Решение SAP Business Integrity Screening для борьбы с мошенническими действиями в компании

Абазьева Мария Павловна

Аннотация: в статье приводится обзор решения SAP Business Integrity Screening, призванного предотвращать мошеннические действия в компании. Описана краткая история разработки продукта, приведена архитектура решения, особое внимание уделено описанию шагов работы с продуктом.

Злоупотребления и несанкционированные действия сотрудников компании вынуждают владельцев искать пути для предотвращения такого поведения. Разработки в области информационных технологий могут стать одним из инструментов, который поможет решить эти проблемы. Следует отметить, что на рынке представлены различные решения в области контроля и предупреждений нелегальных манипуляций со стороны персонала.

В данной работе в качестве объекта исследования одного из таких решений выбран продукт SAP Business Integrity Screening, призванный предотвращать мошеннические действия в компании. В статье описана краткая история разработки продукта, приведена архитектура решения, особое внимание уделено описанию фаз работы с продуктом, обозначены достоинства и недостатки, приведены примеры использования.

Согласно исследованию компании ACFE, каждый год компании теряют до 5% своего дохода из-за мошеннических действия со стороны персонала. Это около 3,7 триллионов долларов в мировом масштабе [1]. В Российских компаниях статистика выглядит следующим образом:

- 45,7 % потерь приходиться на капитальное строительство;
- 44,9% потери в инвестиционных проектах;
- 37,5% потери в закупках сырья и материалах;
- 33,8% потери при закупках услуг и приемки выполненных работ.

SAP Business Integrity Screening (SAP BIS) – продукт компании SAP AG, появившийся в ноябре 2017 г. Ранее данный продукт назывался SAP Fraud Management [2]. SAP BIS не входит в стандартный набор SAP ERP, SAP S/4 HANA on-primes, SAP S/4 HANA cloud. Это отдельная продукт из линейки SAP GRC (Governance, Risk & Compliance), работающий на базе SAP HANA.

Цель SAP BIS, как следует из его названия, – полное сканирование действий сотрудников в информационных системах компании для предотвращения несанкционированных действий. Основными задачами SAP BIS являются:

- обнаружить подозрительные действия в информационной системе раньше, чем это приведет к финансовым потерям компании;
- повысить точность распознавания несанкционированных действий в системе, не увеличивая финансовые затраты на выполнение этих действий;
- предупредить возможные мошеннические действия в системе.

