

ИНТОСАИ

|  |  |
| --- | --- |
| ИССАИ 5450 | Международные стандарты высших органов аудита (ИССАИ) выпускаются Международной организацией высших органов аудита(ИНТОСАИ). Для получения дополнительной информации см. веб-сайт *www.issai.org* |

**Руководство по аудиту информационных систем управления государственным долгом**

**Декабрь 2016**

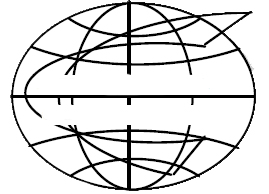
Комитет по профессиональным стандартам ИНТОСАИ

Секретариат Комитета по профессиональным стандартам

Rigsrevisionen • Landgreven 4 • Абонентский почтовый ящик 9009 • 1022 Копенгаген K • Дания   
(P.O. Box 9009 • 1022 Copenhagen K • Denmark)

Тел.: +45 3392 8400 • Факс: +45 3311 0415 • E mail: [info@rigsrevisionen.dk](mailto:info@rigsrevisionen.dk)

ИНТОСАИ



ОПЫТ ВЗАИМОДЕЙСТВИЯ

ДЛЯ ВСЕОБЩЕГО БЛАГА

Генеральный секретариат ИНТОСАИ – RECHNUNGSHOF

(Счетная палата Австрийской Республики)

DAMPFSCHIFFSTRASSE 2

А-1033 ВЕНА

АВСТРИЯ

Тел. ++43 (1) 711 71 • Факс: ++43 (1) 718 09 69

АДРЕС ЭЛЕКТРОННОЙ ПОЧТЫ: intosai@rechnungshof.gv.at;

САЙТ ВО ВСЕМИРНОЙ СЕТИ: http://www.intosai.org

**ИНТОСАИ**

Рабочая группа по государственному долгу

Руководство по аудиту информационных систем управления государственным долгом

**Декабрь 2016**

Содержание:

[ПРЕДИСЛОВИЕ 5](#_Toc506204119)

[СПИСОК СОКРАЩЕНИЙ 7](#_Toc506204120)

[ВВЕДЕНИЕ 8](#_Toc506204121)

[1. ПЛАНИРОВАНИЕ 10](#_Toc506204122)

[2. ОБЩИЕ СРЕДСТВА КОНТРОЛЯ 14](#_Toc506204123)

[3. ПРИКЛАДНЫЕ СРЕДСТВА КОНТРОЛЯ 17](#_Toc506204124)

[3.1. СТАНДАРТЫ ДОКУМЕНТАЦИИ 17](#_Toc506204125)

[3.2. КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ВВОДА ДАННЫХ 18](#_Toc506204126)

[3.3. КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ОБРАБОТКИ ДАННЫХ 21](#_Toc506204127)

[3.4. КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ВЫВОДА ДАННЫХ 23](#_Toc506204128)

[3.5. ТЕСТИРОВАНИЕ ПРИКЛАДНЫХ СРЕДСТВ КОНТРОЛЯ 24](#_Toc506204129)

[3.6. ОТЧЕТНОСТЬ О РЕЗУЛЬТАТАХ АУДИТА 25](#_Toc506204130)

[Приложение I: Таблица планирования 26](#_Toc506204131)

[Приложение II: Матрица тестирования для общих контрольных процедур 30](#_Toc506204132)

[Приложение II: Матрица тестирования прикладных средств контроля 37](#_Toc506204133)

[Рисунок 1: Аудиторские проверки государственного долга, выполняемые ВОА: Бразильский случай 58](#_Toc506204134)

[Рисунок 2. Аудиторские проверки государственного долга, выполняемые ВОА: Молдавский случай 62](#_Toc506204135)

[БИБЛИОГРАФИЯ 63](#_Toc506204136)

ПРЕДИСЛОВИЕ

Государственный долг является ключевым вопросом в любом обсуждении управления государственными финансами. Стремясь расширить масштабы экономики своей страны и улучшить систему социального обеспечения, большинство правительств испытывают значительную потребность в финансовых ресурсах. Теоретически, государственный долг является эффективным инструментом для экономического роста и справедливого распределения налогового бремени между нынешним и будущим поколением налогоплательщиков. Но в силу его значимости для экономического равновесия, важно очень внимательно оценивать государственный долг и управлять им.

Основной задачей управления долгом является получение стабильного финансирования при минимально возможных затратах и оправданных уровнях риска для поддержания деятельности правительства. *Пересмотренные руководящие принципы управления государственным долгом* Всемирного банка и Международного валютного фонда (МВФ) предоставляют набор рациональных методов по внутреннему контролю управления долгом. Среди них есть утверждение, что «деятельность по управлению долгом должна опираться на точную и комплексную информационную систему управления с надлежащими мерами защиты.» Страны, заинтересованные в обеспечении эффективного управления государственным долгом, должны уделять первоочередное внимание разработке надежных систем учета долга и представления отчетности по долгу. Это необходимо не только для получения данных о долге и обеспечения  
своевременности платежей по обслуживанию долга, но и для повышения качества бюджетной отчетности и прозрачности государственной финансовой отчетности, что поможет директивным органам и управляющим государственным долгом в достижении целей управления государственным долгом.

Аудит информационных систем управления государственным долгом направлен на обеспечение эффективности и результативности управления государственным долгом. По этой причине такой аудит следует считать аудитом эффективности. Кроме того, такая работа может также иметь большое значение в отношении аудита финансовой отчетности, задачей которого является определение того, соответствует ли финансовая информация, представленная правительством, нормативной базе, применимой к представлению финансовых отчетов, и является ли информация надежной, без ошибок и искажений. В этом отношении такая работа приобретает большое значение, поскольку она может способствовать реализации информационной системы, которая собирает и представляет точную и достоверную информацию об одном из наиболее важных государственных финансовых элементов: государственном долге.

Данное руководство предоставляет аудиторам наглядные инструкции по проведению аудита информационных систем управления государственным долгом. Поскольку в Международной организации высших органов аудита (ИНТОСАИ) уже есть несколько документов по аудиту информационных технологий (ИТ), разработанных Рабочей группой по аудиту ИТ (WGITA), данное руководство делает акцент на контрольных процедурах на уровне приложений, которые должны быть специфическими для информационной системы управления государственным долгом.

СПИСОК СОКРАЩЕНИЙ

CAAT - компьютеризованные методы аудита

CS-DRMS - Система учета долга и управления долгом Секретариата Содружества

ДМФАС - Система управления долгом и анализа финансового положения

Служба управления государственным долгом

DRP - План аварийного восстановления

FMIS - Система информационного обеспечения финансового менеджмента

Международный валютный фонд (МВФ)

ИНТОСАИ - Международная организация высших органов аудита

IT - информационные технологии

PDMIS - информационная система управления государственным долгом

SID - Единая система долга федерального правительства Бразилии ЮНКТАД - Конференция ООН по торговле и развитию WGITA - Рабочая группа по аудиту ИТWGPD - Рабочая группа по государственному долгу

ВВЕДЕНИЕ

В соответствии с кругом обязанностей, установленным Управляющим советом ИНТОСАИ, Рабочей группе по государственному долгу (WGPD) было поручено опубликовать руководящие принципы и другие информационные материалы для использования Высшими органами аудита (ВОА), чтобы создать условия для надлежащего предоставления отчетности о государственном долге и рационального управления государственным долгом.

Это руководство ориентировано на то, чтобы увеличить потенциал WGPD путем установления общих принципов, которые могут быть использованы в проверках ВОА для оценки общих контрольных процедур и прикладных средств контроля информационных систем управления государственным долгом (PDMIS). Нужно учитывать, что в соответствующих источниках PDMIS подразумевают одну или несколько информационных систем, используемых в области управления государственным долгом.

По мере развития ИТ правительственные организации во все большей степени зависят от их использования при выполнении деловых операций и предоставлении услуг, а также обработке, сохранению и передаче важной информации. В соответствии с рабочим документом МВФ FMIS (Система информационного обеспечения финансового менеджмента) обычно относится к компьютеризации процесса управления государственными расходами, включая составление бюджета, исполнение бюджета и ведение учета при помощи полностью интегрированной системы управления финансами отраслевых министерств и других бюджетных организаций.»

Стандарт 1471 Института инженеров электротехники и электроники определяет системы как «совокупность компонентов, организованных для выполнения определенной функции или набора функций». В частности, основной задачей системы при управлении долгом является ведение базы данных кредитов государственного сектора с использованием программного обеспечения, которое подходит как для отражения в учете, так и для выполнения аналитических функций Министерства по управлению долгом (DMO).

Аудит ИТ можно классифицировать в зависимости от основных подходов, следующим образом:

* управление ИТ,
* аудит данных,
* аудит информационной системы,
* заключение договоров в отношении ИТ, и
* риски информационной безопасности:

Как правило, аудитор ИТ работает с несколькими подходами; однако он может выбрать преобладающий подход. В данном руководстве, преобладающим подходом является *аудит информационной системы.*

Руководство состоит из трех разделов: планирование, оценка общих контрольных процедур и оценка прикладных средств контроля.

1. ПЛАНИРОВАНИЕ

PDMIS можно рассматривать как совокупность взаимозависимых частей (физические структуры, персонал и технические средства), которые взаимодействуют с целью ведения учета, контроля, оценки и управления операциями, возникающими при привлечении заемного капитала, обслуживании и погашении государственного долга.

Этот этап помогает аудитору получить представление о связанных с системой операциях и контрольных процедурах и сопутствующих рисках с учетом рисков движения денежных средств, присущих последовательности операций по обслуживанию государственного долга. Основываясь на этих сведениях, аудитор оценивает общую среду управления, определяет системы, используемые в управлении государственным долгом, изучает всю документацию по этим системам и выполняет предварительную оценку рисков. Результат оценки будет определять масштабы процедур, которые следует выполнить на этапе тестирования.

ВОА также изучает все элементы, относящиеся к ведомству по управлению государственным долгом, как например, персонал, процесс, вид задолженности, безопасность данных, технические средства и др.

На этом этапе аудитор должен выполнить предварительную оценку структуры управления государственным долгом и последовательность операций по обслуживанию государственного долга, включая следующие:

* Как организована PDMIS: какие системы используются для записи, обработки, предоставления отчетности, контроля и управления государственным долгом и какие основные процессы и функции выполняет каждая система.
* Функционирование внутреннего аудита.
* Результаты предыдущих проверок (внутренних или внешних) в отношении PDMIS.
* Физическое хранение документации по операциям.
* Использование аппаратного и программного обеспечения и ответственность за его обслуживание.
* Операции обрабатываемые информационными системами и их относительная значимость.
* Связь между составляющими информации о государственном долге.
* Методы и процедуры выполнения новых операций или изменения существующих.
* Предыдущая оценка внутренних контрольных процедур DMO. Если контрольные процедуры DMO ранее не оценивались, эту оценку должен выполнить ВОА. Эта процедура очень важна для оценки степени существующих рисков и, следовательно, для определения необходимых аудиторских исследований.

