– как это делать. Необходимо соблюдение принципов и алгоритма формирования системы экономической безопасности организации. В основу должно быть положено суждение, что любое действие, нарушающее нормальное функционирование организации, понимается как угроза ее экономической безопасности.

Для создания атмосферы информационной безопасности эффективны меры и мероприятия, которые в первую очередь связаны с повышением общей информационной культуры сотрудников в организации. Следует создавать и максимально укреплять четкую целевую установку на повышение надежности и ответственности по различным направлениям защиты информации. Так, во многих зарубежных компаниях действует двухуровневая система защиты информации:

1) достижение информационной безопасности силами специальных служб;

2) культивирование атмосферы бдительности и ответственности с помощью соответствующих так называемых координаторов (могут быть назначены из служащих среднего звена).

Новые условия развития современной экономики требуют перехода к инновационному типу экономического развития. Организации, внедряя новые технологии в производство, обновляя основные средства, выпуская новые виды продукции, повышая их качество, создают и укрепляют свой имидж. От уровня инновационной активности, масштаба и характера применения технологических инноваций по всем направлениям деятельности зависит эффективность деятельности организации, возможность достижения устойчивого развития в современных условиях.

Список литературы:

1. Информационное общество [Электронный ресурс] / Официальный сайт Министерства связи и информатизации РБ. – Минск, 2020. – Режим доступа: www.mpt.gov.by. – Дата доступа: 15.10.2020.

2. Корнеенко, О. Е. Проблемы и перспективы подготовки специалистов для инновационной экономики. О. Е. Корнеенко, О. Л. Пугачева // Современное образование: преемственность и непрерывность образовательной системы «школа–университет–предприятие» [Электронный ресурс] : XII международная научно-методическая конференция (Гомель, 14–15 февраля 2019 г.) : [материалы] / М-во образования Респ. Беларусь, Гомельский гос. ун-т им. Ф.Скорины, Главн. управл. образования Гомельского облисполкома ; редкол. : И. В. Семченко (гл. ред.) [и др.]. – Гомель : ГГУ им. Ф. Скорины, 2019. – С. 465–468.

3. Корнеенко, О. Е. Тенденции распространения угроз информационной безопасности. О. Е. Корнеенко, Д. В. Дорошев / «Securitatea informaţională 2013», conferinta internationala (ediţia a X-a Jubiliară), 19 aprilie 2013 Chişinău, Moldova / resp. de ed.: S. Ohrimenco. (X Международная конференция по информационной безопасности «Securitatea Informationala 2013» (19 апреля 2013 года), Молдавская экономическая академия, Кишинев. – Ch.: ASEM, 2013. – 127 p. – С. 113-116.

4. Международная экспертная оценка проекта «Закона об информации, информатизации и защите информации» РБ / [Электронный ресурс]. – Режим доступа: http://www.e-belarus.org/docs. – Дата доступа: 02.09.2020.

УДК 330

СОВЕРШЕНСТВОВАНИЕ МЕТОДИКИ ВЫЯВЛЕНИЯ МОШЕННИЧЕСКИХ ДЕЙСТВИЙ ПРИ ПРОВЕДЕНИИ АУДИТОРСКИХ ПРОВЕРОК В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

Савлук А. С.
Брестский государственный технический университет, г. Брест, РБ
Научный руководитель: Сенокосова О. В., доцент

В современных условиях значимой частью экономической отрасли является аудит, позволяющий установить достоверность финансовой отчетности и совершенных хозяйственных операций законодательству Республики Беларусь.

Постоянное изменение активов и обязательств организации может привести к различным ошибкам и неточностям в их отражении в документации, а также возникновению «злого умысла».

Актуальность темы обусловлена недостаточно развитыми теоретическими исследованиями в данной области, отсутствием нормативной базы, регламентирующей понятие, технологию проведения, порядок формирования результатов аудита мошенничества.

Мошенничество – преступление против чужого имущества путем искажения информации, сокрытия истины в личных целях [1].

Для решения данной проблемы привлекаются внешние независимые аудиторы и развивается внутрифирменная система контроля.

Аудит мошенничества – изучение отчетности и хозяйственной деятельности организации с целью выражения мнения о наличии фактов мошеннических схем [1].

С целью более эффективного выявления мошенничества предложено аудиторам рассматривать их в разрезе двух групп:

а) мошенничества, совершаемые работниками организации с целью получения личной выгоды (ущерб наносится собственнику организации, и аудитор обязан ему об этом сообщить);

б) мошенничества, совершаемые собственниками организации (уклонение от уплаты налоговых платежей в бюджет, вывод имущества), – ущерб государству.