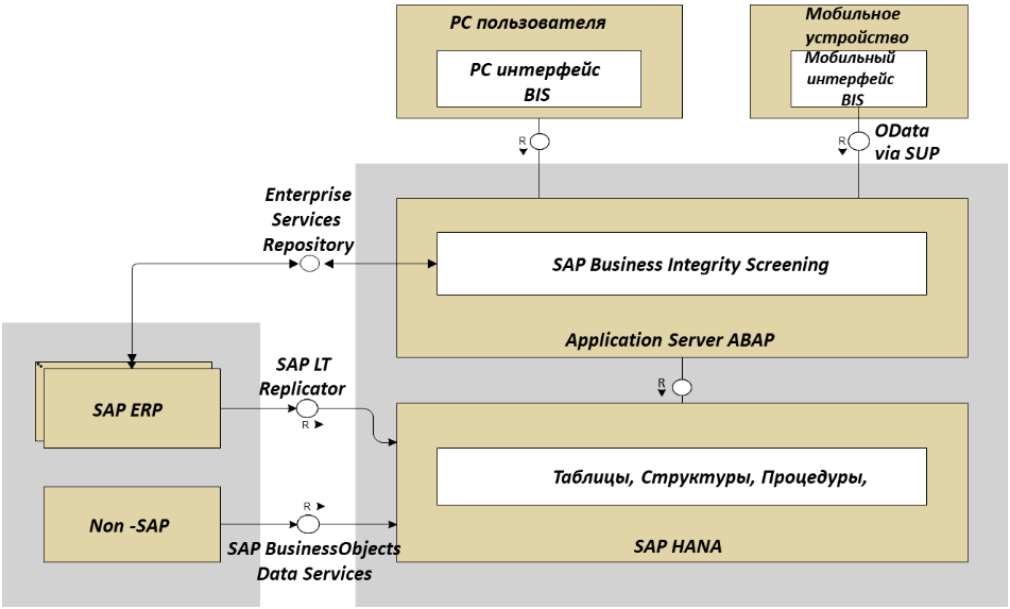

Рис. 1. Архитектура SAP BIS

Далее рассмотрим, каким образом SAP BIS решает поставленные задачи. На рис.1 представлена архитектура SAP BIS, ниже приведены описания:

- Enterprise Service Repository – репозитарий интерфейсов для взаимодействия SAP ERP (S/4 HANA) и SAP BIS;
- SAP LT Replicator (Landscape Transformation Replication Server) – инструмент для загрузки и репликации данных в режиме реального времени или по расписанию из SAP и не SAP систем в SAP HANA;
- SAP Business Objects Data Services – инструмент для интеграции с не SAP системами;
- OData (Open Data Protocol) – это открытый веб-протокол для запроса и обновления данных;
- SAP HANA – база данных HANA;

- Application Server ABAP – сервер приложений, где обрабатываются действия пользователя;
- PC интерфейс SAP BIS – интерфейс SAP BIS, развернутый на настольном компьютере пользователя;
- мобильный интерфейс SAP BIS – интерфейс SAP BIS, развернутый на мобильном устройстве пользователя.

Пользователь работает с SAP BIS через свой PC или мобильное устройство, отправляя запросы на получение данных. Application Server обращается к базе данных SAP HANA для извлечения необходимой информации. В базу данных в реальном времени или по расписанию передаются данные от SAP и не-SAP систем. После обработки запроса пользователь получает результат на своем PC или мобильном устройстве.