Уровень сложности системы не влияет на оценку общих контрольных процедур, которые должны выполняться в любом случае. Однако он определяет процедуры аудита, которые следует выполнить, и показывает, сколько специалистов необходимо для выполнения аудиторской проверки. Рекомендуется, чтобы в группе экспертов был хотя бы один ИТ-специалист для выполнения работ, связанных с системами. Для аудиторов в группе, которые впервые выполняют аудит ИТ важно получить знания об общепринятых терминах. В этом случае хороший технический словарь по ИТ является важным капиталовложением для ВОА. Для этой цели подходит созданный WGITA Глоссарий терминов по Проведению аудита информационных систем. Также могут быть полезными некоторые веб-глоссарии; см. <http://www.webopedia.com> или <http://whatis.techtarget.com>.

Аудиторы, которым уже знакома терминология ИТ, также должны знать терминологию, используемую в DMO, особенно сокращения и аббревиатуры (виды заголовков, разделов DMO, кредиторов, названия систем, программного обеспечения, используемого в DMO, и др.). Важно приобрести эти знания до проведения опросов. Полезный глоссарий, разработанный Конференцией ООН по торговле и развитию (ЮНКТАД), можно найти по следующим ссылкам:

* <http://unctad.org/en/Docs/pogiddmfasm3r3.en.pdf> - Глоссарий по долгу и ДМФАС (английская версия)
* <http://www.unctad.org/sp/docs/Zpogiddmfasm3r3.sp.pdf> - Глоссарий по долгу и ДМФАС (испанская версия)

Полностью разбираться в PDMIS означает знать характерные для нее потоки данных и информации. Таким образом, очень важно на этапе планирования обозначить ключевые процессы управления государственным долгом (запись, обработка, контроль, обеспечение безопасности, предоставление отчетности и анализ) и понять, как эти процессы выполняются при помощи информационной системы. После этого необходимо выполнить оценку рисков с целью выявления более высоких рисков, связанных с ключевыми операционными и управленческими процессами управления государственным долгом, учитывая их воздействие и вероятность возникновения. Оценка риска помогает определить объем процедур, необходимых для управления уровнями сопутствующих рисков. ISSAI 5410, Руководство по планированию и проведению аудита внутреннего контроля государственного долга, содержит инструкции по проведению оценки риска. Кроме того, оценка риска может быть выполнена в рамках аудиторских проверок финансовой отчетности.

Потоки данных PDMIS почти всегда локализуются в DMO. Другие ведомства могут также отвечать за ввод данных о долге, например, в случае договорного долга. Если DMO подразделяется на бэк-офис, мидл-офис и фронт-офис, то каждый из них имеет свои собственные потоки данных и информации. Фронт-офис, как правило, отвечает за выполнение операций на финансовых рынках, включая организацию тендеров и другие формы заимствования средств, а также других финансовых операций. Бэк-офис занимается расчетами по сделкам и ведением финансовой отчетности. Отдельный мидл-офис или отдел по управлению риском, обычно проводит анализ рисков, выполняет мониторинг и предоставляет отчеты о рисках, связанных с портфелем, а также оценивает эффективность специалистов по управлению долгом на основании стратегических целей/контрольных показателей. Большинство потоков данных, связанных с государственным долгом, включая внешние данные, находятся в бэк-офисе, который отвечает за ввод данных и осуществление контроля.

Поскольку многие страны используют готовые системы, разрабатываемые и обновляемые сторонними международными организациями (например, Систему управления долгом и анализа финансового положения (ДМФАС) или Систему учета долга и управления долгом Секретариата Содружества (CS-DRMS)) в области управления государственным долгом, большое значение имеет использование отчетов по эффективности, например, запросов на обслуживание системы и записей происшествий.

Программа ДМФАС, разработанная ЮНКТАД, основное внимание уделяет деятельности «на последних этапах». Сюда относится ведение баз данных по обслуживанию долга, проверка правильности информации по долгу, долговые операции, предоставление внешних и внутренних отчетов по долгу, ведение статистики и базовый анализ задолженности, а также создание системных связей между управлением долгом и другим финансовым программным обеспечением. Они дополняют мероприятия «на более ранних этапах», такие как анализ приемлемости величины долга, осуществляемый другими исполнителями, такими, как Всемирный банк. Кроме того, программа все чаще помогает странам в установлении связей между ДМФАС по управлению долгом и другими правительственными программами (например, которые используются для составления бюджета, управления денежными средствами и управления пособиями) или в пределах комплексных, интегрированных систем управления финансами в рамках общих усилий стран по управлению государственными финансами. Дополнительная информация доступна по адресу <http://unctad.org/dmfas>.

Приложение CS-DRMS, предоставленное Секретариатом Содружества, оказывает ВОА помощь в записи, управлении и анализе долга в целом. Оно предоставляет центральное хранилище данных для нескольких категорий внешнего и внутреннего долга, обеспеченного государственным и частным сектором, включая краткосрочную задолженность. Система также работает с субсидиями, кредитованием правительства и перекредитованием. Дополнительная информация доступна по адресу <http://www.csdrms.org>.

Что касается стран, использующих ДМФАС или CS-DRMS в управлении государственным долгом, отчеты о результатах аудита PDMIS, проводимого другими странами (другими ВОА) могут быть полезны для выявления недостатков, которые являются наиболее частыми и/или оказывают наибольшее влияние.

Таблица, содержащая необходимую информацию, процедуры и вопросы, на которые должен ответить ВОА, используемые группой аудиторов на этапе планирования аудиторской проверки систем управления государственным долгом, содержится в приложении I.

1. ОБЩИЕ СРЕДСТВА КОНТРОЛЯ

Общие контрольные процедуры устанавливают принципы всеохватывающего контроля над функциями ИТ.[[1]](#footnote-1) Эти контрольные процедуры предназначены для решения проблем развития, функционирования и поддержания среды. Целями общих контрольных процедур являются защита данных, защита прикладных программ и обеспечение непрерывного выполнения компьютерных операций в случае неожиданных сбоев.

Хотя аудит системы управления государственным долгом требует проверки общих контрольных процедур в отношении ИТ, этот документ не рассматривает эти контрольные процедуры подробно, поскольку ИНТОСАИ издала документы по аудиту ИТ, которые детально рассматривают контрольные процедуры в отношении ИТ.

Группе аудиторов рекомендуется при выполнении аудита системы использовать ISSAI 5310, Методику проверки безопасности информационных систем (ISec), руководство по проверке безопасности информационной системы в государственных организациях.

Еще одним документом, который может оказаться полезным при планировании общих контрольных процедур, является разработанное WGITA Руководство IDI по аудиту ИТ для высших органов аудита, которое содержит необходимую информацию и ключевые вопросы, необходимые для эффективного планирования аудиторских проверок ИТ.

Приложение II содержит матрицы тестирования с несколькими общими контрольными процедурами и рекомендуемыми процедурами тестирования, которые могут помочь аудиторам при выполнении общих контрольных процедур.

Полный комплекс различных категорий общих контрольных процедур содержит элементы, описанные ниже.

*Организационные контрольные процедуры*

К организационным контрольным процедурам относятся методики, процедуры и организационная структура, установленные для обеспечения рациональной кадровой политики и методик управления, разделения обязанностей и политики информационной безопасности, а также для предоставления методов оценки эффективности и обеспечения оперативных контрольных процедур и эффективности.

*Контрольные процедуры физического доступа*

Контрольные процедуры физического доступа включают правила и практики по предотвращению несанкционированного доступа и вмешательства в предоставление ИТ-услуг, включая административные процедуры, в частности требование от персонала носить бейджи и контроль посетителей, а также физические меры, такие, как механические и электронные замки, камеры и другие средства для ограничения физического доступа к серверам и другим критически важным объектам инфраструктуры.

*Контрольные процедуры логического доступа*

Контрольные процедуры логического доступа используют встроенные средства обеспечения безопасности компьютерной системы для предотвращения несанкционированного доступа к важным файлам и данным, и обеспечивают, чтобы все пользователи имели права доступа, ограниченные требованиями их должностных инструкций. Эти контрольные процедуры включают брандмауэры, антивирусное программное обеспечение, а также обнаружения вредоносного программного обеспечения и сетевых атак.

В современных системах эти контрольные процедуры достигаются многочисленными и разнообразными способами. Они реализуются посредством прикладного программного обеспечения, операционной системы, системы управления базами данных, программного обеспечения контроля доступа, программ, контролирующих обработку деловых операций в режиме "онлайн", серверов, сетей, локальных сетей и, возможно, другого программного обеспечения.[[2]](#footnote-2)

*Контрольные процедуры в отношении окружающей среды*

Контрольными процедурами в отношении окружающей среды являются правила, практики и предусмотренные условия по предотвращению повреждений, вызванных электрическими сбоями, пожаром, пылью, водой, пищей, экстремальными температурами, влажностью или статическим электричеством.

Хотя основное внимание этих контрольных процедур сосредоточено на центре хранения и обработки данных (или области, посвященной ИТ-оборудованию, которое требует определенных условий окружающей среды или, по крайней мере, защиты от кражи), они также применяются для условий окружающей среды во всей организации.

*Контрольные процедуры в отношении изменения программ*

Контрольные процедуры в отношении изменения программ включают правила, призванные обеспечить, чтобы все изменения конфигурации системы выполнялись правильно, полностью и своевременно.

Обновления и изменения должны иметь формальный процесс для обеспечения регистрации всех изменений и предоставления возможности отменить выполненные изменения, если возникнут проблемы с новой версией.

Прежде, чем перевести программы из тестовой среды в основную, должно быть получено официальное одобрение, и вся системная, операционная и программная документация должна храниться в полной; современный; и в соответствии со стандартами, политики и процедур.

Планирование непрерывности бизнеса и План аварийного восстановления

Планирование непрерывности бизнеса (BCP) и соответствующий план аварийного восстановления (DRP) предназначены для решения задач эксплуатационной пригодности. Планирование на случай чрезвычайных ситуаций и планирование аварийного восстановления, жизнеспособность плана, тестирование, мониторинг, и необходимость постоянного обновления планов являются критическими факторами.[[3]](#footnote-3)

Планирование непрерывности бизнеса является комплексным подходом к обеспечению альтернативных путей поддержки критических бизнес-процессов в случае чрезвычайных ситуаций, стихийных бедствий или других сбоев. Основное внимание уделяется выживанию всего бизнеса а не только ИТ. Однако комплексный план должен включать рассмотрение информационных систем и требования к сети телекоммуникаций. Эта часть BCP также является DRP.

