правовых норм, которые заложены в основополагающих международных договоренностях по обеспечению международной безопасности. Это очень важно осознать и учитывать. В процесс противостояния втянуты не только «верхние» уровни государственной власти, но и конкретные предприятия, конкретные личности. Готовы ли мы к такому противостоянию?

Появление новых угроз требует разработки адекватных мер реагирования со стороны государства. Чем мы ответим? Как это отразится на основных показателях экономического развития страны, на ее безопасности? Приемлемо ли это для Российской Федерации?

Вот тот перечень важных, по-моему, вопросов, на которые надо найти ответы в ходе конференции.

Удачи вам, заинтересованных обсуждений и плодотворной работы, участники конференции.

Уважаемые Коллеги!

Владимир Анатольевич ЛИТВИНЕНКО,

к.воен.н., заместитель руководителя Управления ФСТЭК России по Центральному федеральному округу

Приветствую вас на международной конференции в стенах одного из ведущих вузов РФ, осуществляющего подготовку специалистов в области информационной безопасности.

Одним из полномочий Федеральной службы по техническому и экспортному контролю, как органа исполнительной власти, является осуществление реализации государственной политики в вопросе обеспечения безопасности информации в системах информационной и телекоммуникационной инфраструктуры, в том числе и на предприятиях.

Стремительное и интенсивное развитие информационных и телекоммуникационных систем и технологий, интеграция в мировое информационное пространство, информатизация практически всех сторон общественной жизни и в первую очередь деятельности предприятий существенно усилили их зависимость от состояния информационной сферы.

Современные угрозы безопасности информации в значительной мере определяются гиперактивным уровнем развития информационных технологий. В этих условиях на одно из первых мест по значимости и объемам добываемой информации выходит компьютерная разведка. Основными ее устремлениями являются информационные системы и информационно-телекоммуникационные сети.

Все это проходит на фоне повышения уровня сложности программного и аппаратного обеспечения, при котором человек утрачивает контроль за происходящими в информационных системах процессами и способность влиять на них. Вследствие увеличения количества уязвимостей информационных систем, увеличивается перечень актуальных угроз, которые могут быть реализованы.

Вот эти проблемы и хотелось обсудить на этом форуме.

Спасибо за внимание!

Светлана
Сергеевна
АНДРИАНОВА,

к.ю.н.,
вице-президент
Межрегиональной
Общественной
Организации
«Аудиторы
Корпоративной
Безопасности»

Уважаемые участники конференции!

Как со-организаторы конференции, рады Вам сообщить, что численный состав участников охватывает все континенты, кроме Австралии. Но мы работаем и в этом направлении.

Конференция стала многоконтинентальной, а не только международной. Мы радуемся каждый раз, когда новые участники приезжают к нам издалека, чтобы поделиться опытом, обрести новых партнеров и коллег по всему миру.

Наши посевы начинают прорастать: молодые ученые продвигают наши методики, молодые специалисты применяют наши отработанные на практике механизмы построения комплексной безопасности предприятий.

И сегодня мы в четвертый раз встречаемся на площадке РГРТУ, чтобы поделиться с Вами своими наработками и опытом.

Самый ценный актив – это знания, навыки и опыт. Недвижимость может быть арестована (санкции), автомобиль сломаться, а знания всегда остаются с Вами. Их нельзя отнять. Это самое ценное инвестирование, которое только можно представить.

Желаю Вам вынести с сегодняшней конференции столько ценных знаний и навыков, сколько сможете взять!

Уважаемые Коллеги!

Наталия
Викторовна
Мамаева,

Председатель Коллегии
медиаторов
Ярославской области

Безопасность бизнеса является важным аспектом для любой организации не зависимо от того, чем она занимается, где находится и сколько людей в ней работает. Реализация деятельности с учетом предпринимательских рисков может осуществляться разными способами. Защита бизнеса зависит от многих факторов: наличия профессиональных кадров, практического опыта, финансовых средств, материальных ценностей, информационных ресурсов, репутации и прочего. Вместе с тем обеспечение безопасности бизнеса имеет ряд задач: защиты законных интересов, обеспечения устойчивого функционирования, предотвращение угроз.

Ведение бизнеса без конфликтных столкновений практически невозможно, которое нередко занимает годы, отвлекает колоссальные силы и средства от нормального ведения бизнеса, разрушает деловые и человеческие связи, подрывает деловую репутацию, ведет к утечке конфиденциальной информации, вызывает недоверие к компании, влечет потери прибыли и дестабилизацию бизнеса. Как правило, разногласия возникают из-за отсутствия или недостатка общения, которое и приводит к конфликту, что в конечном итоге приводит к принятию кардинальных мер путем подачи иска в суд. Обращение в суд самое неприятное, утомительное и нервное мероприятие. Вместе с тем существует множество способов урегулировать спор, не доводя его до суда.

Бессмысленность и бесполезность судебных разбирательств приводит к мысли о необходимости обращения к институту медиации, позволяющей участникам конфликтов (споров) добровольно урегулировать разногласия. Медиатор поддерживает стороны конфликта, чтобы они могли сами начать искать решения своих проблем, не ожидая приговора, подсказки, влияния, как это происходит в судебном порядке. Целью медиации является совместный поиск взаимоприемлемого решения задачи, что, несомненно, благотворно влияет на безопасность бизнеса. Практика показывает, что большинство споров, урегулированных с помощью медиации, разрешаются в пользу предпринимателей!

СЕКЦИЯ: ИНЖЕНЕРНО-ТЕХНИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 69.035.4

Авагян М.Л.

Технология и безопасность проведения взрывных работ при строительстве метрополитена

Расчет паспорта буро-взрывных работ

Определим удельный расход взрывчатого вещества и примем его тип. При данных горно-геологических условиях строительства наиболее целесообразно применить аммонит №6 ЖВ, в патронах диаметром 32 мм. Электродетонаторы типа ЭДКЗ-ПМ-15 с сериями замедления - 0; 0.15; 0.30; 0.45; 0.60 сек.

$$q = q_1 f_1 V e m$$, кг/м3,

где q1= 0.1f, где f = 4 - крепость вмещающих пород по профессору Протодьяконову;

$$q_1 = 0.1 \cdot 4 = 0.4$$,

$$f_1 = 1.5$$

$$V = \frac{6.5}{\sqrt{S_{пр\,ох}}}$$,

где Sпрох - сечение ствола в проходке

$$S_{пр\,ох} = S$$ ВЧ м2

Sвч=28.26 м2

$$V = \frac{6.5}{\sqrt{29.637}} = 1.19$$

$e = \frac{A_{№6\,ЖВ}}{A_{ВВ}} = \frac{360}{360} = 1$ - коэффициент работоспособности;

$$m = \frac{36}{d_{ДЗГР}} = \frac{36}{32} = 1.125$$

$$q = 0.4 \cdot 1.5 \cdot 1.19 \cdot 1 \cdot 1.125 = 0.89$$ кг/м3.

Определим количество шпуров в сечении

$$N = \frac{1.27 q S_в}{a \Delta b m}$$,

где

$$a = 0.5$$

$$\Delta = 1.2$$

$$b = 1$$

$$m = 1.125$$

$$N = \frac{1.27 \cdot 0.89 \cdot 28.26}{0.5 \cdot 1.2 \cdot 1 \cdot 1.125} \approx 47$$ шпуров.

Определим и зададим остальные параметры буро-взрывных работ:

глубина шпура - $l_ш = 1.2$ м;

глубина заходки - $l_{зах} = 1.0$ м;

КИШ=0.8 ($\eta = 0.8$);

Определим расход взрывчатого вещества за цикл:

$$Q_{вв} = qS_{пр\,ск} l_ш \eta,$$

$$Q_{вв} = 0.89 \cdot 29.673 \cdot 1.2 \cdot 0.8 = 25.3 \text{ кг/цикл.}$$

Заряжание шпуров призводится следующим образом:

в центральный (буферный) шпур заряжается одна шашка массой 250 грамм, во врубовые - 3 шашки, в отбойные - 2 шашки. Общее число шашек - 98 штук. Взрывание производится методом обратного инициирования. Материал забойки - песок средних фракций. Взрывание производится с четырьмя степенями замедления.

После взрыва не происходит деформации тюбингов? Или взрыв направленный в глубину породы?

Взрывы направленные.

Взрыв происходит с замедлением по секциям и в несколько уступов.

Таблица.1.

Матрица распределения времени замедления при буровзрывных работах

Порядковый номер ступени замедления	Число шпуров в ступени замедления	Номер серии ЭД	Величина замедления мс	Масса ВВ на ступень замедления, кг
1	4	3	50	1,2
2	4	5	100	1,2
3	6	6	125	1,8
4	6	13	400	1,8
5	6	16	600	1,8
6	6	18	800	1,8
7	6	20	1000	2,2
8	10	22	1500	4
9	8	24	2000	3,2

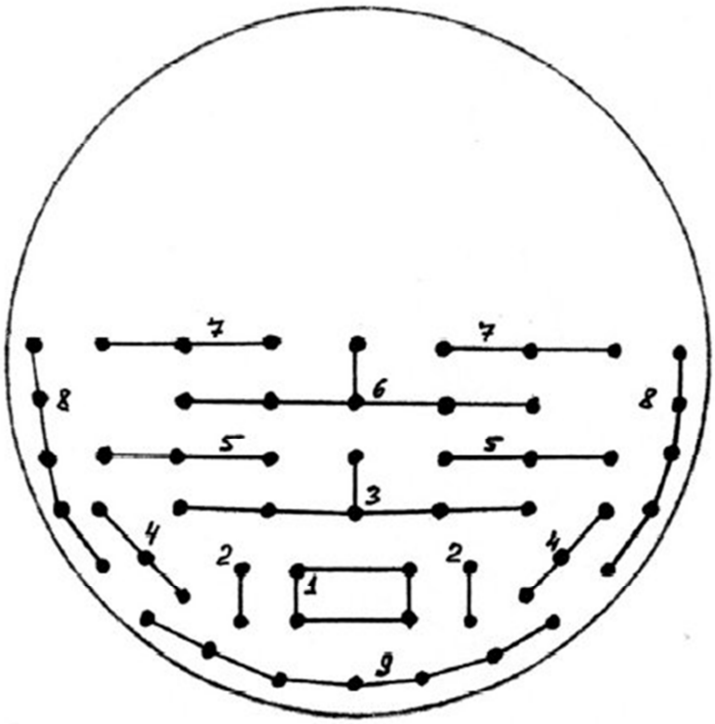


Рис.1 Схема расположения шпуров и последовательности взрывов при проведении буровзрывных работ наклонным типом на станцию метрополитена.

Сначала взрывается специальное место для отвала породы (вруб) в ненарушенной горной породе, затем остальные скважины под действием последующих серий взрывов производят осыпание породы. Мощность каждой секции, уступа, их количество, корректируются по факту по ГОСТ Р 52892–2007 по данным производственного мониторинга.

Литература

1. Баклашов И.В., Картозия Б.А. «Механика подземных сооружений и конструкций крепей» - М., Недра, 1992, 543 с.

2. Насонов И.Д., Федюкин В.А., Шуплик М.Н., «Технология строительства подземных сооружений» - М., Недра, 1992, 285 с.

3. Насонов И.Д., Шуплик М.Н. «Закономерности формирования ледопородных ограждений при сооружении стволов шахт» - М., Недра, 1976, 237 с.

4. Храпов В.Г. «Тоннели и метрополитены» - М., Транспорт, 1989, 383 с.

5. Белый В.В. «Справочник инженера шахтостроителя» в 2-х томах - М., 1983г.

6. Туренский Н.Г., Ледяев А.П. «Строительство тоннелей и метрополитенов» - М., Транспорт, 1992, 264 с.

7. Богомолов Г.М., Голицынский Д.М. Сеславинский С.И. «Справочник инженера-тоннельщика» - М., Транспорт, 1993, 389 с.

УДК 656.073.7

Аравгиев Б.А., Алибеков М.Э.

Оптимизация процесса транспортировки буровых установок

Нефтегазовая компания ОАО «НК «Роснефть» активно сотрудничает с машиностроительным предприятием ООО «Уралмаш НГО Холдинг» в сфере закупок нефтегазового оборудования. В данной статье рассмотрена проблема доставки буровой установки с места её изготовления до места ее непосредственной её эксплуатации. В нашем случае объектом транспортировки является буровая установка УРАЛМАШ 5000/320 ЭК-БМЧ, изготавливаемая компанией ООО «НГО Холдинг» в Свердловской области в городе Екатеринбург.

На разбуривание Ванкорского месторождения необходимо доставить 11 буровых установок, 10 их которых будут в активном состоянии, а 1 для случая выхода из рабочего состояния одной из работающих установок. Это позволит нам избежать непредвиденных негативных простоев, что приведет к невыполнению утвержденных планов, и как следствие к финансово – экономическим потерям. По условиям контракта установки типа БУ 5000/320 ЭК-БМЧ будут поставлены до конца августа 2015 года.

Был проведен анализ данной проблемы и предложен план по оптимизации транспортировки буровой установки от места изготовления до места ее применения (рис. 1).

Транспортировка будет вестись железнодорожными путями от г. Екатеринбург до п. Коротчаево, Ямало-Ненецкого автономного округа. Далее более выгодно и удобно будет доставить буровую установку до Ванкорского месторождения воздушным транспортом.

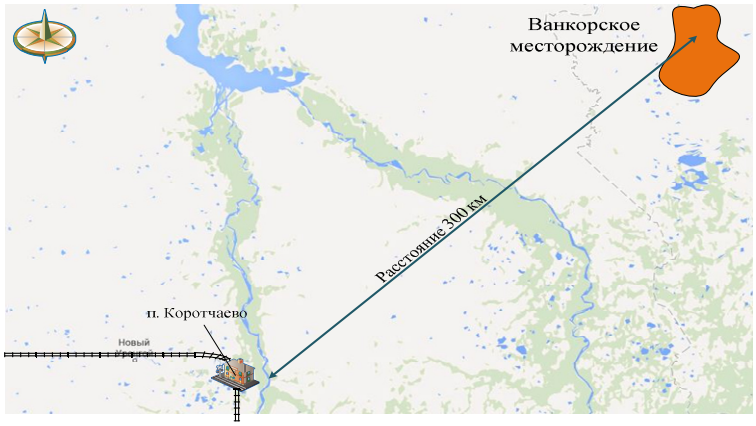


Рис. 1. Карта транспортировки буровой установки.

Для определения оптимального количества воздушных суден была решена логистическая задача.

Состав и масса буровой установки типа УРАЛМАШ 5000/320 ЭК-БМЧ:

- буровая вышка УМ 46/320 ОР – 19000 кг;
- лебедка ЛБУ-1500 АС-1 – 32900 кг;

- буровой насос УНБТ-1180L – 24632 кг;
- крюкоблок УТБК 6-320 – 7520 кг;
- вертлюг УВ320МА – 2980 кг;
- кронблок УКБ-6-325 – 5990 кг;
- система верхнего привода СВП 320 ЭЧР – 15000 кг;
- ротор Р-950 – 7000 кг;
- система очистки ЛСГС – 2100 кг.

Зная состав и массу всех комплектующим, выберем грузовой вертолет МИ-26ТС со следующими необходимыми характеристиками:

- грузоподъемность – 20000 кг;
- дальность при максимальной загрузке – 450 км;
- крейсерская скорость – 265 км/ч;
- объем топливных баков – 12000 л.

Зная расстояние от ж/д Коротчаево до Ванкорского месторождения и скорость вертолета можно рассчитать время на доставку груза:

$$t = \frac{S}{V}$$

где,S – расстояние от ж/д Коротчаево до Ванкорского месторождения;

V – крейсерская скорость вертолета МИ-26

Так же немаловажно лобовое сопротивление воздуха, оказывающее влияние на траекторию движения вертолета.

$$V_1 = C_{x0} (\rho V^2 /2)*S,$$

Где: C_{x0}- безмерный аэродинамический коэффициент сопротивления воздуха (в данном случае=0,00125),V- скорость тела в полете,ρ- плотность воздуха,S-площадь тела

$$V_1 = 0{,}00125 * (1{,}112*73{,}61^2)/2 * 17{,}59 = 66{,}24 \text{ м/с} \approx 238 \text{ км/ч}$$

$$t = \frac{S}{V1} = \frac{300 \text{ км}}{238 \text{ км/ч}} = 1, 26 = 1 \text{ ч. } 15 \text{ мин.}$$

Учитывая крайне нестабильный климатический район, округлим рассчитанное время полета до 1 ч. 30 мин. и составим полную временную схему доставки одной буровой установки (рис. 2).

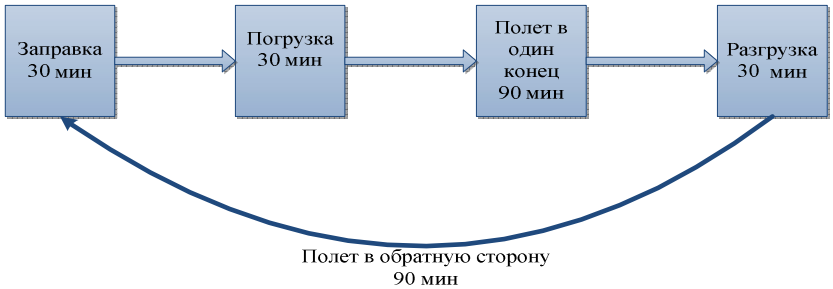


Рис. 2. Временная схема доставки буровой установки

Для оптимальной доставки необходимо совершить семь рейсов, при условии, что масса груза на каждый рейс не будет превышать 20000 кг:

I. буровая вышка = 19500 кг;
II. буровая лебедка = 19000 кг;
III. буровая лебедка (13900 кг.) + вертлюг (2980) + система очистки (2000 кг.) = 18880 кг;
IV. буровой насос = 19000 кг;
V. буровой насос (5632 кг.) + крюкоблок (7520 кг.) + кронблок (5990 кг.) = 19142 кг;
VI. система верхнего привода и другие, мелкие комплектующие = 19000 кг;
VII. ротор и др. = 19000 кг.

2 вертолета:

$$(N * T) – R_1 = T^2_{общ} = (3 * 270 \text{ мин}) - 30 \text{ мин} = 780 \text{ мин} = 13 \text{ ч}$$

где, N – количество рейсов; T – время в пути (включая заправку, погрузку, разгрузку); R_1 – время заправки одного вертолета; $T^2_{общ}$ – общее время полетов двух вертолетов.

Так как нам необходимо совершить еще один рейс №VII, то в доставке будет участвовать только один вертолет:

1 вертолет:

$$(N * T) – F_2 = T^1_{общ} = (1 * 270 \text{ мин}) – 90 \text{ мин} = 180 \text{ мин} = 3 \text{ ч}$$

Общая продолжительность доставки всей буровой установки составит:

$$T^2_{общ} + T^1_{общ} = 780 \text{ мин} + 180 \text{ мин} = 960 \text{ мин} = 16 \text{ ч}.$$

Исходя из расчетов, можно сделать вывод, что рационально и целесообразно задействовать в транспортировке два вертолета типа МИ-26ТС

Список литературы:

1. Гусман А.М., Порожский К.П. Буровые комплексы. Современные технологии и оборудование. – Екатеринбург: УГГА, 2009. -592 с.

2. Руководство по технической эксплуатации. Вертолет Ми-26 ТС, ОАО «РОСТВЕРТОЛ», 2000 г.

3. Рекламные материалы предприятий: ООО «Уралмаш НГО Холдинг», ОАО «НК «Роснефть».

УДК 628.51

Воробьев А.Е., Джимиева Р.Б., Шамшиев О.Ш.

Классификация шахтных отвалов и определение риска воздействия на окружающую среду

В настоящее время в пределах г. Донецка (Донецкая народная республика), расположено свыше 140 шахтных отвала, занимающих площадь около 10 млн. $м^2$ [5]. Высота этих отвалов угольных шахт изменяется в пределах 8–124 м.

Существует типизация шахтных отвалов по ряду признаков [3, 5].

Так, по тепловому состоянию породные отвалы делятся на горящие, потухшие и не горевшие. Значительная доля действующих породных отвалов является горящими (№1 ш. Горького, №1 ш. им. Челюскинцев и №3 ш. Абакумово) – 28 из 32. Среди терриконов, выведенных из эксплуатации, 25 горящих (№12 Ф. Кона, №1-7 Ветка) и 81 не горящих или потухших (№2 Ф. Кона, №2 Паровичная и №1-2 ш. Горького).

По морфологии шахтные отвалы подразделяются на [5]:

- конические (№1 ш. Кировская, №20 ш. Мушкетовская, №1-7 Ветка и др.);
- усеченные конические (№1 ш. Панфиловская, №1 ш. 6 - Красная Звезда, №30 ш. и др.);
- хребтовидные;
- плоские (№2 ш. Заперевальная, №1 ш. Горького, №3 ш. Абакумова).

По наличию рекультивации на:

- озелененные (№1 и 2 ш. Ливенка, №7-8 им. Калинина, №1-7 Ветка);
- не озелененные (№2 Ф. Кона, №1 ш. Заперевальная).

Породная масса как компонент геологической среды представляет собой техногенные осадки, находится в неравновесном состоянии и под действием внутренних и внешних факторов претерпевает закономерные преобразования, которые определяются понятием диагенеза [1,2,5]. При этом ведущая преобразующая роль принадлежит аэробным и анаэробным микроорганизмам при активном участии метеорных вод.

В теле породных отвалов формируется временная или постоянная зона водонасыщения [5]. При этом залегающие в основании отвала суглинки, аллювиальные глины или глинистые коры выветривания, служат водоупором для формируемого техногенного водоносного горизонта. Верхняя часть зоны водонасыщения обогащена кислородом, что в присутствии высокой концентрации сульфидной серы и органического вещества благоприятствует развитию окислительных процессов с выделением тепла.

Температурное воздействие на отвальные породы сопровождается преимущественно их выгоранием и спеканием [1,5]. Гораздо реже процесс горения породной массы приводит к плавлению.

Наиболее широко распространены окислительные изменения отвальных пород без значительного температурного воздействия [5].

Наибольшую экологическую опасность представляют активно горящие породные отвалы [2,5]. В процессе проведенных исследований на всех обследованных отвалах даже при отсутствии очевидных очагов горения отмечаются следы окислительных процессов, проявленные выделениями свежей фумарольной сульфатной минерализации.

Анаэробные процессы преобразования породной массы терриконов, проявлены в нижней части зоны водонасыщения [1,2,5].

Вся совокупность процессов преобразования отвальных пород представляет экологическую опасность. Окислительные процессы

сопровождаются выбросами различных окислов, паров серной кислоты, летучих соединений металлов и токсичных элементов [5]. Анаэробные процессы сопровождаются выбросами аммиака, сероводорода. При этом аэробные и анаэробные процессы с разной степенью активности могут одновременно происходить в одном отвале.

Обследование поверхности отвалов позволяет разделить их по температурному режиму, прошедших ранее процессов окисления и горения [5]. Наиболее высокие температуры (более 800 °С), вызвавшее плавление пород, установлены на отвале ш. Путиловская и №1 ш. Панфиловская (рис. 1).

Рисунок 1 – Отвал ш. Путиловская [5]. В образце аргиллита отчетливо проявлено послойное плавление. Продукты плавления в виде пористого шлакообразного материала

На значительной части отвалов установлено очаговое горение породной массы, сопровождавшееся спеканием и литификацией обломков [5]. Признаки такого уровня температур (200-800 °С) установлены на отвалах шахт: им. Ф. Кона, №1, Мария, им. Калинина №7-8 и др.

Около половины обследованных отвалов с поверхности, даже при наличии глубоких срезов вершины и склонов, не обнаруживают признаков активного горения породной массы [5]. Подобными признаками отличаются отвалы: ш. Владимир, №4 ш. им. Горького.

Литература

1. Воробьев А.Е., Арутюнян В.О., Чекушина Т.В. Отрицательная обратная связь как фактор самоорганизации терриконных геохимических ландшафтов // Синергетика геологических систем. – Иркутск: ИЗК, 1992. – С. 120-121.
2. Воробьев А.Е., Арутюнян В.О., Чекушина Т.В. Самоорганизация терриконных геохимических ландшафтов в решении экологических задач // Синергетика геологических систем. – Иркутск: ИЗК, 1992. – С. 105-106.
3. Воробьев А.Е., Чекушина Т.В. и др. Способы и методы формирования техногенных минеральных объектов при открытой разработке сложноструктурных месторождений. – М.: ЦНИИЦВЕТМЕТ экономики и информации, 1990. – 68 с.
4. Воробьев А.Е., Чекушина Т.В. и др. Общие закономерности геологического строения угольных терриконов и вулканов // Естественные и технические науки N 2. 2013. С. 144-147.
5. Горбачева Е.Ю. Эколого-геохимическая оценка состояния породных отвалов угольных шахт. - Донецк, ДонНТУ – 2012.

УДК 656.01

Воробьев А.Е., Ибройева Л.

Транспортная безопасность Кыргызстана

Автомобильные дороги Кыргызстана составляют дорожную сеть протяженностью около 34000 км, включая 18700 км дорог общего пользования и 15300 км дорог городов, сел, сельскохозяйственных, промышленных и других предприятий, которые связывают области и районы республики, а также обеспечивают выход в международные транспортные коридоры.

В настоящее время из 2700 км международных транспортных коридоров (с учетом альтернативной дороги «Север – Юг») реабилитировано около 1400 км (50%), также практически полностью завершена реабилитация автодорог «Бишкек – Ош» (за исключением участков «Бишкек - Кара-Балта» и «Маданият - Джалал-Абад»), «Бишкек – Георгиевка», «Сарыташ – Карамык», «Ош – Сарыташ – Иркештам» и 2 участка «Тараз – Талас – Суусамыр».

Продолжается работа по реабилитации участков автомобильных дорог международных коридоров как «Бишкек – Нарын – Торугарт» и «Ош – Баткен – Исфана», производится процедура ратификации 3 фазы «Тараз – Талас – Суусамыр», также прорабатываются вопросы по разработке ТЭО альтернативной автомобильной дороги «Север – Юг».

Важным вопросом экономической безопасности Кыргызстана является обеспечение ее транспортной независимости, для чего необходимо строительство объездных дорог в местах сопряжения приграничных территорий, и в обход территорий соседних государств. Так, в настоящее время осуществляется строительство объездной дороги «Айгульташ – Согмент – Таян», кроме этого

ведутся подготовительные работы по строительству автодорог в Баткенской области («Бель – Согот – Божой» и «Кокташ – Аксай – Тамдыки», а также 2-х мостов на автодороге «Кулунду – Максат»).

Для стабильного функционирования дорожной отрасли предстоит продолжить дальнейшую работу по реформированию дорожного сектора, включающую оптимальную структуру управления дорожной отраслью, совершенную систему финансирования, предусматривающую средства на ремонт и содержание автодорог в полном объеме в соответствии с нормативными сроками ремонта, разработку и внедрение механизмов государственного частного партнерства и привлечение частного сектора в строительство и реабилитацию автодорог, создание платных дорог, а также внедрение консультационных услуг и надзора.

Автомобильный транспорт, учитывая труднодоступность к многим населенным пунктам Кыргызстана, является наиболее приоритетным, им перевозится около 95 % грузов и 97 % пассажиров.

Показатели перевозок пассажиров и грузов за последние годы, в удельном весе объемов автоперевозок без резких перепадов, указывают на стабильность развития этого сектора. Тенденция роста парка автомобилей продолжается. Если в 2008 г. количество автотранспортных средств республики составляло 300 тыс. единиц, то в настоящее время оно увеличилось более чем в 2,5 раза и достигло 735 тыс. единиц.

При этом автотранспортные средства годом выпуска более 10 лет составляют более половины от их общего количества. До 2009 г. в страну массово ввозились автотранспортные средства, срок службы которых превышает 10 лет, которые в большей степени являются источником загрязнения воздуха, в сравнении с более новыми транспортными средствами.

В целях ограничения ввоза «старых» автотранспортных средств, в конце 2008 г. ставки единой таможенной пошлины и налогов были увеличены более, чем в 11 раз для автомобилей, год выпуска которых превышает 13 лет. Эта мера дала положительный эффект. Так, в 2009 г. по сравнению с 2008 г. ввоз автотранспортных средств старше 10 лет сократился в 4 раза. Более того, в 2012 г. наметилась положительная тенденция снижения завоза легковых автомобилей старше 10 лет, которые составили 46,3 % от общего количества (в отличие от 93,4 % в 2008 г.), и увеличение ввоза автомобилей с возрастом эксплуатации от 5 до 10 лет составило 50,8 %.

Все же важной проблемой данного сектора является продолжение старения парка автомобильного транспорта, вызывающее увеличение выбросов загрязняющих веществ, включая парниковые газы, а также неполный охват населенных пунктов страны маршрутным сообщением и недостаточно развитая законодательная база для проведения единой политики автомобильной отрасли.

Кыргызская железная дорога протяженностью 424,6 км представлена географически разделенными 2-мя участками и характеризуется отсутствием железнодорожного транзита. Северный участок протяженностью 323,4 км «Балыкчи – Луговая» (Казахстан) и южный участок - 101,2 км.

Анализ перевозок грузов и пассажиров железнодорожным транспортом за последние годы свидетельствует об увеличении показателей по грузообороту при снижении перевозок пассажиров. Показатели грузооборота и пассажирооборота железнодорожного транспорта в республике являются низкими по сравнению с другими видами транспорта из-за отсутствия системы железнодорожного сообщения, проходящего через территорию республики. Проблемами сектора железных дорог являются разрозненные участки железной дороги на севере и юге республики, а также неразвитость транзитных возможностей железной дороги (из-за железнодорожного транспортно-коммуникационного тупика).

Гражданская авиация является одним из быстрых, удобных и, в отдельных случаях (с учетом горного рельефа) практически незаменимых видов транспорта в республике. С 2008 г. по 2012 г. наблюдался рост объема перевозок пассажиров в среднем на 17 %. За этот же период при снижении объема перевозок грузов в среднем на 2 % с 2011 г. наблюдается рост объема перевозок грузов и в 2012 г. он составил 22 %.

В Кыргызской Республике имеется 4 международных аэропорта («Манас», «Ош», «Иссык-Куль» и «Каракол») и 7 внутренних аэропортов («Исфана», «Баткен», «Жалал-Абад», «Кербен», «Нарын», «Казарман» и «Талас»), В настоящее время международные полеты регулярно выполняются только из аэропортов «Манас» и «Ош». Регулярные полеты по внутренним воздушным линиям выполняются только в 4 аэропорта – «Ош», «Исфана», «Баткен» и «Жалал-Абад». В остальные местные аэропорты регулярные полеты не выполняются ввиду практического отсутствия пассажиропотока.

Проблемами сектора гражданской авиации являются недостаточно развитая инфраструктура международного аэропорта «Манас» (здание аэровокзала, средства наземного обслуживания воздушных судов и др.) для преобразования в узловой международный транзитный аэропорт (хаб). Также недостаточная инфраструктура и состояние технических характеристик (взлетно-посадочной полосы, рулежных дорог, стоянок и других составляющих аэродрома, здание аэровокзала, средства наземного обслуживания воздушных судов) международных и всех внутренних аэропортов, которые не отвечают современным условиям. Подавляющее большинство аэронавигационного оборудования, установленного в аэропортах и на территории республики, уже физически и морально устарело.

Литература

1. Воробьев А.Е., Ибройева Л. Современные парадигмы и концепции развития регионов // Материалы VII Международной конференции «Горное, нефтяное, геологическое и геоэкологическое образование в XXI веке» (Москва-Кызылкия). – М.: Изд-во РУДН. 2013. – С. 146-148.

2. Воробьев А.Е., Сарбаев В.И. Оценка экологической безопасности автомобильных дорог методом ландшафтно-геохимического картирования территорий. – М.: МГИУ, 2000. – 51 с.
3. Воробьев А.Е., Сарбаев В.И., Шилкова О.С. Автомобиль – дорога – окружающая среда. – М.: МГИУ, 2001. – 180 с.

УДК 656.085

Воробьев А.Е., Лысенкова З.В., Кумбикила Дж. К., Тчаро Х., Гомеш Ж., Эмирия Ж., Алонге О.Л.

Организация работы по предупреждению и ликвидации чрезвычайных ситуаций в странах Африки

В странах Африки чрезвычайные ситуации, как и в других регионах мира, по своему генезису подразделяются на природные и техногенные. Однако здесь масштаб и содержание чрезвычайных ситуаций (ЧС) отличаются от других регионов мира. Данное обстоятельство в значительной степени определяется региональной спецификой, обусловленной конкретными природными (климатическими, гидрологическими, геолого-геоморфологическими, биотическими и др.) и социально-экономическими факторами (численность и плотность населения, уровень развития и доступность для населения транспортной и т.п. инфраструктуры, хозяйственная специализация и т.д.).

Необходимо отметить частое отсутствие в странах Африканского континента специального министерства, как, например, МСЧ РФ. Организация деятельности по предупреждению чрезвычайных ситуаций и борьбы с ними в таких странах, как Бенин, Республика Конго, Нигерия и Танзания передана в ведение Министерств внутренних дел.

Организационная структура по предупреждению и борьбе с ЧС в Республике Конго. - Министерство внутренних дел является одним из наиболее важных в этой стране. Министр внутренних дел в Правительстве республики Конго является ответственным за различные направления деятельности, к которым также относится обеспечение общей внутренней безопасности страны (в том числе в отношении природных катастроф). Чрезвычайные ситуации и гражданская оборона находятся в ведении Управления безопасности (*Sécurité Civile*) и суб-директората пожарной службы (*Sapeurs-Pompiers*).

В настоящее время министр внутренних дел Республики Конго - господин Раймон Зефирен Мбулу.

Наибольшее количество ЧС в этой стране связано с наводнениями и засухой, землетрясениями и оползнями, пожарами, болезнями животных и эпидемиями (вирус Эбола, Ямбуку, корь, менингит, птичий грипп и др.). Особую группу ЧС образуют те ситуации, которые обусловлены промышленной и сельскохозяйственной деятельностью. Здесь нередко возникают ЧС, связанные с загрязнением воды и воздуха, с радиоактивным загрязнением и т.п.

Организационная структура по предупреждению и борьбе с ЧС в Нигерии. – В Нигерии предупреждение и борьба с ЧС также находится в ведении Министерства внутренних дел. Отдельно Министерство нефтяных ресурсов курирует всю нефтяную тематику, в том числе – вопросы аварий на объектах нефтяной и газовой отрасли. Специальный отдел этого министерства - Отдел нефтяных ресурсов - обеспечивает профилактику несчастных случаев на нефтяных и газовых объектах, а также соблюдение мер по обеспечению стандартов безопасности здоровья и окружающей среды (HSE).

Существует следующая структура Министерства нефтяных ресурсов Нигерии (в настоящее время министр – г-н George Osahon):

- Департамент мониторинга и контроля качества в нефтяной отрасли (руководитель Emmanuel Bekee).
- Департамент нефтяного мониторинга и контроля качества в газовой отрасли.
- Инженерный Департамент (Alfred Ohiani).
- Департамент корпоративных услуг.
- Департамент безопасности (Mordecai Ladan).
- Финансовый департамент (Olukayode Ojo).
- Департамент планирования (Olugbenga Koku).
- Энергетический департамент (Maigida Mudei).

Деятельность Министерства нефтяных ресурсов происходит в тесном сотрудничестве с Национальным агентством обнаружения нефтяного разлива и реагирования (NOSDRA) и Министерством по вопросам окружающей среды. Результатом этого сотрудничества являются законопроекты по управлению чрезвычайными ситуациями в нефтегазовом комплексе этой страны. Усилия NOSDRA направлены также на совершенствование применяемых технологий по утилизации отходов на нефтепромыслах, а также на более широкое использование экологически безопасных методов бурения.

Свой вклад в организацию борьбы с аварийными ситуациями в нефтегазовом комплексе Нигерии вносит совершенствование законодательства этой страны.

Так, в 1990 г. был принят специальный закон («Закон о нефтяном загрязнении» - OPA), который регулирует деятельность по предупреждению и ликвидации аварийных разливов нефти. Данный закон фактически включает в себя комплексный план по обеспечению достаточных финансовых ресурсов для ликвидации последствий аварийных ситуаций, в том числе - выплаты компенсации лицам, пострадавшим в результате разлива нефти. OPA определяет ответственность промышленных предприятий по организации и реализации превентивных мер в нефтедобыче и нефтепереработке. В целом, «Закон о нефтяном загрязнении» на национальном уровне регламентирует деятельность по предотвращению аварийных ситуаций в нефтяной отрасли и борьбе с их последствиями.

Хорошим дополнением к ОРА являются национальные законы, а также международные соглашения, подписанные Нигерией. К ним, например, относятся:

- Африканская конвенция об охране природы и природных ресурсов (1968 г.);

- Международная конвенция о создании международного фонда для компенсации ущерба от загрязнения нефтью (1971 г.);

- Конвенция о предотвращении ущерба загрязнения морской среды (1972 г.) и др.

Организационная структура по предупреждению и борьбе с ЧС в Бенине. - В Бенине предупреждение и борьба с ЧС также находится в ведении Министерства внутренних дел. Министр внутренних дел является членом и председателем делегации премьер-министра. В структуре Министерства внутренних дел Бенина следующие подразделения имеют непосредственное отношение к ЧС:

1. Генеральная инспекция администрации – IGA.
2. Высший совет территориального управления государства – CSATE.
3. Главное управление гражданской защиты и управления в кризисных ситуациях – DGSCGC.
4. Отделение национальной полиции – DGPN.
5. Отделение внутренней безопасности.
6. Генеральная дирекция Национальной Жандармерии – DGGN.
7. Отделение местной власти – DGCL.
8. Делегация безопасности и дорожного движения – DSCR.
9. Обслуживание, связанное с генеральной дирекцией национальной полиции и главным управлением национальной жандармерии: Обслуживание информационных систем и информационной безопасности (STSI2).
10. Обслуживание, связанное с генеральной дирекцией национальной полиции, с генеральной дирекцией национальной жандармерии и отделением гражданской защиты и с управлением в кризисных ситуациях (DGSCGC).
11. Управление международного сотрудничества (DCI).

Организационная структура по предупреждению и борьбе с ЧС в Республике Танзания. - В Танзании предупреждение и борьба с ЧС находится преимущественно в ведении Министерства энергетики и минеральных ресурсов.