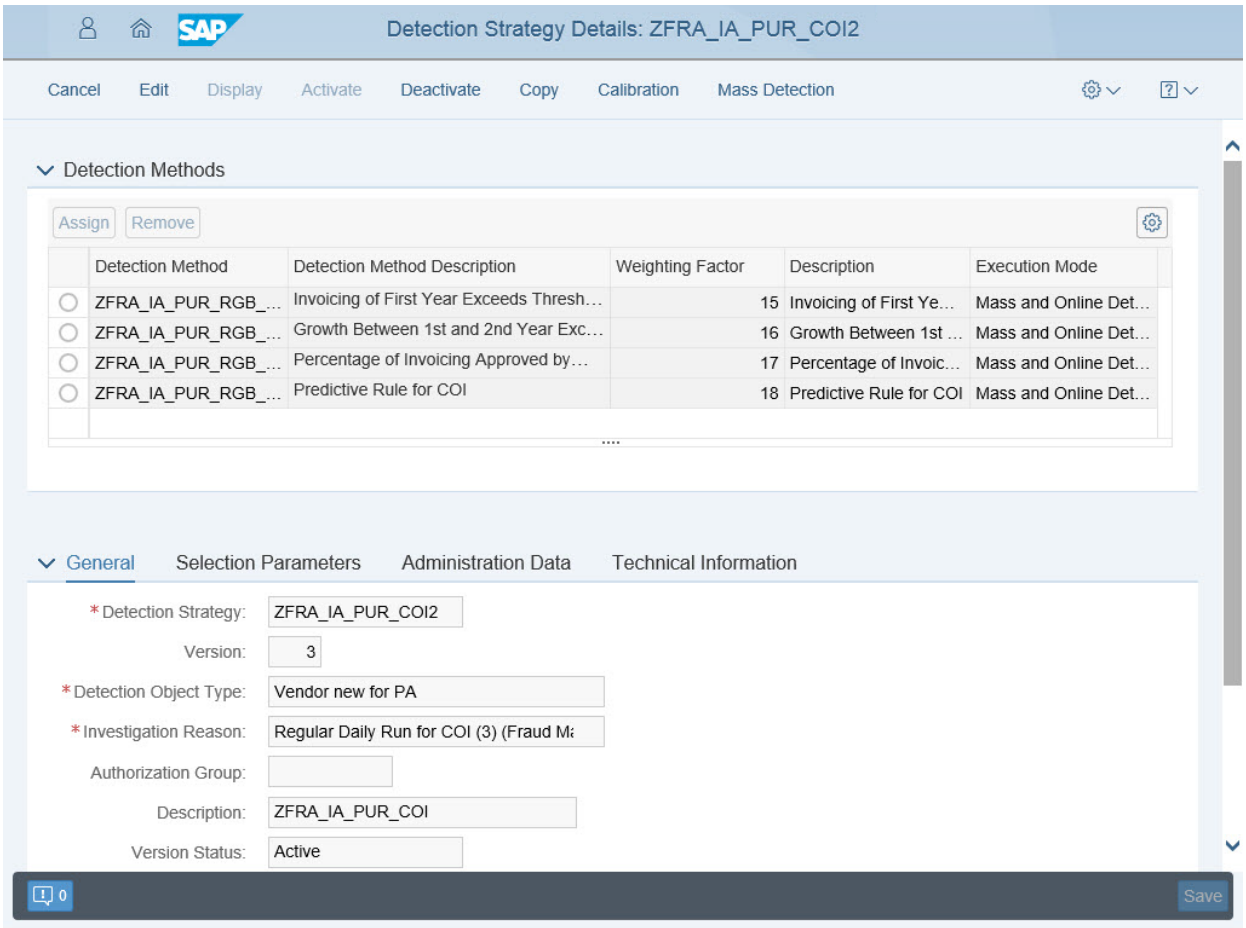

Рис. 2. Настройка правил в SAP BIS

Рассмотрим подробно как происходит работа SAP BIS. Процесс работы с SAP состоит из нескольких фаз: дизайн, настройка, обнаружение, расследование,

мониторинг и отчетность. На фазе «Дизайн» ведется сбор шаблонов, паттернов известных нарушений и несанкционированных действий. Фаза «Настройка» подразумевает внесение информации, полученной на предыдущей фазе, в SAP BIS, тонкую настройку критериев, правил (рис.2) и стратегий для определения действий, которые должны быть классифицированы как несоответствующие типовым, а также моделирование в реальном времени работы стратегии (рис.3). SAP BIS уже имеет в стандартной поставке предустановленные правила обнаружения угроз, например проверка поставщика по его местоположению (высоко рисковые страны), слишком частое изменение основной записи поставщика в системе компании и т.д.