BCP и соответствующий DRP могут разрабатываться одновременно, так что параллельно рассматриваются все аспекты. Как минимум, план должен включать процедуры и критерии для определения, когда ситуация становится критической, лицо, ответственное за такое определение, и процедуру официального объявления чрезвычайной ситуации и приведения плана в действие.

1. ПРИКЛАДНЫЕ СРЕДСТВА КОНТРОЛЯ

Прикладные средства контроля автоматизированы в приложениях информационной системы для содействия обеспечению авторизации, целостности, точности и действительности операций. Они заложены в процесс создания программы приложения и характерны для операций ввода, обработки и вывода данных приложения. Их цель заключается в том, чтобы обеспечить полноту, достоверность и точность обработки данных.

Прикладные средства контроля включают проверки формата введенных данных, чтобы предотвратить ввод недопустимых данных, контрольные процедуры обработки, которые не дают пользователям проводить запрещенные операции, и предоставление подробных отчетов и контроль всех операций для обеспечения их полной и точной регистрации.

Прикладные средства контроля можно разделить на следующие виды:

* Исходные данные
* обработка, и
* *Непосредственный результат*
  1. СТАНДАРТЫ ДОКУМЕНТАЦИИ

Стандарты документации обеспечивают ведение соответствующей и отвечающей современным требованиям документации по приложению. Также важное значение имеет регулярное обновление документации.[[4]](#footnote-4)

Надлежащая документация имеет важное значение для определения, какие существуют или должны быть контрольные процедуры.

Хорошая документация по приложению также снижает риск того, что пользователи не будут выполнять контрольные процедуры, предусмотренные руководством. Изучение всеобъемлющей, актуальной документации помогает аудитору понять, как работает каждое приложение, и может способствовать выявлению определенных аудиторских рисков.

* Документация по приложению: Помогает сопровождающим приложение программистам понять работу приложения, устранить проблемы и выполнить улучшения. Документация оформляется на каждом этапе процесса разработки и может быть создана в различных форматах, таких как блок-схемы, диаграммы, таблицы или текст. Документация может включать сведения об источнике данных, атрибутах данных, экранах для ввода данных, проверках данных, процедурах обеспечения безопасности, описание расчетов, разработки программ, интерфейсов для других приложений, процедур контроля, обработки ошибок, руководства по эксплуатации, архивированию, резервному копированию и процедурам хранения и восстановления. Документация по приложению должна обновляться по мере изменения приложения.
* Документация включает описания как автоматизированных, так и неавтоматизированных потоков операций,   
  для оказания помощи в начальном обучении работе в приложении и для обращения к ним при последующем использовании. В обоих случаях документация пользователя должна обновляться по мере изменения приложения.

Документация должна содержать

* обзор прикладных средств,
* спецификацию требований пользователя,
* описания и распечатки программы,
* описания ввода/вывода данных,
* описание содержимого файла,
* руководства пользователя,
* инструкции службы поддержки,
* описания управления безопасностью приложения,
* краткие результаты последней оценки безопасности,
* последнее заключение по безопасности и рекомендуемые действия, и
* состояние выполнения рекомендуемых действий.
  1. КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ВВОДА ДАННЫХ

Контрольные процедуры ввода данных имеют огромное значение для снижения риска ошибок или мошенничества в компьютерных приложениях. Контрольные процедуры в отношении входной информации имеют ключевое значение для целостности данных.

Контрольные процедуры ввода данных помогают обеспечить авторизацию, точность, полноту и своевременность данных, введенных в приложение. Авторизация обеспечивается за счет требования дополнительного согласования операций, превышающих определенное пороговое значение. Точность обеспечивается путем проверок редакционных изменений, которые проверяют введенные данные до принятия операции в обработку. Полнота достигается за счет процедур обработки ошибок, которые обеспечивают ведение журнала, предоставление отчетов и исправление ошибок. Своевременность обеспечивается за счет контроля потока операций, ведения журнала и предоставления отчетности по отклонениям.

Контрольные процедуры ввода данных могут быть в

* экранах ввода данных,
* процедурах подготовки данных,
* авторизации ввода данных,
* сохранении исходных документов,
* проверке ввода данных,
* процедурах на случай ошибки при введении данных, и
* вспомогательных механизмах введения данных.

Указанные выше контрольные процедуры можно обойти, если есть возможность вводить или изменять данные вне приложения. Необходима автоматическая проверка целостности приложения, которая будет выявлять и сообщать о любых внешних изменениях данных. Например, должна быть разработана проверка для обнаружения и сообщения о несанкционированных изменениях, внесенных в основную базу данных об операциях.

*Экраны ввода данных*

Стандартизированные экраны ввода данных могут обеспечить последовательный ввод данных. PDMIS может включать следующие функциональные возможности:

* экраны ввода данных, оформленные в стандартном виде и по стандартной схеме;
* поля ввода данных, которые устанавливают ограничения в отношении того, какие пользователи имеют доступ к вводу данных;
* обязательный ввод данных для определенных полей; и
* функция помощи (например, F1), чтобы помочь пользователям заполнять поля ввода данных.

*Процедуры подготовки данных*

Цель процедур подготовки данных заключается в том, чтобы избежать сбоев во время процедур ввода данных.

PDMIS может включать встроенную среду для процедур совместного использования данных, чтобы передавать данные другим приложениям.

*Авторизации ввода данных*

Целью авторизации ввода данных является обеспечение того, чтобы все вводимые данные были зарегистрированы и санкционированы соответствующим лицом.

PDMIS может включать следующие функциональные возможности:

* требование ввода пароля доступа;
* внесение записей в журнал доступа при ручном вводе данных; и
* требование двойного согласования для некоторых особо важных операций (например, активация контрактов, изменение процентных ставок и изменение стоимости контракта).

*Сохранение исходных документов*

Это направление контрольных процедур ввода данных относится к сохранению и контролю исходных документов, помогающих вести записи данных о долге. В случае автоматического обмена файлами между приложениями PDMIS необходимо сохранить исходные данные, полученные от других приложений, в течение времени, установленного DMO.

*Проверка ввода данных*

Контрольные процедуры проверки данных предназначены для обеспечения того, чтобы входные данные были достоверными и точными.

PDMIS может включать следующие функциональные возможности:

* Автоматические контрольные списки проверяют отсутствие значений (например, при загрузке статистических рядов показателей, PDMIS проверяет, нет ли пропусков ежедневных, ежемесячных или ежегодных значений).
* Все экраны ввода данных четко определяют обязательные к заполнению поля, а приложение допускает подтверждение операции, только если введена вся обязательная информация.
* Каждая таблица базы данных должна содержать определенное правило в отношении полей, где не допускается дублирование данных.
* Если приложение определит, что вводятся повторяющиеся данные, оно не будет принимать запись до тех пор, пока вопрос дублирования не будет решен.
* Приложение не позволяет изменять некоторые данные после вводы (например, обменный курс на день операции). Что касается других данных, приложение может разрешить изменения, если будут выполнены некоторые условия (например, если у контракта статус «Заблокирован» или «Заключен», данные изменить невозможно).
* Некоторые поля после заполнения требуют внести данные в другие поля (например, если пользователь вводит комиссионные за обязательства по контракту, он должен также ввести налоги, связанные с такими обязательствами).
* Поля «Дата» имеют важное значение для общего контроля долгового контракта. Они особенно полезны при расчетах траншей, чтобы избежать задержек платежей, взимания штрафов и так далее. Таким образом, указание даты должно быть среди основополагающих правил приложения.
* Если не считать моделируемых операций, системное приложение не позволяет регистрацию данных будущей датой, например, выдача транша, возврат транша, аннулирование контракта или добавление контракта.

*Ошибки ввода данных*

Аудиторский след или журнал аудита являются хронологическими записями, относящимися к обеспечению безопасности, совокупностью записей, или местом назначения и источником записей, которые содержат документальные подтверждения последовательности действий, повлиявших на определенные операции, процедуры или события. Доступ к аудиторскому следу или журналам регистрации должен быть предоставлен только соответствующим сотрудникам.

PDMIS может включать следующие функциональные возможности:

* DMO должен определить ответственность за регистрационные файлы;
* программы для ведения журнала ошибок, предоставления отчетов об ошибках открытия и записи исправлений ошибок должны быть встроены в приложение;
* в процессе автоматической загрузки данных когда приложение определяет пробелы в серии, автоматически отправляется электронное письмо соответствующим пользователям для выполнения последующих мероприятий; и
* приложение должно периодически отправлять соответствующим сотрудникам отчеты о неисправленных ошибках — в том числе о том, как долго ошибки оставались неисправленными и их приоритете.

*Вспомогательные механизмы введения данных*

Эти контрольные процедуры относятся к вспомогательным процедурам в DMO, которые помогают пользователям вводить данные в компьютерное приложение, выполнять повторную инициализацию приложений и отслеживать действия пользователей во избежание возможных отклонений от установленных правил.

Эти механизмы часто включаются в общие контрольные процедуры.

* 1. КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ОБРАБОТКИ ДАННЫХ

Контрольные процедуры обработки данных обеспечивают точность, полноту и своевременность представления данных во время обработки данных в пакетном режиме или режиме онлайн. Эти контрольные процедуры способствуют обеспечению того, чтобы данные правильно обрабатывались в приложении, и чтобы в процессе обработки данные не были добавлены, потеряны или изменены.[[5]](#footnote-5)

Полнота может быть обеспечена во время обработки данных в пакетном режиме путем сопоставления операций, полученных системой, с операциями, отправленными вспомогательной системой.