Министр энергетики и минеральных ресурсов – г-н Мбарак Абдулвакил, зам. министра – г-н Мвамини Малеми.

В структуре министерства существуют различные специализированные департаменты.

Наиболее тесно связан с предупреждением и борьбой с ЧС Департамент по борьбе с пожарами и аварийными ситуациями (Fire and Rescue Force). В за-

дачи этого департамента входят предупреждение и минимизация рисков природного и техногенного происхождения: пожары, наводнения, землетрясения, дорожно-транспортные происшествия и другие ЧС.

Департамент находится в подчинении заместителя министра и имеет следующие подразделения:

- пожарной безопасности;
- оперативной деятельности;
- административное управление;
- юридический отдел;
- региональные пожарные отделы;
- пожарные и аварийные станции;
- колледж по подготовке специалистов в сфере борьбы с ЧС (пожарное дело и др.).

Функции Департамента:

- инициировать, развивать, анализировать и проводить деятельность по предупреждению и ликвидации ЧС;
- усиливать профессиональную подготовку в сфере предупреждения и ликвидации ЧС;
- усиливать управление службами по ЧС;
- развивать и поддерживать услуги по предупреждению и ликвидации ЧС на национальном уровне.

Учитывая природную и социально-экономическую специфику страны, Департамент имеет различные программы деятельности, которые посвящены таким направлениям деятельности, как: техническое обновление оборудования, медицинскую подготовку кадров, связи с общественностью, повышение квалификации сотрудников, выполнение работ по тематике ЧС в морских условиях, развитие международного сотрудничества в сфере борьбы с ЧС – особенно с соседними странами. К деятельности Департамента относится также консультирование правительства и соответствующих организаций по вопросам предупреждения ЧС в промышленности, в том числе – на нефтяных и газовых объектах.

Развитие деятельности Департамента в целом направлено на обеспечение экологической безопасности и здоровья населения в соответствии с национальными и международными стандартами.

Очевидно, что деятельность по предупреждению чрезвычайных ситуаций и борьбе с их последствиями требует решения многих организационных вопросов. Среди них – развитие и совершенствование законодательства, создание национальной инфраструктуры по борьбе с ЧС, профессиональная подготовка кадров, создание базы данных и проведение мониторинга, а также обеспечение финансирования комплексной деятельности по предупреждению ЧС и ликвидации последствий чрезвычайных ситуаций природного и техногенного характера.

Как было показано в кратком обзоре современного состояния деятельности по борьбе с ЧС в ряде африканских стран, в этом регионе ведется целенаправленная работа, направленная на обеспечение экологической безопасности

населения. Одним из важных аспектов успеха деятельности в данном направлении является укрепление международного сотрудничества, которое позволяет объединять имеющиеся ресурсы. При этом в африканском регионе остается много нерешенных проблем, для которых будет полезен учет международного опыта, в том числе и России.

УДК 656.085

Воробьев А.Е., Тахир Муса

Прогнозирование последствий чрезвычайных ситуаций на нефтепроводах

Эксплуатации нефтепровода является опасным для персонала, населения и окружающей среды. Этот риск характеризуется следующей спецификой основных нефтепроводных систем:

• значительной протяженностью линейной части нефтепровода;

• большой массой циркуляцирующих опасных веществ в системе;

• пожарной опасностью, высокой биологической активностью перекачиваемого продукта (нефти),

• способностью вызывать неблагоприятное воздействие на людей и экосистемы окружающей среды.

Нефтепроводный транспорт жидких и газообразных углеводородов, отнесен к категории «А» третьей группы, куда включены пожаровзрывоопасные объекты и СТС, на которых они хранятся.

В дальнейшем, транспортируемые продукты, при определенных условиях приобретают способность к возгоранию или взрыву, загрязнению окружающей среды, поэтому при авариях и отказов они представляют значительную угрозу населению, инженерным сооружениям и природным объектам.

Поэтому к нефтепроводам и нефтехранилищами предъявляются высокие требования по обеспечению надежности и безопасности их функционирования.

Нефтепроводные системы уже в настоящее время покрывают 35 % территории России, на которой проживает 60 % ее населения. В густонаселенной европейской части 2,8 тыс. зданий и сооружений находятся на минимально допустимом расстоянии от магистральных нефтепроводов. 15 тыс. раз эти магистрали пересекают железные и шоссейные дороги, 2 тыс. раз реки, каналы и озера.

По данным Госгортехнадзора с 1992 по 2001 гг. на магистральных нефтепроводах произошло 545 аварий.

В 2001 г. на внутрипромысловых нефтепроводах произошло 42 тыс. случаев разгерметизации. На рельеф местности вылилось свыше 60 тыс. $м^3$ нефти и пластовой воды.

Выброс нефти в окружающую среду в результате аварии является главной возможной опасностью в работе и эксплуатации магистральных нефтепроводов.

Согласно действующим нормативным документам, под параметрами «Риск» (либо «Степень риска») принимаются соответственно комбинация 2-х элементов – вероятности (частоты) конкретного опасного события и серьезности его последствий.

При оценивании риска чрезвычайных ситуаций обычно учитываются:

- оценка вероятности наступления чрезвычайной ситуации;
- определение количества опасных веществ, которые могут участвовать при инциденте;
- установление площади разлива нефти и зон взрывоопасных концентраций в ходе испарения нефти;
- оценка возможных последствий чрезвычайного происшествия для человека, окружающей среды и инфраструктурных объектов.

В процедуру оценки риска чрезвычайных ситуаций входит:

- прогноз частоты (вероятности) возникновения чрезвычайных ситуациях;
- оценка количества опасных веществ, способных участвовать в чрезвычайных ситуациях;
- определение площади разлива нефти, а также зоны взрывоопасных концентраций при испарении нефти с поверхности разлива;
- оценка последствий чрезвычайных ситуаций для человека, окружающей природной среды и самого объекта.

УДК 65.011.56

Голь С.А., Борисов А.Г., Леушкин В.С., Лукша С.С.

Типовые навигационные сценарии робототехнических комплексов

Мощный импульс к интенсификации исследований в области применения мобильных робототехнических комплексов (далее - МРТК) к задачам инженерно-технической безопасности и экологии дала авария на АЭС Фукусима-1. Опыт применения телеуправляемых устройств показал, что востребованы значительно большие показатели автономности функционирования и времени автономной работы, чем могут предложить существующие на рынке решения. Для определения направлений развития информационно-управляющих систем современных МРТК необходимо обозначить основные задачи, решаемые комплексами, а также сформулировать и исследовать в полевых условиях сценарии применения МРТК. Частным случаем сценария применения является навигационный сценарий - набор приемов и правил, определяющий траекторию и режим движения МРТК в процессе его практического применения

Основные задачи, решаемые наземными МРТК, сформулированы по итогам научно-практической конференции «Перспективы развития роботизированных комплексов и БПЛА», проходившей в сентябре 2014 года. К ним относятся:

1. Исследование аварийных зон. Данная задача подразумевает множество взаимосвязанных подзадач: визуальный контроль территории,

сооружений и оборудования; радиационный и химический контроль; анализ состояния технологического оборудования; выявление мест и характера повреждений; поиск объектов с заданными характеристиками, в том числе людей, нуждающихся в эвакуации.
2. Доставка оборудования и материалов в аварийную зону, вывоз опасных объектов в зону утилизации.
3. Очистные работы, работы по обеззараживанию местности, помещений и оборудования; пожаротушение.

Большинство из этих задач должны решаться в различное время суток, зачастую круглосуточно, в сложных погодных и природных условиях, при воздействии дополнительных мешающих факторов.

Указанные выше задачи позволяют выделить следующие основные навигационные сценарии МРТК:

1. «Конвой» (следуй за мной) - следование за ведущим: человеком, транспортным средством или телеуправляемым робототехническим комплексом. Ведущий определяет маршрут и конечную цель движения, задача МРТК - двигаться на заданной дистанции от ведущего по определенной им траектории. В ходе движения необходимо отслеживать возникающие на пути препятствия.
2. «Мул» - челночное движение по заданному маршруту. Маршрут задается либо в виде траектории движения, либо в ходе обучения. Чаще всего в процессе обучения используется предыдущий сценарий: МРТК следует за ведомым из начальной точки в конечную, а в дальнейшем самостоятельно передвигается по маршруту в прямом и обратном направлении. В ходе движения по маршруту необходимо отслеживать возникающие препятствия и принимать все возможные меры по их преодолению или огибанию.
3. «Рекогносцировка» - автономное построение маршрута и движение по построенному маршруту. Маршрут строится таким образом, чтобы обеспечить наиболее полное исследование некоторой территориальной области на местности. Область построения маршрута часто имеет нечетко определенные границы. Карта исследуемой территориальной области либо недостоверна, либо полностью отсутствует.

Разработки студенческого конструкторского бюро РГРТУ реализуют перечисленные выше навигационные сценарии в построенных исследовательских МРТК как по отдельности, так и в комплексном варианте. Сценарии прошли неоднократные полевые тесты и практическую отработку в ходе испытаний на российском и международном уровнях (полевые испытания «Робокросс» в г. Нижний Новгород, M-ELROB, г. Варшава). Результаты испытаний показывают перспективность выбранного направления исследований и пути совершенствования программного и аппаратного обеспечения исследовательских МРТК.

Библиографический список

1. Nagatani, K., Kiribayashi, S., Okada, Y., Otake, K., Yoshida, K., Tadokoro, S., Nishimura, T., Yoshida, T., Koyanagi, E., Fukushima, M., Kawatsuma, S. Emergency response to the nuclear accident at the Fukushima Daiichi Nuclear Power Plants using mobile rescue robots. Journal of Field Robotics, 30(1):44–63.

2. Wirth, S., Pellenz, J.: Exploration transform: A stable exploring algorithm for robots in rescue environments. Proc. IEEE Intl. Workshop Safety, Security, and Rescue Robotics (2007) 1–5

3. Борисов А.Г., Голь С.А., Корнеев В.Е. Открытая аппаратная платформа для тестирования программного обеспечения беспилотного автомобиля // Вестник РГРТУ. № 4 (вып. 46, ч. 3). Рязань, 2013. С. 50 – 55.

4. Артёмкин В.В., Лукша С.С., Маликов А.Ю. Реализация сценария «следуй за мной» беспилотной системы управления автомобилем-роботом на основе данных лидара и видеодатчика // Вестник РГРТУ. № 4 (вып. 46, ч. 3). Рязань, 2013. С. 28 – 34.

УДК 65.012.8

Гостин А.М., Сапрыкин А.Н.

Информационная безопасность открытого программного обеспечения

Когда мы говорим об информационной безопасности програмного обеспечения (ПО), мы предполагаем, что данное ПО должно отвечать неким заданным базовым требованиям безопасности, например, уровню отсутствия недекларируемых возможностей, степени криптоустойчивости и т.д. Эти требования могут существенно отличаться, в зависимости от целей и задач, стоящих перед пользователями. Поэтому в целом об информационной безопасности открытого ПО можно говорить очень условно и только после проведения сравнительного анализа, имея некоторые усредненные статистические показатели.

Проведенный в 2014 году анализ более 1500 проектов с открытым кодом зарубежной фирмой Coverity выявил, что количество найденных уязвимостей в открытом ПО в целом сравнимо с количеством уязвимостей проприетарного ПО, хотя и немного меньше для средних проектов. Эксперты отмечают, что хорошим результатом развития открытого ПО также является неуклонное уменьшение среднего времени исправления уязвимостей.

Вместе с тем стоит отметить, что некоторые уязвимости, например, такие как известная критическая уязвимость Heartbleed в реализации библиотеки OpenSSL, случайно обнаруженная в 2014 году, могут годами оставаться нераскрытыми. Отчасти это свидетельствует о невысоком профессионализме части разработчиков и недостаточном внимании администраторов к вопросам информационной безопасности своих проектов.

Существует ряд особенностей открытого ПО, отличающих его от проприетарного ПО:

1. Открытое ПО не более и не менее безопасно, чем проприетарное. Это подтверждается вышеприведенными статистическими исследованиями, которые показывают не худшие результаты для открытого ПО.

2. Открытое ПО не проще деструктивно модифицировать. Во-первых, модификацию открытого кода легче обнаружить. Во-вторых, злоумышленники модифицируют чаще всего не исходные коды, а загружаемые файлы, что не зависит от открытости ПО. Тем не менее, риск деструктивной модификации может оставаться в больших проектах, где его сложнее обнаружить. Так ядро Linux содержит более 20 млн. строк исходного кода.

3. Открытое ПО в целом не хуже из-за того, что его может писать любой желающий. Несмотря на некоторые проблемы и риски, связанные с неквалифицированной разработкой, во многих случаях качество открытых проектов не уступает проприетарному софту.

4. Открытое ПО не означает беспрепятственное его использование. Возможность использования ПО в том или ином случае определяется видом лицензии и условиями лицензирования. В настоящее время существует более 20 видов лицензий открытого ПО. Открытое не означает бесплатное.

5. Использование пакетов и патчей из недостоверных источников может привести к нарушению безопасности. Как и в случае с проприетарным софтом, для загрузки обновлений открытого ПО необходимо использовать официальные репозитории.

6. «При достаточном количестве глаз баги выплывают на поверхность». Пресловутый закон Линуса предполагает неоспоримое преимущество открытого ПО. На деле же лишь небольшое количество экспертов может оценить безопасность коммитов отдельно взятого приложения. Более верный тезис: «Большое количество глаз - это всего лишь множество ресниц».

7. В целом все большая часть пользовательских функций реализуется с помощью открытого ПО. Определенное движение в этом направлении за последние годы показывает, что открытое ПО становится более качественным, функциональным и востребованным.

8. Использование того или иного вида продукта все чаще зависит от личных предпочтений пользователя и его привычек, а не от действительных характеристик ПО. Этот тезис иллюстрируется появлением на рынке мобильных устройств открытой платформы Android, базирующейся на ядре Linux.

Открытое ПО все чаще декларируется в качестве исходной базы для национальных платформ. Рассматривая это явление с позиции информационной безопасности мы видим, что увеличение количества используемого открытого ПО в школах, университетах и других бюджетных учреждениях прямо ведет к уменьшению финансовой зависимости от крупных зарубежных фирм - разработчиков софта, таких как Microsoft, Adobe Systems, Autodesk Inc. и др. Понимая это, коммерческие разработчики вынуждены конкурировать с открытым софтом и даже распространять свои нара-

ботки в рамках открытых и полуоткрытых лицензий с целью привлечения внимания к своим технологиям, например IBM или Oracle.

В заключении можно сказать, что в настоящее время мы наблюдаем эволюцию открытого ПО, которое может использоваться в решении самых различных задач, причем использование этого ПО также может быть безопасным.

УДК 504.064

Гудзев В.В., Шилин А.В.

Снижение токсичности процесса пробоподготовки биообъектов для исследований в растровом электронном микроскопе атомно-силовом

Большинство веществ, которые используют для подготовки биологических материалов в лабораториях растровой электронной микроскопии и лабораториях атомно-силовой микроскопии, являются токсичными, следовательно, опасными для работников лаборатории. Целью проводимой работы является разработка методики подготовки биообъектов для исследования в растровом электронном микроскопе (РЭМ) и атомно-силовом микроскопе (АСМ), которая позволит сохранить структуру образца и снизить токсичность процесса пробоподготовки.

Для исследования биологических объектов на АСМ был использован метод, при котором исследуемый образец иммобилизируется на предметном стекле.

1. Взвесь клеток (10-20 мкл) наносится на чистое предметное стекло, обработанное спирт-эфиром и промытое под проточной водой.
2. Клетки распределяются ровным слоем на предметном стекле. Толщина мазка убывает вдоль направления размазывания.
3. Стекло высушивается на чистой сухой поверхности.
4. Выбирается область, где клетки расположены в один слой. Сканирование проводится в полуконтактном режиме.

Методика проведения подготовки биообразцов для исследования в РЭМ следующая:

1. Взятие пробы. Величина образца ограничена размерами камеры микроскопа и предметным столиком (200 мм диаметром, 80 мм толщиной).
2. Промывка в тёплом растворе Хенкса. Раствор Хэнкса представляет собой раствор неорганических солей и глюкозы в очищенной воде. Не токсичен. Предназначен для работ с культурами клеток.
3. Фиксация образца 2% глутаральдегидом на 0,1М фосфатном буфере (pH=7,2 - 7,4). Продолжительность фиксации 1 - 4 часа (зависит от размеров и плотности образца). Замена раствора 4 раза.
4. Промывка образца в трёх сменах фосфатного буфера в течение 5 минут каждая. Фосфатный буфер является изотоническим и нетоксичен для клеток.
5. Обезвоживание в растворах этилового спирта различной концентрации (60%, 70%, 80%, 90%, 100% - 2раза) по 10 минут в каждой порции. Преимущество данного вида обезвоживания в том, что образец не подвергается внезапным измене-

ниям концентрации и поэтому не деформируется. Так как дозы этилового спирта крайне малы и контакт с ними не превышает 1 часа, вдыхание паров не приведет к опасным воздействиям на организм человека. Чтобы избежать попадания спирта на кожу рук следует проводить работу в резиновых перчатках.

6. Сушка образца

6.1. В случае наличия на поверхности объекта ворсинок и выростов применяется сушка в критической точке.

6.2. В иных случаях возможно использование сушки на воздухе.

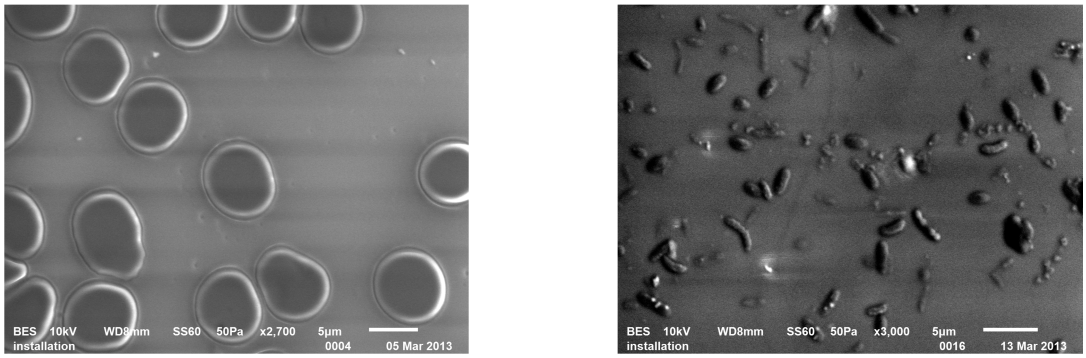


Рисунок 1. РЭМ-изображения клеток крови (слева) и бактерий (справа).

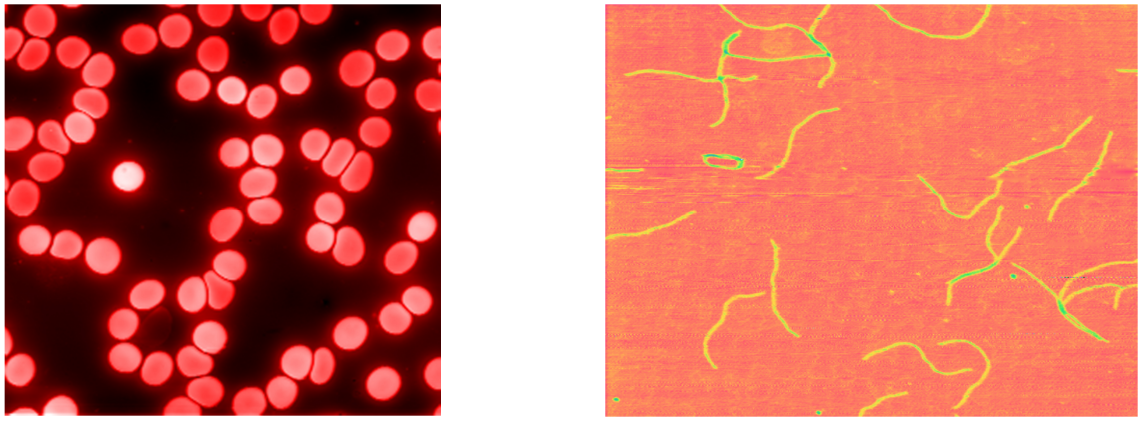


Рисунок 2. АСМ-сканы клеток крови (слева) и ДНК плазмиды (справа)

УДК 331.45

Зайцев Ю.В.

Особенности специальной оценки условий труда

Одна из составляющих безопасности любой организации – защищённость её персонала от вредных и опасных производственных факторов. Кроме того, безопасные условия труда расцениваются работниками как достойный труд, позволяющий достичь высоких результатов деятельности.

С 1 января 2014 г. во всех организациях введена специальная оценка условий

труда (СОУТ) рабочих мест [1], которая призвана заменить существовавшую до того аттестацию рабочих мест по условиям труда. СОУТ несколько отличается от аттестации рабочих мест по условиям труда.

Процесс аттестации рабочих мест складывался из двух частей: идентификации опасностей и реализации мер по их устранению.

В определении СОУТ, которое дано в законе [1], отсутствует упоминание о необходимости приведения условии труда в соответствие с государственными нормативными требованиями. Получается, что условия труда просто оцениваются без дальнейшего их улучшения. В законе даже не упоминается о льготах за неблагоприятные условия труда, а вместо этого говорится о каких-то гарантиях.

Не совсем понятны разъяснения относительно аналогичных рабочих мест, которые находятся в однотипных помещениях, с однотипными оборудованием, технологическим процессом, материалами. Практика аттестации рабочих мест по условиям труда показывает, что перечисленные показатели не гарантируют аналогичности рабочих мест.

СОУТ не проводится для рабочих мест, которые включены в списки, с учётом которых осуществляется досрочное назначение трудовой пенсии или на которых работникам предоставляются гарантии и компенсации за работу с неблагоприятными условиями труда. Таким образом, СОУТ не проводится на рабочих местах с заведомо вредными и опасными условиями труда, что противоречит ст. 212 Трудового кодекса РФ.

Методика специальной оценки условий труда, вступившая в действие с 8 апреля 2014 г. [2] позволила реализовать задачу по сокращению оснований для установления вредных условий труда на значительной части рабочих мест. Это затрагивает все офисные рабочие места и места, оборудованные ПЭВМ по факторам естественного освещения, пульсации освещения, напряжённости труда, так как эти показатели были исключены в методике. Именно эти показатели давали вредные условия труда на большинстве рабочих мест офисных работников.

Из исследуемых факторов исчез контактный ультразвук, хотя в производственных условиях контактный и воздушный ультразвук неразрывны.

В указанном законе [1] отдаётся приоритет средствам индивидуальной защиты (СИЗ) работников вместо средств коллективной защиты (СКЗ). Однако среди защитных мер приоритет всегда отдавался и отдаётся СКЗ, а СИЗ применялись в крайних случаях. Использование СИЗ не только не устраняет вредные факторы в рабочей зоне, но и затрудняет работу, снижает производительность труда. В результате вредный фактор как таковой не устраняется, а условия труда формально считаются улучшенными. Таким образом, «обеспечения приоритета сохранения жизни и здоровья работников» (ст. 210 ТК РФ) не наблюдается.

Законом [1] определено декларирование соответствия условий труда нормативным требованиям охраны труда. При этом эксперт «при помощи своих органов чувств осуществляет идентификацию опасных или вредных факторов на рабочих местах». Если таковые им не обнаружены, то условия труда признаются допустимыми, а работодатель получает возможность их декларировать на 5 лет с последующим про-

длением срока ещё на 5 лет. Нельзя не отметить, что говорить о наличии или об отсутствии производственных факторов можно только после измерения характеристик среды рабочей зоны и оценки показателей тяжести и напряжённости трудового процесса. Что касается их идентификации согласно статье 10 Закона, то она, как представляется, может носить субъективный характер. Считаю такой метод оценки условий труда очень сомнительным.

Если на задекларированном рабочем месте происходит несчастный случай или профессиональное заболевание, действие декларации для данного рабочего места прекращается и проводится внеплановая специальная оценка условий труда на данном рабочем месте. При этом даже аналогичных рабочих мест эта процедура не касается.

В стране ещё не сформирована система отношений, способствующих сохранению и укреплению здоровья работающего человека, отсутствует ответственность работодателей в принятии конкретных мер по обеспечению безопасности условий труда. Необходимо отметить, что СОУТ является коммерческой услугой, навязанной работодателю, которая ограничивают его предпринимательскую свободу и приносит экономический ущерб, не улучшая условий труда.

Список использованной литературы:

1. Федеральный закон от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда».
2. Методика проведения специальной оценки условий труда (утв. приказом Минтруда России от 24.01.2014 № 33н).

УДК 504.064

Зубков М.В., Шилин А.В.

Использование метода атомно-абсорбционной спектроскопии для определения тяжелых металлов

Основные области применения атомно-абсорбционных спектрометров — медицина, контроль объектов окружающей среды, анализ пищевых продуктов и сырья для их изготовления, геология, металлургия, химическая промышленность, научные исследования.

Преимущество метода атомной абсорбции перед многими методами анализа состоит в его высокой селективности, скорости, точности низких пределах обнаружения элементов, в простоте подготовки проб к анализу, поскольку в большинстве случаев отпадает необходимость проведения операций, связанных с отделением мешающих элементов, а также в универсальности конечной продукции анализа, т.е. возможности определения нескольких элементов-примесей из одного раствора по единой методике с получением конечных результатов в единицах концентрации. Он может быть также успешно применен при анализе проб нестандартного состава в случае относительно больших концентраций определяемых элементов.

Разработка атомно-абсорбционного спектрометра позволит повысить уровень существующих разработок, расширить область применения прибора. В связи с вышеуказанным разработка атомно-абсорбционного спектрометра является технически обоснованной и экономически целесообразной.

Атомно-абсорбционный анализ используется в клинических анализах крови, сыворотки и т.д. на свинец, ртуть, висмут и другие элементы. Образец вносят в пламя, аналогично пламенному фотометру, в результате чего оно начинает поглощать свет с длиной волны, характерной для данного элемента. Поглощается очень узкая полоса света (доли нанометра). Поэтому для измерений необходим линейчатый источник света. В качестве такого источника служат специальная лампа, внутри баллона которой находятся разогретые пары того самого элемента, концентрация которого определяется. Лампа питается от источника 500…600 В с погрешностью не более сотых долей процента. Необходимость установки для каждого определяемого элемента своего источника возбуждения конструктивно усложняет прибор, так как каждую лампу необходимо юстировать. В качестве монохроматора используется дифракционная решетка, а интенсивность излучения измеряется с помощью ФЭУ.

Разработана функциональная схема установки атомно-абсорбционного анализа (рисунок 1).

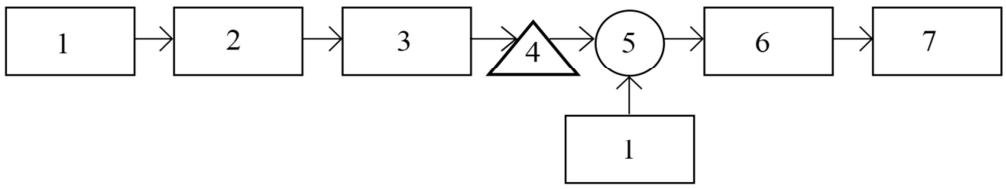


Рисунок 1. Функциональная схема установки атомно-абсорбционного анализа:
1 – высоковольтный стабилизатор; 2 – лампа с полым катодом;
3 – горелка; 4 – монохроматор; 5 – фотоэлектронный умножитель;
6 – измерительный блок; 7 – ЭВМ.

Сама установка представляет собой сложное устройство, поэтому на первом этапе стоит задача разработки измерительного блока (рисунок 2).

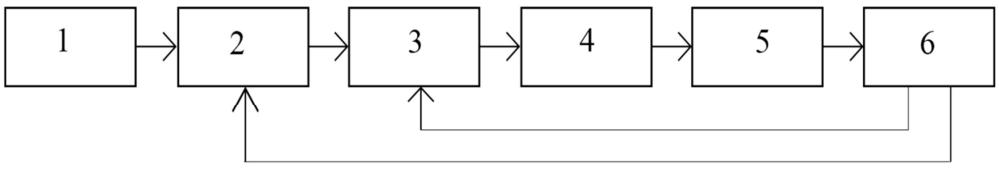


Рисунок 2. Функциональная схема измерительного блока атомно-абсорбционного анализа: 1 – высоковольтный стабилизатор; 2 – лампа с полым катодом; 3 – интегратор; 4 – логарифматор; 5 – горелка;
6 – микроконтроллер.

УДК 504.064

Зубков М.В., Шилин А.В.

Разработка алгоритма работы блока атомарно-абсорбционной спектроскопии

Алгоритм работы устройства представлен на рисунке 1.

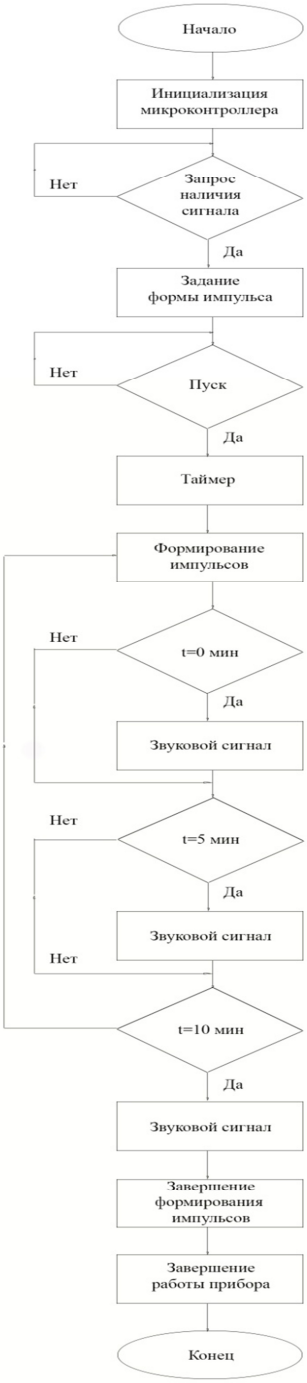


Рисунок 1. Алгоритм работы

После включения кнопки «СЕТЬ», происходит инициализация микроконтроллера. Затем происходит запрос наличия сигнала микроконтроллером. Микроконтроллер ждет задачи формы импульса. Она осуществляется нажатием на кнопку

«Режим». После выбора формы импульса и нажатия кнопки «Пуск» происходит запускание таймера и формирование импульсов.

Продолжительность проведения атомно-абсорбционного анализа (15±2) мин. После пяти минут работы устройство подает звуковой сигнал, после 10 минут работы подается двойной звуковой сигнал и после пятнадцати минут работы подается тройной звуковой сигнал и прекращается подача импульсов.

Затем после повторного нажатия кнопки «СЕТЬ» происходит завершение работы прибора, и все процессы в нем прекращаются.

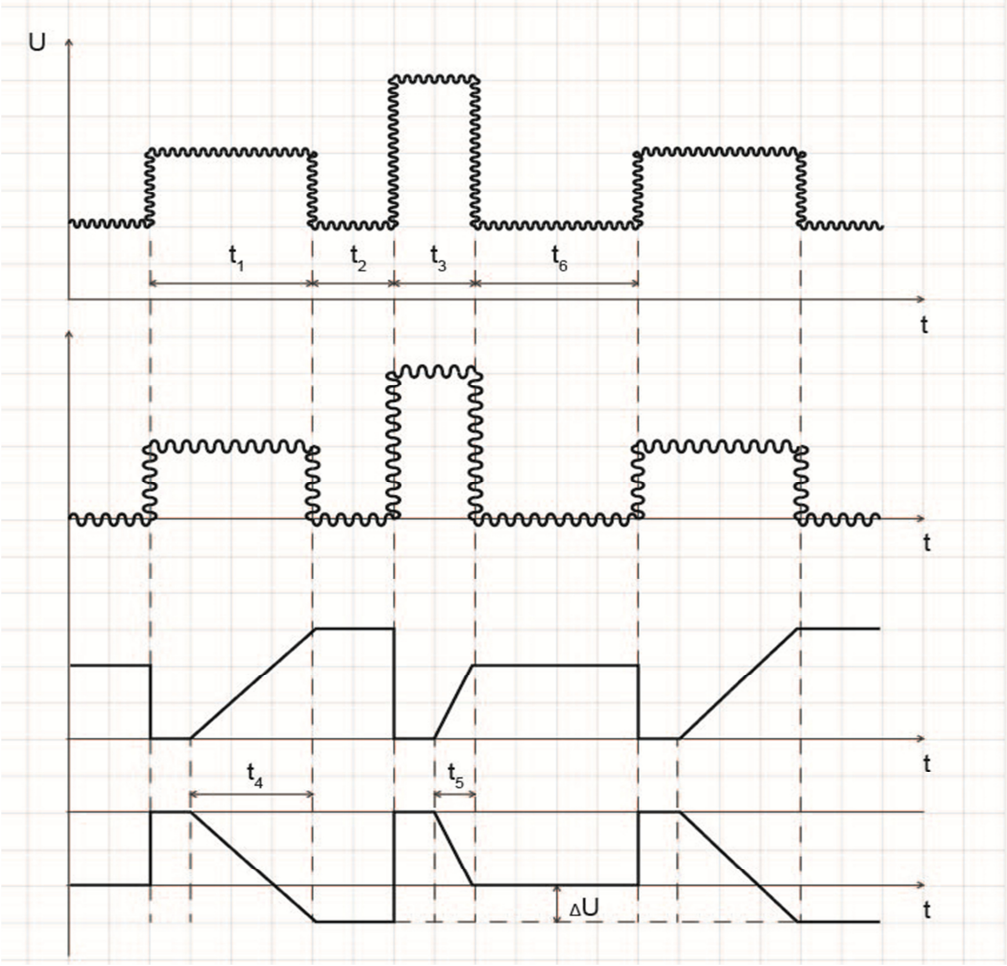


Рисунок 2. Форма сигнала с выхода вычитающего устройства.

УДК 796.8

Зудашкин Г.Н., Фокин А.Н.

Организация специальной физической подготовки с членами студенческого отряда охраны правопорядка

Созданный в октябре 2008 года студенческий отряд охраны правопорядка (далее – СООПр) Рязанского государственного радиотехнического университета (далее – РГРТУ), принимает активное участие в обеспечении непосред-

ственно или совместно в ОВД охраны общественного порядка в помещениях университета, студенческого городка и на ближайших территориях. СООПр с 2013 г. формируется, как правило, из числа студентов, проходящих обучение в военно-учебном центре и на военной кафедре РГРТУ.

Для успешного выполнения основных задач с бойцами СООПра организованы дополнительные занятия по специальной физической подготовке. Занятия проводятся по расписанию, утвержденному проректором по режиму и безопасности, по программе, разработанной кафедрой физического воспитания университета на основе рабочих программ специализированных учебных заведений правоохранительных органов (МВД, ФСИН, ФСКН, МЧС). Занятия проводят преподаватели, имеющие соответствующий спортивно-педагогический опыт. Программа рассчитана на 64 часа в год (2 часа в неделю) и имеет следующий тематический план по 4-ем разделам.

Раздел №1 «Общая физическая подготовка» (18 часов):

тема 1 - легкая атлетика и ускоренное передвижение;

тема 2 - атлетическая гимнастика;

тема 3 - преодоление препятствий типа «город».

Раздел №2 «Специальная физическая подготовка» (24 часа):

тема 1 - способы задержания, сопровождения, сковывания действий;

тема 2 - техника рукопашного боя, удары, защита от ударов, броски;

тема 3 - использование подручных средств самообороны, активной защиты и нападения;

тема 4 - применение спецсредств.

Раздел №3 «Тактика применения специальных средств» (20 часов):

тема 1 - специальные средства;

тема 2 - средства активной обороны и защиты;

тема 3 - взаимодействие в составе групп.

Раздел №4 «Прием контрольных нормативов по общефизической и специальной подготовке» (4 часа).

Из бойцов СООПра организованы 3 учебные группы, распределенные по состоянию физической подготовленности бойцов: 1 группа – спортсмены разрядники, имеющие навыки в различных видах единоборств (борьба, рукопашный бой, бокс и пр.); 2 группа – студенты с высоким уровнем физической подготовленности (как правило, выпускники ДЮСШ по игровым видам спорта, легкой атлетике и пр.); 3 группа – студенты, способные по своим деловым, моральным качествам и состоянию своего здоровья осуществлять охрану общественного порядка, но не имеющие достаточного уровня физической подготовленности.

В зависимости от распределения, занятия по группам проводятся с конкретной направленностью: повысить уровень основных физических качеств (сила, выносливость, скорость, ловкость), овладеть специальными навыками и умениями, оказать первую медицинскую (доврачебную) помощь при неотложных ситуациях, а так же по безопасности жизнедеятельности членов СООПра.

УДК 624.9

Конон Н., Бергер А.

Задача обеспечения индивидуальными средствами спасения с высотных зданий должна стать государственной

В проблеме комплексной безопасности населения мегаполисов России нерешенным до настоящего времени остается вопрос спасения людей в чрезвычайных ситуациях находящихся в высотных зданиях и сооружениях.

Различные программы, в числе которых аппаратно-программный комплекс «Безопасный город», утверждённый распоряжением Правительства РФ от 3 декабря 2014 г. № 2446-р, оставляют без внимания и никак не решают важнейшую задачу при угрозе жизни и здоровья людей в чрезвычайных ситуациях – их защита и спасение с мест чрезвычайных ситуаций и происшествий.

Общеизвестно, что при террористических и техногенных угрозах, а также пожарах высшей и средней категории, в первую очередь, выходят из строя штатные пути эвакуации граждан (запасные выходы, лестничные пролёты и т.д.). А отсутствие в помещениях, где работают и живут люди индивидуальных средств спасения, отнимает у них надежду на спасение с высотного здания в любой чрезвычайной ситуации.

К сожалению, на сегодня нормативные и правовые документы в этой области не соответствуют требованиям времени и необходимому уровню защищенности человека в чрезвычайной ситуации. К примеру, в течение нескольких лет дорабатывается, но не принимается остро необходимый современный свод правил СП «Средства индивидуальной защиты и спасения людей при пожаре. Нормы и правила размещения и применения», в котором сформулированы требования к оснащению и применению индивидуальной защиты и спасения людей при пожаре в строящихся, сданных в эксплуатацию и реконструируемых сооружениях. Указанный регламентирующий и законодательный документ определяет нормы и обязывает собственника размещать в помещениях, где находятся люди, индивидуальные средства защиты и спасения с высотных зданий и сооружений, для которых расчётная величина индивидуального пожарного риска превышает установленные законодательством допустимые значения, что является конкретной мерой по снижению гибели людей, находящихся в таких зданиях, и тем самым способствуют снижению финансовой нагрузки на государство по выплате компенсаций в случаях гибели людей при пожарах в высотных зданиях и сооружениях. Следовательно, оснащение высотных зданий и сооружений средствами индивидуальной защиты в разы увеличивает безопасность и является тем фактором, который окажет положительное влияние и приведёт к экономии бюджетных средств.