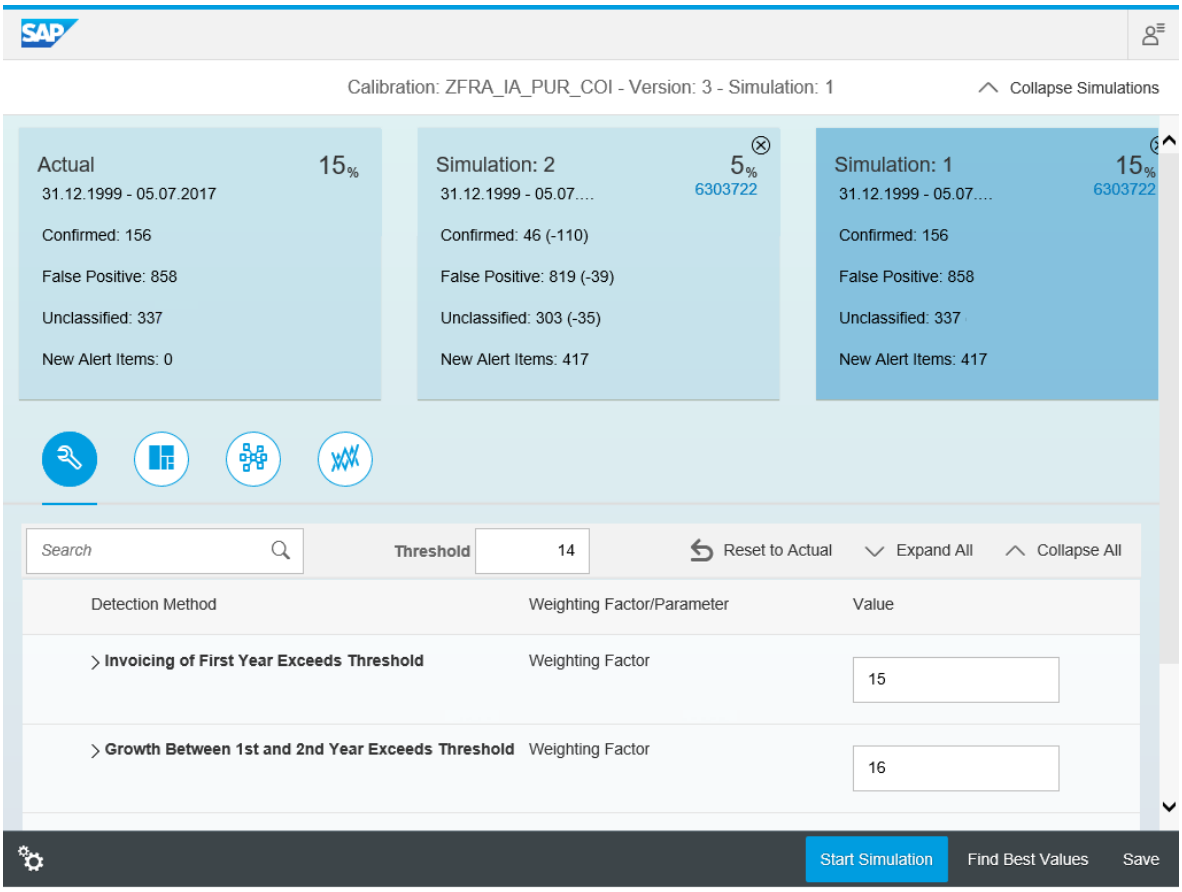

Рис. 3. Моделирование работы стратегии

На фазе «Обнаружения» проводится непосредственный поиск несанкционированных действий на основе данных, которые размещены в SAP HANA или поступают в нее в режиме реального времени, согласно созданным стратегиям. Кроме того, на данном этапе происходит рассылка уведомлений ответственным лицам (рис.4).