Сопоставление должно осуществляться между приложениями, совместно использующими общие данные, путем создания акта сверки, содержащего данные как из приложений, так и из отчетов о любых различиях для группы пользователей.[[6]](#footnote-6)

Сопоставление итогов должно включать счетчик операций и итоговые значения для всех полей, содержащих суммы, по каждому типу операций и перекрестные итоги для полей данных и полей итогов.[[7]](#footnote-7)

В файлах где нет значимых итогов, можно создавать хэш-итоги, которые складывают все цифры в столбце, чтобы убедиться, что такой же итог принят следующим процессом. Например, суммирование номеров долговых соглашений не имеет смысла, но эта сумма может использоваться для проверки, что все правильные номера долговых соглашений включены в обработку.[[8]](#footnote-8)

PDMIS может включать следующие функциональные возможности:

* При взаимодействии с другими системами между приложениями, если есть ошибка в обработке файлов, создается файл ошибки и записывается в системное приложение. Пользователям следует разработать более всесторонний подход к обеспечению взаимодействия для технических конфигураций и проведению обучения во всей организации.
* Приложение содержит запланированные пакетные задания для многих задач, например, обновления запасов, финансового планирования, индексов и будущих платежей. Пользователи должны оценить выходные данные систем мягкого реального времени, основное внимание уделяя журналам пакетной обработки данных, а также возможности жесткого реального времени для оценки обработки обновляемой информации.
* В случае ошибки при обработке пакетных заданий приложение отправляет пользователю сообщение с информацией об ошибке. Пользователь может проверить возможности консолидации в рамках системы для соблюдения политики исправления ошибок и настройки процедур контроля.
* После завершения операции приложение отображает сообщение, подтверждающее, что обработка была успешной и представляющее краткое содержание введенных данных.
* После изменения ранее зарегистрированных данных приложение отображает сообщение, что изменение выполнено успешно и представляет краткое содержание измененных данных.
* После удаления ранее введенных данных приложение отображает сообщение, что удаление выполнено успешно и представляет краткое содержание удаленных данных.
* Если удаление записи влияет на реляционную целостность базы данных, приложение не позволяет выполнить удаление и отображает сообщение, указывающее, что запись не может быть удалена. Например данные кредитора банка нельзя удалить из таблицы кредиторов, если он имеет действующие контракты в приложении.
* Приложение выполняет некоторые сверки данных фронт и бэк-офиса. Например, оно делает бэк-офису запрос на проверку входных данных с аукционов. Пользователи могут проверить состояние средств связи для архитектуры данных взаимосвязей между компонентами и системами с целью проверки потока данных в соответствии со схемой взаимодействия.
  1. КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ВЫВОДА ДАННЫХ

Контрольные процедуры вывода данных обеспечивают целостность вывода данных и правильное и своевременное распределение полученной выходной информации.[[9]](#footnote-9) Недостатки в обработке может иногда компенсировать строгий контроль над выводом данных. Хорошо контролируемое приложение в отношении ввода и обработки данных может быть полностью дестабилизировано, если не контролируется вывод данных.[[10]](#footnote-10)

Полнота и целостность выходных отчетов зависит от ограничения возможности внесения изменений в выходные данных и включения проверок полноты, таких как номера страниц и контрольные суммы[[11]](#footnote-11)

Выходные файлы должны быть защищены с целью снижения риска несанкционированного изменения. Возможные мотивы для изменения вывода данных компьютером включают, скрытие несанкционированной обработки или подделывания нежелательных финансовых результатов.[[12]](#footnote-12)

Выходные данные из приложения ИТ могут формировать входные данные для другого приложения. Если это так, аудитор должен искать контрольные процедуры, обеспечивающие точную передачу выходных данных от одной стадии обработки к другой.[[13]](#footnote-13)

В PDMIS контрольные процедуры вывода данных также могут быть введены в программу для определения критической информации, требующей приоритетных действий со стороны лиц, ответственных за управление государственным долгом. Например для контрактов, срок действия которых истекает в текущем месяце, приложение может показывать ежедневные оповещения на первом экране системы о контрактах, чьи сроки платежа истекают в ближайшие 5 дней.

Приложение может также позволить определенным пользовательским конфигурациям создавать отчеты в режиме приоритета, что позволит приложению устанавливать приоритеты для формируемых отчетов.

PDMIS может включать следующие функциональные возможности:

* приложение обеспечивает автоматическое сопоставление суммы изначальных данных с суммой обработанных данных;
* приложение должно информировать пользователей о состоянии запросов на генерацию отчетов, например, «не начат», «выполняется» и «сформирован;» и
* в конце процесса генерации отчетов, приложение отправляет сообщение сделавшему запрос пользователю, информирующее его, что задача выполнена.
  1. ТЕСТИРОВАНИЕ ПРИКЛАДНЫХ СРЕДСТВ КОНТРОЛЯ

После определения контрольных процедур, следующим шагом аудиторской проверки является проверка их эффективности.

Это может быть достигнуто путем

* представления комплекса тестовых данных, которые, если приложение работает должным образом, выдадут известные результаты;
* разработки независимых программ для воспроизведения алгоритма приложения; и
* оценки результатов приложения.

Указанные выше процедуры проверяют целостность программы, встроенной в PDMIS, а не целостность данных.

Если приложение содержит тестовую среду, то она может использоваться для тестирования контрольных процедур до тех пор, пока она является подтвержденной копией рабочей среды.

Для того чтобы проверить правила расчета, такие как те, что относятся к обновлению запасов или обслуживанию долга, аудитору может понадобиться использовать компьютеризованные методы аудита (CAAT), которые включают различные инструменты и методы, такие как универсальные аудиторские программы, служебные программы, тестовые данные, трассировка и составление схем программ и специализированные аудиторские программы. Они могут содержать инструменты, анализирующие алгоритмы электронных таблиц и точность расчетов. Инструменты могут также использоваться для анализа приложений баз данных и создания логических блок-схем. Универсальные аудиторские программы могут использоваться для анализа данных, получаемых из большинства приложений.

Аудитор должен оценить необходимость использования CAAT. При их использовании следует учитывать сложность приложения по управлению государственным долгом.

Данный документ содержит предложенную матрицу тестирования (см. приложение III), которая может использоваться группой аудиторов в качестве ориентира для выполнения тестирования контрольных процедур приложения. Эта матрица определяет некоторые требования и функциональные возможности, которые должны обеспечить системы управления государственным долгом, запросы, которые они должны быть в состоянии выполнять и минимальные технические требования для таких систем.

Следует отметить, что, поскольку долг каждой страны имеет разную структуру и характеристики, системы управления долгом также представляют различные функции. Таким образом в обязанности группы аудиторов входит определить, при необходимости скорректировать и использовать элементы, применимые к системе управления долгом своего государства.

* 1. ОТЧЕТНОСТЬ О РЕЗУЛЬТАТАХ АУДИТА

Помимо выполнения Лимской декларации руководящих принципов финансового контроля, в соответствующих случаях, предоставление аудиторской отчетности в PDMIS должно выполняться в соответствии с требованиями

ISSAI 5440, «Руководство по проведению аудита государственного долга - применение теста на существенность в финансовых проверках», раздел 2.6 Предоставление отчетности по результатам аудита

Как отмечалось ранее, аудит PDMIS является аудитом эффективности, поэтому важно, чтобы отчет соответствовал стандартам представления отчетности по аудиту эффективности, как указано в ISSAI 3000, Стандарты и руководства по аудиту эффективности, основанные на стандартах аудита ИНТОСАИ и практическом опыте (часть 5), а также ISSAI 300, Основополагающие принципы аудита эффективности (стр. 16).

Приложение I: Таблица планирования

|  |
| --- |
| ***Необходимая информация, документы и отчеты*** |
| * Перечень информационных систем, используемых DMO, и соответствующая системная документации |
| * Опись операционных систем компьютеров и сетей, используемых DMO. |
| * Обновленные схемы последовательностей выполнения процессов DMO |
| * Предыдущие отчеты по аудиторским проверкам DMO |
| * Предыдущие аудиторские отчеты, относящиеся к ИТ-системам управления государственным долгом |
| * Законы и нормативные акты, относящиеся к концепции DMO и управлению государственным долгом |
| * Перечень менеджеров DMO и управления ИТ, управления непрерывностью бизнеса, управления людскими ресурсами, управления рисками, внутреннего аудита и других, с указанием их должностных функций, адресов, адресов электронной почты и телефонных номеров |
| * Документы, предназначенные для отображения функций DMO и/или его систем, такие как следующие служебные инструкции и методические руководства DMO или министерства финансов: |
| * + Управление персоналом   + Риски информационной безопасности:   + Управление изменениями   + Физический доступ   + Требования к окружающей среде/местоположению ИТ   + Логический доступ   + Планирование непрерывности бизнеса (BCP)   + План восстановления в аварийных ситуациях (DRP)   + План резервного копирования   + Услуги третьих лиц (ИТ-услуги)   + Предварительные отчеты об оценке рисков   + Краткие результаты последней оценки безопасности   + Последнее заключение по безопасности и рекомендуемые действия   + Состояние выполнения рекомендуемых действий   + Согласие высшего руководства на использование системы |
| * Отчеты, распространяемые сторонними организациями, ответственными за обеспечение обслуживания системы |
| * Другие документы, имеющие отношение к DMO и/или его системе (например, слайды, тексты, плановые задания и ежегодные отчеты по управлению долгом) |
| * Количество сотрудников DMO, являющихся пользователями системы, и их профили доступа |
| * Количество сотрудников сферы ИТ и квалификационные требования (список служебных обязанностей) для DMO и/или ИТ-персонала |
| * Список сотрудников, имеющих доступ к серверной комнате |
| * Описание профиля доступа PDMIS |
| * Формальная спецификация порядка и регулярности обновления операционной системы, брандмауэров и антивирусных программ | |
| * Функции физических препятствий и автоматических средств, используемых для предотвращения несанкционированного доступа к центральному компьютеру, рабочим станциям, серверам и другим объектам DMO | |
| * Расположение каждого помещения внутри и снаружи DMO | |
| * Список персонала, рабочих станций и серверов | |
| * Бюджетные ассигнования за последние 5 лет | |
| * Список предварительной подготовки по использованию PDMIS (для персонала DMO) и обновлению ИТ (для ИТ-персонала) | |
| * Установленные правила, практики и заложенные указания по предотвращению повреждений, вызванных электрическими сбоями, пожаром, пылью, водой, пищей, экстремальными температурами, влажностью или статическим электричеством. | |
| * Технические условия для функционирования источника бесперебойного питания (при его наличии) | |
| * Журналы учета ошибок PDMIS по запросу DMO или отчеты об использовании инструкций | |
| * Отчеты о регистрации фактов нарушения безопасности | |
| * Список изменений в PDMIS за последние 12 месяцев | |
| * Журналы и отчеты о результатах предварительных тестов BCP и DRP и эффективные мероприятия | |
| * Документация по приложению и пользовательская документация | |
| * Условия использования каждого приложения | |
| * Руководство по процедурам устранения ошибок обработки | |
| * Выборка данных для повторного выполнения операций по тестированию контрольных процедур на уровне приложений и расчетов | |
| ***Процедуры*** | |
| * Изучение системной документации руководств и условий использования) для понимания того, как осуществляются основные процессы по управлению долгом в информационных системах; при отсутствии достаточной документации о процессах DMO, группа аудиторов должна исследовать и зафиксировать эти процессы | |
| * Проверка наличия правовых норм, касающихся использования, обслуживания и делового администрирования PDMIS | |
| * Формулирование по результатам предыдущих проверок выводов, касающихся слабых сторон последовательности операций по обслуживанию государственного долга и/или систем управления государственным долгом | |
| * Определение основных общих контрольных процедур на основе системной документации | |
| * Определение основных контрольных процедур на уровне приложений на основе системной документации: контрольных процедур ввода, обработки и вывода данных | |
| * Проведение оценки риска, исходя из этих основных общих контрольных процедур и контрольных процедур на уровне приложений, чтобы определить, какие риски влияют на эти системы и степень их воздействия на управление государственным долгом | |
| * Определение, какие из этих систем затрагивают важнейшие функции и данные, такие как ввод, обработка и вывод данных, список кредиторов, расчет государственного долга, предоставление отчетности и принятие решений | |
| * Определение внутренних контрольных процедур, выполняемых для минимизации или снижению обнаруженных рисков | |
| * Ранжирование систем и процессов, основанных на оценке рисков и определение охвата аудита | |
| * Оценка ресурсов и оперативных планов | |
| * Проведение собеседований с руководителем ИТ- подразделения, менеджерами и техническим персоналом, отвечающим за работы по развитию/обслуживанию/эксплуатации системы | |
| * Разработка матрицы для аудита общих контрольных процедур и контрольных процедур на уровне приложений и определение, какие тесты следует выполнить (см. предложенную матрицу в приложении III) | |
| ***ВОА должен ответить на следующие вопросы*** | |
| * Каковы информационные системы управления государственным долгом и какова роль каждой системы в управления государственным долгом? | |
| * Была ли PDMIS разработана исключительно DMO или ее приобрели у третьей стороны? В последнем случае выполнялась ли индивидуальная настройка под особые потребности DMO? | |
| * Кого следует опросить по вопросам общих контрольных процедур ИТ в DMO? | |
| * Кого следует опросить для уточнения контрольных процедур на уровне приложений PDMIS? | |
| * Кто являются основными пользователями PDMIS? | |
| * Каковы общие контрольные процедуры PDMIS и контрольные процедуры на уровне приложений? | |
| * Способны ли внутренние контрольные процедуры снизить риски информационных систем, которые могут повлиять на управление государственным долгом? | |
| * Каковы наиболее высокие риски, связанные с вводом, обработкой и выводом данных PDMIS? | |
| * Какие следует выполнить тесты в отношении общих контрольных процедур и контрольных процедур на уровне приложений? | |