В «Правилах противопожарного режима в Российской Федерации» имеется упоминание о необходимости содержать в исправном состоянии индивидуальные средства спасения, но в нем также не прописана такая норма оснаще-

ния мест нахождения людей необходимым количеством индивидуальными средствами спасения с высоты.

Однако, несмотря на отсутствие указанных необходимых законодательных документов, отечественные производители предлагают пути решения данной проблемы и уже сегодня разрабатывают индивидуальные средства спасения с высоты при пожарах и других чрезвычайных ситуациях. Так, закрытое акционерное общество «Международный институт геоинформатики» серийно выпускает инновационный конкурентоспособный продукт исключительно российского производства – канатно-спускное устройство «Спасмиг», которое принадлежит к классу индивидуальных спасательных средств и по важнейшим характеристикам превосходит зарубежные аналоги, в том числе по таким характеристикам, как по высоте зданий и сооружений, так и по допуску веса, также и по массе изделия, а главное достоинство нашего средства – это цена, позволяющая экономить бюджетные средства в миллиардных объемах! Указанное спасательное устройство имеет сертификат соответствия от 4.12.2014 г. № С- RU.ПБ04.В.02116, выданный органом по сертификации ФГБОУ ВПО Академия ГПС МЧС России и подтверждающий, что устройство «Спасмиг» соответствует требованиям технических регламентов о требованиях пожарной безопасности (Федеральный закон от 22.07.2008 г. № 123-ФЗ), ГОСТ Р 53272-2009.

Особо отметим, что индивидуальное спасательное устройство «Спасмиг» неоднократно представлялось на международных и отечественных выставках, на пресс-конференциях и презентациях. В ходе рабочих встреч с руководителями различных ведомств, на семинарах и других мероприятиях идея создания такого устройства горячо поддерживается. Однако организация обеспечения российских потребителей нашим устройством сталкивается с серьёзными трудностями.

Особую актуальность приобретает проблема обеспечения российских организаций и граждан индивидуальными средствами спасения в связи с требованием Президента Российской Федерации по импортзамещению товаров ввозимых в Россию на продукцию отечественных производителей.

К сожалению, приведение к современным требованиям комплексной безопасности указанных нормативных и правовых документов практически невозможно из-за бюрократического противодействия некоторых чиновников и фактически тормозит выполнение прямых указаний и требований Президента Российской Федерации и полностью им противоречит.

Также хотелось бы отметить, что ЗАО «Международный институт геоинформатики» занимается не только созданием индивидуальных спасательных средств в области пожарной безопасности, но и разработками и внедрением инновационных проектов в других областях.

Например, уже реализован проект и подготовлен к серийному производству инновационный продукт – растворимый кофе в твёрдой форме. Совместно с другими отечественными предприятиями ведётся разработка проектов по созданию высокоскоростных амфибийных транспортных средств для специальных служб, в том числе и МЧС, системы мониторинга акваторий морских пор-

тов роботизированными планирующими аппаратами (глайдерами), современные системы утилизации бытовых отходов и другие.

Таким образом, содействие и поддержка в организации обеспечения российских потребителей отечественными индивидуальными спасательными средствами позволит сберечь для общества тысячи жизней российских граждан, оказавшихся в очаге пожара и другой чрезвычайной ситуации в высотных зданиях.

УДК 65.012.4

Мандур А.С., Фокин А.Н., Чернышев С.В.

Опыт привлечения студентов, обучающихся на военной кафедре, в студенческий отряд охраны правопорядка РГРТУ

РГРТУ исторически является важнейшим кадрообразующим учебным заведением г. Рязани и Рязанской области. Его выпускники работают на многих предприятиях региона, в различных учреждениях, органах власти и силовых структурах. В результате проводимых в последнее время реформ в МВД, ФСБ и других силовых структурах возникла острая потребность в технически подготовленных кадрах, способных работать со сложной техникой. Однако, помимо технической грамотности, выпускники должны иметь хорошую правовую и физическую подготовку.

Данным критериям в полной мере соответствуют бойцы студенческого отряда охраны правопорядка (далее – СООПр) РГРТУ, который был создан в октябре 2008 г.

Изначально численность отряда составила 56 человек. В течение первых четырех лет существования он постоянно пополнялся добровольцами из числа студентов и сотрудников университета, при этом лица, закончившие обучение и прекратившие работу в университете, автоматически отчислялись из отряда в соответствии с положением о СООПр. Однако с 2012 года наблюдается спад добровольческой активности и численность отряда стала сокращаться. Так, к середине 2013 она составляла 26 человек.

При этом задачи стоящие перед отрядом неуклонно росли и усложнялись. Если в 2008 году СООПр выполнял свои задачи исключительно на территории учебных корпусов университета, то с 2013 года он работает на территории студенческого города, прилегающей уличной территории, стадиона, бизнес-инкубатора, бассейна. Кроме этого с 2009 года отряд совместно с сотрудниками полиции начал патрулирование территорий учебных корпусов и мест компактного проживания и отдыха студентов и сотрудников, в том числе пл. Театральной, ЦПКиО, ЦСК, ДС «Олимпийский». Также отряд активно взаимодействует по вопросам охраны правопорядка, профилактике правонарушений и преступлений с участковыми уполномоченными полиции и иными правоохранительными органами.

В связи со сложившейся ситуацией, руководство университета предложило привлечь к охране правопорядка наиболее дисциплинированных студентов уни-

верситета – студентов военной кафедры (ВК). При этом учитывалось, что в отряде проводится дополнительная физическая, правовая и психологическая подготовка, поэтому, прежде всего, предложение о вступлении в СООПр получили студенты ВК, которым было необходимо подтянуться по физической подготовке.

Всего предложение о вступлении в СООПр в 2013 г. получили 52 студента ВК, из них изъявили добровольное желание о вступлении в СООПр - 31 студент, 21 студент не захотели вступать в отряд, а 2 студента ВК записались в отряд самостоятельно. Зачисление в отряд проводилось на общих основаниях, при этом сдача тестов по физической подготовке не проводилась, так как студенты ВК данную дисциплину обязаны изучать в соответствии с учебными планами.

Все студенты ВК, вступившие в ряды СООПр, также изъявили желание вступить также и в отряд Добровольно-народной дружины г. Рязани при РГРТУ. Общая численность отряда вместе с кандидатами с декабря 2013года после вступления студентов с ВК составила 73 человека, из них – членов СООПР, зачисленных с военной кафедры – 33 человека (45%).

В связи с тем, что все члены СООПр должны были пройти трехмесячный испытательный срок, они активно участвовали в деятельности отряда, в ходе которой изучали правовые основы добровольчества в сфере охраны правопорядка, а также нормативно-правовые документы, регламентирующие соблюдение правопорядка и обеспечение безопасности внутри учебного заведения, общежитий и прилегающей территории.

В 2014 году работа по привлечения студентов в состав СООПр была продолжена. Предложение о вступлении в СООПр получили 67 студентов ВК, 25 из них отказались вступать в отряд, а 12 студентов ВК и учебно-военного центра (УВЦ) записались самостоятельно. Увеличение числа бойцов СООПр с ВК и УВЦ вызвано положительным опытом их работы в 2013 г., а также возникшим пониманием студентами более широкой возможности трудоустроится на перспективную, престижную и высокооплачиваемую работу за счет приобретения определенного опыта правоохранной деятельности, возникшими контактами с сотрудниками МВД, ФСБ и другими силовыми структурами. В настоящее время, численность СООПр составляет 86 человек.

Увеличение численности бойцов, их мотивация к работе и дисциплина позволили успешно решать задачи по вопросам охраны правопорядка в университете и в г. Рязани при проведении общественных мероприятий совместно с сотрудниками правоохранительных органов.

УДК 658.29

Кулибали М.

Управление охраной труда и промышленной безопасностью золотодобывающей компании в Республике Гвинея

Основными задачами охраны здоровья и систем управления безопасностью являются: реализация политики в области охраны труда и промышленной безопасности, соблюдения помещений, нормативные документы «Anglo Gold Ashanti»; обеспечение противо-аварийной устойчивости и снижение уровня травматизма; разработка, согласование и реализация (в соответствии со стратегическими целями и основными направлениями политики в области охраны труда и промышленной безопасности) программ, планов и других организационно-распорядительных документов; управление основными производственными рисками; обеспечение приемлемого уровня промышленной безопасности и охраны труда в структурных подразделениях «Anglo Gold Ashanti» [1].

Рис. 1: Структура системы управления охраной труда и промышленной безопасностью [3].

В решении перечисленных задач принимают участие все службы и работники компании, от генерального директора до рабочего, в соответствии с установленными для них функциями. Выполнение функций системы управления охраной труда и промышленной безопасностью (СУОТ и СУПБ) обеспечивается в рамках работы единой (жесткой) организационной структуры. Выполнение функций системы управления совершенствованием (СУС) предполагает создание гибкой организационной структуры, как показано выше на схеме, таким образом, что методики проекта БТ в рамках единой Бизнес Системы Северстали интегрируются в СУОТ и СУПБ, совершенствуя процессы управления безопасностью производства. Жесткая организационная структура

обеспечивает постоянное взаимодействие по обеспечению безопасности производства, определенные требованиями законодательных и нормативно-технических документов и корпоративными методиками безопасности труда. Инновационный элемент вводится в СУОТ и ПБ для повышения уровня безопасности производства и обеспечения эффективного развития. Структура СУС и методы ее работы основаны на лучших международных практиках и методологиях - «Du Pont», «International Labour Organization» (ILO), и переработаны под конкретные условия функциональной структуры «Anglo Gold Ashanti». Все функции системы управления охраной труда и промышленной безопасностью реализуются поэтапно, по универсальному алгоритму, основанному на принципе замкнутой системы управления [1,2]. Универсальный алгоритм реализации системы управления СУОТ и ПБ и контроля своевременности и качества их исполнения выглядят следующим образом:

- Планирование;
- Выполнение;
- Мониторинг;
- Корректировка.

Ответственность за выполнение каждого этапа, любой из функций СУОТ и ПБ закреплена за службами, отделами, участками и должностными лицами ОАО «Anglo Gold Ashanti».

Конкретные обязанности руководителей, специалистов и исполнителей по каждому этапу функций СУОТ, СУПБ и СУС изложены в должностных инструкциях, инструкциях по охране труда и безопасным методам производства работ для рабочих профессий, а также в «Положении о Системе управления охраной труда и промышленной безопасностью» - раздел «Распределение функциональных обязанностей в области охраны труда и промышленной безопасности между руководителями всех уровней управления предприятия» [2,3].

Литература:

1. Отчеты о функционирования золоторудного месторождения Сигири (Республика Гвинея) 2003-2013гг..
2. Mr El-Hadj Alpha Kabine Traore Administrateur Explorateur SIGUIRI GOLD MINE ANGLOGOLDASHANTI.
3. Аналитический выпуск «Проблемы национальной безопасности – 2» под ред. Кимлацкого О.А. М.: Совет Федерации, Аналитическое управление, www.council.gov.ru.

УДК 658.562

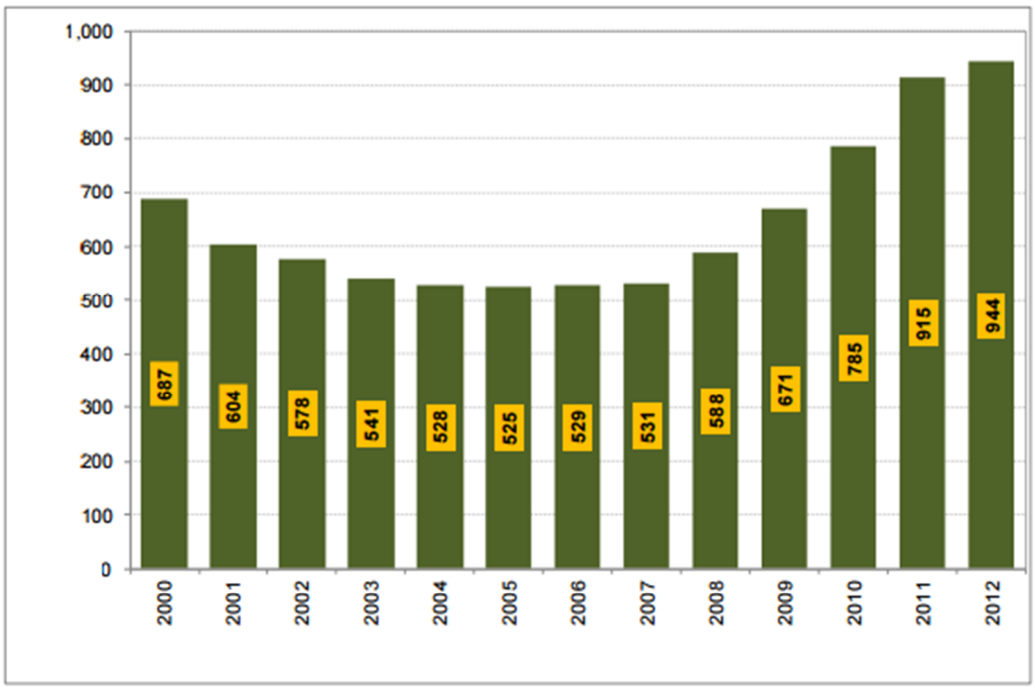
Нонато Х.Э., Альварадо М.Дж.Э.

Экологический аспект роста добычи нефти в Колумбии

До и после войн XIX века, когда в Колумбии эксплуатация природных ресурсов осуществлялась иностранными компаниями, такая эксплуатация привела к социальной войне 1940-х годов. В этот же период была создана первая нефтяная компания Колумбии «ECOPETROL».

Компания занималась эксплуатацией месторождений нефти и газа в Колумбии и принесла с собой радикальные изменения. В XX веке пейзаж джунглей в районах, где были обнаружены месторождения нефти, резко изменился и превратился в зону колонизации и зону пересеченных дорог и портов, в основных реках страны, таких как Рио-Магдалена или Ориноко, леса превратились в нефтяные скважины, вырубка и сжигание лесов для заготовки древесины и строительных материалов превратилась в повседневную жизнь в районах добычи нефти и полезных ископаемых в Колумбии.

Промышленное развитие принесло с собой не только разрушение и изменение пейзажа, а также перемещение местных жителей в районы плотной застройки и, следовательно, покидая поля. Экономической базой районов уже не являются ни сельское хозяйство, ни животноводство.



Ось асбцисс – годы.
Ось ординат – обьем добычи, в тысячах баррелей в день.

Рис. 1, Динамика роста объемов добычи нефти в Колумбии (2000-2012 гг.).

В заключение, на сегодняшний день Колумбия стремится исправить воздействие на окружающую среду, что вызвало эксплуатацию без разбора нефтяных ресурсов и минералов в первые десятилетия промышленного развития в стране.

СПИСОК ЛИТЕРАТУРЫ:

1. PLAN NACIONAL DE DESARROLLO MINERO [Электронный ресурс] – Электрон.дан. – Режим доступа: http://www.upme.gov.co/Docs/Plan_Minero/2012/PNDM2014.pdf // Unidad de Planeación Minero Energética – UPME Bogota D.C., 2012.
2. PLAN NACIONAL DE DESARROLLO MINERO [Электронный ресурс] – Электрон.дан. – Режим доступа: http://www.upme.gov.co/Docs/Plan_Nal_Des_Minero_2007_2010.pdf // Unidad de Planeación Minero Energética – UPME, ISBN: 978-958-98138-5-0. Bogotá, agosto de 2007.

УДК 504.054

Рожков С.В.

Программно-аппаратный комплекс «Мониторинг»

Одним из основных принципов организации комплексной системы экстренного оповещения населения (КСЭОН) является исключение человеческого фактора при срочном оповещении. Концепцией КСЭОН также предусмотрен выход с информационной составляющей о мониторинге окружающей обстановки в социальные сети (Одноклассники, Твиттер, ВКонтакте и т. д.) По сути дела речь идет о создании системы мониторинга окружающей среды нового типа.

Предлагаемый аппаратно-программный комплекс «Мониторинг» позволяет создать такую систему с минимальными затратами. Основа предлагаемого решения - компьютер, причем программное обеспечение «Мониторинг» работает в фоновом режиме, т.е. не влияет на работоспособность компьютера, который может продолжать выполнять свои основные функции, например, офисного компьютера. Компьютер снабжается устройством ввода-вывода, с помощью которого необходимая информация вводится в компьютер, а компьютер, в свою очередь управляет аппаратными средствами, служащими для измерения параметров окружающей среды. Полученные значения измеренных параметров с помощью Internet, непосредственно после измерения, становятся доступны пользователям, подписанным на данный сервис.

Пилотный проект аппаратно-программного комплекса «Мониторинг» в настоящее время (октябрь 2014 –апрель 2015года) работает в Приокском поселке г.Рязани, на компьютере оперативного дежурного ЕДДС. В качестве пара-

метра измеряемой среды выбрана радиация. Мощность дозы измеряется с помощью известного измерителя мощности дозы ДП-5В. Этот прибор подключен к компьютеру, через устройство сопряжения. Управления питанием ДП-5В осуществляется компьютером по расписанию, причем, периодичность измерения, может быть установлена какой угодно. Важно отметить, что прибор ДП-5В работает в штатной комплектации и не подвергался доработкам. Результаты измерений доступны в любом компьютере, подключенном к сети Интернет.

В дальнейшем список измеряемых параметров может быть расширен, к примеру, может быть измерена температура, скорость и направление ветра, концентрация газа и т.д. Система может быть дополнена, программно, инструментами автоматического анализа, вывода информации в социальные сети и даже возможностью дистанционного управления, причем расстояние значения не имеет.

УДК 65.011.8

Саттарова И.В.

Формирование инновационного потенциала промышленного предприятия

Вопросы формирования и развития инновационного потенциала довольно широко освещены в литературе. Предложено достаточно много определений инновационного потенциала, которые можно условно разделить на две группы. Первая группа рассматривает инновационный потенциал как количество экономических ресурсов, которые в каждый момент общество может использовать для своего развития.

Вторая группа рассматривает инновационный потенциал предприятия как совокупность научно-технических, технологических, инфраструктурных и иных возможностей, способных обеспечить получение инноваций. Среди определений инновационного потенциала нет противоречий, но нет и однозначности. Различия в определениях связаны с тем с позиций какого подхода исследуется данная категория. Некоторыми авторами отождествляется термин «инновационный потенциал» и «ресурсы».

Если бы эти термины были идентичны, то предприятия, имеющие одинаковые по величине ресурсы, должны были бы иметь одинаковый инновационный потенциал.

Однако, практика показывает, что это не так. Существуют предприятия с большими ресурсами и низким уровнем инновационного потенциала. И наоборот, есть предприятия с незначительными ресурсами и высоким уровнем инновационного потенциала.

Предложено следующее определение инновационного потенциала: инновационный потенциал - это восприимчивость руководства и всего коллектива к инновациям, научный и научно-технический потенциал, ресурсы в достаточном количестве.

Поясним это определение – почему на первом месте восприимчивость производства и коллектива? Потому что, если руководство и коллектив не готовы воспринимать инновации, то все остальные составляющие уже не играют существенной роли. Необходимо время пока смениться руководство и коллектив. Если восприимчивость руководства и коллектива положительная, то далее необходимы научная и научно-техническая составляющие. Научная составляющая выделена особо потому, что только научные идеи, изобретения, инновационные модели изделий ученые могут представить инновационно. Научно-технический потенциал - это результаты НИР и ОКР, инновационные, экспериментальные и опытные образцы изделий, комплекты конструкторской и технической документации на инновационные изделия, ресурсы - это плацдарм для формирования инновационного потенциала.

Следующие основные компоненты, имеющие различное функциональное назначение:

- материально-технические,
- нематериальные активы,
- информационные,
- финансовые,
- кадровые.

Материально-технические ресурсы определяют технико-технологическую базу потенциала, которая будет влиять на масштабы и темпы инновационной деятельности. Информационные ресурсы это базы данных, модели, алгоритмы, программы, которые являются движущей силой инновационного потенциала. Финансовые ресурсы характеризуются совокупностью источников и запасов финансовых возможностей, которые есть в наличии и могут быть использованы для реализации инновационного потенциала. Кадры - это совокупность знаний, навыков, способностей, которыми владеет человек и которые он использует при реализации инновационного потенциала. Инновационный потенциал, являясь частью экономического потенциала, способствует созданию общих предпосылок воспроизводственного процесса, определяющим его экономическую природу.

Интегральная сущность потенциала промышленного предприятия, работающего в условиях рынка, рассмотрена Е. Поповым. Этот метод заключается в количественной оценке рыночного потенциала промышленного предприятия, что позволяет повысить его конкурентоспособность и реализовать ресурсный подход в управлении.

Автор в качестве составных частей первого уровня выделяет два блока: потенциал маркетинговой деятельности и потенциал управленческой деятельности. А. Банчевой предложено сместить акценты и дополнить элементы оценки потенциала организации. Составляющими блоками при этом являются: блок 1-управление, блок 2-инструменты, блок 3-ресурсы.

Для оценки инновационного потенциала будем использовать методику расчета рыночного потенциала (т.к. инновационный потенциал является частью

как экономического так и рыночного потенциала). Инновационный потенциал, являясь интегральной величиной, включает следующие структурные единицы:

$$ИП=П1+П2+П3,$$

Где ИП-инновационный потенциал, П1-ресурсы, П2-научно-технический потенциал, П3-уровень инновационной культуры.

Величина инновационного потенциала выражается в процентах и показывает уровень использования инноваций, передовых методов и технологий. Методика расчета инновационного потенциала заключается в балльной оценке показателей, которые приводятся в ходе анкетного обследования объектов и вычисления интегрального показателя.

УДК 681.3.06

Ситников Д.А., Митрошин А.А., Чернышёв С.В.

Подсистема визуализации больших графов для программных средств моделирования содержания учебного процесса

При разработке программных средств моделирования содержания образовательного процесса [1] возникает необходимость визуализации больших графов. Это связано со сложностью восприятия конечным пользователем достаточно объёмных деревьев понятий.

В рамках разработки программных средств моделирования содержания образовательного процесса создана подсистема визуализации больших графов.

Подсистема позволяет отображать деревья понятий в нескольких видах. На рисунке 1 показано представление дерева понятий в виде классического дерева, в котором вершины графа понятий отображаются в виде прямоугольников. Реализован и аналогичный режим, в котором вершины дерева отображаются кругами.

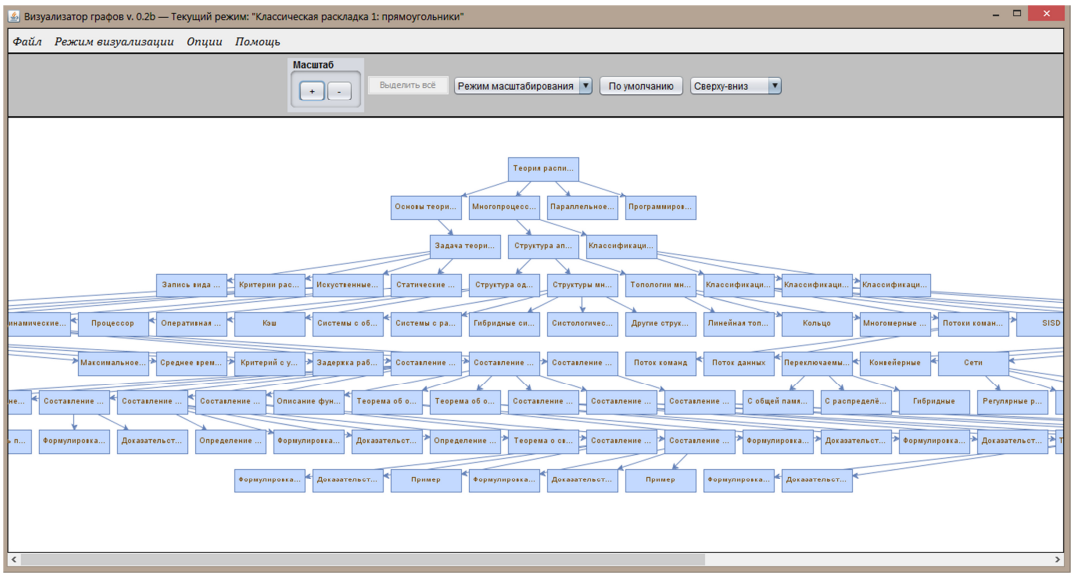


Рисунок 1. Визуализация большого дерева

Реализованы также отображения радиальный и шаровой режим визуализации (рисунки 2 и 3). Каждый из режимов отображения позволяет визуально выявлять отдельные специфические особенности учебных курсов. Так шаровой режим позволяет визуально определять концентрированность понятий учебного курса в группах понятий.

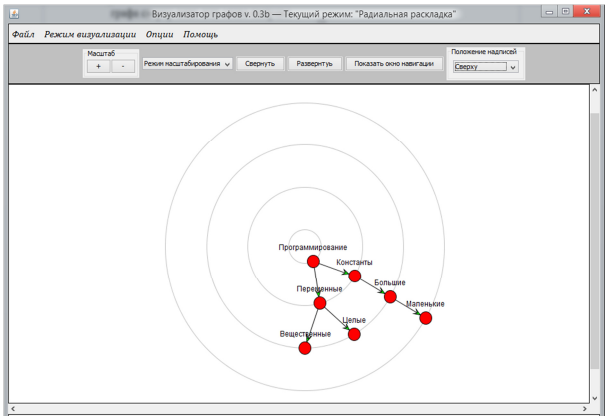


Рисунок 2. Радиальный режим отображения дерева

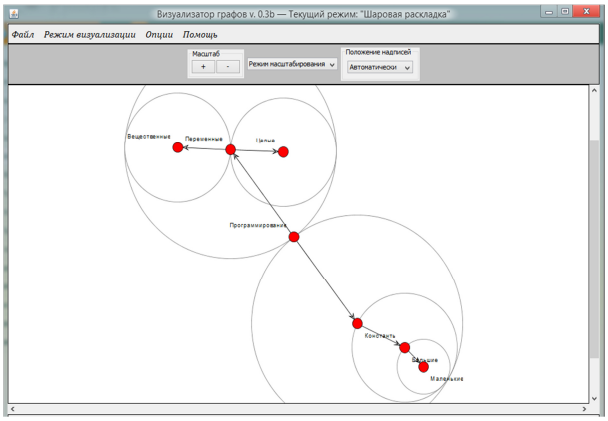


Рисунок 3. Шаровой режим отображение дерева

Разработанная подсистема отображения позволяет также сохранять полученные визуальные представления в формате pdf.

Подсистема визуализации существенно повышает потребительские качества системы моделирования содержания учебного процесса, способствует повышению качества создания моделей и их дальнейшего анализа и, следовательно, вносит определенный вклад в совершенствование содержания образовательного процесса, существенно влияющий на экономические показатели деятельности ВУЗа.

Библиографический список

1. Митрошин А.А., Чернышев С.В. Модель содержания учебного процесса // Материалы IV Всероссийской научно-практической конференции «Методы обучения и организация учебного процесса в вузе». – Рязань: РГРТУ, 2015.

УДК 622.23.05

Тчаро Х.

Обеспечение безопасности использования горных машин и оборудований

Проблемы сохранения здоровья и обеспечения безопасности труда, с которыми сталкивается Африка, многократны[1]. Проведение горных работ связано с большими опасностями, такие как аварии и выделение смертельных газов и т.д.

Предотвращение аварий, вызванных использованием горных машин и оборудования, имеет первостепенное значение при проведении разработки месторождения полезных ископаемых, как подземным, так и открытым способом.

В Буркина-Фасо число потерпевших при авариях продолжает уменьшаться благодаря иностранным горным компаниям, действующим с соблюдением международных мер безопасности. Однако, несмотря на это 2008-2010 гг. имели место несчастные случаи при использовании горных машин и оборудования. (Табл.1).

Таблица 1: Статистика несчастных случаев на руднике по добыче Au в Буркина-Фасо (по материалам SMB-SA, 2010г.)

Вид аварии	2008	2009
Легкие травмы	10	59
Кратность	2%	8.3%
Итого за отчетный период (год)	0,2%	0,7%
Травмы с отдыхом	2	9
Кратность	0,4%	1,3%
Итого за отчетный период (год)	0%	0,1%
Тяжелые травмы	1	2
Кратность	0,2%	0,3%
Итого за отчетный период (год)	0%	0%
Смертельный травмы	1	0
Кратность	0,2%	0
Итого за отчетный период (год)	0%	0%

Все машины и оборудования, используемые при открытом способом разработки, независимо от их типа или назначения, должны быть хорошо спроектированы, прочно изготовлены из подходящего качественного материала[3],

быть надежны, не иметь дефектов, оборудованы соответствующими предохранительными устройствами и обслуживаться в соответствии с регламентом [2].

Малые горные предприятия, которые не имеют собственных ресурсов, должны объединить свои ресурсы с другими предприятиями или принять любые другие меры для удовлетворения требований безопасности.

Компетентное лицо должен следить за механическим оборудование для создания и реализации плана работ всего оборудования карьера или шахты, независимо от его типа или назначения.

Этот план должен включать в себя:

- проверка и испытания каждой машины перед вводом ее в эксплуатацию и после установки, переустановки или ремонта;
- проверка и систематический тест любой машины для горных работ, чтобы обеспечить ее надежное техническое обслуживание;
- частота проверок и испытаний машин может отличать в зависимости от используемых материалов и компонентов[2];
- система проверок и испытаний, которые должны быть выполнены;
- порядок регистрации результатов всех проверок и испытаний, проведенных в соответствии с планом;
- хранение, на срок, указанный в национальном законодательстве, результатов всех проведенных проверок и испытаний.

Соблюдение национальных, внутрикорпоративных и международных требований безопасности снижает риски возникновения нечастных случаев при проведении горных мероприятий, особенно что касается горным машинам и оборудованиям.

Литература:

1. Безопасность ведения горных работ и горноспасательное дело: Учебник для вузов Ильин А.М., Каледина Н.О., Кирин Б.Ф., Ушаков К.З., Сребный М.А., Диколенко Е.Я., Семёнов А.П. Горная книга 2008 г. 490 с

2. Rapport de la Réunion de l’Effort Conjoint OMS/OIT pour la Santé et la Sécurité au Travail, Abidjan, 28-30 mai 2001

3. La sécurité et la santé dans les mines à ciel ouvert. Recueil de directives pratiques du BIT Genève, Bureau international du Travail, 1991 / Recueil de directives /, / Sécurité du travail /, / Santé au travail/, /Industrie minière /. 13.04.2 ISBN 92-2-207103-4

УДК 681.3.06

Цуканов А.В., Новиков А.А., Митрошин А.А. Чернышёв С.В.

Программные средства управления программными активами высшего учебного заведения

Программное обеспечение (ПО) является одним из наиболее важных активов ВУЗов, используемых во всех сферах деятельности (учебной, научной, управленческой и т.д.), при этом затраты на него могут быть существенными. Как и традиционные активы, ПО имеет жизненный цикл, который включает в себя закупку, развертывание, передачу, эксплуатацию и списание. Поэтому процедуры для управления программными активами необходимы для ВУЗа, желающего эффективно использовать финансовые средства, направляемые на закупки коммерческого ПО. В этой связи программные продукты, предназначенные для управления программными активами (SAM - Software Asset Management – управление программными активами) становятся все более актуальными и востребованными.

SAM - это методология, направленная на оптимизацию процессов корпоративного управления программным обеспечением и на их защиту. В нее входят следующие основные процедуры сопровождения «жизненного цикла» ПО: учет программного обеспечения и его использования, лицензий и документов, подтверждающих наличие прав на использование (лицензионные договоры, сертификаты, лицензионные свидетельства, бухгалтерские документы); разработки и применения регламентов и политик закупки ПО; ввода его в эксплуатацию, эксплуатация и вывод из эксплуатации.

Основными преимуществами использования SAM являются:

- минимизация юридических и финансовых рисков, связанных с нарушением условий использования ПО;
- возможность определить, какие программные продукты действительно необходимы, что даёт возможность сократить расходы на обучение персонала и техническую поддержку используемого ПО;
- обеспечение условий информационной безопасности.

Внедрение SAM состоит из 4-ех этапов, которые можно обозначить как инвентаризация, сопоставление с лицензионными документами, обеспечение соответствия с лицензионными документами на «фиксированную дату», поддержание достигнутого результата в будущем.

1. Инвентаризация. На этом этапе выясняется, сколько персональных компьютеров и серверов имеется в ВУЗе и какие программы на них используются. Это работа может быть выполнена рутинно вручную, или с помощью специальных программ, позволяющих автоматизировать этот процесс, таких как OCS Inventory.

2. Сопоставление с лицензионными документами. Производится сбор лицензионной документации, поскольку часто у ВУЗа нет единого реестра

лицензий. После этого проверяется соответствие установленных программ условиям лицензионных соглашений.

3. Обеспечение соответствия с лицензионными документами на «фиксированную дату». В случае нахождения ПО, используемого без достаточных оснований, оно деинсталлируется.

4. Поддержание достигнутого результата в будущем. При выполнении первых трех этапов, решена первоочередная задача – наведен порядок в лицензиях по состоянию на текущий день. На заключительном этапе используется комплекс мер, позволяющих закрепить полученный результат.

В настоящее время существует ряд программных продуктов, позволяющих обеспечивать учет и контроль использования лицензий, таких как AuditPro и GLPI (распространяется под лицензией GNU/GPL version 2). Однако они обладают различными недостатками (дороговизна, избыточность функциональных возможностей и т.п.), которые ограничивают их использование в ВУЗах.

В РГРТУ разработано программа, позволяющая осуществлять учёт лицензий ПО и осуществлять контроль за его использованием. Программа реализована как Интернет-приложение на языке Ruby. На рисунке приведен один из экранов приложения.

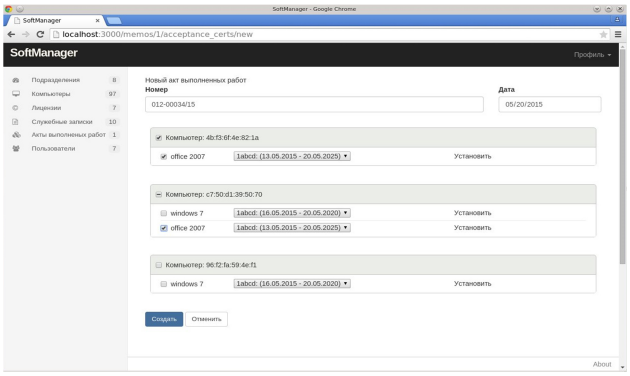


Рис. 1. Один из экранов программы по учёту ПО и контроля за его использованием.

Разработанное приложение внедрено в практику работы управления ТКиИР РГРТУ и позволяет повысить качество и оперативность процесса учёта лицензий ПО и контроля за их использованием в университете.

УДК 504.064

Шилин А.В, С.Г., Гудзев В.В.

Идентификация и исследование высокодисперсной пыли в производственных помещениях

На некоторых производствах в силу особенностей производственных процессов происходит интенсивное образование пыли. Такую пыль называют про-

мышленной, она может представлять угрозу для рабочих и самого производства, а так же ухудшает условия труда.

На предприятиях существует множество технологических процессов, таких как таких как просев, дробление, истирание, обточка, размол, распил, пересыпка, сгорание, плавление и прочие, которые сопровождаются выделением вредных веществ в виде пыли, газов и паров в воздух рабочего помещения.

По размеру частиц (дисперсности) различают:

1) видимую пыль размером более 10 мкм;

2) микроскопическую — от 0,25 до 10 мкм;

3) ультрамикроскопическую — менее 0,25 мкм.

Наиболее опасна высокодисперсная пыль размеры частиц которой не превышают 5 мкм. Мелкая пыль, попадая в легкие, надолго оседает на лёгочную ткань, вызывая её поражение. Кроме того, мелкая пыль при той же массе имеет большую поверхность соприкосновения с легочной тканью, поэтому она более активна. Высокодисперсная пыль представляет большую опасность, чем низкодисперсная, так как она дольше находится в воздухе во взвешенном состоянии.

Высокодисперсная пыль, оседая на кожные покровы, закупоривает сальные и потовые железы, вызывает раздражение, зуд, покраснения кожи, сухость, гнойничковые образования, воспаления.

Пыль, попавшая в глаза, вызывает воспалительный процесс их слизистых оболочек — конъюнктивит, который выражается в покраснении, слезотечении, иногда припухлости и нагноении.

Кроме вреда здоровью, пыль является опасным фактором и для самого производства, поскольку в некоторых случаях скопления пыли могут вызвать сбои в работе оборудования.

Так как высокодисперсная пыль имеет малые размеры, зачастую трудно определить ее наличие в воздухе помещения, а тем более изучить ее состав более детально.

Для идентификации и исследования высокодисперсной пыли в производственных помещениях могут успешно использоваться атомно-силовой микроскоп (АСМ) и растровый электронный микроскоп (РЭМ), а так же рентгеновский микроанализатор для определения состава пыли.

Для исследования пыли в РЭМ, частицы крепятся к подложке с помощью липких лент и полимеров.

Подготовка частиц пыли для исследования на АСМ выглядит следующим образом:

1. Слюдяная подложка очищается с помощью спирта и промывается дистиллированной водой.
2. Термопластичная смола нагревается до $T = 100^0C$ в течении 3 минут. В расплав опускается подложка.
3. При высыхании на поверхность слюды наносятся частицы.

4. Измерения проводятся в контактном режиме с помощью твердых кантилеверов.