Основные схемы мошенничества в зависимости от их направления показаны в таблице 1 [2, с. 8]:

Таблица 1– Основные схемы мошенничества

Наименование	Виды
1	2
Хищение денежных активов	кража наличных денег, паролей к платежным системам; ложные требования об уплате; кайтинг; мошенничество с банковскими переводами; неучтенные продажи или дебиторская задолженность
Хищение не денежных активов	кража запасов; ложные записи по списанию запасов; кража внеоборотных активов, в том числе компьютеров и других ИТ-активов; продажа важной информации на сторону
Манипуляции с оплатой труда	использование фиктивных работников («мертвые души») для начисления заработной платы; фальсификация часов работы
Фальсификация финансовой отчетности	подписание документов «задним числом», проведение фиктивных продаж и поставок; неправильная классификация доходов и расходов при их отражении в бухгалтерском учете
Фальсификация нефинансовой отчетности	поддельные данные сотрудников при приеме на работу; поддельные данные сотрудников по квалификации и рекомендациям
Конфликты интересов	вознаграждения в обмен на получение выгодной схемы сотрудничества; «откаты» высшему руководству; личные интересы: сговор с клиентами и (или) поставщиками
Мошенничество в условиях цифровизации экономики	кража цифровой подписи; дистанционное заключение электронного договора; использование электронных БСО; кража паролей к платежным системам и перевод денежных средств

Источник: собственная разработка

Проникновение информационных технологий в экономику обострило проблемы охраны персональных данных. Вопрос защищенности своих данных от мошенников очень остро стоит у организаций во всех странах мира.

Специфика сети Интернет затрудняет идентификацию личности преступника. Следовательно, у мошенников появляется возможность осуществлять свои преступные замыслы, избегая наказания.

Правовая база, регулирующая вопросы безопасности в электронном мире, на сегодняшний день не является совершенной, что приводит к большим рискам в предпринимательской деятельности.

Все субъекты хозяйствования понимают, что необходимо защищать свои данные не только от потери в результате вирусной атаки, но и от кражи. Для этого необходимо разрабатывать оперативные методы и приемы, которые позволят выявить мошенничество не только внешнего, но и внутреннего (которое зачастую приносит большой вред предприятию) характера.

Существует большое многообразие методов, которые применяют аудиторы для обнаружения мошенничества.

К современным методам обнаружения мошеннических схем относят программы, основанные на законе Бенфорда (использование методов математического анализа, основанные на законе аномальных чисел, с целью выявления сфальсифицированных или подложных документов, искажения в суммах бухгалтерских проводок и другое) [3].

В 1997 году было разработано шесть математических тестов, основанных на законе Бенфорда. В каждом из этих тестов цифровые данные сравниваются с эталонной последовательностью и расследуется причина их отклонения. Тесты на основе закона Бенфорда гораздо эффективнее применять в отношении большого объема данных [3].

Кроме тестов на основе Бенфорда существуют и другие современные методы обнаружения фальсификации отчетности [1, с. 15]:

1) классификация: нейронные сети; наивный байесовский метод; деревья решений; метод опорных векторов;

2) кластеризация: метод K-ближайшего соседа; наивный Байесовский классификатор; самоорганизующиеся карты;

3) прогнозирование: нейронные сети; логистическая модель;

4) выявление аномалий или обнаружение выбросов;

5) регрессия: логистическая; линейная;

6) визуализация.

Одним из самых популярных методов выявления мошенничества является методология оценки деловой надежности (расчет Индекса деловой надежности), которая представляет собой факторную модель с наборов факторов, субфакторов и коэффициентов весомости, определяемые аудитором самостоятельнов зависимости от конкретного вида деятельности субъекта.

Индекс деловой надежности выражается следующим уравнением [4]:

$$ИДН = (f_1d_1 + f_2d_2 + f_3d_3 + f_4d_4 + \ldots + f_8d_8) * f_9, \quad (1)$$

где ИДН – индекс деловой надежности,

d_1-d_8 – коэффициенты весомости факторов,

f_1-f_9 – факторы.

Сумма коэффициентов весомости факторов должна быть равна единице, как и все факторы, равные между собой. При этом коэффициент f_9 определяется самостоятельно аудитором как оценка допустимости этих свидетельств [4].

В данном методе проводится сбор и оценка доказательств 67 индикаторов. Их результативность представлена в таблице 2 [4].