Приложение II: Матрица тестирования для общих контрольных процедур

|  |  |  |  |
| --- | --- | --- | --- |
| Общие средства контроля | | | |
| Целями общих контрольных процедур являются защита данных, защита прикладных программ и обеспечение непрерывного выполнения компьютерных операций в случае неожиданных сбоев. | | | |
| **ТРЕБОВАНИЯ / ФУНКЦИОНАЛЬНОСТЬ** | **ОБЩИЙ КОНТРОЛЬ** | **ПРЕДЛОЖЕННЫЕ ПРОЦЕДУРЫ ТЕСТИРОВАНИЯ** | |
| Общие вопросы | Действия ИТ-сектора должны соответствовать миссии DMO  Необходимо выполнять мониторинг эффективности PDMIS с учетом целей DMO  Периодически следует проводить внутренний аудит операций DMO/PDMIS | Изучение примеров решений руководства или служебных записок, относящихся к действиям в сфере ИТ, чтобы убедиться, что они ясные, хорошо обоснованные и соответствующие миссии DMO  Оценка критериев эффективности для PDMIS на основании ожидаемых показателей и обеспечение того, чтобы высшее руководство согласилось с таким критериями  Оценка отчетов по предыдущим внутренним аудиторским проверкам общих контрольных мероприятий в сфере ИТ для выявления серьезных недостатков  Оценка относительного количества и функционала ИТ-рабочих станций и других ИТ-устройств и обеспечение того, чтобы персонал обладал необходимыми навыками  Оценка относительного объема бюджетных ассигнований и сравнение его с аналогичными показателями предыдущих периодов, а также с секторами ИТ других государственных учреждений | |
| **Организационные контрольные процедуры** | Руководство DMO или министерства финансов должно быть заинтересовано в развитии и поддержании надлежащей общей ИТ-среды  DMO и персонал в сфере ИТ должны периодически проходить соответствующее обучение, включающее знание требований мер безопасности  Должна быть разработана программа обучения | Опрос руководства DMO в отношении их заинтересованности в ИТ для того, чтобы оценить их стремление к развитию и поддержанию надлежащей общей ИТ-среды  Изучение доказательств проведения обучения  Опрос пользователей DMO и | |
|  | Должны быть письменные инструкции и стандартные процедуры в отношении:   * + Риски информационной безопасности:   + людские ресурсы;   + ИТ-услуг, предоставляемых третьими лицами   + Управление изменениями   + Физического и логического доступа   + Планирования непрерывности бизнеса и аварийного восстановления | ИТ-персонала по следующим вопросам:   * + периодичность обучения   + потребность в знаниях/обучении   + знание политики   Оценка пригодности письменных инструкций и стандартных процедур для ИТ-услуг | |
|  | Следует периодически обновлять политику и стандартные процедуры  Высшее руководство DMO должно надлежащим образом обеспечить ознакомление с этой политикой | стандартные процедуры (определены в руководстве) | |
|  | Сотрудники DMO должны знать эти инструкции |  | |
|  | Необходимы задокументированные процедуры для всех видов деятельности по управлению долгом |  | |
|  | Организация должна осуществлять надлежащее разделение обязанностей для обеспечения того, чтобы пользователи не имели больше полномочий чем требуется для выполнения их работы |  | |
| **Физические контрольные процедуры** | Физический доступ к центральному компьютеру и серверам должен быть ограничен (например, за счет использования замков, дверей и т.д.)  Необходимо вести видеонаблюдение | Проверка эффективного существования и функционирования физических препятствий, которые предотвращают несанкционированный доступ к центральному компьютеру, серверам и рабочим станциям DMO | |
|  | Окна помещения, где расположены центральный компьютер и серверы должны быть защищены от принудительного доступа  Каждый, кто осуществляет доступ к серверной комнате, должен иметь на это полномочия | Проверка, действуют ли административные меры для персонала, предотвращающие несанкционированный доступ и посягательство на ИТ-услуги, как это официально установлено  Для того, чтобы выявить любые недостатки в автоматических контрольных мероприятиях, выполняется наблюдение за тем, как работают электронные замки, электронные системы блокировки, камеры и другие средства, ограничивающие физический доступ к серверам - а также другим критическим объектам инфраструктуры | |
|  |  | В случае механической системы блокировки, проверяется совместное использование паролей среди сотрудников | |
| **Логические контрольные процедуры** | Если ИТ-услуги в сфере управления государственным долгом предоставляются сторонними организациями, в договоре должны быть определены надлежащие контрольные процедуры для обеспечения отсутствия у сторонней организации доступа к коммерческим тайнам, важным данным и стратегиям управления государственным долгом  Не должно быть бывших сотрудников, лиц, не работающих в DMO, или «виртуальных» пользователей с активным профилем доступа  Права доступа должны периодически пересматриваться  Должны работать обновленные антивирусные программы, брандмауэры и программное обеспечение для обнаружения атак и вредоносных программ  Необходимо систематическое обновление операционной системы на рабочей станции (станциях) и сервере (серверах)  Организация должна определить свои процедуры авторизации, отмены или изменения полномочий доступа при изменении условий (наем новых сотрудников, увольнение, изменение обязанностей, и т.д.)  Организация должна сообщить о своей политике или руководящих принципах в отношении безопасности паролей и других контрольных процедур (ключ-карты, и др.) всем пользователям PDMIS | Оценка, основаны ли профили доступа на должностных функциях сотрудников  Проверка, есть ли активные профили доступа у бывших сотрудников или лиц, не работающих в DMO  Проверка, есть ли брандмауэры и обновленные антивирусные программы, а также программное обеспечение для обнаружения атак и вредоносных программ  Проверка, обновляется ли систематически операционная система на рабочих станциях и серверах  Оценка, должным ли образом реализуется политика паролей  Проверка, определены ли и оформлены ли документально соответствующие процедуры | |
| **Контрольные процедуры в отношении окружающей среды** | По всей серверной комнате должны быть проложены трубы (подачи воды, отопления, подачи электричества и др.)  Должны быть установлены датчики воды, тепла и влажности  В серверной комнате должна быть установлена система антипотопа | Проверка и оценка окружающих условий в помещении сервера базы данных  Проверка наличия и эффективного обслуживания устройств, используемых для предотвращения пожара, наводнения и избыточной влажности  Проверка существования и | |
|  | Должны быть установлены датчики дыма/пожарной сигнализации  Должно быть съемный пол, или оборудование должно быть расположено на подставках на высоте 15-20 сантиметров от пола  Должен быть источник бесперебойного питания для обеспечения функционирования центрального компьютера и серверов | эффективное функционирование альтернативных источников питания, чтобы избежать прерывания предоставления ИТ-услуг |
| **Контрольные процедуры в отношении изменения программ** | Руководство ИТ должно вести аудиторский журнал неисправностей в эксплуатации, происшествий и ошибок  Журнал должен отслеживать каждое происшествие от основной причины то его устранения  В службе поддержки пользователей не должно быть нерешенных важных вопросов по эксплуатации PDMIS  Должна быть реализована передача разрешения проблем на более высокий уровень для критических событий и соответствующий уровень реагирования, основанный на приоритете события  Должен быть реализован отчет о нарушениях безопасности, который представляется менеджерам DMO  Предыдущие изменения должны быть выполнены в соответствии со стандартными процедурами  Если используется нестандартная система управления долгом, организация должна документально оформить свои процедуры контроля изменений и описать, кто имеет право выполнять изменения системы  Организация должна отслеживать и контролировать все изменения системы управления долгом (аудиторский след) | Оценка времени, затраченного на выполнение требований DMO, связанных с использованием инструкций или сбоями в функционировании PDMIS  Определение наиболее частых сбоев PDMIS и вероятных причин  Сопоставление предыдущих изменений со стандартными процедурами |
| **BCP и DRP** | DMO должно установить BCP и DRP  Персонал, отвечающий за непрерывность работы должен знать свои должностные функции и обязанности  Необходимо отчитываться о слабых сторонах, выявленных при предыдущих тестированиях BCP и DRP или эффективных мероприятиях, а также мерах, принятых DMO для устранения таких слабых сторон  Кредитная документация должна храниться в надежном месте и быть защищена от кражи, пожара, наводнения или других происшествий, которые могут ее повредить или уничтожить | Оценка согласованности и полноты BCP и DRP и выполняются ли их обновления  Оценка отчетов о предыдущих тестированиях BCP, DRP и плана резервного копирования  План резервного копирования  Проверка были ли BCP и DRP должным образом доведены до сведения всех сотрудников  Проверка в каком состоянии находятся удаленные резервные копии и могут ли они использоваться для перезапуска системы в случае сбоя |