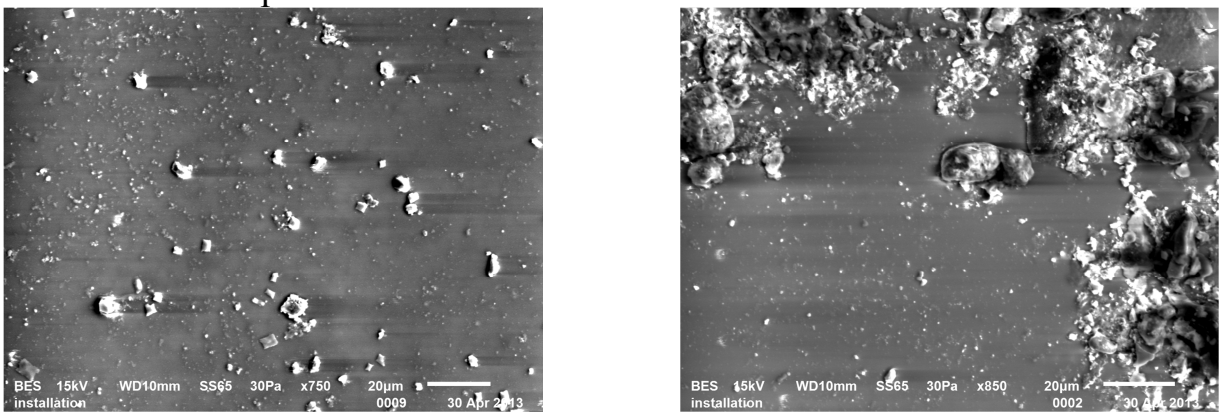


Рисунок 1. РЭМ-изображения частиц пыли

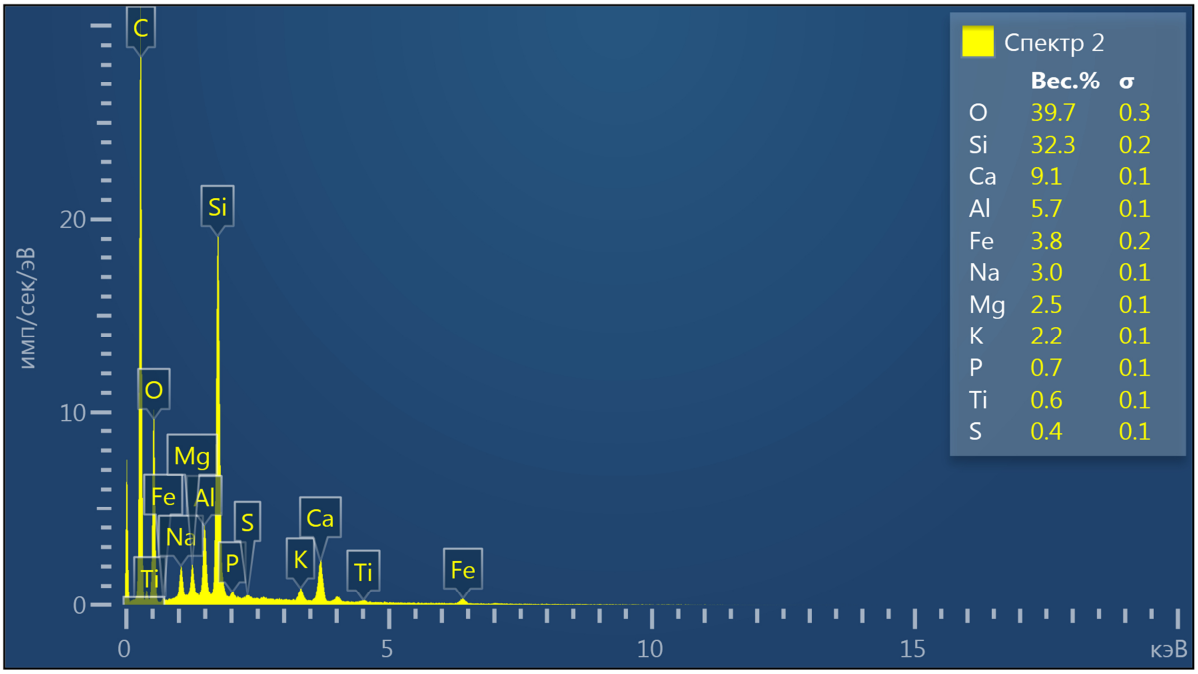


Рисунок 2. Рентгеновский микроанализ частиц пыли

УДК 681.3.06

Шошин Е.В., Митрошин А.А., Чернышёв С.В.

Программные средства моделирования содержания учебного процесса

Основным видом деятельности высшего учебного заведения является образовательная деятельность, которая является и основным источником поступления ВУЗовских финансовых средств. Изменение финансовых показателей образовательной деятельности оказывает существенное влияние на финансовые показатели ВУЗа в целом.

Качественное осуществление образовательной деятельности невозможно без качественно спланированного, планово реализуемого и управляемого учебного процесса, основой которого является его содержание, то есть то, что изучается в его рамках (содержание образования). В [1] предложена модель содержания образования и высказано утверждение о том, что предложенная модель является перспективной с точки зрения разработки программных средств, его реализующих.

В РГРТУ разработан прототип программы, реализующий описанную в [1] модель.

Программа представляет собой приложение рабочего стола, позволяющее создавать и редактировать дерево понятий, описывающего содержание описываемой дисциплины, определять вид учебных занятий (лекции, лабораторные работы и т.п.) на которых изучаются те или иные понятия, описывать последовательность изучения понятий. Определение логических связей между понятиями в настоящее время не поддерживается.

На рисунке 1 приведено главное окно программы.

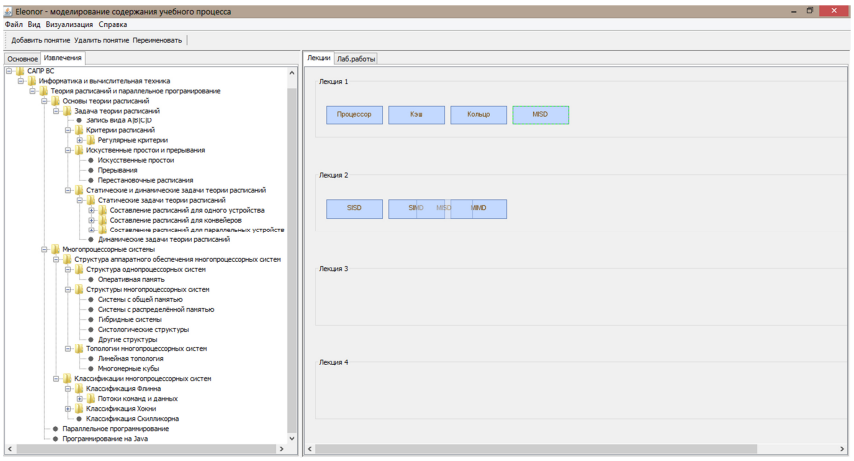


Рисунок 1. Главное окно программы моделирования содержания учебного процесса

Окно, позволяющее описывать параметры моделируемого курса, показано на рисунке 2.

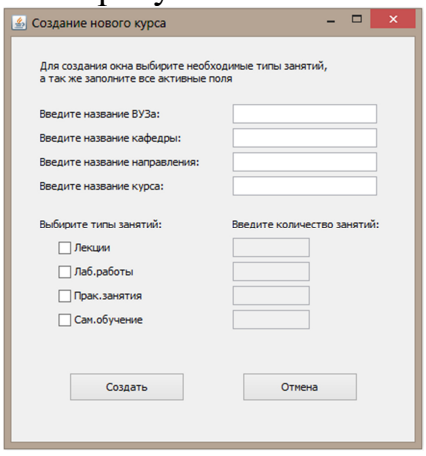


Рисунок 2. Окно описания моделируемого курса

Программа написана на языке программирования Java, что делает её кроссплатформенной. Для хранения данных используется формат XML.

В настоящее время создана модель одного из курсов, читаемых студентам второго года обучения на направлении «Информатика и вычислительная техника».

Работа с программой показала, что реализованная в ней модель содержания учебного процесса вполне может использоваться в практической деятельности.

На основе реализованной модели возможно создание информационной системы управления содержанием образования, которая позволит на качественно новом уровне управлять содержанием образования, создавать конкурентноспособные учебные программы, востребованные у студентов и работодателей, соответствующие существующим Федеральным государственным образовательным стандартам.

Библиографический список

Митрошин А.А., Чернышев С.В. Модель содержания учебного процесса // Материалы IV Всероссийской научно-практической конференции «Методы обучения и организация учебного процесса в вузе». – Рязань: РГРТУ, 2015.

СЕКЦИЯ: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

УДК 456.52

Гостин А.М., Самохина Н.В., Чернышев С.В.

Особенности обработки персональных данных в ВУЗе

Обработка персональных данных в ВУЗе регулируется требованиями ФЗ-152 «О персональных данных», ФЗ-149 «Об информации, информационных технологиях и защите информации», ФЗ-273 «Об образовании в Российской Федерации», Трудового Кодекса, Постановления Правительства РФ №687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемых без использования средств автоматизации», Постановления Правительства РФ № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», а также другими нормативно-правовыми актами.

Особенностью обработки персональных данных в РГРТУ является наличие следующих категорий субъектов персональных данных (ПДн):

4. абитуриенты;
5. школьники (учащиеся подготовительного отделения и городской школы программистов, члены спортивных секций и т.д.);
6. обучающиеся (студенты, аспиранты, слушатели курсов повышения квалификации);
7. работники (ППС и УВП, в том числе совместители).

Опыт работы РГРТУ за прошедшие несколько лет в области обработки и защиты персональных данных, позволяют сформировать обобщенные требования к этой работе, которые могут быть полезными для ВУЗов и других образовательных учреждений.

Для каждой из категорий субъектов ПДн необходимо установить категории обрабатываемых ПДн, а также определить какие из этих категорий будут обрабатываться в информационных системах персональных данных (ИСПДн).

В комплекс необходимых организационных мер включается выпуск приказа по организации о назначении ответственных за обработку персональных данных, пользователей и администраторов ИСПДн с обязательным ознакомлением всех лиц под роспись.

В качестве нормативных документов рекомендуется разработать отдельное Положение об обработке персональных данных, в котором указывается организационная структура, прописывается четкий регламент действий и ответственность всех лиц, причастных к обработке ПДн.

Положение об обработке персональных данных должно включать: принципы, условия и цели обработки ПДн, утвержденные категории субъектов ПДн и обрабатываемых данных, виды обработки, порядок получения и передачи ПДн, обеспечение прав субъектов ПДн при обработке их ПДн в университете, обязанности университета, как оператора, меры, осуществляемые в ВУЗе по

обеспечению безопасности ПДн при их автоматизированной обработки и при обработки без использования средств автоматизации.

Для всех лиц, причастных к обработке ПДн, необходимо разработать отдельные должностные инструкции по обработке ПДн, а также заключить дополнительное соглашение к трудовому договору, в котором указать требование о неразглашении обрабатываемых персональных данных субъектов ПДн.

Со всех субъектов ПДн необходимо получить письменное согласие на обработку ПДн, которое должно содержать: данные субъекта (включая паспортные данные), данные оператора (юридического лица), категории обрабатываемых ПДн, цель обработки, основания обработки, виды обработки, сроки обработки, условия прекращения обработки, перечень третьих лиц, которым передаются ПДн, основания передачи. Для школьников, как отдельных субъектов ПДН, которым не исполнилось 18 лет, указанные письменные согласия дают их родители или уполномоченные лица.

Персональные данные субъектов ПДн, обрабатываемые без использования средств автоматизации, должны храниться в специально отведенных местах, обеспечиваться раздельное хранение ПДн, обработка которых осуществляется в различных целях, а также соблюдаться условия, обеспечивающие сохранность ПДн и исключающие несанкционированный доступ к ним.

Для создания и ввода в эксплуатацию ИСПДн (например, использующихся в кадровом учете и бухгалтерии) в ВУЗе рекомендуется разработать технический проект на создание системы защиты информации ИСПДн, определяющий состав и категории обрабатываемых ПДн, угрозы безопасности ПДн, уровни защищенности, требования к защите ПДн, состав и содержание технических мер по обеспечению безопасности ПДн в ИСПДн, перечень АРМ и состав серверного оборудования, перечень помещений, где происходит обработка ПДн.

Ввод в эксплуатацию ИСПДн в ВУЗе осуществляется на основании приказа о вводе в эксплуатацию с назначением пользователей, эксплуатационного персонала, а также лица, ответственного за обработку ПДн в ИСПДн. При необходимости назначается администратор безопасности ИСПДн.

Для учета ПДн, обрабатываемых в ИСПДн заводятся отдельные журналы учета съемных машинных носителей информации, журналы учета передачи ПДн, акты об уничтожении ПДн, журналы учета периодических проверок соответствующими должностными лицами. Проверки должны осуществляться не реже, чем один раз в три года.

На АРМ и серверное оборудование, входящие в состав ИСПДн должен быть получен аттестат соответствия, подтверждающий наличие выполнения организационно-технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

Выполнение в РГРТУ всего комплекса указанных выше мероприятий позволило университету пройти плановую проверку по обработке ПДн, проводимую Управлением Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по Рязанской области (март 2015

года) с одним замечанием, устранение которого потребовало минимальных временных и административных усилий.

УДК 65.012.16

Дорохов В.Э.

Необходимость управления репутационными рисками вследствие инцидентов информационной безопасности для хозяйствующего субъекта

Подход к обеспечению информационной безопасности (далее – ИБ) в Российской Федерации, практикуемый как государственными, так и коммерческими организациями, можно сравнить с конструктором, поскольку известно, что в настоящее время не существует целостного подхода к обеспечению ИБ.

Для коммерческого сектора обеспечение ИБ можно сформулировать в виде трех основных направлений:

- развитие технологий, направленных на нейтрализацию угроз ИБ при помощи технических средств защиты информации;
- усовершенствование контроля над процессами использования информации, то есть предотвращение утечек информации путем разработки определенного перечня необходимых организационных мероприятий;
- контроль над информационным полем вокруг организации: направление наименее развитое, тесно перекликающееся с другими аспектами управления в компаниях, такими как взаимоотношения с сотрудниками (HR), связи с органами государственного и муниципального управления(GR), связи с общественностью (PR), связи с инвесторами (IR).

Рассмотрим каждое из представленных выше направлений.

Развитие технологий защиты информации непосредственно связано с развитием технологий обработки информации. Чем больше способов информационного взаимодействия с применением средств вычислительной техники и каналов передачи информации, тем больше уязвимостей, которыми может воспользоваться злоумышленник. Для принятия оптимального решения по составу программно-аппаратных средств защиты информации необходимо проанализировать следующие аспекты работы с информацией в организации:

- Использование средств вычислительной техники для работы с критически важной информацией; наличие технических средств с обязательной функцией обмена данными через сеть Интернет; технологии работы с информацией (виртуализация, системы управления базами данных (СУБД), прикладные программные средства и т.д.).
- пользование специализированного программного обеспечения при работе с критически важной информацией; учет особых требований на совместимость данного программного обеспечения; анализ порядка его разработки.

- Территориальное распределение важных сегментов организации, объединенных по принципу работы с одним и тем же составом критически важной информации.
- Модернизация сетевой инфраструктуры, в частности, возможность образования новых сегментов локальной вычислительной сети предприятия.

Для предотвращения инцидентов ИБ, реализованных путем разглашения сотрудниками информации ограниченного доступа, актуальным средством является повышение осведомленности сотрудников организации в вопросах обеспечения ИБ. Положения по работе со сведениями, составляющими важность для организации, должны быть задокументированы и однозначно понятны для всех сотрудников. Построение организационных мероприятий зиждется на следующих основных принципах:

- Определение перечня сведений, составляющих критически важную информацию для организации. Здесь необходимо учитывать возможное дополнение сведений, связанное с открытием новых направлений работы организации либо развитием старых, а также связанное с этим увеличение количества работников компании.
- Определение направлений деятельности, связанных с обработкой критически важной информации. Также необходимо понимание, увеличится ли объем критичной информации, будут ли открываться новые направления деятельности с привлечением потенциальных стратегических партнеров и др.
- Степень лояльности сотрудников, задействованных в обработке информации, и их количество. Важно учитывать, планируется ли сокращение штата сотрудников по направлениям, в которых осуществляется работа с критически важной информацией.
- Анализ условий работы сотрудников в организации на предмет соответствия конкурентным условиям на рынке труда. Также необходимо проанализировать, осуществляются ли мероприятия для работников по неразглашению ими условий труда.
- Анализ существующих организационных мероприятий на предмет соблюдения требований регуляторов в области ИБ. В том числе анализ актуальных законодательных актов в части обеспечения ИБ. Также необходимо учитывать, планируются ли изменения нормативных документов регуляторов, и в какие временные сроки.
- Анализ осведомленности персонала по вопросам ИБ посредством анкетирования либо тестирования.

Информационное поле вокруг организации, по сути, формирует ее имидж. Имидж, в свою очередь, оказывает прямое влияние на прибыль компании. В данном направлении необходимо проводить мероприятия по минимизации инцидентов ИБ влекущих за собой репутационные потери для организации. Согласно проводимым исследованиям автора [1], [2] понятие репутационного риска в контексте ИБ отсутствует в нормативных документах Российской Фе-

дерации в области информационной безопасности. В соответствии со спецификой возникновения данного риска вследствие инцидентов информационной безопасности, данное понятие можно представить следующим образом:

Репутационный риск (информационная безопасность) **–** понятие, характеризующееся совокупностью качественных и количественных параметров ущерба для предприятий и организаций, возникающего вследствие отсутствия подходящих организационных и технических мероприятий по противодействию разглашению информации ограниченного доступа и распространения, приводящему к потере репутации, для основных видов взаимоотношений: взаимоотношения с работниками, связи с общественностью, связи с органами государственного и муниципального управления, связи с инвесторами, - а также вероятностью его возникновения на основе возможных инцидентов информационной безопасности в перечисленных видах взаимоотношений.

С целью осуществления эффективного контроля над информационным полем вокруг организации, необходимыми для анализа являются:

- Частота появления в СМИ сведений о направлениях деятельности организации, в рамках которых предполагается обработка критически важной информации. Тенденция повышения интереса читателей к рубрикам, которые освещают подобные проблемы.
- Наличие у сотрудников личных блогов в сети Интернет при отсутствии должного уровня осведомленности с Политикой ИБ (если данный документ утвержден в организации).
- Наличие и тенденция обсуждения направлений в тематических формах (количество пользователей из числа работников, активность – количество сообщений). Данную информацию можно собрать анкетированием на этапе анализа проблемы.
- Развитие смежных направлений в организации, имеющих повышенную конкуренцию, в том числе среди компаний, использующих «черный пиар».

Проведем анализ требований по обеспечению информационной безопасности в нормативных документах Российской Федерации с целью определить полноту рекомендуемых мер для минимизации репутационного риска.

Рассмотрим нормативные документы Российской Федерации, регламентирующие порядок обеспечения ИБ. Под термином «информационная безопасность» довольно часто понимается процесс защиты информации с использованием программных, аппаратных и программно-аппаратных решений с целью предотвращения утечки информации по техническим каналам. В этой области существует ряд нормативных документов Российской Федерации, регулирующих вопросы безопасности информации. Среди регуляторов стоит отметить ФСТЭК России, ФСБ России, Центральный банк Российской Федерации, Роскомнадзор.

Требования по ИБ изложены в следующих основных документах:

- Конституция Российской Федерации.
- Доктрина информационной безопасности Российской Федерации.

- Указ Президента РФ от 06.03.1997 №188 «Об утверждении Перечня сведений конфиденциального характера».
- Федеральный закон от 27.07.2006 №149-ФЗ (ред. от 28.12.2013) «Об информации, информационных технологиях и о защите информации».
- Федеральный Закон от 27.07.2006 №152-ФЗ «О персональных данных», включая:
    - Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».
    - Постановление Правительства РФ от 15.09.2008 №687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации».
    - Постановление Правительства РФ от 06.07.2008 № 512 (ред. От 27.12.2012) «Об утверждении требований к материальным носителям биометрических персональных данных вне информационных систем персональных данных».
    - Постановление Правительства РФ от 21.03.2012 №211 (ред. 20.07.2013) «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами».
- Федеральный закон от 06.04.2011 №63-ФЗ «Об электронной подписи».
- Федеральный закон от 29.07.2004 № 98-ФЗ (ред. от 11.07.2011) «О коммерческой тайне».
- Федеральный закон от 27.06.2011 № 161-ФЗ (ред. от 23.07.2013) «О национальной платежной системе».
- Постановление Правительства РФ от 13.06.2012 №584 «Об утверждении Положения о защите информации в платежной системе».
- Нормативные документы государственных регуляторов (ФСТЭК России, ФСБ России, Роскомнадзор, Центральный Банк Российской Федерации).

Вместе с тем помимо основных законов и подзаконных актов Российской Федерации, необходимо учитывать требования отраслевых нормативных актов в части ИБ. Стоит отметить, что в большинстве случаев обеспечение безопасности информации начинается с анализа основного закона отрасли, и следом, на основании проведенного анализа, строится работа по защите информации в организации. Для каждой отрасли необходимо учитывать специфические требования по обработке информации, определению конфиденциальности информации и др.

Исходя из анализа существующих нормативных актов, регламентирующих обеспечение ИБ, можно сделать вывод о необходимости проведения мероприятий по защите информации ограниченного доступа от утечки по техническим каналам. К таким мероприятиям относятся:

- Установка и настройка технических средств защиты информации на автоматизированные рабочие места сотрудников организации, на которых производится обработка информации ограниченного доступа.
- Использование защищенной среды передачи данных для исключения возможности утечки информации ограниченного доступа при обмене информацией во внутренней сети организации, а также при использовании внешних сетей.

Одновременно стоит отметить, что помимо утечки информации по техническим каналам для коммерческого сектора не менее важно учитывать вероятность возникновения событий иного характера, от которых трудно защититься только техническими средствами защиты, таких как:

- публикация в читаемом интернет-блоге о внутренних проблемах организации;
- размещение на официальном сайте государственного регулятора информации о нарушениях организацией требований законодательства;
- заявление в средствах массовой информации (СМИ) работника крупного банка об убытках его организации;
- разглашение работником важной информации внутри коллектива, например, сведений о заработной плате;
- заказная публикация от компаний-конкурентов в СМИ ложных сведений, дискредитирующих действия компании;
- появление в открытых источниках сведений о стратегических партнерах компании, желающих остаться инкогнито;
- и другие;

Все подобные ситуации объединяет фактор влияния общественного мнения. Злоумышленники применяют ряд способов воздействия на репутацию организации, основными из которых являются несанкционированные операции с информационными активами организации, в том числе нарушение конфиденциальности, целостности, доступности как основных свойств, и аутентичности, достоверности и др. как дополнительных свойств защищаемой информации. Как правило, исходами вследствие подобных инцидентов являются кадровые и финансовые потери. Другими словами, организация терпит крупные убытки, порой несопоставимые с возможностью продолжения дальнейшей деятельности. В связи с этим представители бизнес-сектора должны уделять внимание предотвращению утечки критически важной информации, так как негативные последствия этих инцидентов очевидны: прямые финансовые убытки, удар по репутации, потеря клиентов.

Исходя из проведенного анализа, важно отметить отсутствие нормативно - регулируемых механизмов по предотвращению или минимизации репутационных рисков для организаций и предприятий. В связи с вышеизложенным, целесообразно будет рассмотреть общепринятые стандарты и наиболее часто встречаемые методики управления рисками на предмет применимости их в настоящее время и учета репутационных рисков, возникающих вследствие инцидентов информационной безопасности.

Принципы и руководящие указания по управлению рисками определяются как в международных, так и в национальных стандартах. Международными организациями International Organization for Stardrdization (далее – ISO) и International Engineering Consortium (далее – IEC) был разработан ряд стандартов, описывающих основные термины и определения в области управления рисками, принципы и руководящие указания по управлению рисками; руководящие принципы, касающиеся выбора и применения систематических методик оценки риска; управления рисками информационной безопасности и др.

Такими стандартами являются:

- ISO/IEC Guide 73:2009 «Risk management – Vocabulary».

Стандарт включает в себя основные понятия, термины и определения, относящиеся к управлению рисками. Терминология, введенная в настоящем стандарте, является общей для управления рисками в любой организации, независимо от того, в какой сфере осуществляется деятельность, и какие цели данная организация преследует. В отличие от стандарта ISO/IEC Guide 51, где основной упор делается на анализ последствий (тем самым рассматриваются аспекты безопасности), данный стандарт охватывает более широкую область. В данном стандарте приведены термины, относящиеся к риску; термины, относящиеся к управлению рисками, а также к процессу управления рисками; термины, относящиеся к обмену информацией и консультированию; термины, относящиеся к контексту; термины, относящиеся к оценке риска; термины, относящиеся к идентификации риска; термины, относящиеся к анализу риска; термины, относящиеся к оцениванию риска; термины, относящиеся к обработке риска; термины, относящиеся к мониторингу и измерению.[3]

На практике, в своей деятельности, различные организации стремятся к применению общего подхода к терминологическому описанию менеджмента рисков, поэтому удобство данного стандарта проявляется в универсальности его применения.

Применение терминологии введенной в данном стандарте необходимо сотрудникам организаций, вовлеченным в процесс управления рисками. Термины, приведенные в данном стандарте необходимо учитывать разработчикам нормативных документов различного уровня (национальных стандартов, отраслевых стандартов и др.), касающихся управления рисками.

- ISO/IEC 31000:2009 «Risk management – Principles and guidelines».

Данный стандарт определяет принципы и руководящие указания по управлению рисками, являющиеся обобщенными для любой сферы деятельности, будь то государственная организация, унитарное предприятие или иные организации[4]. Тем самым, использование данного стандарта не привязано к конкретным отраслевым направлениям. Стандарт определяет для организации, заинтересованной в безопасности своих решений, основные принципы, придерживаясь которых, достигается наиболее эффективное использование управления рисками. Основополагающей идеей данного стандарта является внедрение процесса управления рисками в структуру управления компанией, введение аспектов

управления рисками при составлении планов и задач, определения стратегии развития, изменения порядка анализа и предоставления отчетности. Применение данного стандарта возможно как для оценки рисков при положительных, так и при отрицательных последствиях. Применение данного стандарта возможно на всем пути развития организации, от принятия начальных решений, до рассмотрения функций и целей организации при последующем развитии. Следует отметить, что данный стандарт не предназначен для сертификации.

- ISO/IEC 31010:2009 «Risk Management – Risk Assessment techniques».

Данный стандарт разработан в дополнение к стандарту ISO/IEC 31000[5]. С учетом требований, приведенных в ISO/IEC 31000, разработаны основные принципы по определению необходимых методик оценки риска. В настоящем стандарте не отражены все имеющиеся методики, более того, для некоторых методик приведены ссылки на нормативную документацию, в которой дано более полное их описание. Рассматриваемый стандарт, как и ISO/IEC 31000 не используется с целью сертификации и не является руководством к выбору методики учитывающей отраслевую специфику различных организаций. Стандарт представляет собой обобщенную политику выбора методики, которая может применяться в любой организации, в том числе и государственного сектора. В данном стандарте не приводятся руководящие действия к обнаружению необходимости анализа риска. Выбор методики оценки риска предполагает дальнейшее использование выбранной методики на каждом этапе развития организации. Настоящий стандарт не специализируется на управлении определенными типами рисков, представляя документ общего характера в области управления рисками.

- ISO/IEC 27005:2011 «Information technology -- Security techniques -- Information security risk management».

В данном стандарте рассматриваются возможные подходы к управлению рисками информационной безопасности [6]. Необходимо отметить отсутствие прямого указания к выбору определенного конкретного подхода к менеджменту рисков информационной безопасности. Возможные подходы формируются в данном стандарте, опираясь, в основном, на требования системы менеджмента информационной безопасности, существующей в организации, согласно ISO/IEC 27001.

Схема взаимосвязи использования стандартов представлена на Рисунке 1.

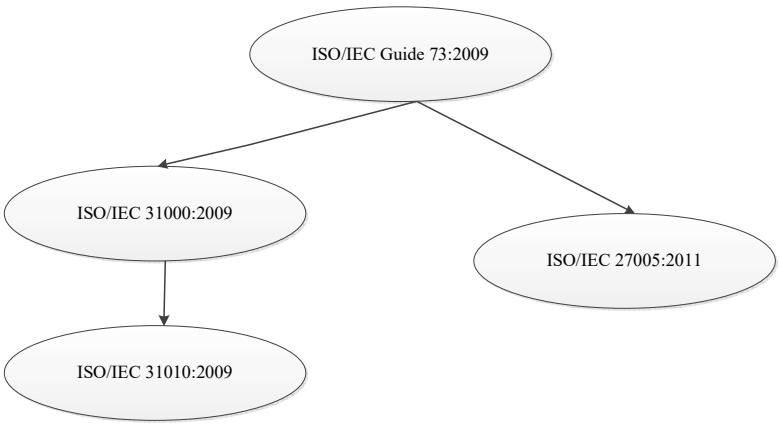


Рисунок 1 Схема взаимосвязи использования стандартов

Стоит отметить существование национальных стандартов по менеджменту рисков являющихся идентичными переводами международных стандартов ISO/IEC. Такими стандартами являются:

- ГОСТ Р ИСО/МЭК 31010-2011 «Менеджмент риска. Методы оценки риска»
- ГОСТ Р 51897-2011 «Менеджмент риска. Термины и определения»
- ГОСТ Р ИСО 31000-2010 «Менеджмент риска. Принципы и руководство»
- ГОСТ Р ИСО/МЭК 27005-2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»

Применение данных стандартов, основанных на международном подходе для оценки рисков вследствие инцидентов информационной безопасности существенно осложнено в Российской Федерации ввиду различия в положениях законов и подзаконных актов, регламентирующих требования к обеспечению безопасности информации. Для регулирования данной тематики необходима разработка принципиально нового документа, основанного на лучших международных практиках, описанных в данном разделе, адаптированного под Российское законодательство и потребности отечественных организаций.

В настоящее время существует ряд методов оценки рисков, разработанных в разные периоды и, в связи с этим, учитывающие различные факторы в развитии информационной безопасности в целом. Рассмотрим некоторые из них:

Методология OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) была разработана в Институте программной инженерии при Университете Карнеги-Меллона [7] и предусматривает активное вовлечение владельцев информации в процесс определения критичных информационных активов и ассоциированных с ними рисков. Ключевые элементы OCTAVE:

- идентификация критичных информационных активов;
- идентификация угроз для критичных информационных активов;
- определение уязвимостей, ассоциированных с критичными информационными активами;
- оценка рисков, связанных с критичными информационными активами.

Метод OCTAVE – это метод оперативной оценки актуальных угроз, критичных активов и основных уязвимостей. Метод подразумевает создание группы, которая направлена на анализ информационной безопасности. Группа анализа, как правило, состоит из сотрудников подразделений организации, эксплуатирующих систему, и сотрудников отдела информационных технологий.

Еще один популярный метод анализа и управления рисками CRAMM (CCTA Risk Analysis and Management Method) [8]. Цель применения данного метода – создание автоматизированной процедуры позволяющей:

1) Убедиться в том, что требования, связанные с безопасностью полностью проанализированы и задокументированы.

2) Избежать расходов на излишние меры безопасности, возможные при субъективной оценке рисков.

3) Оказать помощь в планировании и осуществлении защиты на всех стадиях жизненного цикла информационной системы.

4) Обеспечить проведение работ в сжатые сроки (косвенный эффект).

5) Автоматизировать процесс анализа требований безопасности.

6) Предоставить обоснования для мер противодействия.

7) Оценить эффективность контрмер, сравнивая различные варианты контрмер.

8) Генерировать отчеты.

Контроль рисков состоит в идентификации и выборе контрмер, позволяющих уменьшить риск до приемлемого уровня.

Методология CORAS разработана в рамках программы Information Society Technologies [9]. Ее суть состоит в адаптации, уточнении и комбинировании таких методов проведения анализа рисков, как Event-Tree-Analysis, цепи Маркова, HazOp (HAZard and OPerability studies) и FMEA (Failure Mode and Effects Analysis). CORAS использует технологию UML (Unified Modeling Language) и базируется на австралийском/новозеландском стандарте AS/NZS 4360: 1999 Risk Management и ISO/IEC 17799-1: 2000 Code of Practice for Information Security Management. В соответствии с CORAS информационные системы рассматриваются не только с точки зрения используемых технологий, но с нескольких сторон, а именно как сложный комплекс, в котором учтен и человеческий фактор.

Также в рамках исследования был проанализирован GTS 1056 «Комплект типовых документов по управлению рисками информационной безопасности», разработанный компанией GlobalTrust. Используемая качественная методология оценки рисков находится в полном соответствии с требованиями стандартов ISO 27001 и ISO 27005 (BS 7799-3), а также опирается на известные методы оценки рисков CRAMM, OCTAVE.

Приведенные методики оценки рисков предполагают оценку вероятности реализации угроз информационной безопасности и тяжести последствий от их реализации. В большинстве методик для определения степени вероятности реализации той или иной угрозы используется качественная экспертная оценка, что не позволяет произвести точную оценку, не зависящую от субъективного мнения, основанного на современных подходах к информационной безопасности. Стоит отметить, что качественная оценка не дает полной картины влияния репутационных рисков. Учитывая специфику современного отношения руководящего звена организаций и предприятий к мероприятиям по обеспечению информационной безопасности, использование вербальных показателей делает оценку субъективной, и часто занижаемой с целью обоснования отсутствия мероприятий по информационной безопасности. Вместе с тем, описанные в данной подборке подходы позволяют при должной доработке осуществлять выбор алгоритма оценки рисков, поскольку предполагают идентификацию информационных активов, входящих в область оценки. Стоит отметить, что приведенные методы

оценки рисков не учитывают ряд факторов, влияющих на репутационную составляющую бизнеса в части определения угроз информационной безопасности. Не определены источники для угроз информационной безопасности. Вследствие, не полным оказывается список угроз. Не раскрыт ущерб, который может понести организация или предприятие вследствие потери репутации при инциденте информационной безопасности.

Проведенный анализ показывает, что проблематика управления репутационными рисками вследствие инцидентов информационной безопасности актуальна в соответствии со следующими факторами:

- На территории Российской Федерации отсутствует законодательное регулирование инцидентов информационной безопасности, приводящих к потере репутации.
- Стандарты по управлению рисками информационной безопасности имеют международный статус, вследствие этого существует правовая коллизия их правоприменительности в Российской Федерации. Также отсутствуют практики для предприятий и организаций на территории Российской Федерации по проведению мероприятий внутри компаний для минимизации рисков потери репутации.
- В существующей практике применения международных методик оценки рисков не приводится процедура оценки ущерба и алгоритм по управлению репутационными рисками для предприятий и организаций с учетом их отраслевой специфики.

Список использованных источников:

1. Дорохов В.Э. «О рисках потери репутации организации вследствие инцидентов информационной безопасности» (статья) // Безопасности информационных технологий. 2014. - №2 с. 80-82
2. Дорохов В.Э., Янкевский А.В. Управление основными видами взаимоотношений хозяйствующего субъекта с учетом риска потери репутации вследствие нарушения информационной безопасности // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 7, №2 (2015) http://naukovedenie.ru/PDF/24EVN315.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ. DOI: 10.15862/24EVN315
3. ISO/IEC Guide 73:2009 «Risk management – Vocabulary».
4. ISO/IEC 31000:2009 «Risk management – Principles and guidelines».
5. ISO/IEC 31010:2009 «Risk Management – Risk Assessment techniques»/
6. ISO/IEC 27005:2011 «Information technology -- Security techniques -- Information security risk management».
7. Software Engineering Institute (SEI) at Carnegie Mellon University, OCTAVE, www.cert.org/octave/ (Дата обращения 04.03.2013).
8. CCTA Risk Analysis and Management Method // www.cramm.com (Дата обращения 02.05.2013).
9. Information Society Technologies // http://coras.sourceforge.net/ (Дата обращения 02.05.2013).

УДК 004.056

Калинкина Т.И.

Анализ систем мандатного разграничения доступа в СУБД

Средства разграничения доступа к ресурсам баз данных (БД) реализуют некоторую модель разграничения доступа, формализующую правила доступа субъектов доступа к объектам доступа.

Существуют различные модели разграничения доступа (дискреционная, ролевая, мандатная, Биба, Кларка-Вильсона и другие). Основными из них, используемые в современных СУБД, являются дискреционная, ролевая и мандатная (полномочная). Для разграничения доступа к данным, имеющим разную степень конфиденциальности или ценности для ее владельца, используется мандатная модель разграничения доступа. В основе мандатной модели разграничения доступа лежат уровни допуска субъектов и категории конфиденциальности объектов. Каждому субъекту системы присваивается один уровень допуска, каждому объекту – одна категория конфиденциальности.

Практика показывает, что мандатные модели находятся гораздо ближе к потребностям реальной жизни, нежели дискреционные, и представляют собой хорошую основу для построения автоматизированных систем разграничения доступа.

Мандатная модель доступа может быть представлена в виде матрицы доступа, строки которой определяются категориями конфиденциальности объектов, а столбцы – уровнями допуска субъектов. В ячейки таблицы на пересечении каждой строки с каждым столбцом записывается список операций над объектами, которые имеют право выполнять субъекты.

Классическим примером мандатной модели является модель Белла-Ла Падула, на основе которой строятся системы мандатного разграничения доступа.

На сегодняшний день реализацию мандатного доступа в СУБД предлагают ограниченное количество мощных корпоративных СУБД, в частности Линтер и Oracle. СУБД Линтер является отечественной разработкой компании Релэкс. Это реляционная многопользовательская СУБД, которая обеспечивает дискреционный и мандатный способ доступа к данным. СУБД Oracle является мощной зарубежной разработкой корпорации Oracle. В СУБД Oracle также предлагаются решения по обеспечению мандатного доступа к данным.

Проведем анализ средств, реализующих в данных СУБД мандатное разграничение доступа к ресурсам БД, и лежащих в основе их моделей мандатного разграничения доступа. Целью анализа является выявление уязвимостей в реализации средств мандатного разграничения доступа к ресурсам данных СУБД, позволяющих произвести несанкционированный доступ к защищаемой информации, хранимой в БД.

СУБД Oracle Database Enterprise Edition разработана корпорацией Oracle Corporation. Мандатное разграничение доступа в СУБД Oracle Database Enterprise Edition реализовано в подсистеме Oracle Label Security. Разграничение доступа происходит на уровне баз данных, таблиц баз данных и строк таблиц.

Каждый выполняемый SQL-запрос анализируется ядром СУБД, и затем принимается решение о разрешении или отклонении выполнения запроса.