Таблица 2 – Результативность факторов

Код группы факторов	Наименование группы факторов	Формула расчета результативности	Метод оценки
1	2	3	4
F_1	Законность деятельности	$f_1 = f_{1.1}d_{1.1} + f_{1.2}d_{1.2} + \ldots + f_{1.5}d_{1.5}$	Социологический
F_2	Телекоммуникации	$f_2 = f_{2.1}d_{2.1} + f_{2.2}d_{2.2} + \ldots + f_{2.7}d_{2.7}$	Социологический
F_3	Выездная поверка	$f_3 = f_{3.1}d_{3.1} + f_{3.2}d_{3.2} + \ldots + f_{3.7}d_{3.7}$	Социологический
F_4	Кадры и квалификация	$f_4 = f_{4.1}d_{4.1} + f_{4.2}d_{4.2} + \ldots + f_{4.20}d_{4.20}$	Социологический
F_5	Качествоуправления	$f_5 = f_{5.1}d_{5.1} + f_{5.2}d_{5.2} + \ldots + f_{5.5}d_{5.5}$	Социологический
F_6	Сбор и исследование документов	$f_6 = f_{6.1}d_{6.1} + f_{6.2}d_{6.2} + \ldots + f_{6.13}d_{6.13}$	Сравнение
F_7	Информационные сети	$f_7 = f_{7.1}d_{7.1} + f_{7.2}d_{7.2} + \ldots + f_{7.7}d_{7.7}$	Сравнение
F_8	Финансы	$f_8 = f_{8.1}d_{8.1} + f_{8.2}d_{8.2} + f_{8.3}d_{8.3}$	Расчетный

Источник: собственная разработка

Оценка свидетельств осуществляется исходя из соответствующих методов: социологических, экспертных, сравнения и расчетных [4].

Каждый из 67 индикаторов задается в баллах от 0 до 10. Результаты оценок складываются внутри каждой группы по конкретному свидетельству, рассчитываются групповые показатели с учетом их значимости, общий ИДН и делается вывод [4].

Метод позволяет за короткий срок получить скрытую информацию о текущей деятельности организации, оценить риски возникновения мошенничества и разработать мероприятия по их предупреждению [4].

Международным холдингом IBAGroupc была разработана система VAS, которая упрощает и ускоряет выявление сложных схем мошенничества.

После загрузки данных инструмент в графической форме отображает связи между объектами анализа, помогает находить мошеннические схемы или подозрительные операции. Данный алгоритм за секунду просчитывает более двух миллионов связей [5].

Проведя анализ различных методик обнаружения мошенничества, можно сделать вывод, что наиболее вероятным способом обнаружения и своевременной ликвидации мошенничества является объединение системыVAS и модели расчета Индекса деловой надежности. Это позволит визуализировать связи, выявить сложные схемы мошенничества, выделить наиболее важные данные для анализа, разобраться в сложных взаимосвязях между объектами и провести анализ с помощью оценки факторов и оценки их допустимости.

С целью увеличения эффективности данного объединения организации необходимо усилить контроль за данными, которые все больше и больше интересуют мошенников, разработать программные обеспечения, различные защитные программы.

Список литературы:

1. Макарова, Л. Г. Аудит-1 (теоретические основы аудиторской деятельности): Самоучитель / Л. Г. Макарова [и др.]. – // Н. Новгород : НФ ГУ-ВШЭ, 2009.

2. Борисов, В. А. Криминальный аудит против мошенничества среди персонала компаний / В. А. Борисов // Бизнес-разведка. – 2008.

3. Зверев, Е. Распределение Бенфорда: выявление нестандартных элементов в больших совокупностях финансовой информации / Е. Зверев [Электронный ресурс]. – Режим доступа: https://www.iia-ru.ru/upload/inner-auditor/articles. – Дата обращения: 09.12.2020.

4. Криони, А. Е. Детективный аудит: методика оценки деловой надежности субъекта малого предпринимательства / А. Е. Криони [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/detektivnyy-audit-metodika-otsenki-delovoy-nadezhnosti-subekta-malogo-predprinimatelstva. – Дата обращения: 09.12.2020.

5. Информационно – аналитический портал Республики Беларусь [Электронный ресурс]. – Режим доступа: https://iba.by/cases/rpa-raspoznavaniya-dokumentov-klassifikaczii/. – Дата доступа: 10.12.2020.

УДК 330

ЦИФРОВИЗАЦИЯ КАК ИНСТРУМЕНТ ЭНЕРГОСБЕРЕЖЕНИЯ НА ПРЕДПРИЯТИЯХ ТОРФЯНОЙ ПРОМЫШЛЕННОСТИ

Царик О. Г.
Белорусский национальный технический университет, г. Минск, РБ
Научный руководитель: Самосюк Н. А., к.э.н., доцент

Республика Беларусь не обеспечена собственными энергетическими ресурсами. Она энергозависима от внешних поставок энергоносителей. Поэтому проблема энергосбережения с каждым годом становится все более актуальной. Разумнее снижать потребление энергии, нежели постоянно увеличивать ее производство. Одним из эффективных инструментов проведения успешного энергосбережения на предприятии является цифровизация за счет внедрения автоматизированной системы контроля и учета энергоресурсов (АСКУЭ) [3].