Приложение II: Матрица тестирования прикладных средств контроля

|  |  |  |  |
| --- | --- | --- | --- |
| **СТАНДАРТЫ ДОКУМЕНТАЦИИ** | | | |
| Целями стандартов необходимой документации является обеспечение того, чтобы контрольные процедуры выполнялись на постоянной основе, а также снижение риска ошибки. | | | |
| **ТРЕБОВАНИЯ / ФУНКЦИОНАЛЬНОСТЬ** | **ПРИКЛАДНЫЕ СРЕДСТВА КОНТРОЛЯ** | **ПРЕДЛОЖЕННЫЕ ПРОЦЕДУРЫ ТЕСТИРОВАНИЯ** | |
| Контроль реализации | Документация по приложению должна быть достаточно полной (с описанием всех функций приложения, а также связанных функций) | Проверка документации | |
| Документация должна обновляться, чтобы отражать изменения приложения | Проверка документации | |
| Прикладные средства контроля, включенные в документацию, должны выполняться и эффективно функционировать | Проверка выборки прикладных средств контроля для определения того, выполняются ли они в соответствии с документацией и насколько эффективно функционируют | |
| **Резервное копирование документации** | Необходимо выполнять резервное копирование документации | Проверка резервного копирования документации | |
| **КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ВВОДА ДАННЫХ** | | | |
| Целью контрольных процедур ввода данных - обеспечить авторизацию, точность, полноту и своевременность данных, введенных в приложение. | | | |
| **ТРЕБОВАНИЯ / ФУНКЦИОНАЛЬНОСТЬ** | **ПРИКЛАДНЫЕ СРЕДСТВА КОНТРОЛЯ** | **ПРЕДЛОЖЕННЫЕ ПРОЦЕДУРЫ ТЕСТИРОВАНИЯ** | |
| **Поля, обязательные для заполнения** | Приложение не позволяет подтвердить операцию, если есть незаполненные поля, обязательные для заполнения | Подтверждение операции с пропуском необходимых данных и выполнение проверки, обрабатывается ли операция  Выполнение такого тестирования для следующих процессов: регистрация контракта, активация контракта, регистрация эмиссии ценных бумаг и т. д | |
| **Правильный и надлежащий ввод данных** | Приложение не принимает данные, если они введены неправильно или некорректно | Проверка формата данных в базе данных  Изучение спецификации ввода данных и выполнение проверки некоторых из них на уровне приложения  Попытка вставить неправильные или некорректные данные и выполнение проверки, принимаются ли данные, и генерируется ли сообщение об ошибке  Проведение таких тестов для следующих процессов: регистрация контракта, активация контракта, регистрация эмиссии ценных бумаг, обновление индекса, погашение ценных бумаг и т. д. |
| Приложение не допускает дублирование данных | Попытка регистрации контракта или ценной бумаги под уже существующим именем и выполнение проверки, принимаются ли данные, и генерируется ли сообщение о дублировании |
| Что касается процентных ставок по контракту, не должно быть наложения периодов или неохваченных периодов в отношении области применения процентных ставок | Проверка базы данных на наличие периодов с наложенными друг на друга процентными ставками или без установленных процентных ставок |
| В случае договора на предоставление дотации приложение должно разрешить ввод выдачи транша без указания амортизационных отчислений и операций по начислению и погашению процентов | Попытка ввода выдачи транша для договора на предоставление дотации и выполнение проверки, потребует ли приложение ввести данные по амортизации и операциям по начислению и погашению процентов |
| В экране ввода выдачи транша, когда пользователь ищет контракты для того, чтобы ввести выдачу транша, приложение должно показывать только контракты, имеющие статус «активный» на этапе выдачи транша или этапе выдачи транша и амортизации | Попытка ввести выдачу транша и выполнение проверки этапа выбора контракта, отображаемого приложением |
| В случае плавающей процентной ставки, приложение должно потребовать указание индекса | Проверка, запрашивает ли приложение индекс при выборе плавающей процентной ставки | |
| Приложение не должно позволять ввод десятичных чисел для количества выпущенных ценных бумаг | Попытка ввести десятичное число в поле количества выпущенных ценных бумаг и выполнение проверки, примет ли приложение такую запись | |
| Приложение должно позволять создание ценной бумаги до ее выпуска | Моделирование создания ценной бумаги без выполнения ее выпуска | |
| **Полнота информации** | В приложение должна быть введена вся соответствующая информация о долге | Выполнение проверки, все ли важные данные о задолженности введены в приложение, например, кредитные операции, гарантии, ссуды, процентные ставки и обменные курсы | |
| **Совместимость дат** | Дата начала для расчета суммы выделенных средств должна быть более ранней, чем дата завершения проекта | Попытка вставить дату начала для расчета суммы выделенных средств, которая является более поздней, чем дата завершения проекта, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
| Дата вступления в силу должна быть более ранней, чем дата завершения проекта | Попытка вставить дату вступления в силу, которая является более поздней, чем дата завершения проекта, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
| Дата вступления в силу должна быть более ранней, чем дата крайнего срока выдачи транша | Попытка вставить дату вступления в силу, которая является более поздней, чем дата крайнего срока выдачи транша, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
| Дата крайнего срока выдачи транша должна быть более ранней, чем дата завершения проекта | Попытка вставить дату крайнего срока выдачи транша, которая является более поздней, чем дата завершения проекта, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
| Чтобы получить отчет по срокам исполнения обязательств, конечная дата погашения ценных бумаг должна быть более поздней, чем начальная дата | Попытка вставить начальную дату, которая является более поздней, чем конечная дата погашения ценных бумаг и выполнение проверки, генерируется ли сообщение об ошибке | |
| Приложение не принимает будущие даты для операций | Попытка выполнить некоторые операции, указав будущую дату, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке  Проведение таких тестов для следующих процессов: регистрация контракта, активация контракта, регистрация выпуска ценных бумаг, обновление индекса, погашение ценных бумаг, запись выдачи транша, добавление контракта и т. д. | |
| Дата выпуска ценной бумаги должна быть более ранней, чем дата ее погашения | Попытка вставить дату выпуска, которая является более поздней, чем дата погашения, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
|  |
| При вводе амортизационных платежей, в тех случаях, когда суммы или даты отличаются от указанных в приложении, приложение должно выводить сообщение, информирующее пользователя о такой ситуации, прежде чем подтвердить операцию | Регистрация платежа с датой или суммой, отличающейся от введенной в приложение, и выполнение проверки, выведет ли приложение соответствующее сообщение | |
| Если расчетная дата отличается от даты погашения, приложение должно потребовать заполнить поля «обоснование» или «подтверждение кредитора» | Введение различных дат для расчета и погашения и выполнение проверки, запросит ли приложение «обоснование» или «подтверждение кредитора» | |
| Периоды запланированных выдач траншей не должны накладываться друг на друга; например, начальная дата второго транша не может быть раньше, чем конечная дата первого транша | Попытка ввести дату второго транша, которая является более ранней, чем дата первого транша, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
| **Безопасность ввода данных и операций** | Приложение не должно позволять посторонним лицам вводить некоторые данные и выполнять некоторые операции | Проверка наличия права доступа и других требований для определенных профилей пользователя  Попытка ввести данные и выполнить некоторые операции без надлежащего профиля и выполнение проверки, будет ли это возможно  Проведение таких тестов для следующих процессов: регистрация контракта, активация контракта, регистрация выпуска ценных бумаг, изменения индекса, погашение ценных бумаг, запись платежа и т.д. | |
| Приложение должно вести журнал регистрации доступов для ручного ввода данных | Проверка наличия журналов ограниченного доступа и подтверждение того, что журналы не могут просмотреть или изменить лица, которые не имеют соответствующих прав доступа | |
| Приложение не должно позволять изменять значения активного контракта | Попытка изменить значение активного контракта и выполнение проверки, будет ли это возможно | |
| Приложение должно запретить изменение данных и удаление контрактов со статусом «аннулирован» или «завершен» | Попытка изменить и удалить некоторые данные или выборку контрактов со статусом «аннулирован» или «завершен», и выполнение проверки, будет ли это возможно | |
| Приложение должно запретить удаление активного контракта, за исключением случаев, когда контракт находится на стадии переговоров | Попытка удалить активный контракт, который не находится на стадии переговоров, и выполнение проверки, будет ли это возможно | |
| Приложение не должно позволять неправомерное исключение выпущенных ценных бумаг, если только нет соответствующей операции, связанной с ценной бумагой | Попытка удалить выпущенную ценную бумагу, которая не связана с операцией, и выполнение проверки, будет ли это возможно | |
| Приложение должно запросить двойное подтверждение для выполнения критических операций | Проверка, требуется ли двойное подтверждение для выполнения критических операций  Проведение таких тестов для следующих процессов: активация контракта, выпуск ценных бумаг, выплата амортизации, погашение ценных бумаг, изменение стоимости контракта, оплата купонов, аннулирование платежа, изменения процентных ставок и т. д. | |
|  | Приложение должно принимать только ввод данных из известных источников; кредит должен быть введен в соответствии с соглашением и принятыми стандартами | Проверка, что ключевые данные введены дважды, и что возникает сообщение об ошибке, если записи не совпадают | |
|  | Приложение должно позволить уменьшить стоимость по контракту, пока сумма уменьшения не превышает сумму «остатка средств, подлежащего выплате» | Попытка уменьшить стоимость контракта на сумму, превышающую остаток средств, подлежащий выплате, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
|  | Приложение должно регистрировать все операции только один раз | Выполнение нескольких идентичных операций (например, выплат амортизации) и выполнение проверки, будет ли обработана операция и продублирована в базе данных | |
|  | При регистрации платежа, если допуск пользователя аннулирован, приложение должно только сообщить об аннулировании, когда пользователь попытается ввести платеж, т.е. есть возможность внести в журнал как неудачную попытку, так и данные, которые пользователь пытался ввести | Попытка зарегистрировать платеж с аннулированным допуском и выполнение проверки, принимаются ли данные, и внесена ли попытка в журнал | |
|  | В случае автоматической передачи файлов между приложениями PDMIS должна сохранить исходные данные, полученные от других приложений, в течение времени, установленного DMO. | Проверка сохранения данных, переданных из других приложений, чтобы убедиться, что данные зашифрованы или защищены от повреждения, потери или нарушения | |
|  | Приложение не должно позволять изменять процентные ставки по очередному платежу, который уже оплачен, и для выполнения изменения процентной ставки требуется второе подтверждение | Попытка изменить процентную ставку по оплаченному платежу и выполнение проверки, приняты ли данные; а также выполнение проверки, запросит ли приложение второе подтверждение для изменения процентной ставки | |
| **Совместимость сумм** | Сумма транша должна быть меньше стоимости контракта | Попытка ввести сумму транша, превышающую стоимость контракта, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
| Стоимость выкупа должна быть меньше, чем стоимость выпущенной ценной бумаги | Попытка выполнить выкуп ценной бумаги по стоимости, превышающей стоимость выпущенной ценной бумаги, и выполнение проверки, будут ли приняты данные, и будет ли сгенерировано сообщение об ошибке | |
| Перед обработкой приложение отображает предупреждение о недополучении платежа или о переплате | Моделирование ситуации недополучения платежа или переплаты и выполнение проверки, будет ли отображено предупреждение | |
| **Исходные документы** | Должно выполняться отслеживание исходных документов для обеспечения достоверности ввода данных | Выбор нескольких введенных данных и проверка наличия соответствующего исходного документа (например, договор займа, сообщение электронной почты и др.) | |
| **КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ОБРАБОТКИ ДАННЫХ** | | | |
| Целью контрольных процедур обработки данных является обеспечение того, чтобы данные правильно обрабатывались в приложении, и чтобы в процессе обработки данные не были добавлены, потеряны или изменены. | | | |
| **ТРЕБОВАНИЯ / ФУНКЦИОНАЛЬНОСТЬ** | **ПРИКЛАДНЫЕ СРЕДСТВА КОНТРОЛЯ** | **ПРЕДЛОЖЕННЫЕ ПРОЦЕДУРЫ ТЕСТИРОВАНИЯ** | |
| **Индикация правильного состояния** | Приложение должно изменить статус контракта после полной выплаты | Моделирование завершения выплаты и выполнение проверки, изменился ли статус контракта с «выплачивается» на «полностью выплачен» | |
|  | Приложение должно изменить состояние ценной бумаги после подтверждения ее выпуска | Моделирование подтверждения выпуска ценной бумаги и выполнение проверки, изменился ли статус ценной бумаги с «неактивная» на «активная» | |
|  | Приложение должно изменить статус контракта или ценной бумаги после полной оплаты | Моделирование выполнения последнего платежа и выполнение проверки, изменится ли статус контракта или ценной бумаги | |
|  | Приложение должно предусматривать хотя бы следующие этапы:   * + Выплата: на этом этапе создаются выдачи траншей   + Полная выплата: выдача траншей на этом этапе не допускается   + Завершение: на этом этапе выдачи траншей не получают финансовых операций и не допускается изменение данных | Создание контракта, | |