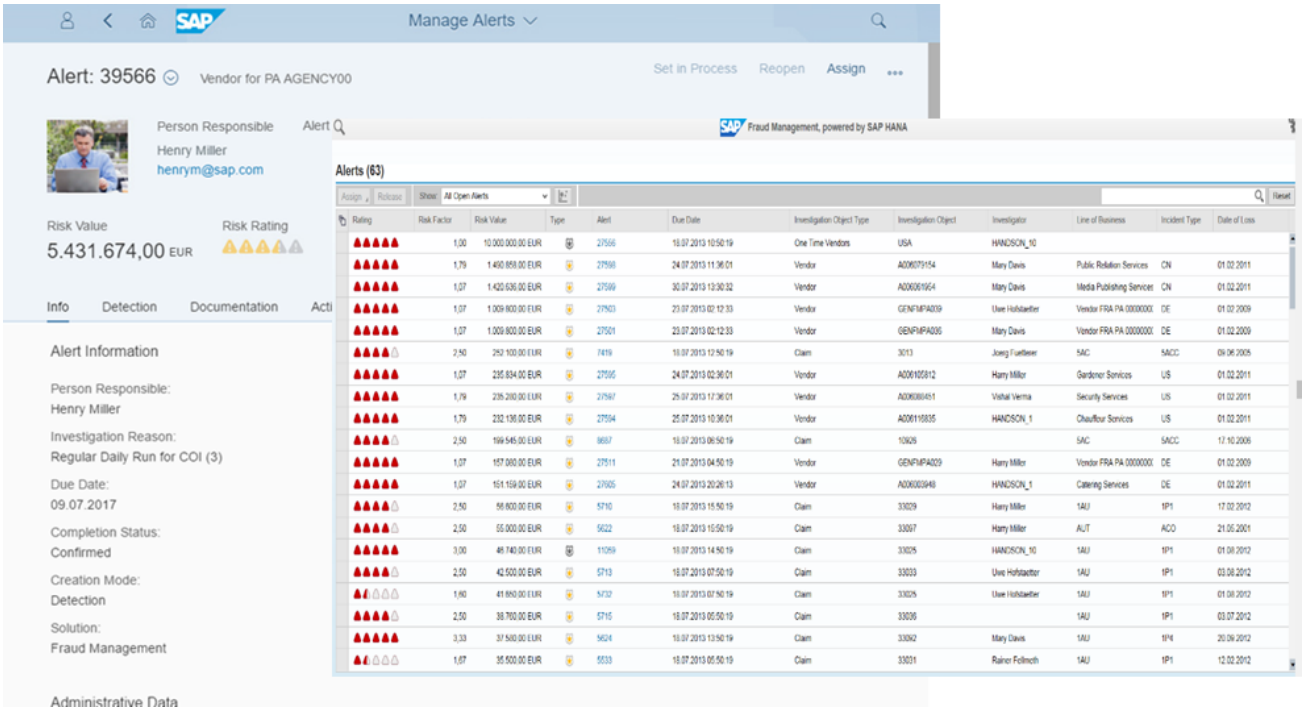

Рис. 4. Моделирование работы стратегии

На фазе «Обнаружения» проводится непосредственный поиск несанкционированных действий на основе данных, которые размещены в SAP HANA или поступают в нее в режиме реального времени, согласно созданным стратегиям. Кроме того, на данном этапе происходит рассылка уведомлений ответственным лицам (рис.4).

Далее на фазе «Расследование» ответственный, получив уведомление о нетипичном поведении или нарушении, решает было ли срабатывание ложным или это действительно подозрительные действия. В последнем случае данные перенаправляются специалисту компании Compliance manager (рис.5). На данной фазе также происходит обучение системы, согласно запатентованному алгоритму SAP Ridge Regression, т.е. система постоянно наполняется шаблонами, которые описывают нарушения и классифицирует их. Это также уменьшает число ложных срабатываний.

На этапе «Мониторинг и отчетность» формируется отчетность по обнаруженным несанкционированным действиям, доступна статистика сколько было ложных и сколько подтвержденных срабатываний (рис.6), также осуществляется мониторинг стратегий поиска угроз и их оптимизация.