Обозначим категорию конфиденциальности объекта $f_0(o)$, а уровень допуска субъекта $f_s(s)$. Формальная модель мандатного разграничения доступа может быть записана так:

а) $r = read, f_s(s) \geq f_o(o)$;

б) $r = write, f_s(s) = f_o(0)$.

Условие а) соответствует ss-свойству модели Белла-Ла Падула. Условие б) соответствует строгому *-свойству модели Белла-Ла Падула.

Обнаружено, что в СУБД Oracle некоторые области таблиц, например, названия столбцов, не контролируются системой мандатного разграничения доступа. А значит, пользователь может переместить защищаемую информацию в эти области и, таким образом, понизить ее категорию конфиденциальности.

СУБД Линтер Бастион разработана группой компаний РЕЛЭКС. В этой СУБД также реализован механизм мандатного разграничения доступа к данным. В документе «СУБД Линтер. Администрирование средств защита данных» приведен список объектов доступа в СУБД: «В СУБД Линтер Бастион разграничение доступа системой мандатного разграничения доступа выполняется на уровне таблиц, столбцов таблиц и строк таблиц».

На самом деле в СУБД Линтер Бастион отдельные строки не могут иметь уровни конфиденциальности. Уровень конфиденциальности каждого отдельного поля строки равен уровню конфиденциальности столбца, к которому это поле принадлежит.

Мандатная модель разграничения доступа может быть записана так:

а) $r = read$;

б) $r = write, f_s(s) \geq f_o(o)$.

Эти условия вовсе не соответствуют модели Белла-Ла Падула. Любой субъект может прочитать системную информацию о таблице, например, узнать ее имя, количество в ней строк, количество столбцов и параметры файлов, в которых записана таблица, и это может способствовать успешной атаке на базу данных с целью похищения защищаемой информации. Любой субъект может модифицировать таблицу более низкой категории конфиденциальности – например, изменить имя существующего столбца, записав в него некоторую конфиденциальную информацию. Это канал утечки информации.

Также видно, что любой субъект может получать информацию о таблицах, категория конфиденциальности которых выше уровня допуска субъекта. Эта информация может помочь злоумышленнику осуществить взлом базы данных.

Обозначим категорию конфиденциальности столбца $f_0(o)$, а уровень допуска субъекта $f_s(s)$. Информация о столбце – это его имя и тип данных. Формальная модель мандатного разграничения доступа может быть записана так:

а) $r = read$;

б) $r = write, f_s(s) \geq f_o(o)$.

Такие условия не соответствуют свойствам модели Белла-Ла Падула. Видно, что любой субъект может узнать информацию об именах столбцов, категория конфиденциальности которых выше уровня допуска субъекта.

Разграничение на уровне полей реализуется следующей формальной моделью мандатного разграничения:

а) $r = read, f_s(s) \geq f_o(o)$;

б) $r = write, f_s(s) \geq f_o(o)$.

Условие а) соответствует ss-свойству модели Белла-Ла Падула. Условие б) соответствует нестрогому *-свойству модели Белла-Ла Падула.

Здесь также есть канал утечки информации. Субъект может записать информацию высшей категории конфиденциальности в поле низшей категории конфиденциальности, при этом категория конфиденциальности поля остается неизменной, хотя в нем может находиться информация, относящаяся к высшей категории конфиденциальности.

Если субъект пытается записать информацию в объект, категория конфиденциальности которого ниже уровня допуска субъекта, то в СУБД Линтер Бастион такие действия субъекта приводят к повышению категории конфиденциальности объекта. В таком случае хранимая в нем ранее информация становится недоступной для пользователей, для которых она была ранее доступна.

В результате изучения реализаций модели мандатного разграничения доступа в СУБД Oracle Database Enterprise Edition и СУБД Линтер Бастион выявлены следующие недостатки:

1. Защищаемая информация может быть перемещена в области таблиц, не контролируемые системой мандатного разграничения доступа – например, в имена столбцов таблиц.

2. Возможность завышения категории конфиденциальности информации.

3. Возможность записи информации в поле, категория конфиденциальности которого ниже категории конфиденциальности, к которой относится данная информация.

4. Возможность получения любым пользователем системной информации о таблице.

Результат анализа также показал сложность и нетривиальность задачи реализации обеспечения мандатного доступа в СУБД. Особо следует выделить сложность разработки модели мандатного доступа для объектов имеющих иерархическую зависимость как, например, таблицы, строки и ячейки в таблицах.

УДК 004.75

Корнилов В.В., Исаев Е.А., Самодуров В.А.

Угрозы безопасности центров обработки данных и методы обеспечения их надежности и безопасности

Согласно общепринятому определению, центры обработки данных (ЦОД, они же data-center, дата-центры) – это вычислительная инфраструктура, предназначенная для централизованной обработки, хранения и предоставления данных, сервисов, приложений и обеспечивающая высокую степень виртуализации своих ресурсов. К основным задачам ЦОД в первую очередь относятся эффективное консолидированное хранение и обработка данных, предоставление пользователям прикладных сервисов, а также поддержка функционирования внешних приложений.

Обязательные компоненты, входящие в состав ЦОД, можно разделить на три основные группы: технические компоненты, создающие условия для эффективной работы центра и включающие собственно серверы информационных ресурсов, приложений, представления информации, а также служебные серверы, систему хранения данных и резервного копирования, сетевую инфраструктуру, инженерную систему эксплуатации ЦОД и систему безопасности; программное обеспечение (ПО), включающее сервисы инфраструктуры ЦОД и обеспечение корректной работы пользовательских приложений; а также среду организации процессов оказания услуг, в первую очередь их качество и доступность. Основным фактором, характеризующим качество услуг, предоставляемых дата-центром, является допустимое время незапланированного простоя оборудования, в идеале стремящееся к нулю.

Прогнозируется, что в течение ближайших пяти лет большая часть организаций откажется от поддержки собственной серверной инфраструктуры и будет стремиться передать управление их данными поставщикам соответствующих услуг – провайдерам ЦОД. При этом от последних потребуется переход на качественно новый уровень эксплуатации ЦОД и предоставления сервиса. Последнее утверждение является особенно актуальным, так как вопросы сохранности данных, информационной безопасности, обеспечения бесперебойного доступа к данным, становятся первоочередными при передаче функций по хранению и обработке данных «в чужие руки».

При рассмотрении различных видов угроз безопасности ЦОД их можно разделить на две основные группы: техногенного характера, когда источниками угроз являются различные технические средства, и антропогенные, при которых угрозой безопасности является человеческий фактор. В качестве дополнительного способа классификации можно предложить разделение угроз безопасности на внутренние и внешние по отношению к структуре ЦОД.

Анализируя причины и источники внутренних угроз безопасности, к которым в первую очередь относятся различные виды отказов серверного оборудования и инженерных систем ЦОД, необходимо отметить, что наиболее ненадёжной состав-

ляющей ЦОД является обслуживающий персонал, основной источник сбоев в работе ЦОД (около 60% отказов) связан с человеческими ошибками на стадии проектирования, монтажа и обслуживания оборудования, в том числе критически долгая, ошибочная или неадекватная реакция обслуживающего персонала на события.

К основным мерам повышения надежности ЦОД относятся дублирование (иногда многократное) основных узлов и систем ЦОД, что, впрочем, значительно увеличивает стоимость как создания ЦОД, так и его эксплуатации, а также автоматизацию всех систем мониторинга и управления инженерной инфраструктурой ЦОД.

Противодействие внешним угрозам безопасности ЦОД в настоящее время становится наиболее актуальным фактором обеспечения их высокой надежности и безопасности. В качестве наибольшей угрозы безопасности в последнее время все чаще называют воздействие вредоносного ПО и так называемые кибератаки (специально организованное целенаправленное покушение на информационную безопасность компьютерной системы), в сумме опасностей такого рода угрозы составляют уже более половины общего количества: вирусы и черви - 27%, шпионские программы и спам - по 11% и, наконец - атаки из Интернета: 10%.

Для противодействия этим видам угроз необходимо уделять постоянное внимание развитию и совершенствованию программно-технических способов и средств обеспечения информационной безопасности, к которым в частности относятся средства защиты от несанкционированного доступа, антивирусные средства, межсетевые экраны, анализаторы протоколов и системы мониторинга сетей, системы аутентификации и контроля доступа.

Наибольшую опасность здесь представляет один из видов кибератак – DoS атаки (от англ. Denial of Service – отказ в обслуживании) – хакерская атака на вычислительную систему с целью довести её до отказа, то есть создание таких условий, при которых легальные пользователи системы не могут получить доступ к предоставляемым системным ресурсам (серверам), либо этот доступ затруднён. Проблема состоит в том, полностью защититься от DoS-атак на сегодняшний день невозможно, так как пока не существует совершенно надежных систем и методов противодействия этой угрозе. Тем не менее, использование современных аппаратно-программных средств защиты, а также правильная организация методов противостояния может существенно повысить безопасность ЦОД.

УДК 004.056

Панченко А.А.

Аппаратно-программный комплекс оценки эффективности блокирования радиосигналов генератором электромагнитного шума

Компьютерные сети современных предприятий, в которых обрабатывается конфиденциальная информация, имеющая реальную коммерческую ценность, являются потенциальной мишенью для злоумышленников. В случае, если такая

сеть подключена к другим сетям, в частности, к сети Интернет, что часто требуется для эффективной работы, проникновение в такую сеть и организация утечки информации из нее в наши дни является лишь вопросом времени при соответствующей квалификации злоумышленника. Естественным решением в таком случае становится полное отключение от всех сетей и создание изолированной системы (так называемый «воздушный зазор», англ. air gap). Однако даже такой радикальный способ не является гарантией полного предотвращения возможности утечки информации.

В 2014 году на 9-й международной конференции IEEE MALCON 2014 исследователи из израильского университета имени Бен-Гуриона показали работающий комплекс программ, позволяющих в типовых условиях получить информацию из изолированной компьютерной системы с использованием побочных электромагнитных излучений (ПЭМИ), генерируемых различными типами видеоинтерфейсов [1]. Источником излучений служили широко используемые сейчас интерфейсы VGA, DVI и HDMI, а в качестве приемника применялся штатный приемник FM-радио из состава смартфона.

Проникновение специально созданной вредоносной программы, выполняющей генерацию требуемых ПЭМИ, в изолированную систему осуществляется со съемных носителей информации (USB Flash накопители) с использованием вновь выявленных уязвимостей операционной системы (ОС) и иного программного обеспечения (ПО). Несмотря на то, что этот способ является сложным, его успешная реализация все же возможна (примерами являются программы семейства StuxNet, проникшие в сети промышленных объектов Ирана и России, а также их последователи). Заражение смартфона, практически всегда имеющего подключение к Интернет, выполнить гораздо проще.

Для блокирования возможности утечки информации за счет ПЭМИ на объектах информатизации (ОИ) применяются широкополосные генераторы электромагнитного шума (ГШ), маскирующие радиосигналы от средств вычислительной техники. Такие ГШ являются сложными устройствами, работающими в продолжительном или даже круглосуточном режиме, и вследствие изменения условий окружающей среды, а также неизбежного «старения» электронных компонентов, параметры генерируемого шумового сигнала могут выходить за допустимые пределы, что создает условия для приема ПЭМИ злоумышленником.

Для оценки эффективности блокирования ПЭМИ с помощью ГШ создается программно-определяемая радиосистема (ПОР, англ. Software Defined Radio, SDR), состоящая из аппаратного модуля, представляющего собой ТВ-тюнер стоимостью менее $12 на основе чипа RTL2832U с радиомодулем Rafael Micro R820T, внешний вид и внутреннее устройство которого представлены на рисунке 1, и программной компоненты, разработанной с использованием свободно распространяемого ПО с открытым исходным кодом.

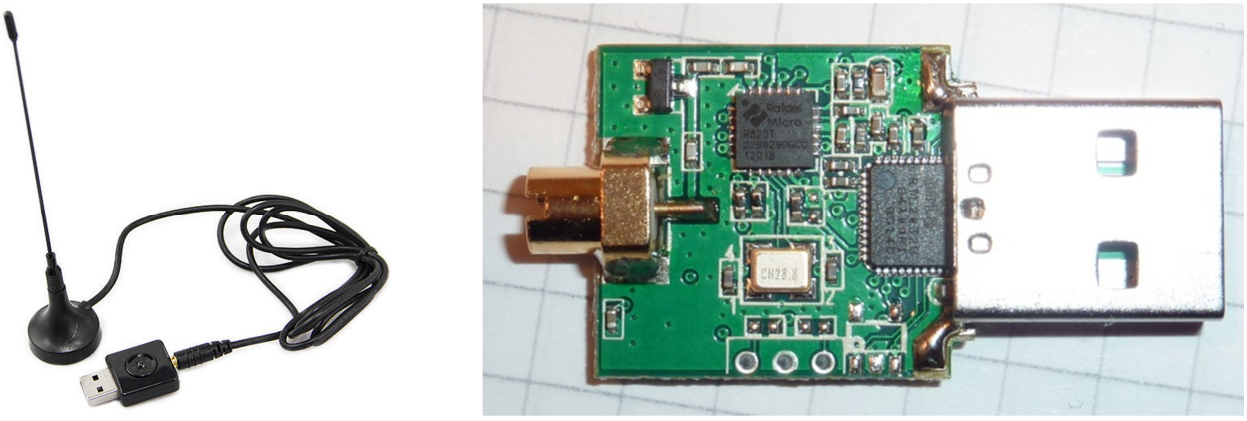


Рисунок 1 – Внешний вид и внутреннее устройство ТВ-тюнера на основе чипа RTL2832U с радиомодулем Rafael Micro R820T

Программная компонента разработанного аппаратно-программного комплекса (АПК) создана с использованием следующего свободно распространяемого ПО с открытым исходным кодом:

– ОС Arch Linux (64-х разрядная);
– интегрированная среда разработки QT Creator 3.4 совместно с библиотекой QT 5.4;
– компилятор C++ из состава GCC 4.8;
– библиотека поддержки работы с ТВ-тюнером rtl-sdr версии 0.5.3;
– библиотека быстрого преобразования Фурье FFTW версии 3;
– библиотека отображения технической графики Qwt версии 6.1.2.

Для заданной несущей (центральной) частоты радиомодуля f_0, которая может находиться в диапазоне от 24 МГц до 1766 МГц, ТВ-тюнер выдает сэмплы в виде синфазной $I(t)$ и квадратурной $Q(t)$ составляющих с максимальной частотой дискретизации $F_{АЦП}$ до 2,4 МГц [2]. После выполнения быстрого преобразования Фурье (БПФ) с числом точек N от 256 до 4096, формируется участок спектра в диапазоне частот

$$\left[f_0 - \frac{F_{АЦП}}{2}, f_0 + \frac{F_{АЦП}}{2} \right]$$

с разрешающей способностью

$$\Delta f = \frac{F_{АЦП}}{N}.$$

На каждой частоте f_0 выполняется серия из M циклов захвата по N сэмплов в каждом. В результате для каждой частотной компоненты спектра формируется выборка из M значений амплитуды $A_i, i = \overline{1, M}$.

Для каждой полученной выборки определяются значения выборочного среднего $\overline{A}$ и выборочной дисперсии S^2 в соответствии с выражениями

$$\overline{A} = \frac{1}{M} \sum_{i=1}^{M} A_i, \qquad S^2 = \frac{1}{M-1} \sum_{i=1}^{M} (A_i - \overline{A})^2.$$

При увеличении объема выборки выборочное среднее стремится к значению математического ожидания μ, а выборочная дисперсия – к значению дисперсии σ^2

$$\lim_{M\to\infty} \overline{A} = \mu \qquad \lim_{M\to\infty} S^2 = \sigma^2,$$

и эти значения используются для построения теоретической функции плотности распределения амплитуд сигнала для нормального закона

$$f(A) = \frac{1}{\sigma\sqrt{2\pi}} e^{-\frac{(A-\mu)^2}{2\sigma^2}}.$$

Для каждой частотной компоненты разработанный АПК производит анализ как амплитуды сигнала, так и соответствия распределения амплитуд сигнала нормальному закону распределения, характерному для идеального шумового сигнала.

Окно программы, отображающее графики, полученные с помощью разработанного АПК, при анализе участка спектра в диапазоне частот от 94 МГц до 98 МГц при выключенном ГШ представлено на рисунке 2 слева, а при работающем ГШ – на рисунке 2 справа.

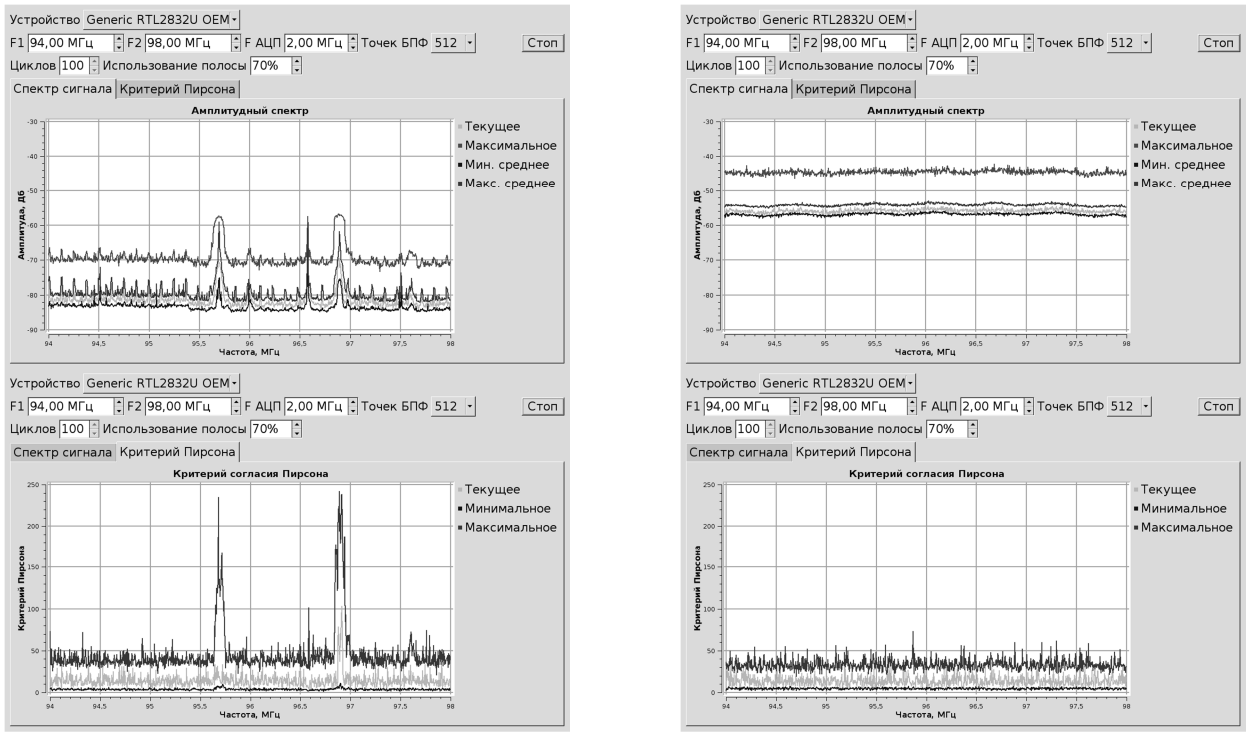


Рисунок 2 – Анализ диапазона частот от 94 МГц до 98 МГц при выключенном ГШ (слева) и работающем ГШ (справа)

В случае, если амплитуда сигнала для каждой из частотных компонент при работающем ГШ становится выше соответствующей амплитуды при выключенном ГШ (рисунок 2 сверху), и значение статистического критерия согласия Пирсона (рисунок 2 снизу), определяющего степень соответствия распределения амплитуд сигнала нормальному закону, не превышает некоторого значения

для всех частотных компонент при работающем ГШ, делается вывод о том, что шумовой сигнал превалирует во всем анализируемом диапазоне частот и ГШ эффективно выполняет маскирование сигнала ПЭМИ.

Библиографический список

1. M. Guri, G. Kedma, A. Kachlon and Y. Elovici, «AirHopper: Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Fre-quencies», in 9th IEEE International Conference on Malicious and Unwanted Software (MALCON 2014), Puero Rico, Fajardo, 2014.

2. Панченко А.А. Оценка возможностей мониторинга радиоэфира с помощью программно-определяемой радиосистемы на основе чипа RTL2832U // Вестник Рязанского государственного радиотехнического университета. 2014. № 50-1. С. 132-135.

УДК 378.2

Пржегорлинский В.Н.

История, состояние, перспективы развития и проблемы подготовки, переподготовки и повышения квалификации кадров в области информационной безопасности в Рязанской области

Подготовка специалистов

Введение

Одним из основных направлений деятельности по обеспечению информационной безопасности Российской Федерации является подготовка, переподготовка и повышение квалификации кадров в области информационной безопасности.

История

В стране

Для подготовки специалистов в области информационной безопасности Минобразование России в 1995 – 1998 годах утверждает три первых государственных образовательных стандарта по специальности 2206 – «Организация и технология защиты информации», предусматривавших подготовку специалистов с квалификациями «математик» (1995 г.), «инженер» (1997 г.) и «менеджер» (1998 г.).

В целях успешной координации и контроля деятельности по подготовке специалистов в области информационной безопасности в ноябре 1996 года на базе Института криптографии, связи и информатики (ИКСИ) Академии ФСБ России создается учебно-методическое объединение (УМО) высших учебных заведений по образованию в области информационной безопасности. Учредительный пленум УМО состоялся в ИКСИ 26-27 ноября 1996 года. В его работе принимали участие и представители Рязанского государственного радиотехнического университета (в то время Рязанской государственной радиотехнической академии (РГРТА)).

В Рязанской области

Единственным вузом в Рязанской области, который решил начать подготовку специалистов в области информационной безопасности, была (в то время) Рязанская государственная радиотехническая академия (РГРТА). Большую практическую помощь в принятии такого решения вузу оказали проректор МИФИ Погожин Николай Семенович, заведующий кафедрой МИФИ Малюк Анатолий Александрович, начальник ИКСИ Академии ФСБ России Погорелов Борис Александрович, зам. начальника ИКСИ Белов Евгений Борисович. В начале 1996 г. была начата работа по получению лицензии на право подготовки специалистов по специальности 2206 – «Организация и технология защиты информации» с квалификацией «математик» - единственной в то время специальности в области информационной безопасности, по которой был утвержден государственный образовательный стандарт высшего профессионального образования.

В разработке основной образовательной программы (ООП) по названной специальности нашему вузу большую помощь оказал коллектив ИКСИ Академии ФСБ России.

В марте 1997 года РГРТА получила лицензию на право подготовки специалистов по названной специальности и с 1 сентября этого же года впервые начала в Рязанской области подготовку специалистов по этой специальности со сроком обучения 5,5 лет. РГРТА была также одним из первых вузов России, в котором была начата подготовка специалистов по этой, тогда единственной утвержденной Минобразованием России, специальности в области информационной безопасности. Подготовка осуществлялась на кафедре ЭВМ факультета вычислительной техники. В 2000-м году специальность 2206 – «Организация и технология защиты информации» с квалификацией выпускника – «математик» была переименована в специальность 075200 – «Компьютерная безопасность» и был разработан и утвержден новый образовательный стандарт по этой специальности. В 2005 году вновь был изменен номер специальности – специальность получила номер 090102, а в 2011 году – номер 090301, а в 2014 году – номер 10.05.01.

Первый выпуск математиков по специальности 2206 – «Организация и технология защиты информации» состоялся в г. Рязани в РГРТА в феврале 2003 года.

Состояние в Рязанской области

В настоящее время наш вуз, получивший в 2006 году статус университета, по-прежнему является в Рязанской области единственным вузом, осуществляющим подготовку специалистов в области информационной безопасности. Набор – 1 группа студентов ежегодно на специальность «Компьютерная безопасность».

За период с 2003 г. (год первого выпуска) по 2015 г. включительно вуз подготовил более 200 специалистов в области информационной безопасности, которые востребованы и работают в органах государственной власти, предприятиях, учреждениях и организациях не только Рязанской области, но и других регионах Российской Федерации.

В 2008-2010 годах в РГРТУ совершенствуется система обеспечения информационной безопасности вуза, интенсивно развивается материально-

техническая база для проведения научно-исследовательских и опытно-конструкторских работ, создаются новые учебно-научные лаборатории для подготовки, переподготовки и повышения квалификации специалистов в области информационной безопасности. Одним из наиболее важных мероприятий, осуществленных в этот период, явилось создание в апреле 2009 г. специализированной кафедры «Информационная безопасность», на которую с 1 сентября этого же года полностью была передана подготовка специалистов по специальности «Компьютерная безопасность».

По итогам широкого экспертного опроса, проведенного в 2010 году в рамках проекта «Лучшие образовательные программы инновационной России», основная образовательная программа по специальности 090102 – «Компьютерная безопасность», реализуемая в РГРТУ, вошла в число лучших образовательных программ инновационной России.

С 1 сентября 2013 года в РГРТУ начата подготовка специалистов с высшим профессиональным образованием по специальности 090303 – «Информационная безопасность автоматизированных систем» с набором одной группы ежегодно.

Перспективы развития в Рязанской области

В 2012 году кафедрой совместно с ректоратом был разработан План инновационного развития кафедры до 2017 года. В соответствии с этим планом в период 2012-2016 годов должно осуществляться дальнейшее развитие подготовки кадров в области информационной безопасности, одним из основных мероприятий этого развития является начало с 1 сентября 2016 года подготовки специалистов со средним профессиональным образованием по специальности 10.02.03 – «Информационная безопасность автоматизированных систем» с набором 1 группы ежегодно.

Проблемы в стране

Основная проблема – отсутствие в Федеральном законе от 21.12.2012 «Об образовании в Российской Федерации» нормы о выдаче выпускнику диплома государственного образца.

Переподготовка и повышение квалификации

История в Рязанской области

Учитывая созданный научный и учебно-методический задел, материально-техническую базу и наличие лицензии на подготовку специалистов по специальности 2206 – «Организация и технология защиты информации» Минобразование России включило РГРТА в число первых четырнадцати вузов Российской Федерации, в которых по его приказу от 20.08.1997 г. № 1781, изданному во исполнение решения Межведомственной комиссии Совета Безопасности Российской Федерации от 28.09.95 г. № 8.3 «О состоянии работ по совершенствованию подготовки кадров по проблеме информационной безопасности», должны были быть созданы региональные учебно-научные центры по проблемам информационной безопасности в системе высшей школы. Во исполнение приказа Минобразования России приказом ректора от 02.02.1998 г. № 14 в РГРТА был создан региональный учебно-научный центр Центрального региона по проблемам информационной

безопасности в системе высшей школы при Рязанской государственной радиотехнической академии (РУНЦ РГРТА «Информационная безопасность»), который в связи с изменением в 2006 году статуса вуза на университет был переименован в РУНЦ РГРТУ «Информационная безопасность».

Основные виды деятельности названного центра – повышение квалификации специалистов, проведение НИОКР и оказание услуг в области информационной безопасности.

РУНЦ РГРТА «Информационная безопасность» в 1998 г. начинает работу по подготовке получения лицензий Минобороны России, ФАПСИ и Гостехкомиссии России на деятельность по защите информации, которая была успешно завершена в середине 2000 г. получением трех лицензий ФАПСИ, одной лицензии Гостехкомиссии России и одной лицензии Минобороны России на деятельность в области защиты информации.

Повышение квалификации специалистов в области информационной безопасности в Рязанской области впервые было начато в РГРТА в октябре 1999 года с обучения группы специалистов ФГУП «ОКБ «Спектр» (г. Рязань) в количестве 10 человек по дополнительной образовательной программе «Защита информации в автоматизированных системах» объемом 72 часа, согласованной с Гостехкомиссией России.

В 2001 году в г. Рязани создается негосударственное образовательное учреждение «Региональный научно-технический центр экономической и информационной безопасности» (РНТЦ ЭКИБ), который с 2005 года начинает повышение квалификации специалистов в области информационной безопасности.

Состояние в Рязанской области

В настоящее время в Рязанской области повышение квалификации осуществляют два образовательных учреждения:

- ФГБОУ ВПО «РГРТУ»;
- РНТЦ ЭКИБ.

В РГРТА, а с 2006 года в ФГБОУ ВПО «РГРТУ», прошли повышение квалификации, в том числе по 72-часовым дополнительным образовательным программам, согласованным с Гостехкомиссией, а затем и с ФСТЭК России, более 100 человек, среди которых более 20 государственных гражданских служащих и более 40 служащих муниципальных органов Рязанской области, в том числе 10 человек на базовой кафедре вуза в ООО IBS Platformix в г. Москве. Всем слушателям после успешного окончания обучения выданы удостоверения государственного образца.

В РНТЦ ЭКИБ, начиная с 2005 года, повышение квалификации по краткосрочным программам объемом 72 часа и 120 часов, согласованным с ФСТЭК России и с 8-м Центром ФСБ России, прошло более 300 человек.

Перспективы в Рязанской области

ФГБОУ ВПО «РГРТУ» планирует в период с 2015 по 2017 годы:

- увеличить количество учебных программ повышения квалификации специалистов в области информационной безопасности с 2-х до 5-и;

- начать в 2015 году совместно с РНТЦ ЭКИБ переподготовку специалистов в области информационной безопасности в объеме до 1200 часов.

Проблемы в стране

Основная проблема та же, что и при подготовке специалистов в области информационной безопасности – невозможность выдачи документов государственного образца.

УДК 004.56.52

Сухов В.Е.

Анализ современных подходов к обнаружению аномалий в функционировании автоматизированных систем и пути их дальнейшего развития

В настоящее время, с совершенствованием вычислительной техники и программного обеспечения, роль автоматизированных систем (АС) в обработке информации неуклонно возрастает. Более 90% важной и критически важной для организации информации или полностью или на каком-либо этапе жизненного цикла обрабатывается в АС и эта доля продолжает неуклонно повышаться. Одновременно растут скорость обработки, объемы обрабатываемой информации, масштабы АС, цена обрабатываемой информации, а отсюда и рост интереса к ней злоумышленников. Таким образом, одной из серьезнейших проблем становится компьютерная безопасность, слежение за состоянием АС, поиск сбоев и аномалий в работе АС. Все это делает особо важной задачу разработки программных средств, решающих задачу обнаружения аномалий в поведении АС, которые несут определенную угрозу как целостности информации, так и ее конфиденциальности.

Основная идея обнаружения аномалий состоит в том, что необычные отклонения в тех или иных данных зачастую могут свидетельствовать о факте проведения атаки. Существующие методы анализируют данные различной природы, которые могут относиться к поведению пользователя [1], режиму работы программ [2], характеристикам сетевого трафика, последовательности системных вызовов от уязвимых процессов к ядру операционной системы и т.д.

Системы обнаружения аномалий, в отличие от других типов систем обнаружения вторжений, являются более гибкими и позволяют обнаруживать неизвестные атаки. Они основаны на предположении, что все действия злоумышленника обязательно чем-то отличаются от поведения обычного пользователя.

Работе систем обнаружения аномалий предшествует период накопления информации, когда строится концепция нормальной активности системы, процесса или пользователя. Она становится эталоном, по которому оцениваются последующие данные.

Построение шаблона нормального поведения часто осложняется отсутствием данных, которые содержат аномалии. Поэтому обучение приходится проводить только на положительных примерах, что значительно усложняет задачу. Часто по

той же причине тестирование систем обнаружения аномалий тоже проводится при отсутствии реальных данных с «содержанием» атак. В этом случае используют перекрестные тесты, когда данные работы одного субъекта проверяются по профилю другого.

В настоящее время имеется ряд трудностей при использовании применяемых методов обнаружения аномалий в поведении АС:

– сложность выделения признаков эталонов, связанная с тем, что практически невозможно адекватно оценить текущее состояние, выделить какие-либо признаки как эталонные на основе только полученных данных;

– необходимость проведения обязательного предварительного сбора информации о нормальной активности системы без возникновения аномалий;

– требуемый значительный объем анализируемой выборки;

– сложность обеспечения высокой оперативности и вероятности обнаружения из-за выявления большого числа фактов, способных вызвать аномалии, значительных вычислительных затрат на анализ поведения АС в штатных режимах;

– сложность обнаружения аномалий в условиях многозадачности, многопоточности.

Необходимо отметить, что большинство сложностей вытекает из применяемых методов и при минимизации одних увеличивается влияние других. Таким образом, задача создания новых эффективных методов быстрого обнаружения аномалий в поведении АС для противодействия сетевым атакам является актуальной на сегодняшний день задачей, имеет первоочередное значение и обуславливает необходимость совершенствования теории и практики их разработки.

Кроме того вне зависимости от метода, лежащего в основе системы обнаружения аномалий, актуальной является проблема получения объективного показателя оценки эффективности методик обнаружения аномалий. Такой показатель окажется полезным не только разработчикам систем обнаружения аномалий для создания новых и более эффективных методик, но и обычным потребителям для выбора наиболее оптимальной системы перед покупкой.

В качестве таких показателей можно использовать такие численные характеристики как количество обнаруживаемых аномалий, вероятность ложного срабатывания, вероятность корректного определения аномалии, количество идентифицируемых воздействий. Однако каждая из этих метрик оценивает различные аспекты и по отдельности не дает полной характеристики системе, не позволяя дать ей объективную оценку. Даже наличие данных о нескольких показателях не дает полной картины для сравнения систем обнаружения аномалий. Например, непонятно какая из них лучше – та, которая обнаруживает больше аномалий или та, которая имеет меньшую вероятность ложного срабатывания при прочих одинаковых показателях.

В работах [3] и [4] авторы предлагают использовать подход теории информации для получения одного емкого показателя эффективности систем обнаружения вторжений (СОВ). Результаты позволяют численно оценить эффективность каждой из СОВ. Результаты показывают значительное отставание СОВ, исполь-

зующих сигнатурный анализ. Системы обнаружения аномалий также не показывают хороших результатов, и поэтому необходима разработка новых методик обнаружения аномалий.

В статье [4] для решения задачи обнаружения аномалий в сетевом трафике предлагается использовать подход на основе реконструкции модели сетевого трафика. Подход заключается в реконструкции модели трафика по временному ряду данных о количестве пакетов, прошедших через канал связи за определенный промежуток времени. Так как авторы пытаются реконструировать уравнения, описывающие изменения системы, то предложенная ими метрика для такого подхода будет выше, чем у других систем обнаружения аномалий.

В 1999 году Уоррендер и соавторы [5] провели сравнительное исследование различных методов распознавания образов, применяющихся для обнаружения аномалий в системных вызовах. Были исследованы такие методы, как анализ последовательностей, частотный анализ, добыча данных (data mining), конечные автоматы. В работе было установлено, что использование скрытых марковских моделей (СММ) для распознавания позволяет добиться наилучших показателей качества обнаружения аномалий, то есть максимальной вероятности правильного обнаружения и минимальной вероятности ложного срабатывания. Достоинством этого метода также является возможность локализовать аномалию с точностью до отдельного системного вызова, в то время как другие методы констатируют лишь факт наличия или отсутствия аномалии в длинных цепочках. Однако метод, основанный на использовании СММ, является более трудоёмким, чем другие рассмотренные методы, в особенности на стадии обучения.

В статье [6] рассматривается возможность уменьшения трудоёмкости метода обнаружения аномалий в системных вызовах с использованием СММ за счёт выбора минимального числа состояний модели, гарантирующего достижение исходно заданных показателей качества обнаружения.

В работе [7] излагается подход к выявлению аномальных событий в потоке сетевого трафика на основе предложенной авторами гибридной корреляции событий (ГКС). Основная идея ГКС состоит в том, что бы аномальные события искать как нарушения нормального течения событий. Нормальное течение событий определяется совокупностью высоковероятных закономерностей, обнаруженных на данных нормального течения событий и определяющих в определённом смысле закон нормального течения событий. Разработанная на базе метода система была применена к анализу данных сетевого трафика сервера системы передачи данных СО РАН. Было обнаружено значимое изменение в закономерностях нормального и анормального течения событий.

Для построения систем обнаружения аномалий можно использовать различные технологии. В последние годы большое внимание уделяется изучению методов биологического моделирования искусственного интеллекта [8,9], таких как искусственные нейронные сети и искусственные иммунные системы, безусловно являющиеся одним из перспективных подходов к решению задач обнаружения аномалий.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Lane T., Brodley C. E. An application of machine learning to anomaly detection // Proc. 20th NIST-NCSC National Information Systems Security Conference. 1997. P. 366-380.

2. Forrest S., Hofmeyr S. A., Somayaji A., Longstaff A. A sense of self for UNIX processes // Proc. IEEE Symposium on Security and Privacy. 1996. P. 120–128.

3. Guofei Gu, Prahlad Fogla, David Dagon, Wenke Lee Measuring Intrusion Detection Capability: An Information-Theoretic Approach – 2006 // Proceedings of the 2006 ACM Symposium on Information, computer and communications security – P. 90-101.

4. Артамонов В. А., Лепешкин О. М. Подход к реализации сетевой системы обнаружения аномалий на основе реконструкции модели сетевого трафика // «Инфокоммуникационные технологии» Том 5, № 3, 2007, с. 145-147.

5. Warrender C., Forrest S., Pearlmutter B. Detecting intrusion using system calls: alternative data models // Proc. IEEE Symposium on Security and Privacy. 1999. P. 133-145.

6. Аникеев М. В. Метод обнаружения аномалий на основе скрытых марковских моделей с поиском оптимального числа состояний, Россия, г. Таганрог, ТРТУ.

7. Витяев Е. Е., Ковалерчук Б. Я., Федотов А. М., Барахнин В. Б., Дурдин Д. С., Белов С. Д., Демин А. В. Обнаружение закономерностей и распознавание аномальных событий в потоке данных сетевого трафика, 2008.

8. Гальцев А.А. Системный анализ трафика для выявления аномальных состояний сети, 2013.

9. Печенкин А.И. Высокопараллельная система выявления сетевых уязвимостей на основе генетических алгоритмов, 2013.

УДК 004.77

Тарасов П.А., Исаев Е.А., Корнилов В.В.

Основные методы обеспечения информационной безопасности сетей WSN

В настоящее время широкое распространение получили беспроводные сети датчиков (Wirelss Sensor Network),- самоорганизующиеся сети из множества пространственно распределенных автономных датчиков (сенсоров), и исполнительных устройств, которые взаимодействуют между собой с помощью радиоканала и служат для сбора данных о различных физических величинах (температура, уровень шума, вибрация, давление, уровень загрязнения и т.д.). Каждый узел в сети WSN обычно состоит из четырех частей:

- Датчик, преобразующим физическое значение, представляющее интерес, в электрический сигнал.