| попытка выполнить выдачу транша на каждом этапе и выполнение проверки, принимаются ли данные, и генерируется ли сообщение об ошибке | |
| Приложение должно содержать правила, чтобы сделать статус контракта (активный или неактивный) совместимым с этапом (выплата, полная выплата, амортизация, выплата и амортизация, и завершение) для того, чтобы предотвратить противоречия в информации; например контракт с неактивным статусом не может быть на этапе выплаты или амортизации | Моделирование нескольких изменений статуса контракт и этапа контракта и выполнение проверки их совместимости | |
| Приложение должно содержать программу для обновления этапа контракта; например когда остаток средств, подлежащих выплате, равен нулю, приложение должно изменить этап с выплаты на полную выплату | Моделирование необходимых условий для изменения этапа контракта и выполнение проверки, происходит ли такое изменение | |
| **Правильный расчет** | Приложение должно выполнять вычисления правильно | Проверка расчета путем повторного выполнения  Выполнение такой проверки расчетов для следующей информации: общая сумма долга (договорного и секьюритизированного), сроки исполнения обязательств, график амортизации (даты и суммы), суммы агентских вознаграждений, поток обеспечительных платежей, финансовая стоимость погашения ценной бумаги и т. д | |
| После нескольких изменений вводимых данных, приложение должно обновить данные | Выполнение нескольких изменений вводимых данных и выполнение проверки, обновились ли данные; например: | |
|  |  | Пример   * + Моделирование оплаты и выполнение проверки, обновились ли остаток долга и поток амортизации   + Изменение нескольких индексов и выполнение проверки, обновилась ли величина общей суммы долга | |
| Приложение должно содержать в своей программной части, по крайней мере следующие методы для расчета периодических платежей: равномерное распределение, простые проценты, частичный платеж, приложение по ценообразованию, приложение по постоянной амортизации, валютная корзина пула (МБРР) и UAC корзины валют (МБР) | Проверка методов, которые система использует для расчета платежей; правильность методов можно проверить с использованием выборки данных | |
| Всякий раз, когда значение поля Стоимость контракта изменяется, приложение должно автоматически пересчитывать значение поля Оставшаяся сумма по контракту, подлежащая выплате | Изменение значения поля Стоимость контракта и выполнение проверки, правильно ли обновилось значение поля Оставшаяся сумма по контракту, подлежащая выплате | |
| Приложение должно автоматически генерировать даты периодических платежей, используя один из следующих доступных методов:   * + Первоначальная дата и фиксированное число платежей   + Первоначальная дата, конечная дата и уменьшающееся число платежей   + Первоначальная дата, конечная дата и фиксированное число платежей   + Начальная дата и количество периодов   + Периоды | Введение данных, необходимых для каждого из возможных методов, и выполнение проверки, верны ли даты платежей | |
| Когда дата платежа попадает на нерабочий день, приложение должно предложить два варианта: передвинуть дату вперед на следующий рабочий день или перенести назад на предыдущий рабочий день | Установка параметров платежа таким образом, чтобы дата попадала на нерабочий день, и выполнение проверки, предлагает ли приложение изменить дату на предыдущий рабочий день либо на следующий рабочий день | |
|  | Система должна автоматически обновлять номинальную стоимость ценных бумаг всякий раз, когда изменяется соответствующий индексатор | Изменение индексатора ценной бумаги и выполнение проверки, обновляется ли соответствующая номинальная стоимость | |
|  | В случае оплаты меньшей суммы, чем сумма, рассчитанная приложением, должно выводиться сообщение в момент ввода платежа; сообщение должно повторяться до даты следующего погашения | Моделирование платежа на меньшую сумму, чем сумма, рассчитанная приложением, и выполнение проверки, будет ли выводиться сообщение, и будет ли оно повторяться до даты следующего погашения | |
|  | В своей базе данных система должна дифференцировать ценные бумаги с имитацией выпуска | Выполнение проверки в базе данных, дифференцируются ли смоделированные ценные бумаги, и не учитываются ли они в расчетах общей суммы долга и сроков погашения | |
|  | Когда пользователь удаляет ценную бумагу, приложение должно удалять соответствующие значения в базе данных | Удаление ценной бумаги и выполнение проверки, удалилось ли соответствующее значение из базы данных | |
|  | Ценные бумаги со статусом «аннулированная» не должны учитываться в расчете долговых ценных бумаг (например, ВСД, срок погашения, и т. д.), то есть, после того, как они будут аннулированы, соответствующие значения должны быть навсегда исключены из базы данных | Изменение статуса ценной бумаги на «аннулированная» и выполнение проверки, не учитывается ли ее стоимость в расчетах (общей суммы, срока погашения, и др.) | |
|  | Приложение должно по-разному обрабатывать периодические платежи и просроченные платежи | Выполнение проверки, правильно ли приложение рассчитывает все платежи по просроченным взносам | |
| **Надлежащий контроль ошибок обработки данных** | Не должны оставаться неисправленными ошибки обработки данных за последние дни/недели | Проверка наличия критериев в отношении количества дней, необходимых для устранения ошибок в системе, проверка наличия сообщений об ошибках и обсуждение с системными менеджерами/менеджерами по управлению долгом мер, принятых для устранения сбоев | |
|  | Если выявлена ошибка обработки данных, приложение должно отменить обработку и сохранить в базе данных информацию о дате, времени и технических причинах проблемы | Моделирование ошибки обработки данных и выполнение проверки, сохранило ли приложение хранит в базе данных информацию о дате, времени и технических причинах проблемы | |
| **Правильная запись** | Приложение должно позволить менеджерам по управлению долгом вести точные записи денежных потоков (связанные с заимствованиями в иностранной валютой и в национальной валюте, хеджированием и торговой деятельностью, гарантиями и кредитованием) для всех операций | Выполнение операции и проверка, является ли ее запись правильной и точной | |
|  | Приложение должно сохранять историю операций на протяжении срока действия контракта и должно содержать подробную информацию о кредиторе, договорной стоимости, а также дате закрытия проекта и предельных сроках для полей выдачи транша | Выбор нескольких контрактов и выполнение проверки, есть ли в каждом из них история всех операций, выполненных на протяжении срока действия контракта, со всеми необходимыми подробностями | |
|  | Приложение должно иметь журнал для каждого долгового инструмента | Проверка соответствия хронологических операций, связанных с ценной бумагой или контрактом, соответствующему долговому журналу | |
| **Правильное планирование задач** | В приложении должен быть реализован автоматический запуск для запланированных задач, установленных DMO для обновления индексов, общей суммы задолженности и т. д. | Проверка наличия автоматического запуска и правильности выполнения данного процесса | |
|  | Для типа ценных бумаг, амортизация которых выполняется с такой же периодичностью, как и процентные платежи (цена, например), система должна обеспечить, чтобы и для процентов, и для амортизации были одинаковые графики платежей | Создание ценной бумаги с амортизацией и процентными платежами с одинаковой периодичностью и выполнение проверки, имеют ли они одинаковый график платежей | |
| **Аудиторский след** | Аудиторский след PDMIS следует сохранить для обеспечения возможности мониторинга долгового контракта или ценной бумаги с момента подписания/выпуска до момента погашения | Проверка наличия аудиторского следа для выборки контрактов и ценных бумаг, с момента подписания/выпуска до момента погашения | |
| **КОНТРОЛЬНЫЕ ПРОЦЕДУРЫ ВЫВОДА ДАННЫХ** | | | |
| Целью контрольных процедур вывода данных является обеспечение целостности вывода данных и правильного и своевременного распределения полученной выходной информации. | | | |
| **ТРЕБОВАНИЯ / ФУНКЦИОНАЛЬНОСТЬ** | **ПРИКЛАДНЫЕ СРЕДСТВА КОНТРОЛЯ** | **ПРЕДЛОЖЕННЫЕ ПРОЦЕДУРЫ ТЕСТИРОВАНИЯ** | |
| Контроль над пользователями информации | Приложение должно иметь журнал предоставления отчетов для записи имен пользователей, которые запросили отчеты, а также дат и времени запросов | Выполнение запроса нескольких отчетов и выполнение проверки, записывает ли приложение информацию по запросам | |
|  | Приложение должно запросить специальное разрешение на загрузку определенных отчетов (особенно тех, что содержат конфиденциальную информацию) | Попытка сгенерировать эти отчеты | |
| **Предоставление своевременной и надежной отчетности** | Приложение должно формировать встроенные отчеты (классификация облигаций, займов и траншей, например, по срокам погашения, статусу, источникам финансирования, виду финансирования, сумме кредита, виду инструмента, срокам, неоплаченным счетам, и др.) | Попытка сформировать несколько встроенных отчетов | |
| # | Приложение должно формировать отчеты должным образом, с обеспечением полноты и | Выполнение проверки, формируются ли отчеты в соответствии с условиями использования  Проверка, есть ли в отчетах номера страниц и итоги  Выполнение такого тестирования в отношении следующих отчетов: Отчет по срокам погашения (для договорного и секьюритизированного долга), Отчет об остатке задолженности, Отчет о поступлениях и т. д | |
|  | Приложение должно обеспечить формирование отчетов, как обобщенных (задолженность по всем ценным бумагам) так и специализированных, как например:   * + По статусу ценных бумаг (выпущенные, аннулированные, выкупленные, и т.д.)   + Для событий за определенный период времени (эмиссии, выкупы и др.)   + Для краткосрочных и долгосрочных ценных бумаг   + По позиции портфеля   + По виду ценных бумаг   + По периодам погашения | Попытка формирования обобщенных и специализированных отчетов, используя в качестве критерия следующие данные:   * + Статус ценных бумаг (выпущенные, аннулированные, выкупленные, и т.д.)   + События за определенный период времени (эмиссии, выкупы и др.)   + Краткосрочные и долгосрочные ценные бумаги   + Позиция портфеля   + Вид ценных бумаг   + Периоды погашения | |
|  | Отчеты должны представить полную и точную информацию | Создание отчетов и повторное выполнение вычислений  Выполнение такого тестирования в отношении следующих отчетов: Отчет по срокам погашения (для договорного и секьюритизированного долга), Отчет об остатке задолженности, Отчет о поступлениях и т. д | |
|  | Отчеты должны представлять точно такую же информацию, как и на экранах приложения | Сравнение отчетов для обеспечения соответствия информации, представленной на экранах приложения  Выполнение такого тестирования в отношении следующих отчетов: Отчет по срокам погашения (для договорного и секьюритизированного долга), Отчет об остатке задолженности, Отчет о поступлениях и т. д | |
|  | Значения, представленные в отчете по срокам погашения, отчете об остатке задолженности и отчете по ценным бумагам, не должны противоречить друг другу | Сравнение этих отчетов на предмет отсутствия противоречивых данных | |
|  | Система должна быть способна формировать отчеты по итоговым суммам задолженности на индивидуальной и совокупной основе с прогнозированием обслуживания долга в отношении существующих и будущих займов и ценных бумаг | Попытка сформировать такие отчеты  Проверка, рассматриваются ли в отчете существующие и ожидаемые долговые операции | |
|  | Приложение должно автоматически формировать ежедневные отчеты по финансовым графикам для всех действующих контрактов; оно должно также предоставлять возможность для определенных контрактов формировать отчеты вручную | Проверка генерации автоматических отчетов для всех активных контрактов и попытка создания отчетов для определенных контрактов вручную | |
| **Правильная передача данных** | Передача данных между приложениями и/или этапами обработки должна быть точной и полной | Моделирование передачи данных между приложениями и проверка точности и полноты данных | |
| **Полезные выходные сообщения** | Когда пользователь обращается к приложению, оно должно вывести сообщение со следующей информацией:   * + Контракты, срок погашения по которым наступит в ближайшие 5 дней   + Контракты с несвоевременным выполнением периодических платежей   + Контракты с частично оплаченными периодическими платежами   + Контракты с просроченными датами выдачи траншей   + Контракты с крайним сроком выдачи траншей в ближайшие 5 дней (приложение должно отправлять ежедневное сообщение, пока не будет произведена выдача, не будет отменена сумма, подлежащая выплате, или изменен крайний срок) | Обращение к приложению и выполнение проверки, отображаются ли все эти сообщения | |
| Приложение должно указывать статус расчета как «выполнение расчета» или «расчет завершен» | Запрос расчета и проверка, указывает ли приложение статус операции | |
| В конце формирования отчета приложение должно вывести сообщение, что формирование отчета завершено, или отобразить запрошенный отчет | Запрос формирования отчета и выполнение проверки, выводит ли приложение сообщение, что операция завершена, либо отображает запрошенный отчет | |
| Приложение должно указать статус формируемого отчета как «выполняется» или «завершен» | Запрос формирования отчета и выполнение проверки, указывает ли приложение статус операции | |
|  |
|  | Если процентные ставки изменяются, приложение должно выводить предупреждающее сообщение | Изменение процентных ставок и проверка отображения предупреждающего сообщения | |
|  | Перед обработкой удаления или выкупа ценной бумаги, приложение должно отобразить экран с удаляемой информацией или информацией по выкупу, чтобы пользователь мог подтвердить операцию | Выполнение попытки выкупить или удалить ценную бумагу и проверка, отобразит ли приложение сообщение для пользователя, чтобы подтвердить операцию | |

