Применимость Intellinx в различных областях

В дополнение к обнаружению внутреннего мошенничества, Intellinx весьма эффективен в следующих областях:

- Уменьшение операционных рисков и обеспечение соответствия Basel II
- Обеспечение соответствия таким требованиям по защите персональных данных, как GLBA & HIPAA (США) и директивы EU 95/46 (Европа)
- Обеспечение соответствия ряду требований Sarbanes-Oxley (SOX)
- Обеспечение соответствия требованиям СТО БР ИББС-1.0-2008
- Соответствие законодательным требованиям по противодействию отмыванию денег
- Обнаружение «кражи личности» и других типов мошенничества при интернет-банкинге и других онлайн-услугах
- Отслеживание активности системных администраторов и других привилегированных пользователей
- Мониторинг доступности и времени отклика в критичных процессах
- Добавление контролей уровня приложений
- Анализ путей исполнения бизнес-процесса конечными пользователями
- Поддержка служб ServiceDesk

1 Basel II

Соглашение Basel II представляет операционный риск как один из рисков, управление которыми является обязательным для банков. Соглашение разделяет рисковые события на семь основных категорий типов событий (Приложение 7):

Категория типа событий (1-й уровень)	Определение	Примени-мость Intellinx
Внутреннее мошенничество	Убытки вследствие действий с намерением осуществить мошенничество, присвоить имущество или обойти нормативные акты, законодательство или политику компаний, исключая случаи дискриминации, с участием, как минимум, одной внутренней стороны	Да*
Внешнее мошенничество	Убытки вследствие намерения совершить мошенничество, похитить имущество или нарушить законодательство с участием третьей стороны	Да*
Кадровая политика и безопасность труда	Убытки вследствие нарушения законодательства о труде, безопасности труда и охране здоровья или в связи с выплатами по искам о нанесении личного ущерба или искам в связи с дискриминацией	Нет
Клиенты,	Убытки вследствие непреднамеренной	Да*

Категория типа событий (1-й уровень)	Определение	Примени-мость Intellinx
продукты и деловая практика	халатности в выполнении профессиональных обязательств по отношению к конкретным клиентам (включая доверительные и квалификационные требования) или вследствие характера или конструкции продукта	
Причинение ущерба физическим активам	Убытки вследствие ущерба или повреждения физических активов в результате природных катастроф или прочих событий	Нет
Нарушения в ведении бизнеса и системные сбои	Убытки вследствие нарушений в введении бизнеса и системных сбоев	Да*
Исполнение, доставка и управление процессами	Убытки вследствие срыва обработки операции или сбоев в процессе либо вследствие взаимоотношений с торговыми контрагентами и продавцами	Да*

* Примеры правил Intellinx для выявления событий по категориям типов событий:

1.1 Внутреннее мошенничество

- Изменение кредитного лимита превышает установленный порог в объёме или процентах по типам клиентов
- Увеличение кредитного лимита с последующей оформлением ссуды в течение 48 часов
- Более одного увеличения кредитного лимита в течение одного месяца по счёту
- Новая кредитная карта не послана клиенту (но забрана из компании)
- Перенос даты выставления счета по кредитной карте на более поздний срок
- Более X счетов просмотрено пользователем в течение дня
- Перевыпуск карты запрошен в течение 10 дней после смены адреса в реквизитах
- Изменения в реквизитах счёта сотрудник (детали, относящиеся к представлению «клиент»)
- Изменения в статусе информирования по почте (информирование остановлено или перенаправлено)
- Изменения в счёте сотрудника, выполненные им самим
- Более двух «спящих счетов» просмотрено одним пользователем в течение дня
- Более X заблокированных счетов разблокировано одним пользователем в течение дня

1.2 Внешнее мошенничество

- ATM / Мошенничество с кредитными картами - Intellinx может отслеживать транзакции с кредитными картами в ATM, передаваемые ISO 8583 и другим протоколам.
  - Чрезмерное количество транзакций на ATM в час
  - Чрезмерное количество отмененных транзакций на ATM в час
  - Чрезмерное количество транзакций или высокие объёмы операций по карте в короткий интервал времени
  - Транзакции по одному счету из географически разнесенных мест в короткий период времени
  - Компрометация PIN-кода – несколько попыток ввода неверного PIN-кода в ATM с последующими транзакциями по кредитной карте для одной карты
- Кража личности – приведено в разделе 6 – Обнаружение мошенничества при интернет – банкинге.