•Микроконтроллер, предусматривающий аналогово-цифровое преобразование и возможности вычисления и хранения.

•Радио-приемопередатчик для обеспечения возможности беспроводной связи.

•Внутренний или внешний источник питания (например, электрохимическая или солнечная батареи).

Возможности датчиков разнообразны и определяются условиями их применения, и это отражается на их стоимости и размерах. Часто пользователями предъявляются жесткие требования к временным задержкам при передаче информации, например, для случая необходимости управления технологическими процессами в режиме реального времени.

Для таких сетей традиционные методы обеспечения информационной безопасности не всегда применимы вследствие следующих причин:

•Доступность среды передачи.

•Относительная незащищенность узлов сети от злоумышленника.

•Динамическое изменение топологии сетей, отсутствие целостной инфраструктуры.

•Относительная невозможность анализа всего трафика на предмет обнаружения аномалий.

•Относительная новизна технологии, подходы к обеспечению безопасности отличаются от проводной среды и недостаточно проработаны.

•Невозможность использования в датчиках стойкой криптографии из-за ограниченности их вычислительных ресурсов. Основное энергопотребление в них уходит именно на передачу данных.

•Концепция построения WSN еще не сформировалась окончательно и не выразилась в четкие аппаратные и программные решения.

По этим причинам беспроводные сети датчиков обладают большей уязвимостью по сравнению с традиционными сетевыми технологиями, тогда как рост популярности WSN, напротив, привлекает к ним дополнительные ресурсы злоумышленников.

В данном обзоре предпринята попытка провести систематизацию видов атак и уязвимостей WSN различных типов. Рассмотрены следующие типы атак: физическое воздействие, Node Replication (клонирование узла), прослушивание и анализ трафика, Jamming (создание помех), Sinkhole (атака воронки), Sybil (атака Сибиллы), Denial of Sleep (отказ в обслуживании), атака на протоколы сихронизации времени, BlackHole/GreyHole (черная и серая дыры), WormHole (червоточина).

Для каждой атаки продемонстрированы возможные средства защиты и предупреждения, обнаружения и возможного противодействия, а такжепоказана необходимость разработки и внедрения новых высокотехнологичных решений по обеспечению безопасности WSN.

УДК 65.012.8

Тетеркин В.Ф., Митрошин А.А., Чернышёв С.В.

Регламент сопровождения межсетевого экрана, сертифицированного ФСТЭК

Межсетевые экраны, сертифицированные ФСТЭК, играют важную роль в обеспечении корпоративной информационной безопасности, в том числе и информационных систем персональных данных. Как показала практика эксплуатации таких экранов в управлении ТКиИР РГРТУ, эффективность и результативность их применения зависит от установленного и жестко выполняемого регламента, который сводится к следующему.

1. Издание приказа по университету, который определяет:

- место размещения межсетевого экрана;
- подразделение, отвечающее за его функционирование;
- дату ввода межсетевого экрана в эксплуатацию;
- состав комиссии по приёмке межсетевого экрана в эксплуатацию;
- лицо, уполномоченное утвердить акт о приёмке в эксплуатацию межсетевого экрана;
- назначение ответственного за сопровождение межсетевого экрана и ведение его формуляра;
- назначение ответственного за проведение проверок, определение периодичности их проведения и набор контролируемых параметров;
- порядок внесения изменений в конфигурационные файлы межсетевого экрана.

2. Назначенное приказом подразделение проводит работы по монтажу межсетевого экрана в определённом приказом месте и осуществляет его начальное конфигурирование. Копии конфигурационных файлов сохраняются установленным в организации образом.

3. В определённое приказом время комиссия комиссия рассматривает результаты выполненных работ и оформляет акт о вводе межсетевого экрана в эксплуатацию. Акт утверждается лицом, определённым в приказе.

4. Лицо, определённое в приказе, вносит в формуляр сведения о начальной конфигурации межсетевого экрана.

5. В процессе эксплуатации межсетевого экрана возникает необходимость внесения изменений в конфигурационный файл. Изменения в конфигурационный файл вносит лицо, определенное в приказе на основании документов, определенных в приказе. При внесении любых изменений делаются соответствующие записи в формуляре межсетевого экрана. Копия конфигурационного файла сохраняется.

6. Определенное приказом лицо с определённой приказом периодичностью проводит проверки по параметрам, определенным приказом. Факт проведения проверки фиксируется в формуляре межсетевого экрана.

7. Вывод межсетевого экрана из эксплуатации осуществляется на основании приказа, определяющего:

- дату вывода из эксплуатации;
- лицо, ответственное за вывод межсетевого экрана из эксплуатации;
- состав комиссии, подтверждающей факт вывода межсетевого экрана из эксплуатации;
- лицо, имеющее полномочия утверждения акта о выводе межсетевого экрана из эксплуатации.

Следование такому регламенту позволяет полностью контролировать все действия, совершаемые с межсетевым экраном, что способствует совершенствованию системы защиты информации в информационных системах.

УДК 004.62

Чибозо Ф. К. Н.

Обеспечение информационной безопасности предприятия

Риски в вопросе о безопасности информации представляют значительную угрозу для предприятий из-за возможных потери денежных средств и нахождении в тяжелых финансовых положений, потери существенных служб сетей, или еще потери доверия клиентов и других покушений на репутацию, которую они вовлекают. Управление рисками - один из ключевых элементов предупреждения подлогов он-лайн, краж личности, ухудшений Web-сайтов, потерь личных данных и других различных инцидентов относительно безопасности информации. Отсутствие крепкой системы управления рисками организации благоприятствует многочисленным типам киберугроз.

Безопасность информационных систем (SSI) - совокупность технических, организационных, правовых и человеческих ресурсов, необходимых и реализованных в целях сохранения, восстановления и обеспечения безопасности информационной системы. Обеспечение безопасности информационных систем является деятельность информационных систем управления.

Сегодня безопасность является важным вопросом для компаний, и для всех игроков вокруг него. Он больше не ограничивается исключительно к роли программиста. Его цель в долгосрочной перспективе является поддержанием доверия пользователей и клиентов. Целью в среднесрочной перспективе является согласованность всей информационной системы. В краткосрочной перспективе, цель в том, чтобы каждый имел доступ к информации, в которой она нуждается. Норма, обсуждающая SMSI - международная Организация нормализации 27001, настаивает на Целостность - Конфиденциальность.

«Информационная система представляет существенное достояние организации, которое необходимо защищать. Информационная безопасность гаран-

тирует использовании материальные или программные ресурсы организации только в предусмотренных рамках»

Безопасность информационных систем имеет следующие цели:

•Наличность: Система должна функционировать без дефекта в течение предусмотренных пляжей использования и гарантировать доступ к службам и ресурсам, установленным с ожидаемым временем отклика.

•Целостность: Данные должны быть теми, что ожидаем, и не должны быть ухудшенными случайно, неправомерно или враждебно. Рассмотренные элементы должны быть точными и полными.

•Конфиденциальность: только уполномоченные лица имеют доступ к информации, предназначенной для них. Несанкционированного доступа должно быть предотвращено.

Другие аспекты могут быть рассмотренными также целями безопасности систем информация, такими, как:

•Разметка (или «Доказательство»): гарантированная, что доступы и попытки доступа к рассмотренным элементам начерчены и что эти следы сохранены и годны для эксплуатации.

•Аутентификация: Идентификация пользователей является основой для управления доступом к соответствующим рабочим областям и поддержания доверия в отношениях обмена.

•Неотрекаемость и вменение: Ни один пользователь не должен иметь возможность оспорить операции которые он провел в рамках его авторизованных действий, и ни одной третьей стороны не должна быть в состоянии приписать себе действия другого пользователя.

Раз определенны цели обеспечения безопасности, воздействующие риски на каждый из этих элементов, могут быть оцененными в зависимости от угроза. Общий уровень безопасности информационных систем определен уровнем безопасности наиболее слабого звена. Предосторожности и контрмеры должны быть рассмотренными в зависимости от уязвимости, присущей контексту, в котором информационная система как ожидается, обеспечит сервис и поддержку.

Надо для этого оценить:

- тяжесть последствий, в случае когда риски осуществились бы,
- вероятность рисков (или потенциал, или вероятность возникновени).

Для обеспечения информационных безопасности систем, процесс включает в себя:

•оценки риска и критичности: какие риски и какие угрозы, на каких данных и какой деятельности, с какими последствиями?

Мы говорим о «карте риска». От качества этой картографии зависит качества безопасности, который будет реализован.

•найти и выбрать парады: что будет в безопасности, когда и как?

Трудный этап выбор безопасности в контексте ограниченных ресурсов (время, навыки и деньги), лишь некоторые решения могут быть реализованы.

•осуществлять защиту, и проверять ее эффективность.

Это завершение фазы анализа и с этого начинается защита информационной системы. Часто слабость этой фазы - забывать проверять, что защита очень эффективна(функциональные испытания в ограниченном режиме, испытания восстановления данных, вредоносных атак тесты, и т.д.).

Планирование безопасности информационных систем

Этап 1: Периметр и Политика.

Этап 2: Оценка опасностей.

Этап 3: Обработка рисков и идентифицировка остаточный риск.

Этап 4: Отбирать меры по осуществлению (Приложение А к ISO27001).

Список литературы:

1. ISO/CEI 27005:2011, Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information
2. http://www.iso.org/iso/fr/home/news_index/news_archive/news.htm?refid=Ref1451
3. Bernard Foray, La fonction RSSI (Responsable Sécurité Système d'Information) - Guide des pratiques et retours d'expérience - 2e édition, Dunod 201
4. Неотложная правовая помощь N°7 2010 г. С. 36 – 48

УДК 004.62

Щучкин А.Е.

Контроль информационных потоков в организации

Важнейшим условием стабильного функционирования организации является грамотная работа с информацией. Для осуществления процесса управления жизненно необходим контроль информационных потоков.

Одним из признаков информации и ее коренным отличием от других продуктов производства принято полагать ее неизменность в процессе копирования. Однако, это не совсем так. В процессе обработки информации всегда участвует человек, Оценивая уровень безопасности системы по самому слабому звену, мы неизбежно вынуждены рассматривать участие человека именно в этом аспекте.

Можно обозначить несколько ключевых точек, при прохождении через которые, информация, обрабатываемая в системе, претерпевает изменения и может быть искажена:

- При получении информации исполнителем. Информация может быть изначально искажена, неправильно понята или получена из некорректного источника.
- При сбоях в каналах связи. Информация может быть искажена, неполна или неактуальна.

- При избыточности информации.
- При обработке информации исполнителем. Возможные причины: недостаточная квалификация, случайные ошибки, временные и факторы, большой объем, недостаточная техническая оснащенность.
- При передаче информации исполнителем. Информация может быть искажена как случайно, так и намеренно, особенно, если затронуты интересы исполнителя.
- Технические сбои.

Это далеко не полный перечень, однако, очевидно, что прохождение информации в организации необходимо контролировать и перепроверять на всех этапах ее обработки.

Кратко обозначим ключевые точки контроля обработки информации:

- Точки входа.
- Точки выхода.
- Места обработки.
- Места хранения.
- Каналы связи.

Для обеспечения непрерывности производственного процесса в организации необходимо использовать службу горизонтального контроля обработки информации. Очевидно, что исполнители любого уровня будут стараться скрыть инциденты с нарушением информационной безопасности или некорректной обработки информации. Одной их функций службы информационной безопасности в организации как раз и является информирование руководства о всех этапах производственного процесса.

С практической точки зрения, важные документы должны проходить как минимум двухуровневую проверку, должна быть развита система отчетности и система обратной связи. У каждого задания должны быть контрольные сроки проверки с учетом времени на необходимые изменения. Кроме того, необходимо внедрять систему персональной ответственности и систему наказаний и поощрений. По ключевым вопросам необходим сторонний контроль извне отдела.

Отдельным вопросом стоит уровень квалификации кадров и соответствие сложности работы и объемов обрабатываемой информации уровню исполнителя. Участи службы информационной безопасности в процессе подбора кадров и оценки уровня работника обязательно.

Важным является также техническое оснащение рабочего места. В зависимости от уровня квалификации исполнителя, от сложности и величины объемов работ необходимо еще на этапе постановки задания планировать сроки его исполнения.

Таким образом, мы можем подытожить вышесказанное:

Система информационной безопасности является органической частью общей системы управления организацией и обеспечивает не только защиту от внешних угроз, но и позволяет организовать непрерывность и эффективность производственного процесса, с помощью контроля мест обработки хранения, резервирования и передачи информации.

УДК 004.6

Фомина К.Ю.

Принципы построения систем мониторинга безопасности информации в составе автоматизированных систем

В современных автоматизированных системах (АС) для обеспечения безопасности информации при ее обработке, хранении, передаче по каналам связи используются различные аппаратные, программные и программно-аппаратные средства защиты информации, входящие в состав комплекса средств автоматизации (КСА) АС. Это средства обнаружения компьютерных и сетевых атак (далее - атак), средства антивирусной защиты, средства защиты информации от утечки по техническим каналам и многие другие средства защиты и средства контроля эффективности защиты информации. Наличие большего количества различных средств защиты информации в составе КСА АС порождает большое количество журналов, в которые осуществляется запись этими средствами сведений о фиксируемых событиях безопасности. Это, в свою очередь, увеличивает нагрузку на администраторов безопасности информации по обработке большого количества данных о безопасности АС. В таких журналах может регистрироваться до нескольких десятков событий в секунду, что делает их анализ в ручном режиме длительным и крайне неэффективным. За счет этого недопустимо увеличивается время выявления начала атак на защищаемые ресурсы АС и принятия решения по реагированию на выявленные атаки, что приводит к существенному снижению общего уровня защищенности информации, обрабатываемой в АС.[3] В следствие этого потребность в многократном сокращении времени обработки данных о событиях безопасности становится одной из наиболее актуальных задач обеспечения безопасности информации в АС. Такое сокращение возможно только за счет автоматизации этого процесса. В связи с этим для АС, на ресурсы которых возможно воздействие атак, становится актуальной задача включения в состав ее КСА системы мониторинга безопасности информации (СМБИ).

Под мониторингом безопасности информации понимается постоянное наблюдение за процессом обеспечения безопасности информации в автоматизированной системе с целью установить его соответствие установленным требованиям.[4] СМБИ предназначена для автоматизации процесса сбора и анали-

за данных о событиях безопасности, поступающих из различных источников, входящих в состав КСА АС.

Эффективная СМБИ должна обеспечивать выполнения следующих основных функций:

1. Экспресс-анализ сведений о событиях безопасности на предмет оценки их информативности и «опасности» событий.

2. Игнорирование малоинформативных сведений о событиях безопасности и сведений о «неопасных» событиях безопасности.

3. Обработка прошедших экспресс-анализ сведений о событиях безопасности с целью определения причины наступления событий безопасности, места их наступления, прямых последствий наступления событий безопасности, прогнозирование дальнейших последствий, а также определение мер по устранению этих последствий.

Информация, получаемая СМБИ в процессе обработки сведений о событиях безопасности, собирается в едином центре, обрабатывается и подвергается анализу в соответствии с заданными правилами по обработке событий безопасности. Результаты анализа в режиме реального времени предоставляются администратору безопасности информации в удобном виде для принятия решений по реагированию на события безопасности.[2]

В обработке прошедших экспресс-анализ сведений о событиях безопасности в СМБИ, в общем случае, можно выделить 5 групп операций, которые можно назвать как фильтрация событий, нормализация событий, агрегирование событий, корреляция событий, приоритезация событий. Фильтрация событий направлена на устранение избыточности информации, об этих событиях на основе критериев, заданных администратором безопасности информации АС или определенных в СМБИ. Нормализация событий представляет собой процесс приведения данных от различных средств защиты информации и средств контроля эффективности защиты информации к единому виду. Агрегирование событий осуществляется с целью объединения однотипных событий безопасности в одно эквивалентное событие безопасности. Эта процедура позволяет значительно сократить объем хранимой информации и время обработки в СМБИ. При корреляции событий происходит выявление наличия комплексных атак, т.е. атак, которые не могут быть выявлены одним устройством с использованием известных сигнатур. Приоритизация событий – это автоматическое присвоение событиям соответствующего уровня приоритета при окончательной их обработке. Уровень приоритета устанавливается исходя из критериев, заданных администратором безопасности информации АС или установленных в СМБИ. [1]

Для эксперсс-анализа сведений о событиях безопасности, поступающих из различных источников, входящих в состав КСА АС представляется перспективным использование механизмов нейронных сетей и искусственных иммунных систем.

При применении для названной цели нейронных сетей функционирование КСА АС представляется в виде траекторий в некотором числовом пространстве

признаков. Эффективность экспресс-анализа при этом зависит от выбора архитектуры нейронной сети и ее обучения.

Искусственные иммунные сети строятся по аналогии с иммунной системой живого организма. Преимуществом искусственные иммунных сетей является то, что их обучение в 40 раз быстрее, чем обучение нейронных сетей, и вероятность ошибки при распознавании в 1,5 раза меньше по сравнению с нейронными сетями. Данные преимущества позволяют использовать этот метод для экспресс-анализа сведений о событиях безопасности, входящих в состав КСА АС.

На сегодняшний день всё большее число операторов и разработчиков АС приходят к осознанию необходимости включения в состав КСА АС систем мониторинга безопасности информации. Такое решение позволяет значительно повысить эффективность использования уже установленных в КСА АС средств защиты информации и средств контроля эффективности защиты информации, а также дает принципиальную возможность в режиме реального времени контролировать уровень защищенности информации, обрабатываемой в АС, на основе полученных данных из различных журналов событий безопасности.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Романов М. Обзор систем мониторинга, анализа и управления безопасностью корпоративных IT-инфраструктур, представленных на российском рынке.// “Storage News” № 1 (30), 2007 с. 21-25.

2. Сердюк В. Hp arcsight – эффективный инструмент для мониторинга событий информационной безопасности // InformationSecurity. Информационная безопасность №1, 2013 с.32–33.

3. Billy S. Thinking about Security Monitoring and Event Correlation. // http://www.symantec.com/connect/articles/thinking-about-security-monitoring-and-event-correlation

4. ГОСТ Р 50922-2006. Национальный стандарт Российской Федерации. Защита информации. Основные термины и определения.

СЕКЦИЯ: ПРАВОВАЯ БЕЗОПАСНОСТЬ

УДК 347.234

Андрианова С.С., Янкевский А.В.

Особенности сделок Автономных некоммерческих организаций по отчуждению имущества

Сделка Автономной некоммерческой организации по отчуждению имущества не может совершаться директором АНО. Признание такой сделки недействительной. Практика применения законодательства.

Автономная некоммерческая организация - это специфический субъект гражданско-правовых отношений, со своими особенностями: плюсами и минусами.

Основная особенность заключается в том, что АНО (будем так именовать Автономную некоммерческую организацию), что исполнительный орган в лице директора самостоятельно не вправе отчуждать имущество АНО.

Предлагаем рассмотреть конкретную правовую ситуацию и разобрать данный вопрос подробно по полочкам.

Между АНО «Ромашка» (должником, факт долга установлен решением суда, вступившим в законную силу) в лице генерального и коммерческой организацией «Василек» (кредитор) заключено соглашение об отступном, по условиям которого должник передает кредитору в качестве отступного, в соответствии с согласованной сторонами стоимостью, принадлежащее должнику на праве собственности нежилое помещение - здание в Москве, общей площадью 2 000 кв.м., и примерной рыночной стоимостью 200 000 000 рублей.

Государственная регистрация перехода права собственности осуществлена в 2012 году.

Вновь назначенный директор выяснил, что произошло несанкционированное отчуждение актива.

Обратился в суд с иском о признании сделки недействительной и применнении последствий недействительности ничтожной сделки.

Как и всякая недействительная сделка, решение органа юридического лица (в том числе об избрании директора) недействительно с момента его совершения в силу части 1 статьи 167 ГК РФ «*Недействительная сделка не влечет юридических последствий, за исключением тех, которые связаны с ее недействительностью, и недействительна с момента ее совершения*.» Поэтому, недействительное решение не порождает правовых последствий и является недействительным с момента его принятия.

В силу пункта 1 ст. 53 ГК РФ юридическое лицо приобретает гражданские права и принимает на себя гражданские обязанности через свои органы, действующие в соответствии с законом, иными правовыми актами и учредительными документами.

В статье 168 действовавшей на дату заседания 03 октября 2011 года редакции Гражданского кодекса Российской Федерации установлено, что сделка, не соответствующая требованиям закона или иных правовых актов, ничтожна.

Статья 167 ГК РФ предусматривает «Недействительная сделка не влечет юридических последствий, за исключением тех, которые связаны с ее недействительностью, и недействительна с момента ее совершения».

А теперь про особенности сделки именно АНО:

Главное основание признании сделки недействительной в том, что право на совершение сделки об отчуждении имущества у Директора АНО отсутствует.

Пунктом 3 статьи 29 Федерального закона «О некоммерческих организациях» к компетенции их высшего органа управления, в том числе, отнесено решение вопросов определения приоритетных направлений деятельности некоммерческой организации, принципов формирования и использования ее имущества, создания филиалов и открытия представительств. Устав АНО содержит аналогичную норму: к компетенции Общего собрания относится:

4) определение приоритетных направлений деятельности Школы, принципов формирования и использования его имущества (75% голосов присутствующих на собрании участников),

5) утверждение финансового плана Школы и внесение в него изменений;

6) утверждение годового отчета и годового бухгалтерского баланса;

Судебная практика подтверждает, что правом на отчуждение имущества некоммерческой организации имеет ее высший орган управления, а не исполнительный орган.

Определением ВАС РФ от 06 сентября 2007 года №10528/07 суд оставил в силе сделку, совершенную от имени АНО «Детско-юношеская спортивная школа «Нептун» членом Совета школы «Нептун» Сидоровым А.В. Исследуя обстоятельства дела, ВАС РФ акцентирует, что «к исключительной компетенции высшего органа управления некоммерческой организации среди прочих относится решение вопросов определения приоритетных направлений деятельности некоммерческой организации, принципов формирования и использования ее имущества».

В итоге, «поскольку решение об отчуждении имущества принято Советом Школы, имеющим необходимый кворум, оформлено протоколами от 16.05.2005 и от 07.07.2005, подписанными всеми его членами…., а договор подписан членом Совета школы С., на основании полномочий, данных Советом школы, суды пришли к выводу об отказе в удовлетворении требований о признании договора недействительным».

Итак директор не имеет полномочий на заключение вышеуказанного соглашения об отступном, в котором были разрешены вопросы, отнесенные законом к компетенции высшего органа управления некоммерческой организацией.

Совершением оспариваемой сделки нарушены имущественные права некоммерческой организации ввиду отсутствия воли собственника имущества – АНО на распоряжение предметом сделки, а также ввиду того, что со стороны

должника действовало лицо, которое не имело права отчуждать имущество, составляющее предмет сделки.

Из вышеизложенного, основаниями для признания недействительной сделки по отчуждению актва стали следующие обстоятельства:

1. Директор не вправе действовать от имени АНО при совершении сделки по отчуждению имущества.
2. Сделка не одобрялась действующим Высшим органом АНО

В силу перечисленных обстоятельств Соглашение об отступном недействительно и не порождает правовых последствий кроме тех, которые связаны с его недействительностью. Судо вынесено решение об удовлетворении исковых требований.

Суд руководствовался положениями статьи 168 Гражданского кодекса Российской Федерации, ст.ст.209, 53 Гражданского кодекса Российской Федерации, ст.ст. 28-30 Федерального закона от 12.01.1996 N 7-ФЗ «О некоммерческих организациях», ст.ст. 125-126 Арбитражного процессуального кодекса Российской Федерации.

Итогом стало приведение сторон сделки в первоначальное состояние: двусторонняя реституция на основании решения суда.

УДК 347.476

Бодров К.А., Бодрова О.В.

Банкротство физлиц, ожидания и реальность

01 октября 2015 года вступит в силу Закон о банкротстве физических лиц. Процесс, к введению которого готовились последние несколько лет, был запущен официально, несмотря на то, что раздел «Банкротство гражданина» давно присутствовал в Федеральном законе «О несостоятельности (банкротстве)». До сих существуют разные мнения относительно того, поможет ли Закон человеку, попавшему в трудную ситуацию, выбраться и встать на ноги, избавит от накапливающихся штрафов и пеней, позволит списать их или загонит должников в еще большую яму.

Изначально было запланировано, что процедура банкротства физических лиц вступит в силу с 01 июля 2015 года. Однако за пару недель до этой даты в Закон были внесены изменения. Этими поправками была перенесена дата вступления в силу банкротства физических лиц, и рассмотрение таких дел было отнесено к юрисдикции арбитражных судов. Суды общей юрисдикции оказались не готовы к разрешению такого рода дел в силу отсутствия опыта применения санации, тогда как арбитражные суды рассматривают дела о банкротстве с 1992 года и имеют достаточно опыта и практики. Однако, чтобы рассматривать дела о банкротстве физических лиц, арбитражным судам нужны дополни-

тельное финансирование и кадры, не только количество судей, но и штат аппарата судов.

Принятие Закона о банкротстве физлиц явилось своевременным мероприятием, так как ситуация с обязательствами граждан за последний год резко ухудшилась. Почти каждый пятый гражданин имеет просроченные финансовые обязательства, в большинстве случаев по кредитам. Большинство граждан гасят свои долги, договариваются с банками, но все равно фактически балансируют на грани банкротства.

Иными словами, банкротство физического лица означает, что гражданин-должник признает свою неспособность заплатить по всем имеющимся у него обязательствам, либо его кредиторы при условии долга не менее 500 000 рублей и просрочки платежа не менее 3-х месяцев с даты наступления требования об уплате долга. Официальный статус банкротства гражданина сохраняется 5 лет. Процедура банкротства физического лица также может быть возбуждена (при необходимости) после его смерти. Заявление в суд могут подать наследники, уполномоченный орган или кредитор.

Процедура банкротства представляет собой фактически финансовое оздоровление гражданина, выраженное в виде реструктуризации его долга с графиком выплаты до 3-х лет. Размер платежей устанавливается судом, а проценты и штрафные санкции (неустойка) в этом случае не начисляются.

Гражданин-должник, имеющий постоянный источник дохода, может договориться с кредиторами о реструктуризации долга, под контролем финансового управляющего. Если у гражданина нет доходов, то спустя шесть месяцев после введения процедуры банкротства он может быть признан банкротом в судебном порядке. Будет введена процедура конкурсного производства и назначен конкурсный управляющий, все имущество гражданина подлежит включению в конкурсную массу для удовлетворения требований кредиторов. Конкурсный управляющий реализует имущество на торгах и за счет вырученных от этого средств погашает все долги гражданина. Большую сложность вызывает вопрос о том, что можно продать у гражданина-должника и как это изъять. Например, нельзя изъять и продать с торгов единственное жилье гражданина, за исключением, если это жилье куплено в ипотеку. А если гражданин является собственником единственного жилья большой площади, например коттеджа, продажа которого сможет погасить все задолженности перед кредиторами, то его нельзя продавать в связи с тем, что это единственное место жительства гражданина. Однако, в законе есть и «подводные камни». Если гражданин проживает в собственном жилье в одном городе, но зарегистрирован по другому адресу, суд вправе выставить его имущество на торги – ведь теоретически ему все равно есть, где проживать.

Первые сложности, которые возникли после вступления закона в силу - это определение имущества должника для включения его в конкурсную массу и раздела имущества семьи. До сих пор не внесены изменения в Федеральный закон «О несостоятельности (банкротстве)», направленный на урегулирование

вопросов при разделе совместной собственности в случае банкротства. При рассмотрении законопроекта авторы предлагают судебный процесс по банкротству гражданина проводить сразу в двух судах – арбитражный суд будет рассматривать процедуру банкротства, а разделом имущества займется суд общей юрисдикции. Арбитраж не сможет осуществлять раздел имущества граждан, так как возникнет множество несогласований в вопросах подсудности.

Другая сложность состоит в том, что в течение первой недели действия закона о банкротстве физических лиц с 1 по 10 октября в Арбитражный суд Москвы поступило более 150 соответствующих исков. Большую часть таких исков в Арбитражный суд направили банки, которые настаивают на несостоятельности заемщиков. По оценкам Центробанка, число граждан, которые потенциально могут прибегнуть к процедуре банкротства, составит 400-500 тысяч. В настоящее время зарегистрировано около 16 000 арбитражных управляющих, из них включены в Сводный государственный реестр арбитражных управляющих Росреестра не более 9500 человек. Если все иски будут пропорционально распределены на всех арбитражных управляющих, то нагрузка на каждого управляющего будет не менее 50 процедур граждан-должников.

Однако, процедура банкротства физических лиц вызывает сомнения у арбитражных управляющих. Кто пойдет работать за те деньги, которые положено получить по закону? Тут тоже есть над чем задуматься: максимальная сумма, которую получит финансовый управляющий, составит единовременно 10 тысяч рублей за всю процедуру, которая может растянуться на 3 года. Эту сумму он получит только по ее окончании. Учитывая, что арбитражный управляющий в большинстве случаев сначала ведет процедуру банкротства за свой счет, а потом получает возмещение и вознаграждение за счет имущества должника, либо кредитора, инициировавшего банкротство, то применительно к процедуре банкротства физических лиц, арбитражный управляющий, как субъект профессиональной деятельности, несколько раз подумает перед тем, как дать свое согласие на назначение на процедуру банкротства физического лица.

В заключении хочется сказать, что статус «банкрот» для физического лица все же доставит определенные неудобства. До полного завершения процедуры, станет невозможным выезд заграницу, открытие лицевого счета, оформления коммерческих сделок, в течение 5 лет – открытия нового бизнеса, повторного взятия кредита без указания фактов банкротства, а также после завершения процедуры банкротства не все долги будут окончательно списаны перед кредиторами.

Пока новый закон о банкротстве физических лиц скорее беспокоит, чем успокаивает, но больший интерес он вызывает у людей, которые являлись поручителями по кредитам юридических лиц, давно не ведущих хозяйственную деятельность, и которые рассматривают процедуру банкротства во избежание солидарной ответственности перед банком.

СЕКЦИЯ: ФИНАНСОВО-ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ

УДК 658.5

Аверина Л.А.

Тотальный менеджмент качества (TQM) как следующий этап развития организации, внедрившей Систему менеджмента качества на основе стандартов ISO серии 9000

В связи со складывающейся политической и экономической ситуацией на территории Российской федерации все большее и большее число компаний борются за своих покупателей на отечественном рынке. А также на данный огромное количество тендеров и конкурсов не обходятся без предоставления компанией-участницей сертификата соответствия системе менеджмента качества [1].

Такой повышенный интерес к системе менеджмента качества (СМК) приводит к тому, что компании начинают ставить перед собой цель не только уменьшить количество брака в выпускаемой продукции, но и предопределить конкурентоспособность всей организации. Именно для этого была разработана Тотальный/всеобщий менеджмент качества (TQM).

Тотальный/всеобщий менеджмент качества (TQM) – это система управления, основанная на производстве качественных с точки зрения заказчика продукции и услуг [2]. TQM определяется как сосредоточенный на качестве, сфокусированный на заказчике, основанный на фактах, управляемый командный процесс.

В основе TQM лежат следующие принципы (Таблица 1):

Таблица 1

Основные принципы Тотального качественного менеджмента

№ п.п.	Принцип TQM
1	Ориентация на потребителя
2	Вовлечение работников, что даёт возможность организации с выгодой использовать их способности
3	Подход к системе качества как к системе бизнес-процессов[1]
4	Системный подход к управлению
5	Постоянное улучшение

Для внедрения методологии TQM необходимо пройти семь ступеней [3], не считая нулевую стадию и подготовку, суть которых состоит в том, чтобы подготовить предприятие к внедрению и сертификации систем менеджмента качества на базе ISO 9000 (Таблица 2).

[1] **Бизнес-процесс** — это совокупность взаимосвязанных мероприятий или задач, направленных на создание определённого продукта или услуги для потребителей.

Таблица 2

Семь ступеней внедрения методологии TQM

№ ступени	Описание внедряемой ступени
0	Мотивация и оценка возможностей
1	Подготовка
2	Разработка системы
3	Создание системы менеджмента качества и его сертификации
4	Создание общей системы менеджмента
5	Реорганизация и повышение эффективности общей системы менеджмента – создание внутренней TQM — системы
6	создание стратегической TQM - системы
7	создание глобальной TQM системы

Основную цель, которой придерживается и стремится TQM, является система, в которой центральным местом управления качеством является – управление качеством во всех видах менеджмента, а именно: менеджмента предприятия и организации, производственного менеджмента, менеджмента персонала, стратегического менеджмента, менеджмента корпоративных структур.

Основными преимуществами TQM являются [4]:

1. Долгосрочные выгоды в виде высокая продуктивность, повышение морального тонуса коллектива, уменьшение затрат и рост доверия Заказчика.
2. Уклонение от ошибок и правильные действия, которые сохраняют время и ресурсы, тем самым фонды и сбережения могут расходоваться на расширение спектра услуг (продукции) или предоставляться сотрудникам для работы, направленной на улучшение качества услуг.
3. Создание атмосферы энтузиазма и удовлетворения выполненной работой с привлечением инструментов премирования и награждения за творческий подход.
4. Применяется командного подхода, передающего, с одной стороны, работникам опыт решения проблем их коллегами и, с другой стороны, позволяющий им применить свои знания и опыт в ходе совместных усилий.

Как и при любой внедряемой системе TQM имеет и свои недостатки, а именно, выполнение рутинных операций, которые присуще и Системе менеджмента качества, так как обе системы нуждаются в систематическом сборе и полной обработке всей поступающей информации.

К сожалению, если Система менеджмента качества распространена в нашей стране, то Тотальный качественный менеджмент на данный момент представлен в отечественных организациях в гораздо меньшем объеме. Система TQM успешно используется международными компаниями, например, в Японии, на протяжении уже более десятка лет и хочется надеется, что передо-

вой опыт сможет быть «подхвачен» нашими специалистами и успешно реализован на российских предприятиях.

В конце хотелось бы подытожить, что TQM – это не программа, не управленческая прихоть, а систематический, интегрированный и организованный стиль работы, полностью направленный на непрерывное улучшение рабочего процесса, вовлечением всего коллектива и повышение конкурентоспособности всей организации.

Список литературы:

1. Тендеры и конкурсные торги//[Электронный ресурс]/Режим доступа: http://www.alltenders.ru/ (дата обращения 31.05.2015).
2. В. Баронов, И. Титовский/Всеобщее управление качеством: зачем оно нужно?//[Электронный ресурс] / Режим доступа: http://www.standard.ru/articles/article02.phtml (дата обращения 31.05.2015).
3. Принципы TQM//[Электронная статья] / Режим доступа: http://www.standard.ru/iso9000/iso9000-txt14.phtml (дата обращения 20.03.2015).
4. Д. Маслов, Пол Ватсон, Э. Белокоровин/ Всеобщее управление качеством в России - труден путь к совершенству//[Электронный ресурс] / Режим доступа: http://www.standard.ru/article.phtml?i=2 (дата обращения 20.03.2015).

УДК 658.5.011

Безукладов Д.А.

Инновационная среда университета как основа политики экпортозамещения

Обострение мировой геополитической обстановки, политика санкций в отношении России со стороны стран Запада и США подтверждают тот факт, что мы вступили в эпоху, когда экономика превращается в оружие на полях внешнеполитических сражений и используется как инструмент давления на страны с неугодным политическим режимом. Несмотря на санкции, угрозу экономической изоляции нашей страны необходимо понимание того факта, что в ближайшее время геополитическая нестабильность будет сохраняться и нужно быть готовыми к работе и развитию экономики в новых непростых условиях.

Российская экономика, сегодня остро нуждающаяся в дополнительных источниках роста, резервах, способных вывести ее на путь стабильного и долгосрочного развития. России нужен запас экономической прочности, чтобы противостоять внешнему давлению. В условиях сокращения внешних инвестиций нужно развиваться, прежде всего, за счет внутренних ресурсов. Если реализовывать грамотную экономическую политику, то Россия не просто переживет период санкций, но выйдет из него более сильной и развитой в экономическом плане.

Однако, работа в таких условиях подобна прогулке по канату над пропастью, стоит лишь потерять равновесие, и катастрофа неминуема. Потеряв доступ к западным товарам и технологиям, правительство РФ было вынуждено

реализовывать стратегию импортозамещения в различным отраслях экономики. Данный подход соответствовал сложившейся ситуации и был направлен на поддержание безопасности страны. Первым на сложившиеся условия отреагировал российский ОПК. Мипромторгом был разработан план импортозамещения продукции военного назначения на ближайшие 2,5 года, в ответ на запрет поставок вооружений, военной техники и комплектующих для предприятий российского ОПК. Основной целью данного плана является независимость российского ОПК от импорта. Ведется активная работа на переориентацию экспорта и импорта на других торговых партнеров – Китай, Индию, Бразилию, Египет, Иран, Казахстан и Белоруссию.

Но, несмотря на очевидные преимущества и положительные стороны данной стратегии, имеются ряд рисков, которые необходимо учитывать. Во-первых, реализация стратегии импортозамещения оказывает прямое негативное влияние на инвестиционную привлекательность страны. Во-вторых, продукт импортозамещения должен был конкурентным на глобальном уровне. Импортозамещение это основа экономической безопасности страны, которая должна была формироваться постепенно, ее вынужденное построение в сжатые сроки несет в себе целый ряд возникающих проблем.

Если мы хотим обеспечить долгосрочный экономический рост, то на смену импортозамещению в ближайшее время должно придти «экспортозамещение». Политика санкций в первую очередь ударила на отрасли, занимающиеся сырьевым экспортом и экспортом продукции низкого передела. Таким образом, для сохранения доходов от экспорта необходимо сделать то, что наша страна должна была сделать уже давно – перейти от сырьевой экономики к экономике, создающей инновационную продукцию, конкурентоспособную на мировом рынке. Эскортозамещение необходимо не только для открытия новых рынков экспорта высокотехнологичной продукции, но и для поддержания уже существующих рынков, например рынка вооружений, где наблюдается крайне высокий рост конкуренции и прежде всего со стороны Китая. Китайские военные инженеры многому научились у своих российских коллег, и в ближайшем времени созданная ими техника начнет вытеснять российские аналоги в сферах производства истребителей, подводных лодок, танков, ЗРК и баллистических ракет. Китайским производителям еще многому предстоит научиться у российских коллег, но во многом они уже догоняют – и, возможно, в ближайшее десятилетие даже обгонят Россию.