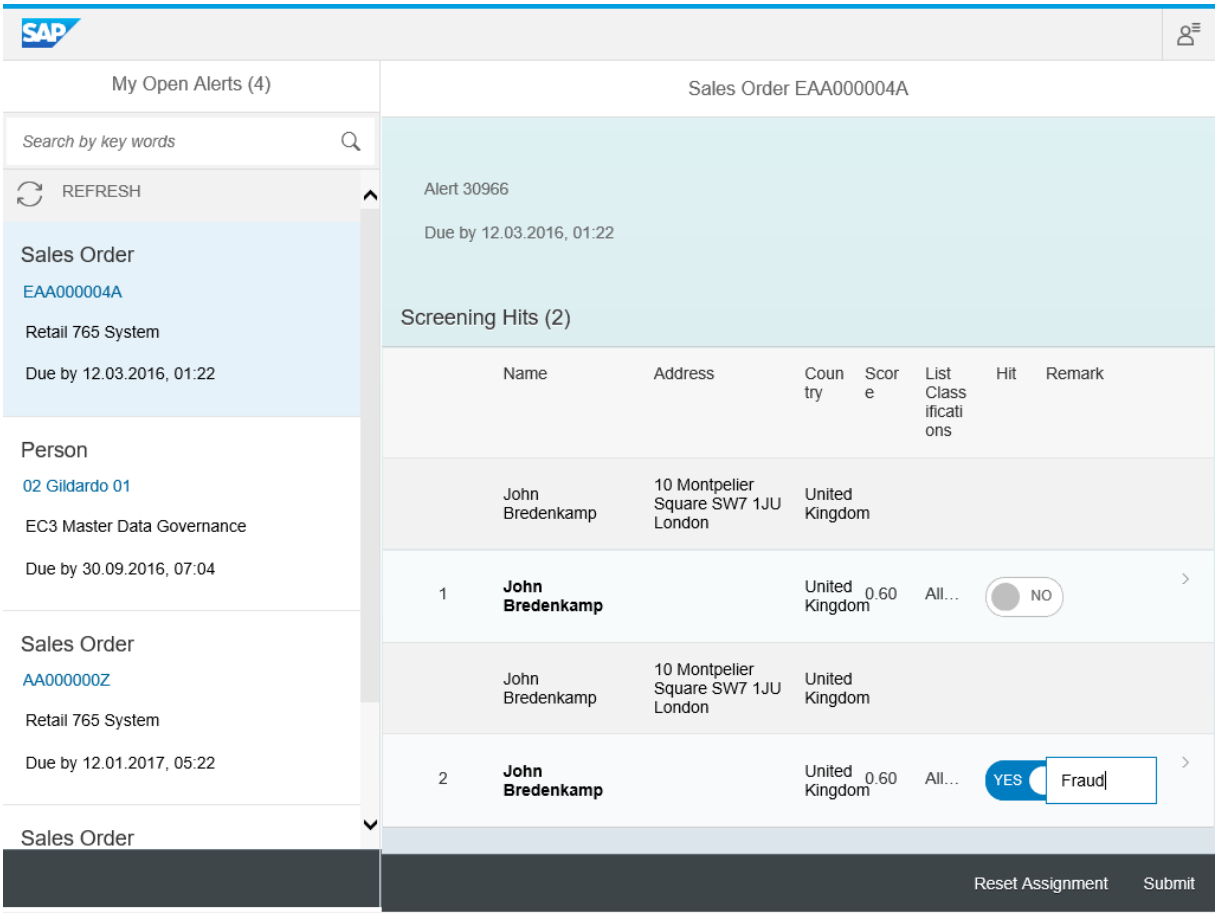

Рис. 5. Приятие решения, что угроза подтверждена

К достоинствам SAP BIS можно отнести следующее:

- быстро разворачивается у клиента (7-10 месяцев) с минимальной командой внедрения;
- пользователи могут сами настраивать правила проверки (требуется минимальное знание SQL);
- можно работать с данными не SAP систем и в режиме реального времени;
- снижение трудозатрат и повышение качества процесса поиска потенциальных угроз,

недостатками данного решения являются:

- высокая цена продукта, зависящая от годового оборота компании;
- может потребоваться отдельный сервер либо выделения достаточно объемного места на текущем сервере для развертывания решения.