1.3 Клиенты, продукты и деловая практика

- Уязвимость в персональных данных и неправомерное использование конфиденциальной информации:
  - Доступ к «чувствительной» информации о клиенте без зафиксированного звонка в тот же интервал времени звонка клиента в колл-центр
  - Поиск информации о счетах клиентов с использованием слишком общих запросов
  - Чрезмерные (или выполняемые в нерабочее время) запросы по счетам клиентов с использованием поиска по именам, выполняемые одним и тем же пользователем
  - Чрезмерный доступ к счетам клиентов одним и тем де пользователем в день
  - Чрезмерный (или выполняемый в нерабочее время) доступ к информации о VIP-клиентах
  - Пользователи, имевшие доступ к указанному счёту в указанный интервал времени
- Противодействие отмыванию денег – приведено в разделе 5 – Противодействие отмыванию денег

1.4 Нарушения в ведении бизнеса и системные сбои

- Приведено в разделе 7 – Отслеживание активности системных администраторов и других привилегированных пользователей

1.5 Исполнение, доставка и управление процессами

Совместное использование логина и пароля несколькими пользователями – эта ситуация может быть обнаружена при определении нескольких логинов в одной сессии с одного терминала

- Одинаковые транзакции (могут быть дубликатами друг друга)
- Нерациональные транзакции (по сравнению с предыдущими транзакциями, или с установленным пределом)

- Нерациональные изменения значений, кредитного лимита, процентной ставки, курсов валют, тарифов
- Сравнение с установленными значениями (процентная ставка по сравнению с таблицей процентных ставок)
- Перевод на счета главной книги, которые не были использованы раньше
- Разделение обязанностей – инициатор и лицо, подтверждающее ссуду, должны быть различными
- Отсутствие информации в обязательных полях (в случае, если это не контролируется банковским приложением)
- «Чувствительные» операции выполняются пользователем, который не выполнял их ранее
- «Чувствительные» операции выполняются пользователем, не принадлежащим к группе, имеющей права на их выполнение.

2 Соответствие требованиям по защите персональных данных

Требования по защите персональных данных, такие как HIPAA и GLBA в США или директива 95/46 ЕС требуют от организаций, которые обрабатывают «чувствительную» информацию о клиентах, собирать и хранить детальные свидетельства доступа сотрудников к информации о клиентах. Эти свидетельства должны содержать записи об операциях чтения данных, а не только об изменениях или удалениях, что, как правило, сохраняется в лог-файлах в большинстве организаций. Свидетельства аудита должны содержать подробную информацию, позволяющую определить, к какой информации какой пользователь имел доступ и когда. Такой уровень детализации обычно можно обеспечить только путем использования лог-файлов приложений. Унаследованные системы, в которых логирование такого уровня не было предусмотрено, могут потребовать огромных усилий по разработке функциональности логирования, поскольку это потребует изменений в каждой из используемых программ. Intellinx решает эту проблему путем накопления весьма детальных свидетельств аудита, включая действия «только чтение», без необходимости изменения ни единой строки кода.

3 Соответствие требованиям СТО БР ИББС-1.0-2008

Согласно п. 7.4.4. в организации БС РФ необходимо документально определить процедуры мониторинга и анализа данных регистрации, действий и операций, позволяющие выявлять неправомерные или подозрительные операции и транзакции. Для проведения процедур мониторинга и анализа данных регистрации, действий и операций рекомендуется использовать специализированные программные и(или) технические средства.

Процедуры мониторинга и анализа должны использовать документально определенные критерии выявления неправомерных или подозрительных действий и операций. Указанные процедуры мониторинга и анализа должны

применяться на регулярной основе, например, ежедневно, ко всем выполненным операциям и транзакциям.

4 Соответствие требованиям Sarbanes-Oxley

Секция 404 Акта Sarbanes-Oxley требует от компаний, акции которых котируются на биржах США создавать и поддерживать эффективную систему внутренних контролей для отслеживания финансовых процессов. Поскольку финансовая отчетность зависит от информации, собираемой из различных информационных систем, таких как АБС, процессинг карт, ERP, CRM и многих других, соответствие требованиям секции 404 требует разработки эффективных кросс-платформенных мер. Правила Intellinx могут быть использованы как такие меры во многих аспектах, требуемых SOX.

4.1 Отслеживание привилегированных пользователей (администраторов систем)

- Изменения данных в системах в промышленной эксплуатации с использованием инструмента построения низкоуровневых запросов
- Изменение исходного кода систем в промышленной эксплуатации
- Изменение «чувствительных» данных в системах в промышленной эксплуатации с терминалов в ИТ подразделениях или с использованием учетных данных привилегированных пользователей
- Сценарий с введением новых модулей в систему в промышленной эксплуатации, работу этих модулей в течение некоторого времени и возврат предыдущих версий модулей (трассировка соответствующих действий).
- Выполнение программ в среде в промышленной эксплуатации

4.2 Отслеживание разделения обязанностей

- Сотрудник, который инициировал обращение о займе, сам одобряет его
- Сотрудник, который инициировал нестандартное увеличение кредита, сам одобряет его
- Сотрудник, который добавил полис «за прошедшее время» в настоящее время добавляет к нему страховое требование