Растущая потребность в идеях новых инновационных продуктах и технологиях, обладающих интересом для мирового рынка и конкурентной способностью, способности довести идеи и разработки до стадии готового изделия или продукции требует изменения подхода к позиционированию и роли высших учебных заведениях в регионах. Современный университет сегодня становится не просто учебным заведением, местом сосредоточения научных разработок и фундаментальных знаний, а играет роль важнейшего субъекта, определяющего темпы развития, структуру и процессы формирования инновационного рыночного поля. Вузы могут быть не только частью создаваемых в регионах инновационных экосистем – у них есть

все возможности для того, чтобы стать интегрирующим звеном в такой системе. Сегодня довольно актуальной проблемой для большинства российских университетов является создание *активной инновационной среды*, содержащей в себе механизмы коммерциализации технологий с последующей интеграцией данных механизмов в инновационную экосистему региона.

Государству следует уделить максимально внимание проблемам формирования и развития инновационной среды в университетах страны, чтобы обеспечить экономику так необходимыми ей сегодня профессиональными кадрами, идеями и технологиями.

УДК 34.08

Борисов Д.П., Феденкова Е.А., Киселева О.В.

Правонарушения, совершаемые бухгалтерами в профессиональной деятельности

Главный бухгалтер — второе лицо в организации после директора. На нем лежит обязанность контролирования соблюдения законодательства Российской Федерации при ведении бухгалтерского учета хозяйствующего субъекта. Бухгалтеры располагают прямым доступом к большинству финансовых документов фирмы, к денежным средствам, к налоговой и зарплатой политике организации. Имеют место факты, когда бухгалтеры совершают правонарушения или даже преступления, используя свои профессиональные возможности.

«Сопричастность» главного бухгалтера к уголовно - наказуемым деяниям в большей степени определяется его служебными полномочиями. В связи с этим, при поступлении на работу бухгалтеру необходимо внимательно изучить содержание трудового договора. Законодательством РФ предусмотрены основные обязанности главного бухгалтера (бухгалтера), которые обязательны к выполнению. В интересах сотрудника следует избегать в тексте договора формулировок вида «а также другие служебные полномочия, которыми главный бухгалтер наделяется по решению руководства». Подобные формулировки способны принять определенный смысл и сделать главного бухгалтера соучастником различного рода мошенничеств.

Уголовная ответственность бухгалтера, как правило, ассоциируется с налоговыми преступлениями. Именно уклонение от уплаты налогов является наиболее распространенным видом преступного деяния в бухгалтерской среде. Ведь профессия бухгалтера предполагает непосредственное отношение к исчислению и уплате денежных средств в пользу государства.

Уклонение от уплаты налогов может заключаться в непредставлении налоговой декларации и иных документов, которые служат основанием для исчисления и уплаты налогов и сборов. Именно с момента сокрытия выручки в первичных документах начинается уклонение от уплаты налогов. Но помимо налоговых платежей, через сотрудников бухгалтерии проходят главные финансовые потоки организации. Благодаря этому факту, бухгалтера чаще всего фигурируют в делах о

мошенничестве, присвоении или растрате, реже – в делах об отмывании незаконно полученных денежных средств, еще реже - о фиктивных и преднамеренных банкротствах. Причина этого кроется в специфике современного документооборота, при котором бухгалтер не располагает прямым доступом к наличным денежным суммам и материальным ценностям компании. В настоящее время значительную часть финансовых расчетов организация осуществляет через систему дистанционного банковского обслуживания «банк-клиент» или с использованием платежных документов. Проанализировав публикации в профессиональных периодических изданиях, нами обобщены некоторые наиболее распространенные виды правонарушений (Таблица 1).

Таблица 1 -Правонарушения, совершаемые бухгалтерами в профессиональной деятельности

Название правонарушения	Содержание правонарушения
1.Подделка платежных поручений	1. Бухгалтер совершает подделку платежных поручений, пользуясь тем, что совместно с руководителем организации имеет право подписи финансовых документов, поэтому руководитель, излишне доверяя бухгалтеру, не обращает особого внимания на содержание платежных поручений, затем бухгалтер пересылает денежные средства другим компаниям по составленным фиктивным договорам и обналичивает нужную ему сумму.
2.Махинации с зарплатными начислениями	2. Данное правонарушение осуществляется в следующем порядке: поддельные зарплатные реестры, где всем работникам к фактической заработной плате приписывается дополнительная сумма, направляются в банк, банк в свою очередь начисляет денежные средства. Затем бухгалтер обналичивает приписанные излишки денежных средств в свое личное пользование, а работники организации получают свою привычную сумму. Также распространена ситуация с оформлением на работу подставных лиц. Здесь бухгалтеры нередко выступают в сговоре с начальством среднего звена. Такая схема выглядит следующим образом: бухгалтер вносит поставных сотрудников в зарплатный реестр, организация выплачивает заработную, затем перечисленные суммы денежных средств, попадают в руки бухгалтера - преступника.
3.Хищения с отмыванием	3. Ситуации, когда бухгалтера обвиняют в «отмывании» незаконно – полученных денежных средств, встречаются достаточно редко. Денежные средства расцениваются как «отмытые» в случае, когда они попадают в легальный денежный оборот. Например, когда присвоенная бухгалтером сумма денежных средств идет на погашение кредита, различного рода приобретения. Совершить данное преступление бухгалтеру помогают его должностные полномочия и современная компьютеризированная система ведения бухгалтерского учета.
4.Создание «персональных однодневок»	4. Нередко организации переводят денежные средства по поддельным договорам на счета фирм - «однодневок». Это делается с целью получения наличных денежных средств, преувеличения расходов компании в целях налогообложения прибыли или вычетов по налогу на добавленную стоимость. Другими словами, организация занимается лжепредпринимательством, то есть регистрирует в качестве предпринимателя или юридического лица, не планируя заниматься соответствующей деятельностью в целях сокрытия, преуменьшения прибыли, доходов и прочих объектов налогообложения [2]. Но бывают ситуации, когда бухгалтер один совершает указанное преступное деяние. В этом случае он понесет ответственность не только за мошенничество, но и за фальсификацию документов

Безусловно, главный бухгалтер (бухгалтер) обязан выполнять приказы (распоряжения) директора компании, вопреки своим внутренним убеждениям о незаконности данного решения. В таких случаях необходимо следовать требованиям пункта 78 статьи 7 ФЗ-402 «О бухгалтерском учете». В случае возникновения разногласий в отношении ведения бухгалтерского учета между руководителем экономического субъекта и главным бухгалтером, главный бухгалтер должен действовать по письменному распоряжению руководителя экономического субъекта, который единолично несет ответственность за созданную в результате этого информацию.

Список литературы:

1.Касьянова. Преступление и наказание в бухгалтерском и налоговом учете.- М. :АБАК 2010.
2.Под редакцией Пласковицкой Е.В., Пласковицкий А.Л.-Ответственность Бухгалтера. 2006. URL:http://plas.by/pravo/pp/ob/glava4.php (дата обращения: 20.05.2015)
3. Бумажный и электронный журнал «Главбух», выпуск от 30 января 2007г URL:http://www.glavbukh.ru/art/10479 (дата обращения: 20.05.2015)

УДК 597.622

Дерябина Ю.В., Киселева О.В.

Ревизия бухгалтерской (финансовой) отчетности

Несмотря на то, что в настоящее время всё чаще используется понятие аудит бухгалтерской (финансовой) отчетности, тема ревизии бухгалтерской (финансовой) отчетности является актуальной. В процессе ревизии решаются вопросы о целесообразности эффективности действий в сфере учета.

Ревизия - это система обязательных контрольных действий по документальной и фактической проверке законности и обоснованности совершенных в ревизуемом периоде хозяйственных и финансовых операций ревизуемой организации, правильности их отражения в бухгалтерском учете и отчетности, а также законности действий руководителя, главного бухгалтера и иных должностных лиц [4, 24].

Перед проведением ревизии бухгалтерской (финансовой) отчетности необходимо составить перечень подготовительных мероприятий (см. Таблица 1).

Проведение предварительной подготовки к ревизии позволяет более четко сформулировать её задачи, выявить по данным предыдущих ревизий, вопросы, которым следует уделить отдельное внимание при проведении ревизии, например, проверке исправления ошибок, выявленных предыдущей ревизией.

После проведения предварительной подготовки переходят непосредственно к составлению рабочего плана проведения ревизии и проведению её на объекте.

Таблица 1 - Перечень и содержание подготовительных мероприятий

Наименование мероприятий	Содержание мероприятий
1. Сбор общих сведений о предприятии	- знакомство с учредительными документами, филиалами; - знакомство с элементами учетной политики, регламентами, регулирующими ведение кассовых операций в филиалах; - знакомство с организационной структурой; - изучение нормативных актов, касающихся особенностей деятельности проверяемого объекта.
2. Изучение документации по результатам прошлых проверок.	- определить основные вопросы, поднятые ревизией; - определить характер и формы вскрытых недочетов и нарушений.
3. Изучение бухгалтерской (финансовой) отчетности	- просмотр форм отчетности и пояснений к отчетности.
4. Изучение документооборота в организации	- изучить, в каком отделе ведутся расчеты по кассе, расчетному и валютному счетам, ценным бумагам, в том числе векселям; - изучить кто и как оформляет взаимозачеты.
5. Изучить наличие контролирующих служб в организации	- ознакомиться с отчетами внутренних контролирующих служб; - сравнить с отчетами внешних.

В ходе проведения ревизии должны быть решены следующие основные задачи [5, 104]:

- проверка состава и содержания форм бухгалтерской отчетности;
- увязка показателей бухгалтерской отчетности, проверка правильности оценки статей отчетности;
- проверка правильности формирования сводной (консолидированной) отчетности;
- установление соответствия применяемой в организации методики бухгалтерского учета и налогообложения действующим в проверяемом периоде нормативным документам, чтобы сформировать мнение о достоверности бухгалтерской (финансовой) отчетности во всех существенных аспектах;
- проверка правильности формирования сводной отчетности.

После определения задач, которые необходимо решить в процессе ревизии, составляется программа проведения ревизии.

При проведении непосредственно самой ревизии первым делом следует обратить внимание на исправление ошибок, выявленных предыдущей ревизией. Если данные ошибки не были исправлены, то ревизор делает пометку о данном нарушении и отражает это в акте о проведении ревизии.

Затем, проводится проверка каждой формы бухгалтерской (финансовой) отчетности отдельно. При её проведении правильность показателей, отраженных в отчетности проверяется их сравнением с соответствующими регистрами. Если в ходе проведения ревизии форм бухгалтерской (финансовой) отчетности обнаружено несоответствие первичным документам и другие ошибки отражения показателей, то ревизором назначается инвентаризация объектов, отражен-

ных неправильно. На рисунке 1 представлена программа ревизии бухгалтерской (финансовой) отчетности.

Утверждаю
Начальник контрольно-ревизионного органа
_____
(должность, подпись)
«___» _____20__г.

ПРОГРАММА РЕВИЗИИ
бухгалтерской (финансовой) отчетности

_____

за период с _____ по _____
ревизором _____

Наименование (содержание) работ	Срок исполнения		Дата представления материала	Отметка о выполнении
	начало	окончание		
Инвентаризация кассы				
Проверка исправления ошибок, выявленных предыдущей ревизией				
Проверка оформления документов				
Проверка результатов проведения инвентаризации				
Ревизия бухгалтерского баланса				
Ревизия отчета о финансовых результатах				
Ревизия отчета об изменениях капитала				
Ревизия отчета о движении денежных средств				
Ревизия пояснений к балансу и отчету о финансовых результатах				
Проверка увязки форм бухгалтерской отчетности				
Определение ответственных лиц, виновных в выявленных ошибках (при их наличии)				
Разработка предложений по исправлению и предотвращению последующих ошибок				
Оформление результатов ревизии				

Рис. 1 — «Программа ревизии бухгалтерской (финансовой) отчетности»

В настоящее время были внесены некоторые изменения в законодательство, регулирующее бухгалтерский учет и бухгалтерскую (финансовую) отчетность. При проведении ревизии бухгалтерской отчетности за 2014 год данные изменения не следует учитывать, но в 2015 году следует обратить внимание на то, как оформлены первичные документы и сама бухгалтерская (финансовая) отчетность. Данные изменения касаются того, что в соответствии с приказом Минфина России от 6 апреля 2015 г. № 57н подпись главного бухгалтера в бухгалтерской отчетности не требуется. Главный бухгалтер может подписывать бухгалтерскую отчетность только по доверенности от руководителя организации.

Так же с 7 апреля 2015 года хозяйствующие субъекты имеющие организационно-правовой статус общества с ограниченной ответственностью или акционерного общества могут работать без круглой печати (82-ФЗ от 06.04.2015 г). Данное изменение должно быть прописано в уставе организации. Поэтому при

проведении предварительной подготовки ревизии следует уточнить данное изменение. При этом, следует учесть, что некоторые документы предусматривают печать и её отсутствие может повлечь штраф и отказ в их достоверности.

После проведения проверки каждой формы бухгалтерской (финансовой) отчетности отдельно нужно проверить их взаимоувязку.

Проверка взаимоувязки форм бухгалтерской (финансовой) отчетности является одним из важнейших аспектов ревизии, так как позволяет получить наиболее полную картину имущественной структуры организации, а так же выявить несоответствия данных, которые содержатся в бухгалтерской (финансовой) отчетности, так как все её формы взаимоувязанны между собой.

Для облегчения работы ревизоров мы хотим предложить использование форм проверки взаимоувязки показателей отчетности. Это поможет ревизору систематизировать наглядно полученные данные и проверить достоверность их отражения. Также данные формы будут полезны начинающим бухгалтерам, для самостоятельной проверки правильности составления годовой отчетности.

Данные формы рекомендуется оформлять таким образом, как это представлено в настоящей статье. В них должны быть указаны название организации, сроки проведения ревизии, ФИО ревизора и обнаруженные несоответствия, по которым ответственное лицо должно дать письменные пояснения. Это поможет ревизорам не только при текущей проверке, но и при последующих, так как данные документы, в отличии от акта, который содержит информацию об общих нарушениях, будут раскрывать информацию о несоответствиях статей, их содержание и причины возникновения. На рисунке 2 приведено примерное заполнение одной из форм. В ней проверяется не только взаимоувязка баланса с отчетом о движении денежных средств, но и соответствие данных за прошлый период, как например в пункте «Денежные средства и денежные эквиваленты (прошлый период)» значения в строке 4450 на начало текущего периода и в строке 4500 на конец прошлого периода должны совпадать, именно поэтому ячейка, где указывается значение по данной строке для них едина.

ФОРМА КОНТРОЛЯ ВЗАИМОУВЯЗКИ
проведения ревизии увязки формы бухгалтерского баланса и отчета о движении денежных средств

_____

за период _____ по _____

ревизором _____

Код строки в отчете	Формула расчета	Значение	Код строки в балансе	Значение	Соответствие
Денежные средства и денежные эквиваленты					
4500	На К.П.	254 000,00	1250	254 000,00	Соответствует
Денежные средства и денежные эквиваленты (прошлый период)					
4450 4500	На НТП На КПП	252 000,00	1250	252 000,00	Соответствует
Денежные средства и денежные эквиваленты (год, предшествующий прошлому)					
4450	На НПП	928 000,00	1250	928 000,00	Соответствует

Расшифровка аббревиатур:
КП - конец периода
НТП - начало текущего периода
КПП - конец прошлого периода
НПП - начало прошлого периода

В ходе проведения были обнаружены следующие несоответствия:

_____
_____
_____
_____
_____
_____
_____

Рис. 2 — «Форма контроля взаимоувязки бухгалтерского баланса и отчета о движении денежных средств»

Колонка соответствие заполняется на усмотрение ревизора. Он может использовать не только значения «Соответствует» и «Не соответствует», но так же ставить галочки и крестики. От значений «+» и « - » следует воздержаться, так как их можно подделать. Строки для описания не соответствия подлежат обязательному заполнению. Даже если не было выявлено несоответствий - это следует указать. В случае установления несоответствия необходимо указать, что к данной форме прилагаются пояснения ответственного лица. После заполнения формы ставятся подписи ревизора, ответственного лица и руководителя организации.

Пояснение должно содержать следующие реквизиты: наименование организации, ФИО ответственного лица, подпись, объяснение причин, по которым формы бухгалтерской (финансовой) отчетности содержат неверную информацию или не взаимоувязаны между собой и подпись ревизора и руководителя организации, ознакомившихся с данным документом. Ревизор должен предоставить руководству рабочие формы взаимоувязки данных отчетности, если ошибки, обнаруженные в ней, были связаны с фальсификацией.

Список использованной литературы:

1. Федеральный закон от 06.12.2011г. №402-ФЗ «О бухгалтерском учете». [Электронный ресурс]:Система ГАРАНТ: http://base.garant.ru (дата обращения 13.05.2015)

2. Федеральный закон от 06.04.2015 г. №82-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в части отмены обязательности печати хозяйственных обществ». [Электронный ресурс]: КонсультантПлюс : http://www.consultant.ru (дата обращения 09.05.2015)

3. Приказ Минфина России от 6 апреля 2015 г. № 57н «О внесении изменений в нормативные правовые акты по бухгалтерскому учету». [Электронный ресурс]: Консультант Плюс : http://www.consultant.ru (дата обращения 09.05.2015)

4. «Контроль и ревизия»: учебное пособие для самостоятельной работы студентов / Мещеряков С.А. - Санкт-Петербург, 2008г.

5. «Контроль и ревизия»: учебное пособие / Федорова Е.А. - издательство «ЮНИТИ-ДАНА», 2011г.

6. [Электронный ресурс]: Главбух: http://www.glavbukh.ru. «36 примеров того, что с чем должно совпадать в балансе и других формах бухгалтерской отчетности», №5 март 2015 (дата обращения: 19.05.2015)

7. [Электронный ресурс]: Главбух: http://www.glavbukh.ru. «Отмена печати», №10 май 2015 (дата обращения: 19.05.2015)

УДК 334.72

Карпунин А.Ю.

Роль предпринимательства в развитии экономики

Разработка эффективного, четкого и прозрачного законодательства является основой развития малого и среднего предпринимательства на современном этапе. По данным международного исследования «Глобальный мониторинг предпринимательства» чуть более 2% россиян изъявляют желание открыть своё частное дело. Это показатель один из самых низких в мире. Это говорит о том, что необходимо заниматься популяризацией малого бизнеса, доносить до потенциальных предпринимателей преимущества и возможности этого направления. Нам представляется, что в России еще жив стереотип о предпринимателе, как о человеке, который построил свой бизнес в результате бандитских и рейдерских захватов, приватизации, авантюризма. Необходимо больше говорить и писать о новом поколении российских предпринимателей - интеллигентах, которые не связаны с властью, силовиками, корпорациями, и которые построили бизнес без связей, взяток и капитала. [2]

Говоря о предпринимательской активности, отметим, что в 2009 году на вопрос планируете ли вы открыть свой бизнес, нет и не планирую этого делать - ответили 51%, а в 2011 году – уже 65%. Проблема в том, что приоритетом государственной политики, является социальная поддержка населения, а не стимулирование самостоятельности и частной инициативы, что приводит к торможению активности и иждивенческим настроениям в обществе. Невозможно постоянно поднимать уровень жизни населения только за счет бюджетных средств. Степень разви-

тости малого и среднего бизнеса и активность предпринимателей, определяют степень демократизации государства и открытость его экономики. [1]

На сегодняшний день в стране наблюдается зависимость бюджета от сырьевых доходов, избавиться от которой можно в том случае, когда основу экономики будут составлять не только крупные государственные и частные компании, но и малый и средний бизнес. Исследованиями установлено сокращение числа субъектов малого и среднего предпринимательства (рис. 1). Мы считаем обоснованным, что смягчить негативное влияние санкций могло бы наличие именно развитого малого и среднего предпринимательства в стране. Однако в нашей стране вклад малого и среднего бизнеса в ВВП не превышает и 20%, в то время как в экономически развитых странах на долю малого и среднего бизнеса приходится более 50% производимого ВВП. Несмотря на все принимаемые государством меры по развитию малого и среднего предпринимательства, статистика фиксирует отрицательную динамику числа зарегистрированных субъектов малого и среднего бизнеса. Наибольшее снижение произошло в части индивидуальных предпринимателей с 2011 г. по 2013 г. на 14% (изменение 2013 г. к 2011 г.). За 2 последних года их число сократилось с 4,1 млн. в 2011 году до 3,5 млн. в 2013 г. Главной причиной резкого роста количества желающих закрыть ИП, стало повышение страховых взносов для малого бизнеса с 2013 г.

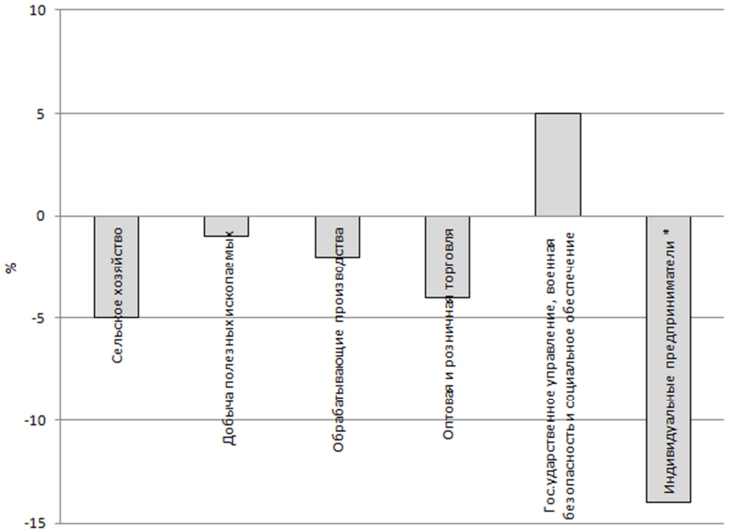


Рис. 1. Изменение числа зарегистрированных компаний по данным ФНС, 2012 г. к 2011 г.

Список использованной литературы:

1. Доклад уполномоченного при Президенте РФ по защите прав предпринимателей [Электронный ресурс] Режим доступа: http:// ombudsmanbiz.ru/ Дата обращения: 15.05.2014.

2. Карпунин А.Ю., Карпунина Е.В. Анализ и перспективы развития малого и среднего бизнеса на современном этапе //Экономика и предпринимательство. 2014. № 6 (47). С. 757-761.

УДК 343.37

Карпунин А.Ю., Карпунина Е.В., Киселёва О.В.

О соотношении понятий «несостоятельность» и «банкротство»

В [2] понятия «несостоятельность» и «банкротство» не дифференцированы. Мы с большой степенью вероятности можем сказать, что понятия несостоятельность и банкротство следует различать и критерием дифференциации указанных категорий может быть способность хозяйствующего субъекта восстановить свою платёжеспособность (прим. авторов: при этом под платёжеспособностью мы понимаем способность организации расплачиваться по своим долгам).

По нашему мнению «несостоятельность» можно рассмотреть как экономическую категорию, имеющую место в случае, когда должник ещё в состоянии расплатиться по своим долговым обязательствам, посредством реализации оздоровительных процедур банкротства, таких как финансовое оздоровление, внешнее управление или мировое соглашение. При этом основным внутренним содержанием данной категории является неэффективная деятельность хозяйствующего субъекта, а внешним проявлением – неплатёжеспособность хозяйствующего субъекта, которая в посредством реализации оздоровительных процедур может быть восстановлена. В случае, когда платёжеспособность восстановлена быть не может, то можно говорить о банкротстве хозяйствующего субъекта.

В этой связи «банкротство» можно рассмотреть как экономическую категорию, применяемую к должнику в случае определения арбитражным судом ликвидационной процедуры банкротства – конкурсное производство. Более наглядно дифференциация категорий «несостоятельность» и «банкротство» представлена на рис. 1.

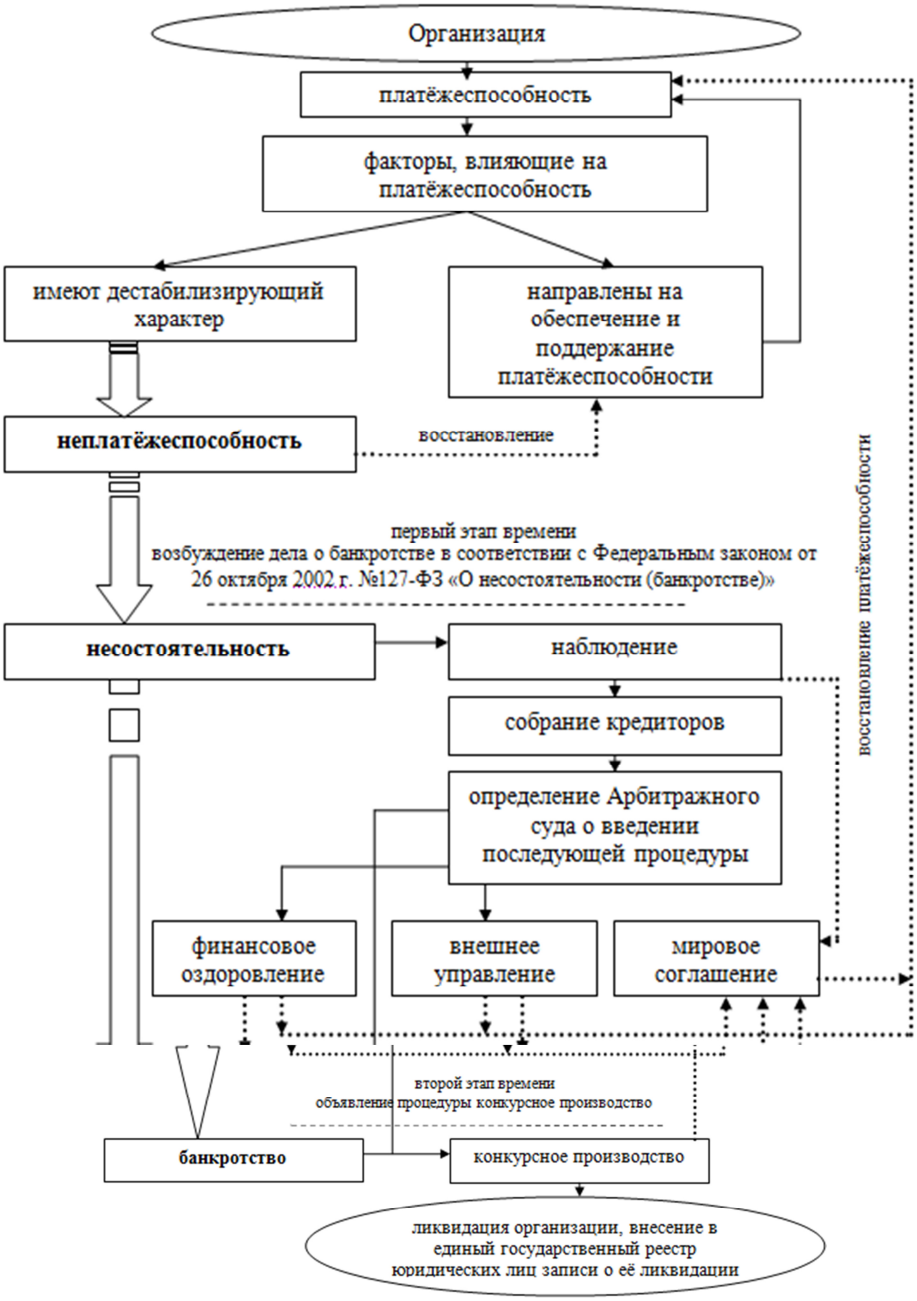


Рис. 1. Дифференциация категорий «несостоятельность» и «банкротство».
Источник: составлено авторами.

Список использованной литературы:

1. Карпунин А.Ю., Карпунина Е.В. Фактор времени при дифференциации понятий «несостоятельность» и «банкротство» сельскохозяйственной организации // Экономика и предпринимательство. 2013. Т. 7. №1 (30). С. 177-181.
2. Федеральный закон от 26 октября 2002 г. №127-ФЗ «О несостоятельности (банкротстве)» [Электронный ресурс] Режим доступа: http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=LAW;n=149150 Дата обращения: 17.12.2012.

УДК 657.6

Карпунина Е.В.

Роль приложений к бухгалтерской отчётности в оценке финансово-хозяйственной деятельности должника

2 августа 2010 года в Минюсте России был зарегистрирован [1], с вступлением в силу которого произошло соответствующие изменение форм бухгалтерской (финансовой) отчётности. Бухгалтерская (финансовая) отчётность является одним из основных источников информации для осуществления арбитражным управляющим финансового анализа в соответствии с [2]. Исследованиями установлено, что на сегодняшний день в соответствии с [1] к числу основных источников информации для проведения финансовой диагностики должника относятся «Приложения к бухгалтерскому балансу и отчёту о финансовых результатах» (далее Приложения), в то время как до вступления в силу указанного Приказа арбитражный управляющий проводил анализ финансового состояния должника преимущественно по данным бухгалтерского баланса и отчёта о прибылях и убытках.

Например, в указанном Постановлении есть такой показатель как «Скорректированные внеоборотные активы», для расчёта которого необходима дополнительная информация, содержащаяся в Приложениях, раскрывающая стоимость деловой репутации организации, стоимость организационных расходов и стоимость капитальных затрат на основные средства, которые находятся в аренде. Однако уточним, что организациям дано право самостоятельно определять спектр информации, подлежащей отражению в Приложениях. Информация о стоимости собственных акций, выкупленных у акционеров потребуется при расчёте стоимости наиболее ликвидных оборотных активов. Данную информацию также можно найти только в составе приложений к отчётности. Аналогичным образом при определении величины краткосрочной дебиторской задолженности из расчёта необходимо исключить задолженность участников (учредителей) по взносам в уставный капитал. В Постановлении имеет место такой показатель как «Потенциальные оборотные активы к возврату», отметим, что единственным источником информации для определения указанной величины будут также именно приложения к бухгалтерскому балансу и отчёту финансовых результатах. При этом в приложениях должна быть отражена информация о списанной в убыток сумме дебиторской задолженности и сумме выданных гарантий и поручительств. До вступления в силу Приказа показатели были отражены в соответствующей Справке, в которой отражали ценности, учитываемые на забалансовых счетах. В частности суммы отражали по таким статьям, как списанная в убыток задолженность неплатёжеспособных дебиторов и обеспечение обязательств и платежей выданные. Аналогичным образом рассчитать величину собственного капитала без привлечения приложений невозможно, так как из расчёта необходимо исключить сумму капитальных затрат имуществу, находящемуся в аренде и задолженность акционеров (участников) по взносам в уставный капитал. Получается, что результаты анализа могут быть поставлены под сомнение в том случае, когда хозяйствующий субъект не детализирует соответ-

ствующую информацию. Мы считаем обоснованным, что изменения законодательства, повлекшие за собой соответствующее изменение форм бухгалтерской (финансовой) отчётности не способствуют прозрачности выводов, которые готовит арбитражный управляющий по результатам исследования. Большая часть информации для проведения исследования находится именно в составе приложений, которые детализируются не одинаково. В связи с тем, что организации самостоятельно определяют степень детализации информации в приложениях, то для детализированного финансового анализа потребуется привлечение дополнительных источников информации, к числу которых можно отнести и регистры первичного, аналитического и синтетического учёта. В противном случае выводы, подготовленные арбитражным управляющим могут быть поставлены под сомнение.

Список использованной литературы:

1. Приказ Министерства финансов РФ от 02.07.2010 г. №66н «О формах бухгалтерской отчётности организаций» [Электронный ресурс] Режим доступа: http://www.consultant.ru/ Дата обращения: 20.05.2015.

2. Постановление Правительства РФ от 25.06.2003 №367 «Об утверждении Правил проведения арбитражным управляющим финансового анализа» [Электронный ресурс] Режим доступа: http://www.consultant.ru/ Дата обращения: 20.05.2015.

3. Карпунина Е.В. Анализ финансового состояния должника по данным бухгалтерской (финансовой) отчетности // Международный бухгалтерский учет. 2014. № 23. С. 66-72.

УДК 658.5.011

Левина Т.А., Кашаева В.Ю.

Факторы, оказывающие влияние на общий уровень экономической безопасности предприятия

В современных условиях нестабильной экономической ситуации как никогда обострилась конкуренция между крупными компаниями. Высокая конкуренция на мировом рынке требует от корпоративных структур поиска новых подходов к управлению, которые позволили бы им удерживать, контролировать и расширять свою долю рынка, обеспечивая необходимый уровень прибыльности и экономической устойчивости.

Сегодня, чтобы остаться на рынке, нет времени на медленное и постепенное освоение современных методов обработки экономической информации, нужно найти такой алгоритм работы, который позволит с наименьшими затратами времени осваивать лучший мировой опыт. На пути увеличения конкурентоспособности компании и для повышения инвестиционной привлекательности компании используют различные экономические информационные системы, которые представляют собой коммуникации связывающие внутренние и внеш-

ние потоки прямой и обратной экономической и иной информации компании, а так же средств и специалистов, принимающих участие в трансформировании информации для принятия правильных управленческого решения.

Качество таких информационных систем может серьезно сказываться на экономической безопасности компании, так как высокая степень централизации информации в корпорации делает ее особенно слабо защищенной и повышает риск доступа третьих лиц к конфиденциальной информации. Таким образом, одной из факторов оказывающих влияние на экономическую безопасности компании является информационная безопасность. Система информационной безопасности позволяет обеспечить защиту слабо защищенных мест компании, предотвратить опасности, угрожающие ей.

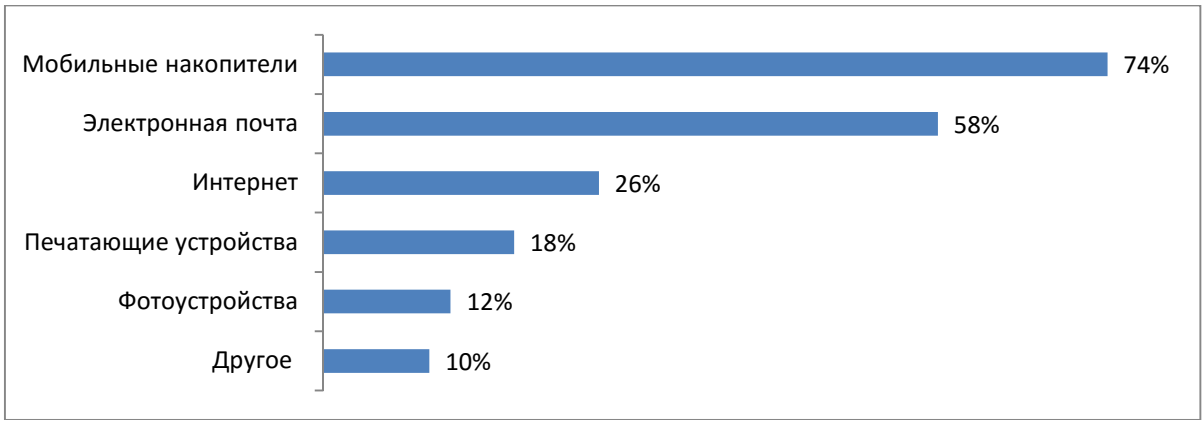


Рис. 1. Результаты опроса специалистов

Виды и количество слабо защищенных мест компании определяется видом бизнеса, характером обрабатываемой информации, технологическими особенностями обработки информации в компании, наличием средств защиты и насколько они морально устарели.

В результате проведенного опроса специалистов, большинство из них считают одной из главной угроз экономической безопасности компании мобильные накопители.

Причина в том, что мобильные накопители являются незаметными, небольшие запоминающие устройства, способные сохранять огромные массивы данных. Их вместимость, мобильность и простота подключения - основные причины использования как инструмента лиц, обладающих какой-либо важной экономической информацией, которые активно действует для собственной выгоды. В тоже время запретить использование мобильных накопителей не всегда представляется возможным, так как они иногда требуются для осуществления прямых обязанностей персонала компании.

В последнее время стали появляться новые технические средства для доступа к экономической информации компании. Кража важных финансовых данных может осуществляться прямым подключением к телефонным и компьютерным коммуникациям, установкой микрофонов, использование микрофонов направленного

действия с усилением получаемого сигнала и другой техники. Для предотвращения несанкционированного доступа существуют меры, такие как средства для шифрования информации, устройства для создания помех подслушивающим устройствами многие другие достижения современной науки и техники. Настоящей проблемой владельцев информации стало вредоносное программное обеспечение, способное внедриться в другие программы и нанести им вред.

Таким образом, информационная безопасность является важным фактором экономической безопасности и конкурентоспособности любой компании. Одной из сложнейших проблем обеспечения информационной безопасности является повсеместное использование мобильных накопительных устройств. Противозаконное использование таких устройств недобросовестным персоналом компании преследующим личную выгоду может привести к утечке секретной информации из экономическое системы компании.

Список используемой литературы:

1. Крошилин С. В., Медведева Е. И. Информционные технологии и системы в экономике: учебное пособие. - М: ИПКИР, 2008. - 485С.

3. Преображенский Е.Л. Инсадерские угрозы в России//Управление персоналом//Корпоративная Периодика. -2009. - №7(209). - 6-10С.

УДК 657.632

С.В. Муравлева, С.Г. Чеглакова

Классификация экономических нарушений, связанных с недостоверным отражением в учете информации о состоянии материальных ресурсов

Экономические нарушения представляют собой совершение действий противоправного характера, влекущих серьезные последствия в экономической деятельности субъекта вплоть до больших денежных потерь, а также совершения экономических преступлений.

Исследовав возможные искажения в учете, нами разработана классификация экономических нарушений, связанных с недостоверным отражением в учете информации о состоянии материальных ресурсов, которая предполагает следующие признаки:

1) Количественный признак, связанный с состоянием материальных запасов на складе (уровнем ликвидности) (Таблица 1);

2) Человеческий фактор:

   а) Недобросовестное отношение работников (Таблица 2);

   б) Некомпетентность персонала в вопросе учета МПЗ (Таблица 3).