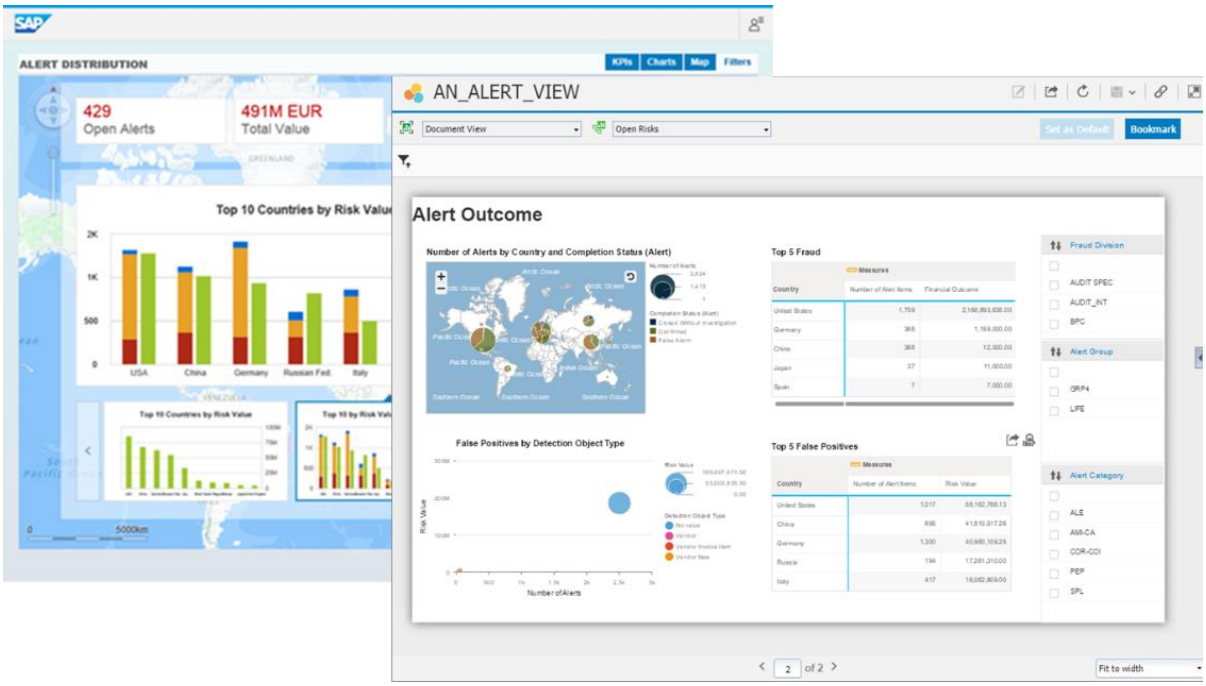

Рис. 6. Отчетность SAP BIS

Лидером по внедрению SAP BIS являются страховые компании, далее следуют банки, компании, занимающиеся предоставлением жилищно-коммунальных услуг, промышленные предприятия. В заключении хочется отметить, что продукт SAP BIS имеет достаточно хорошие перспективы для развития. Особенно его внедрение может заинтересовать те компании, которые уже перешли на SAP и внедрили свои основные бизнес-процессы, т. е. являются «зрелыми» в плане информационных технологий и фактически готовы оцифровывать бизнес-процессы второго порядка.

Литература

1. ACFE 2018 Report to the Nations. ACFE. 2018. Availably at: https://www.acfe.com/report-to-the-nations/2018/
2. SAP Business Integrity Screening. SAP. 2019. Availably at: https://www.sap.com/products/fraud-management.html

Выходные данные статьи

Абазьева М.П. Решение SAP Business Integrity Screening для борьбы с мошенническими действиями в компании // Корпоративные информационные системы. – 2019. – №2(6). – С. 31-38. – URL: http://corpinfosys.ru/archive/issue-6/60-2019-6-sapbis

Об авторе

Абазьева Мария Павловна – руководитель проектов внедрения корпоративных информационных систем. Эксперт по направлению технического обслуживания и ремонта оборудования. Имеет 10-летний опыт работы с программными решениями на базе SAP. Принимала участие в проектах имплементации ERP-систем в транспортных, нефтяных и металлургических компаниях.