4.3 Управление изменениями

- Отслеживание передачи в промышленную эксплуатацию программ, отмеченных как прошедших тестирование авторизованными тестерами

5 Противодействие отмыванию денег

Intellinx может отслеживать шаблоны поведения клиентов и транзакционную активность в системах он-лайн банкинга, сообщениях в форматах FIX, Swift и других протоколах. Основываясь на сохраненных данных и используемых правилах, Intellinx может генерировать предупреждения и отчёты, требуемые регуляторами в области противодействия отмыванию денег. Ниже приведено несколько примеров:

- Приобретение валюты в объёме, требующем оповещения контролирующих органов
- Последовательные транзакции с объёмом, приближающимся к границе оповещения контролирующих органов
- Вложение с последующим снятием в большом объеме в короткий период времени
- Множество одинаковых вложений/ снятий по одному счёту
- Множество транзакций с одним целевым счётом в месяц
- Новый клиент (частное лицо, организация, орган, страна), находящееся в «черном» списке (OFAC, FATF, NCCT, PEP и других).
- Изменения адреса, после которого две и более несвязанных сущностей имеют один адрес
- Профилирование клиентов – классификация счёта как принадлежащего к какой либо категории (высокий риск, низкий риск и т.д.) в целях мониторинга транзакций/активности. Операционный риск может быть связан с продуктом, индустрией, географическим регионом и т.п.
- Изменения в активности по счёту в сравнении с предыдущими шаблонами в отношении количества и объёма вложений, трансфертов и снятий

6 Обнаружение мошенничества при интернет – банкинге

Intellinx может отслеживать активность пользователей, использующих он-лайн доступ к банковским систем и шаблоны их поведения. Отклонения от нормальных значений могут быть обнаружены правилами Intellinx. Ниже приведено несколько примеров:

- Последовательные неудачные логины в систему
- Выходящие за стандартные отклонения время работы пользователя с системой и/или типы транзакций
- Изменения в реквизитах счёта
- Необычные трансферты денег
- Чрезмерные транзакции по покупке/продаже одних и тех же акций, производимые различными клиентами в один день

7 Отслеживание активности системных администраторов и других привилегированных пользователей

Мониторинг действий привилегированных пользователей является сложной задачей для большинства организаций. С одной стороны, эти пользователи создают большие риски, чем обычные сотрудники, поскольку они имеют более высокие полномочия. С другой стороны, они часто используют административные утилиты и средства разработки, которые не оставляют «аудируемых следов» в большинстве случаев. Intellinx может отслеживать действия привилегированных пользователей, таких как системные администраторы, администраторы баз данных, программисты и тому подобное.

Система формирует шаблоны нормального поведения и генерирует предупреждения в реальном времени при фиксируемом отклонении от них. В дополнение, специалисты, занимающиеся расследованием, могут просматривать подозрительную активность «экран за экраном». Далее приведено несколько примеров:

- Изменения данных в системах в промышленной эксплуатации с использованием инструмента построения низкоуровневых запросов
- Изменение исходного кода систем в промышленной эксплуатации
- Изменение «чувствительных» данных в системах в промышленной эксплуатации с терминалов в ИТ подразделениях или с использованием учетных данных привилегированных пользователей
- Сценарий с введением новых модулей в систему в промышленной эксплуатации, работу этих модулей в течение некоторого времени и возврат предыдущих версий модулей (трассировка соответствующих действий).
- Выполнение программ в среде в промышленной эксплуатации

8 Мониторинг доступности и времени отклика в критичных процессах

- Выход из системы с последующими попытками входа одновременно во множестве пользовательских сессий
- Повторяющиеся попытки входа во множестве пользовательских сессий
- Ошибки приложений (экран ошибки или соответствующий код возврата) в одно и то же время во множестве сессий
- «Плохое» время отклика критичных транзакций в одно и то же время во множестве сессий
- Множество кодов возврата “No response from Host” во множестве сессий 3270/ 5250 в одно и то же время
- Транзакции MQ или HTTP, которые не получили ответа от сервера

9 Добавление контролей уровня приложений

Intellinx может быть использован для добавления контролей к существующим приложениям без их изменения (доработки).

Примеры:

- Разделение обязанностей – примеры в секции 4.2 – Отслеживание разделения обязанностей
- Обнаружение ошибок обработки – примеры в секции 1

10 Анализ путей исполнения бизнес-процессов конечными пользователями

Intellinx может быть использован для анализа того, как конечные пользователи используют информационные системы организации для их

последующей оптимизации, повышения потребительских свойств приложений и обучения пользователей.

11 Поддержка служб ServiceDesk

Intellinx может помочь операторам ServiceDesk обрабатывать звонки по поводу проблем информационных систем и приложений, предоставляя возможность просмотреть действия пользователя, которые привели к появлению (обычно во время звонка в ServiceDesk пользователь не помнит, какие его действия привели к ошибке).