Таблица 1. – Содержание экономических нарушений по признаку: количественный признак, связанный с состоянием материальных запасов на складе (уровнем ликвидности)

Нарушения в учете по отражению состояния МПЗ	Содержание искажения	Последствия искажения
Инвентаризация складских запасов материально-производственных ценностей		
а) Нарушения графика проведения инвентаризации	Отсутствие разработанного графика	Возникновение условий, способствующих хищению
б) Нерегулярная сверка данных по движению материально-производственных запасов в бухгалтерии и на складах организации	Непроведение в установленные сроки инвентаризаций или их формальное проведение	
в) Хранение большого количества неиспользуемых материально-производственных запасов	Низкая оборачиваемость запасов	Отрицательное влияние на уровень платежеспособности и деловой активности

Таблица 2. – Содержание экономических нарушений по признаку: недобросовестное отношение работников

Нарушения в учете по отражению состояния МПЗ	Содержание искажения	Последствия искажения
1. Неправильное и несвоевременное оформление документов по движению материально-производственных ценностей	Неверное оформление в учете движения материальных ценностей; Неполнота заполнения реквизитов форм первичного учета должностными лицами	Возникновение условий, способствующих хищению материальных ресурсов; Неверное отражение данных в бухгалтерском балансе; Возникновение противоречий с поставщиками и подрядчиками
2. Не заключаются договора о материальной ответственности с кладовщиками (материально-ответственными лицами)	Отсутствие документов, подтверждающих ответственность должностного лица за сохранность материальных ресурсов	Появление внеплановых расходов

Таблица 3. – Содержание экономических нарушений по признаку: некомпетентность персонала в вопросе учета МПЗ

Нарушения в учете по отражению состояния МПЗ	Содержание искажения	Последствия искажения
1. Неправильное формирование фактической себестоимости материально-производственных запасов	Искажение в учете стоимости материальных ресурсов;	Совершение непреднамеренных расходов организации
2. Неправильное списание материально-производственных запасов по видам расходов	Способ определения фактической себестоимости может отличаться от установленного в учетной политике	Расхождение полученных финансовых результатов при фактическом списания мпз и результатов, полученных в соответствие со способом, указанным в учетной политике
3. Искажения в учете НДС по поступившим материально-производственным запасам	Неверное отражение НДС	Увеличение стоимости МПЗ, по которой они учитываются при поступлении

Таблица 3. Продолжение.

4. Нарушения, связанные с ведением регистров бухгалтерского учета:		
а) Несоответствие данных аналитического и синтетического учета или сопоставимых данных по отчетным периодам	Неверная корреспонденция счетов по операциям учета МПЗ	Увеличение расходов; Создание условий для хищения ресурсов
б) Противоречие между взаимосвязанными данными на разных счетах бухгалтерского учета	Хищения с участием должностных лиц (бухгалтер); Халатное отношение бухгалтера к должностным обязанностям	
5. Отклонение фактических экономических показателей от плановых, нормативных или расчетных, а также неоправданные изменения в динамике отдельных расчетных показателей	Увеличение фактического расхода в суммовом выражении на единицу продукции относительно нормативного расхода, предусмотренного технологическими нормами	Возникновение внеплановых расходов

Для того чтобы недопустить совершение действий, способствующих искажению фактов в бухгалтерском учете о состоянии материальных ресурсов, рекомендуется применять следующие инструменты контроля:

1) проводить необходимые мероприятия по разработке в организации Положения по учету материально-производственных запасов, отражающего специфику производства предприятия и соответствующего Методическим указаниям по бухгалтерскому учету МПЗ;

2) осуществлять контроль за наличием документов (приказ об определении круга материально-ответственных лиц, договоры о материальной ответственности) и сверять, соответствует ли метод учета списания материально-производственных запасов (фактически применяемый на практике в организации, утвержденному в учетной политике);

3) четко руководствоваться требованиями Налогового кодекса по документальному оформлению и экономической целесообразности произведенных расходов при их формировании.

Таким образом, незначительные нарушения в учете материальных ресурсов могут повлечь за собой серьезные последствия, которые могут повлиять на недостоверное отражение показателей финансовой деятельности в бухгалтерской (финансовой) отчетности и как следствие спровоцировать экономические нарушения.

Список литературы

1. Приказ Минфина РФ от 09.06.2001 N 44н (ред. от 25.10.2010) "Об утверждении Положения по бухгалтерскому учету "Учет материально-

производственных запасов" ПБУ 5/01" (Зарегистрировано в Минюсте РФ 19.07.2001 N 2806) // "Российская газета", N 140, 25.07.2001

2. Приказ Минфина РФ от 28.12.2001 N 119н (ред. от 24.12.2010) "Об утверждении Методических указаний по бухгалтерскому учету материально-производственных запасов" (Зарегистрировано в Минюсте РФ 13.02.2002 N 3245) // "Российская газета", N 36, 27.02.2002

3. Судебная бухгалтерия: Учебник / С.П.Голубятников, Е.С.Леханова, В.А.Тимченко; под ред. С.П. Голубятникова. — М.: Юрид. лит., 1998. — 368с.

4. Уткина, С.А. Восстановление бухгалтерского учета, или как «реанимировать» фирму [Электронный ресурс], Электронная библиотека TheLib.Ru, 2006-2015. – Режим доступа: http://thelib.ru, свободный. (Дата обращения: 15.05.2015 г.)

УДК 65.01

Орешина А.Ю., Чеглакова С.Г.

Количественные показатели энергоэффективности в оценке деятельности предприятий энергетического комплекса

Энергетика является базовой инфраструктурной и стратегической отраслью, не имеет возможности максимизировать свои тарифы и вынуждена учитывать требования отраслевых ценовых регуляторов. [1]

В этих условиях должна быть налажена четкая система прямой и обратной связи с оперативным выявлением отклонений от заданных параметров и принятия на их основе эффективных управленческих решений. Для более полной оценки деятельности предприятия энергетического комплекса важны не только стоимостные показатели, но и физические. Введение показателей энергоэффективности, как потенциала системы выработки энергии, может способствовать оценке, на каком уровне технического прогресса получают энергию и какой предел может быть.

Энергетическая эффективность — это характеристики, отражающие отношение полезного эффекта от использования энергетических ресурсов к затратам энергетических ресурсов.[2] Удельные показатели эффективности передачи энергии представляют собой отношение абсолютных значений потерь энергии в системе к характерным параметрам системы. Устанавливаемые в учетных регистрах значения показателей эффективности передачи энергии должны охватывать весь рабочий диапазон параметров системы. [3]

С учетом вышеизложенного система аналитического обеспечения должна базироваться на данных учетных подсистем и содержать следующие показатели энергоэффективности.

Таблица 1 – Рекомендуемая система количественных показателей энергоэфективности

Показатель	Обозначение	Единицы измерения	Содержание
Электрическая мощность	N	Ватт	Среднегодовое значение установленной мощности: по видам, по источникам генерации, по видам носителей.
Коэффициент использования оборудования	$К_{ио}$		Число часов использования
Коэффициент технического использования оборудования	$К_{тио}$		Готовность к несению нагрузки
Общая выработка электроэнергии	$В_э$	кВт·ч	Выработка электроэнергии, в том числе и по теплофикационному циклу
Структура использования топлива	Графическое представление (диаграммы,график и т.п.)		Среднегодовая структура использования сожженного топлива и его характеристики
Расход энергии на собственные нужды	$Э_{исп}$	кВт·ч	Фактические и нормативные значения расходов электроэнергии и теплоты на собственные нужды
Удельный расход топлива	$УР_т$	Единицы параметров, входящих в определение.	Фактические, номинальные и нормативные значения удельных расходов топлива на отпущенную электроэнергию
Перерасход топлива	$П_т$	Единицы измерения условного топлива	Годовые значения величин перерасходов топлива из-за отклонения фактических показателей обородувания от нормативных
Потери электроэнергии	ПЭ	кВт·ч	Фактические и нормативные потери электроэнергии в электрических сетях за отчетный период

Таким образом, рекомендуемая система количественных показателей энергоэффективности позволит всесторонне и более детально оценить результаты хозяйственной деятельности предприятия энергетического комплекса, отразить все сильные и слабые стороны в организации системы управления хозяйствующего субъекта.

Библиографический список

1) Н.Г. Кузьмина Экономика энергетических предприятий: учебное пособие /Л.А.Коршунова, Н.Г. Кузьмина – Томск: Изд-во ТПУ, 2006. – 156 с.
2) В.И.Шлапаков Показатель «энергоэффективность» – основной критерий развития энергетики/ В.И.Шлапаков – Энергоснабжение, №3(21), 2008 г – с.23-25

УДК 657.6.012.16

Прошина О.А., Чеглакова С.Г.

Выявление финансового риска по данным статистической отчетности организаций Рязанской области

В условиях рыночной экономики и современного экономического кризиса в России конкурентоспособность и целесообразность деятельности организаций в будущем основываются на эффективности их функционирования. Эффективность работы организаций можно оценить по финансовому результату их деятельности. Так в соответствии с информацией Министерства финансов Российской Федерации № ПЗ-9/2012 «О раскрытии информации о рисках хозяйственной деятельности организации в годовой бухгалтерской отчетности» (далее – Информация) с целью формирования полного представления о финансовом положении организации, финансовых результатах ее деятельности и изменениях в ее финансовом положении в годовой бухгалтерской отчетности организации раскрываются показатели и пояснения о потенциально существенных рисках хозяйственной деятельности, которым подвержена организация. Раскрытие указанной информации является одной из составляющих системы внутреннего контроля совершаемых фактов хозяйственной жизни организации.

В соответствии с вышеназванным нормативным документом риски хозяйственной деятельности организаций группируются по следующим видам: финансовые, правовые, страновые и региональные, репутационные, и ряд других.

К примеру, Т.А. Журавлева рекомендует классифицировать риски хозяйственной деятельности по группам: финансовые (риски ликвидности, кредитные риски, рыночные риски) и нефинансовые (страновые и региональные, правовые и репутационные) риски. [2]

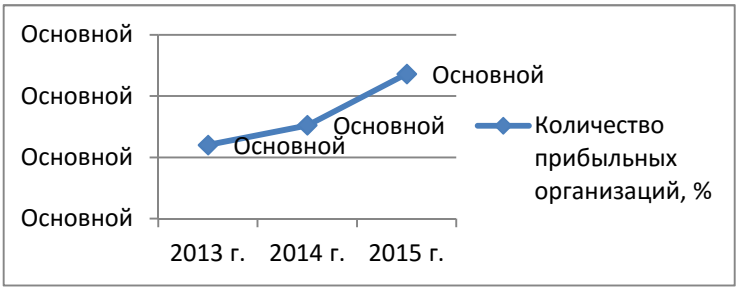
Основными рисками коммерческих организаций являются рыночные, кредитные и риски ликвидности.

Рыночные риски - связаны с возможными неблагоприятными для организации последствиями в случае изменения рыночных параметров (цен и ценовых индексов процентных ставок, курсов иностранных валют.

На сегодняшний день резкое изменение курса американского доллара и евро, условия экономических санкций против Российской Федерации могут повлечь за собой угрозу отрицательной динамики финансовых результатов деятельности коммерческих организаций, то есть рыночные риски будут иметь существенное значение.

При анализе сальдированного финансового результата организаций Рязанской области за 1 квартал 2015 г. можем наблюдать положительную динамику. Данный показатель составил 6091,9 млн. руб. прибыли, в то время как за аналогичный период 2014 г. данный показатель составлял 3845,6 млн. руб. Доминирующую долю в структуре сальдированного финансового результата области на протяжении последних лет занимают организации обрабатывающих производств.

По итогам работы за отчетный период в экономике области убыточными были 28,2% организаций, сумма полученных ими убытков составила 2025,2 млн. руб., в то время как сумма прибыли составила 8117,1 млн. руб.



Отметим также положительную динамику количества прироста прибыльных организаций в процентах к общему количеству организаций за аналогичные периоды 2013, 2014 г.г. Так в 2013 г. данный показатель составлял 66%, в 2014 - 67,6 % , на данный период он составляет 71,8 %. Лидирующее положение вновь занимают организации обрабатывающих производств.

Если к вышеизложенному анализу добавить динамику финансового результата организаций по Рязанской области с 2008-2012 г. (Таблица 2), то можно сделать вывод об эффективности бизнеса в целом на территории региона за последние годы.

Таблица 1. Динамика финансового результата организаций Рязанской области 2008-2012 г.г.

Годы	Сальдированный финансовый результат		Количество организаций (в % к общему количеству организаций)	
	млн. рублей	% к предыдущему году	Прибыльных	Убыточных
2008	7497,3	85,4	76,0	24,0
2009	7472,2	88,6	71,9	28,1
2010	13802,9	155,1	72,1	27,9
2011	12291,6	91,7	74,2	25,8
2012	13952,5	112,9	77,4	22,6
2013	17887,7	123,0	72,7	27,3

Кредитные риски - связаны с возможными неблагоприятными для организации последствиями при неисполнении (ненадлежащем исполнении) другими лицами обязательств по предоставленным им заемным средствам.

Риски ликвидности - связаны с возможностями организации своевременно и в полном объеме погасить имеющиеся на отчетную дату финансовые обязательства: кредиторскую задолженность поставщикам и подрядчикам, задолженность заимодавцам по полученным кредитам и займам (в том числе в форме облигаций, векселей), др.

Анализ динамики задолженности по обязательствам за период 2011-2015 г. (Таблица 2) показывает, постоянное увеличение суммы задолженности, в том числе аналогичная тенденция наблюдается и при анализе просроченной задолженности. Но вместе с тем в 2015 г., по сравнению с 2014 г. наблюдается снижение последнего показателя (снижение составляет 1028,2 млн. руб.), что несет собой по-

ложительную динамику уменьшения кредитного риска для организаций Рязанской области, так как просроченная кредиторская задолженность приводит к выплате штрафов и как следствие ухудшению финансового состояния организаций.

Таблица 2.Динамика величины задолженности по обязательствам, млн. руб.

	2011г.	2012г.	2013г.	2014г.	2015г.
1. кредиторская задолженность	48133,2	59189,9	72934,0	81255,1	94382,0
1.1. в том числе просроченная	5050,1	4973,9	4718,6	6339,4	5470,9
2. задолженность по кредитам банков и займам	65155,9	73269,1	86939,3	100000,7	117211,1
2.1. в том числе просроченная	569,4	164,6	240,5	239,8	80,0
Суммарная задолженность по обязательствам	113289,0	132459,0	159873,4	181255,8	211593,1
В т. ч. просроченная	5619,5	5138,6	4959,1	6579,1	5550,9

Анализ динамики дебиторской задолженности за аналогичный период (Таблица 3) показывает, также постоянное увеличение суммы дебиторской задолженности. Рост дебиторской задолженности не всегда оценивается отрицательно, а снижение - положительно. Необходимо различать нормальную и просроченную задолженность. В 2015 г., по сравнению с 2014 г. наблюдается снижение просроченной дебиторской задолженности (снижение составляет 1337,3 млн. руб.), но вместе с тем в 2014 г. по сравнению с 2013 г. данный показатель был увеличен на 1280,80 млн. руб.

Таблица 3 – Динамика дебиторской задолженности, млн. руб.

	2011г.	2012г.	2013г.	2014г.	2015г.
Суммарная дебиторская задолженность	45470,7	51205,8	61684,6	74400,2	79261,0
В т. ч.просроченная	3730,7	3621,3	2611,3	5229,4	3892,1

Наличие просроченной дебиторской задолженности, как правило, создает финансовые затруднения, так как на деятельности организаций отразится недостаток финансовых ресурсов для приобретения производственных запасов, выплаты заработной платы и так далее. Кроме того, замораживание средств в дебиторской задолженности приводит к замедлению оборачиваемости капитала.

Подводя итог анализа некоторых показателей статистической отчетности в контексте выявления финансового риска можно сделать вывод о подверженности организаций Рязанской области финансовым рискам. В соответствии с Информацией организациям следует оценивать имеющиеся риски, группировать их по определенным показателям и давать им соответствующую оценку. Раскрытие информации о потенциально возможных рисках перед пользователями позволит сделать правильные выводы и принять адекватные управленческие решения.

Список литературы:

1) <Информация> Минфина России N ПЗ-9/2012 «О раскрытии информации о рисках хозяйственной деятельности организации в годовой бухгалтерской отчетности» // «Бухгалтерский учет», N 11, 2012.

2) Журавлева Т.А. Учетно-методическое обеспечение управления финансовыми рисками предприятий по производству кожи [Текст]: Дис. Канд.экон. наук: 08.00.12/ Т.А. Журавлева; [Рязан. гос. радиотех. Ун-т]. – Рязань, 2014. – 165 с.

3) Шевелев, А. Е. Риски в бухгалтерском учете: учебное пособие для вузов по специальности «Бухгалт. учет, анализ и аудит» / А. Е. Шевелев, Е. В.Шевелева. - М.: КноРус, 2009. - 304 с.

4) Официальные статистические публикации ТОГС: Рязаньстат [Электронный ресурс]//Режим доступа: http://ryazan.gks.ru/wps/wcm/connect/rosstat_ts/ryazan/ru/publications/official_publications/ (дата обращения 25.05.2015г.).

УДК 331.108.2

Скрипкина О.В., Кашаева В.Ю.

Кадровая безопасность как основной элемент системы экономической безопасности хозяйствующего субъекта

Экономическая безопасность хозяйствующего субъекта нацелена на обеспечение стабильности его функционирования, получение прибыли независимо от существующих рисков.

Система экономической безопасности хозяйствующего субъекта состоит из таких элементов, как: экологическая безопасность, кадровая безопасность, финансовая безопасность, информационная безопасность, правовая безопасность.

Кадровая безопасность, являясь одним из элементов системы экономической безопасности, представляет собой процесс ликвидации отрицательных воздействий на экономическую безопасность предприятия за счет предотвращения или снижения рисков и угроз, которые связаны с поведением персонала.

Существует два вида угроз кадровой безопасности: внешние и внутренние. Внутренние угрозы, возникают непосредственно внутри хозяйствующего субъекта, к ним относятся:

- квалификации сотрудников не соответствует предъявляемым к ним требованиям;
- малоэффективная система мотивации персонала;
- потеря квалифицированных работников;
- низкий уровень качества проверки персонала при приеме на работу и др.

Внешние угрозы - явления или процессы, которые не зависят от работников организации и влекут за собой нанесение серьезного материального или репутационного ущерба организации.

К внешним угрозам целесообразно отнести:

- лучшие условия мотивации у конкурентов;
- попадание персонала в группу риска;
- инфляционные процессы.

Для любой организации будет крайне нежелательным присутствие в коллективе персонала, который входит или может потенциально войти в группу риска. Это работники с наркотической, алкогольной и игровой и другими зависимостями.

Риски для кадровой безопасности из-за присутствия работников, страдающих различными зависимостями, в организации заключаются в следующем:

- возможность управлять работником, входящим в группу риска, организациями - конкурентами, что может быть направлено на дестабилизацию организации (увод важных клиентов, разглашение коммерческой тайны и т.д.);
- склонность к незаконным действиям в результате удовлетворения своих зависимостей;
- работник, входящий в группу риска, пытается распространить влияние своих вредных привычек в коллективе, увеличивая количество представителей группы риска в организации.
- использование работником для удовлетворения своих зависимостей материальных ресурсов организации.

В результате осознанных и неосознанных действий работника, входящего в группу риска, происходит разрушение стабильного работоспособного коллектива.

Для предотвращения отрицательных влияний работников, входящих в группу риска на кадровую безопасность предприятия необходимо:

- во-первых, контроль пристрастий и зависимостей потенциального работника (полное анкетирование, проведение тестирования, проверка заявленных сведений, проверка профилей соискателя в популярных социальных сетях). Первичный контакт с кандидатом следует максимально использовать для сбора информации. Рекомендуется обращать внимание потенциального работника на характерные особенности и режим предстоящей деятельности. Целесообразно исключить кандидатуры, связь которых с криминальными сообществами и фирмами-конкурентами была установлена в ходе сбора предварительной информации.
- во-вторых, контроль во время испытательного срока или периода адаптации работника;
- в-третьих, администрация должна быть готова к увольнению работника, принадлежащего к группе риска, при неукоснительном соблюдении требований Трудового Кодекса РФ.

Таким образом, кадровая безопасность, являясь важнейшим элементом экономической безопасности организации, нацелена на установление таких отношений в коллективе, которые бы способствовали эффективной работе хозяйствующего субъекта.

УДК 658.5.011

Цейковец Н. В.

Роль анализа макроэкономических рисков и угроз в обеспечении комплексной безопасности предприятия

На сегодняшний день руководители предприятий всё чаще приходят к пониманию необходимости целенаправленной работы по обеспечению комплексной безопасности, которая уже не ограничивается простой силовой защитой, но также включает в себя и учёт правовых рисков, угроз информационной безопасности, контроль за экономическими показателями и прочие аспекты защиты бизнес-процессов. Тем не менее, в подавляющем большинстве случаев система комплексной корпоративной безопасности не включает в себя анализ макроэкономических рисков и угроз, ограничиваясь в лучшем случае отраслевым горизонтом рассмотрения. В итоге, обеспечение экономической безопасности предприятия не выходит за пределы работы с бухгалтерскими показателями, что в условиях нестабильной ситуации в национальной экономике является абсолютно недостаточным.

Экономическое положение фирмы в значительной степени зависит от общей ситуации в национальной экономике, происходящих реформ, которые опосредовано могут сказаться на отдельных отраслях или регионах, от динамики фундаментальных макроэкономических показателей, а также от множества других факторов, зачастую не имеющих прямого отношения к сфере деятельности фирмы. Как правило, риски и угрозы подобного рода принято списывать просто на неблагоприятную конъюнктуру и воспринимать как имманентное (неотъемлемое) свойство рыночной экономики, тогда как в большом числе случаев они могут быть полностью или частично парированы, при условии проведения должного предварительного анализа.

Каждое предприятие, работающее в определённой отрасли и определённом регионе, так или иначе зависит как от ряда системно значимых отраслей, так и от общей макроэкономической ситуации. В зависимости от сферы деятельности и специфики бизнес-процессов отдельного предприятия набор таких «макроэкономических зависимостей» может различаться, а значит и совокупность соответствующих им рисков и угроз также варьируется от фирмы к фирме. Однако остаётся неизменным сам факт существования макроэкономических зависимостей, так как в экономике невозможно полностью обособленное функционирование фирмы. Разумеется, в отдельных случаях бизнес-процессы могут быть в достаточной степени изолированы от общей макроэкономической ситуации, что даёт возможность до определённой степени пренебречь существующими макроэкономическими зависимостями, но это характерно для абсолютного меньшинства предприятий, как правило, имеющих существенную долю государственного участия и специфическую сферу деятельности, например, гособоронзаказ. Подавляющее же большинство предприятий таким «запасом прочности» бизнес-процессов похвастаться не могут, поэтому, игнорируя макроэконо-

мические риски и угрозы, создают брешь в своей системе комплексной безопасности.

Важным аспектом неблагоприятных для предприятия макроэкономических процессов является их строго экзогенный (внешний) характер, то есть на них невозможно как-либо повлиять. От части именно поэтому многими они и игнорируются, так как воспринимаются как неизбежное зло. Тем не менее, уже сам факт понимания отложенных неблагоприятных эффектов тех или иных макроэкономических процессов может дать достаточную информацию для принятия управленческих решений, которые в будущем способны компенсировать потери фирмы или вообще спасти её от закрытия.

Например, ряд неблагоприятных процессов в российской экономике 2014-2015 годов был обусловлен непрогнозируемыми событиями, но некоторые риски и угрозы вполне чётко прослеживались ещё за два-три года. Одной из таких вполне прогнозировавшихся угроз было ослабление курса рубля, которое стало одним из главных факторов снижения финансовой безопасности многих импортоориентированных предприятий. Разумеется, в значительной степени девальвация национальной валюты была обусловлена непрогнозируемыми факторами, однако сам процесс понижения курса рубля, пускай и не в такой степени, являлся вполне прогнозируемым следствием денежно-кредитной политики, план которой был объявлен ещё за несколько лет до событий 2014 года. Это подтверждается и тем, что первая волна девальвации рубля в 2014 году началась ещё до кризиса власти на Украине, который стал первым непрогнозируемым фактором.

Таким образом, при должном анализе, предприятие вполне может парировать макроэкономические риски и угрозы, обеспечивая более высокий уровень своей экономической безопасности.

УДК 657.622

Чеглакова С.Г.

Ошибки в бухгалтерском учете как провоцирующий фактор экономических нарушений

Экономические нарушения всегда являются следствием искажения экономических показателей в информационном обеспечении.

Получить реальную информацию о деятельности субъекта хозяйствования возможно только на основе достоверной информации, которая формируется по данным бухгалтерского учета. Однако в учетных регистрах по разным причинам имеют место быть различного рода ошибки, которые впоследствии можно квалифицировать, как экономические нарушения.

Ошибкой признается неправильное отражение (неотражение) фактов хозяйственной деятельности в бухгалтерском учете и (или) бухгалтерской отчет-

ности (1), которая должна обязательно исправляться, чтобы обеспечить достоверность информации, содержащейся в бухгалтерской отчетности.

В зависимости от природы возникновения и последствий их проявления все ошибки можно классифицировать по следующим признакам: качество работы информационных технологий и человеческий фактор.

Ошибки, связанные с качеством информационных технологий обычно возникают вследствие некорректно работающих информационных систем (сбои в работе компьютера).

В свою очередь, ошибки, связанные с человеческим фактором, можно представить двумя группами: технические ошибки и ошибки по содержанию. Их отличительные особенности в том, что технические ошибки не искажают экономической сущности хозяйственных операций, но влияют на итоговые показатели бухгалтерской отчетности. В основном это - арифметические ошибки, описки, пропуски.

Ошибки по содержанию, приводят к искажению экономической информации об осуществленных операциях. Они возникают:

1. при документировании операций. Такие ошибки связаны с нарушением правил оформления первичных учетных документов, нарушением графика документооборота, которые в итоге могут привести к искажению оценки объектов учета и появлению ошибок в периодизации.

Нарушение правил оформления первичных документов можно декларировать:

а) отсутствием первичных документов. Это ситуация, когда хозяйственная операция была произведена, а первичный документ ни в момент ее совершения, ни после ее окончания не был составлен, что является прямым нарушением законодательства. (ч.3 ст.9 Федерального закона от 06.12.2011 № 402-ФЗ «О бухгалтерском учете»).

б) несвоевременным получением организацией первичных документов. Здесь уместно говорить о недобросовестных действиях должностных лиц организации, когда хозяйственная операция осуществлена, но документы по ней не оформлены.

в) отсутствием или нарушением графика документооборота.

Учитывая то, что в нем утверждаются правила создания первичных документов, порядок и сроки передачи их для отражения в бухгалтерском учете, наличие ошибок пунктов а) и б) может являться следствием нарушения пункта в).

г) некорректным использованием понятийного аппарата. В основном, это «расходы будущих периодов» и «доходы будущих периодов», где могут иметь место факты неправомерного признания отдельных видов затрат в составе расходов отчетного периода или, наоборот, непризнания расходов в том отчетном периоде, к которому они фактически относятся.

Наличие ошибок при документировании операций нетрудно выявить путем проведения инвентаризации имущества организации или взаимной сверки задолженностей с дебиторами и кредиторами.

2. в периоде отражения. Такие факты имеют место при осуществлении хозяйственной операции в одном отчетном периоде, а отражение ее в бухгалтерском учете и бухгалтерской (финансовой) отчетности в следующем периоде.

Для выявления наличия ошибок такого типа рекомендуется по отчету о финансовых результатах изучить динамику показателей выручки и себестоимости продаж, которая должна иметь одинаковую тенденцию. В противном случае можно констатировать наличие ошибки.

3. в корреспонденции счетов. Их может спровоцировать невнимательность и некомпетентность исполнителя. В любом случае результат – неправильные хозяйственные операции, искажающие экономическую сущность осуществленных операций.

Распространенным способом их выявления является тестирование бухгалтерских записей на основе оборотно-сальдовой ведомости, которая позволяет проследить все бухгалтерские записи.

4. при нарушении установленных правил определения первоначальной и фактической стоимости объектов учета, начисления амортизации, исчислении стоимости материально-производственных запасов при их списании формирования резервов и т.д.;

Возникновение данных ошибок базируется на профессиональных знаниях (незнаниях) бухгалтера.

Например, изменение суммы начисленной амортизации за месяц при использовании линейного метода ее начисления может происходить, только если в предыдущем месяце было введено или списано основное средство, либо по каким-то объектам учета прекратилось начисление амортизации.

5. в уровне качества представления информации по статьям в бухгалтерской (финансовой) отчетности.

При составлении бухгалтерской (финансовой) отчетности могут произойти случайные ошибки. Например, «свернуто» сальдо по расчетным счетам 60, 62, 76 или отражено сальдо счета 58 в составе оборотных активов, в то время как в составе финансовых вложений организации были и краткосрочные, и долгосрочные вложения.

Избежать возникновения данных ошибок возможно при проверке увязки ключевых показателей, значения которых должны совпадать.

Таким образом, знание причин возникновения ошибок в бухгалтерском учете и отчетности, а также инструментов их устранения, позволит минимизировать риск не только экономических нарушений, но и обеспечить уровень надежности инвестируемым ресурсам.

УДК 657.62

Шафранская А.М., Чеглакова С.Г.

Экономические нарушения, связанные с недостоверным отражением в учете информации о состоянии нематериальных активов

Нематериальные активы можно определить как неденежный актив, не имеющий физической формы, оформленный и оценённый надлежащим образом и способный приносить в течение длительного срока (не менее 1 года) экономические выгоды организации.

В настоящее время нематериальные активы широко используются в различных областях экономики. Призванные изначально для решения проблемы несоответствия балансовой и рыночной стоимости организаций, по мере интенсификации использования, нематериальные активы выделились в отдельный инструмент оптимизирования финансовых потоков.

В данном контексте нематериальные активы имеют двойственную сущность. С одной стороны, функция нематериальных активов заключается в реализации бухгалтерской оценки рыночной стоимости конкурентных преимуществ организации. С другой стороны, функцией нематериальных активов является возможность перераспределения получаемого доходы между участниками рыночных отношений путём использования нематериальных активов как обособленного предмета сделок.

Тот факт, что нематериальные активы не имеют физической формы, а их ценообразование – процедура непрозрачная, законность операций с такими активами может быть подвергнута сомнениям. Все хозяйственные операции с нематериальными активами должны иметь соответствующее отражение в бухгалтерском и налоговом учёте.

В связи с этим можно выявить требования к оформлению нематериальных активов:

- должны быть законодательно подтверждены;
- должны быть надлежащим образом оформлены в учете и должна присутствовать возможность отчуждения у собственника, то есть являться объектом купли-продажи;
- должны иметь реальную цену.

Возможность завышения фактической стоимости и завышения фиктивных сделок с нематериальными активами, делают их привлекательным объектом для целей отмывания преступных доходов и финансового терроризма.

Схемы отмывания доходов с использованием такого инструмента как нематериальные активы весьма запутаны. Основным слабым местом формирования величины нематериальных активов в подобных ситуациях являются субъективизм ценообразования таких активов и сложность определения их действительного наличия.

Чтобы обеспечить требования в формировании наличия данной информации, нами обоснованы классификационные признаки экономических нарушений, связанных с нематериальными активами.

Таблица 1. – Содержание экономических нарушений, связанных с интеллектуальной собственностью, в разрезе классификационных признаков

Нарушения	**Регламентирующий нормативный акт**
I Фальсификация документов	
Подделка документов, подтверждающих право собственности на нематериальные активы	Статья 327 УК РФ. Подделка, изготовление или сбыт поддельных документов, государственных наград, штампов, печатей, бланков
Уменьшение налогооблагаемой базы с целью уклонения от уплаты налогов	Статья 199 УК РФ. Уклонение от уплаты налогов и (или) сборов с организации
II Фактическая кража и использованием в корыстных целях объектов интеллектуальной собственности	
Выпуск и продажа продукции под торговой маркой, на использование которой не имеются подтверждающие документы	Статья 1229 ГК РФ. Исключительное право «Другие лица не могут использовать соответствующие результат интеллектуальной деятельности или средство индивидуализации без согласия правообладателя»
Использование технологий, являющихся интеллектуальной собственностью других организаций	
Кража конфиденциальной информации организации с последующей перепродажей	Статья 139 ГК РФ. Служебная и коммерческая тайна «Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки»

Своевременное выявление и предупреждение неверного отражения в отчетности информации о нематериальных активах позволит выявить нарушения в данной отчетности, которые могут перерасти в экономические преступления. Выявление сомнительных финансовых операций, связанных с нематериальными активами, возможно при помощи инструментов экономического анализа. В качестве инструментов можно рассматривать приёмы и методы экономического анализа и данные бухгалтерской (финансовой) отчетности, как информационную базу.

Список литературы:

1. Уязвимые места операций с нематериальными активами (в частности, интеллектуальной собственности), позволяющие их использовать для отмывания денег и финансирования терроризма / Материалы 17-го пленарного заседания Евразийской группы по противодействию легализации преступных доходов и финансирования терроризма – 5-9 ноября 2012 г.
2. Уголовный Кодекс Российской Федерации: Федеральный закон от 13 июня 1996 г. N 63-ФЗ // Российская газета. – 1996.

3. Гражданский Кодекс Российской Федерации: Федеральный закон от 30 ноября 1994 г N 51-ФЗ // Российская газета. – 1994.

УДК 657.6

Шурчкова И.Б.

Расширение границ аудиторской деятельности как основной вектор обеспечения экономической безопасности

Основные угрозы экономической безопасности организации находятся в экономической сфере, их выявление, оценка и устранение подвластны специалистам в области права, учета, налогообложения, управления организациями и др., т.е. специалистам аудиторской отрасли.

Как показано в [5, с. 23], «в настоящее время традиционный финансовый аудит фактически способен удовлетворить интересы заинтересованных лиц не более чем на треть от необходимого им объема информации. А это означает, что только аудит в широком его понимании способен в полной мере обеспечить всех заинтересованных лиц необходимой информацией».

Востребованное расширение границ аудиторской деятельности требует развития теоретических положений аудита в широком его понимании как аудита бизнеса [2, с. 73], одним из направлений которых является предложенная автором концепция аудиторской деятельности как многоуровневой системы и созданная в ее рамках концепция закономерности «трех начал аудита», трансформирующие само понимание аудиторской деятельности как «эргатической системы управления», главную доминирующую роль в функционировании которой играет аудитор, вооруженный информационными технологиями, сочетающей интеллектуальные возможности человека и возможности информационных технологий по информатизации и автоматизации одного из сложнейших видов профессиональной деятельности – аудита. В данной системе услуги и их совокупности позиционируются как элементы, компоненты и страты, взаимодействие которых подчиняется объективно существующим закономерностям [3, с. 20; 4, с. 28; 5, с. 22].

Основной принцип многоуровневой системы аудиторской деятельности: «учет результатов ранее оказанных услуг на любом из уровней системы аудиторской деятельности повышает объективность профессионального суждения аудитора».

Концепция «закономерности трех начал аудита» представлена законом и двумя постулатами.

Первое начало аудита (страта 3): «подтверждение достоверности бухгалтерской (финансовой) отчетности организации не является подтверждением эффективности деятельности этой организации».

Второе начало аудита (страта 2): «прогнозная информация о непрерывности деятельности организации на долгосрочную перспективу свидетельствует

об эффективности этой деятельности при условии, что бухгалтерская (финансовая) отчетность подтверждена».

Третье начало аудита (страта 1): «анализ эффективности стратегии развития организации неуместен, если не подтверждена непрерывность деятельности организации на долгосрочную перспективу».

Основой экономической безопасности организации является подтверждение непрерывности деятельности организации на долгосрочную перспективу, а также стратегия устойчивого развития бизнеса, оценка которой возможна на основе методического инструментария второго и первого начала аудита.

Вопросы экономической безопасности находят отражение на всех «трех началах аудита» - от налоговой безопасности (страты 3 и 2) до анализа непрерывности деятельности на долгосрочную перспективу (страты 2 и 1). По нашему мнению, приоритетом в обеспечении экономической безопасности организации должна явиться стэйкхолдерская теория фирмы и теория устойчивого развития.

По мнению М.А Азарской, «при выражении мнения о достоверности отчетности аудитором даются определенные оценки эффективности деятельности. Однако такие оценки, в частности, способность организации осуществлять деятельность в обозримом будущем в условиях неопределенности внешней среды и рисков хозяйственной деятельности, эффективность менеджмента в выборе и реализации стратегии деятельности и др., не позволяют сформировать мнение об эффективности деятельности организации» [1, с. 423]. Данные оценки могут быть получены только при расширении границ аудиторской деятельности.

Таким образом, аудиторский контроль и использование его современного инструментария является основным вектором обеспечения экономической безопасности.

Библиографический список

1. Азарская, М.А. Аудит бизнес-процессов // Аудит и финансовый анализ. – 2014. - № 6. – С. 423-428.

2. Аудит бизнеса. Практика и проблемы развития: монография /Р.П. Булыга, М.В. Мельник; под ред. Р.П. Булыги. – М.: ЮНИТИ-ДАНА, 2013. – 263 с.

3. Шурчкова, И.Б. Концепция аудиторской деятельности как многоуровневой системы //Аудитор. – 2012. - № 5. – С. 20-29.

4. Шурчкова, И.Б. Обобщенная модель многоуровневой системы аудиторской деятельности // Аудитор. – 2013. - № 3. – С. 28-37.

5. Шурчкова, И.Б. Концепция закономерности «трех начал аудита» как теоретическая основа аудита в широком его понимании //Аудитор. – 2014. - № 7. – С. 22-32.

Для заметок:

СБОРНИК НАУЧНЫХ ТРУДОВ
IV МЕЖДУНАРОДНОЙ НАУЧНО-ПРАКТИЧЕСКОЙ КОНФЕРЕНЦИИ
«ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ:
ПРОБЛЕМЫ И РЕШЕНИЯ»

Руководители проекта: С.С. Андрианова,
Д.А. Безукладов,
А.В. Янкевский

Компьютерная верстка и
оформление обложки: Дизайн-студия Dr.Master
(www.design-atelier.biz)

Подписано в печать __.__.2015. Формат бумаги 60x90 1/16.
Бумага офсетная. Шрифт Times New Roman. Усл. печ. л. 9,25
Тираж 200 экз. Заказ № _____

Отпечатано: Типография
ФГБОУ ВПО «Рязанский государственный радиотехнический университет»,
г.Рязань, Россия