|  |
| --- |
| Рисунок 1: Аудиторские проверки государственного долга, выполняемые ВОА: Бразильский случай |
| ***Аудиторская проверка, проведенная Счетной палатой Бразилии для Интегрированной системы управления долгом (SID) Федерального правительства Бразилии в 2014 г.*** |
| С учетом того, что SID тестируется в отношении внутреннего секьюритизированного долга, группа ревизоров решила сосредоточиться только на тестировании процессов, связанных с внешним долгом (секьюритизированным и договорным). Сделаны следующие аудиторские наблюдения и выводы: |
| **Стратегия и общее управление системы ИТ** |
| В соответствии с Руководством по эксплуатации после того, как SID будет полностью реализована, она будет выполнять следующие функции: |
| 1. различные расчеты, такие как обновленная номинальная стоимость, цена единицы товара, общая сумма (как договорного, так и секьюритизированного долга), финансовое планирование контрактов, а также сроки погашения контрактов и ценных бумаг; |
| 1. разнообразные поиски и отчеты о регистрации данных и результатах расчетов; |
| 1. финансовые операции, такие как выпуск облигаций, погашение обязательств по контракту, выкупа и передача; в числе прочих; и |
| 1. информационный регистр, используемый в полной мере в различных бизнес-модулей. |
| В отношении стратегии системы ИТ и общего управления были сделаны следующие основные замечания и аудиторские заключения: |
| * Отсутствует программа обучения для наиболее часто используемых систем управления государственным долгом, Seorfi и SID. |
| * Отсутствует предполагаемая дата полной реализации SID, в том числе для внутренних секьюритизированных долгов. |
| * Некоторые важные операции, такие как активация контракта, выплаты, обратные выплаты, изменение процентных ставок, или изменение стоимости контракта, выполняет только один человек. Система не требует подтверждение или двойную авторизацию. Безопасность операций зависит исключительно от надежности профиля, что создает проблему разделения обязанностей. |
| * Еще одной проблемой разделения обязанностей является нехватка персонала для разработки SID; ее разрабатывают сотрудники DMO, выполняя при этом обычные функции ведомства. |
| * Выполнена оценка подверженности операционным рискам для процессов ИТ, но оценка минимизации этих рисков еще не проводилась. |
| **Контрольные процедуры в отношении безопасности и окружающей среды** |
| В отношении контрольных процедур касательно безопасности и окружающей среды были сделаны следующие основные замечания и аудиторские заключения: |
| * DMO не назначило управляющего по информационной безопасности и коммуникациям а Комитет по информационной безопасности, который отвечает за назначение менеджера, не начал эффективно работать. |
| * Отсутствует документально оформленное BCP, а рабочие процессы управления государственным долгом рассматриваются с целью подготовки BCP. |
| * В процессе анализа группа аудиторов отметила наличие трех активных основных пользователей, что не соответствует рекомендуемым нормам ИТ, основанным на п. 11.2.1 стандарта ISO / IEC 27002: 2005, который рекомендует использовать уникальную идентификацию пользователей для обеспечения подотчетности каждого пользователя в системе. |
| * Хотя предоставление доступа к SID должно осуществляться только через цифровой сертификат A3, а доступ по национальному идентификационному номеру и паролю должен быть исключением, анализ базы данных пользователей SID показывает, что отсутствует установленный граничный срок, после которого запрещено использовать такое исключение. |
| * Анализ базы данных пользователей SID выявил недостатки в процессе проверки доступа пользователя. |
| * Группа аудиторов также обнаружила недостатки в ежедневном автоматическом регламентном обслуживании базы данных пользователей SID. |
| * SID не ведет записи аудиторского следа для большинства своих операций, и в результате DMO не выполняет периодический обзор аудиторского следа, созданного системой, а также не отслеживает транзакции в SID. |
| * В SID отсутствует функция аудита, которая регулярно создает, хранит и анализирует системный журнал. |
| * Группа аудиторов отметила отсутствие плана тестирования и его соответствующих результатов в системах наиболее часто используемых DMO, Seorfi и SID. |
| * Группа аудиторов не получила подтверждение того, что для компьютерных сетей была создана группа реагирования на происшествия, ответственная за получение данных, анализ и реагирование на нарушения безопасности. |
| * Группа аудиторов отметила отсутствие плана обеспечения непрерывности обслуживания ИТ, который является надлежащим образом оформленным документом, описывающим программы обеспечения непрерывности для всех ИТ-услуг в ведении учреждения или организации. |
| **Операционные контрольные процедуры и документация** |
| В отношении операционных контрольных процедур и документации были сделаны следующие основные замечания и аудиторские заключения: |
| * Интерфейс является не очень дружественным, поэтому пользователям SID требуется больше первоначальных знаний о системе. |
| * Отсутствует руководство пользователя для SID. |
| * Низкая скорость выполнения расчетов. Это не позволяет одновременно выполнять расчеты и формировать отчеты. Поскольку к системе подключено несколько параллельных пользователей, данная проблема может снизить эффективность системы. Группа аудиторов предложила DMO определить пути улучшения в целях повышения производительности обработки системы. |
| **Прикладные средства контроля** |
| После проведения группой аудиторов контрольных испытаний для ввода, обработки и вывода данных в SID в отношении внешнего государственного долга, были сделаны следующие заключения и замечания: |
| * Многие сообщения об ошибках являются неясными и иногда не выводятся пользователю. |
| * С помощью контрольных испытаний ввода данных в приложение группа аудиторов обнаружила несколько сообщений об ошибках, которые не объясняет причину ошибки. |
| * С помощью контрольных испытаний обработки данных приложением для договорного внешнего долга, группа аудиторов обнаружила отличия в значениях в финансовом отчете о движении денежных средств, в отношении возврата средства, который не был учтен в этом отчете. |
| * В контрольных испытаниях вывода данных приложением, группа аудиторов обнаружила, что если введенные данные являются неправильными, приложение не создает некоторые отчеты по договорному долгу, как предусмотрено, но при этом приложение также не сообщает об ошибке пользователю. |
| * С помощью контрольных испытаний вывода данных приложением группа аудиторов выявила ошибки в отчетах по договорному долгу вследствие использования системой необновленных индексов. |
| * Некоторые отчеты по договорному долгу были сформированы с неполной информацией. |
| **Рекомендации** |
| Принимая во внимание заключения и замечания аудиторов, группа ревизоров рекомендовала Секретариату по национальному достоянию в течении 90 дней разработать план действий, содержащий график выполнения следующих мероприятий: |
| * Установление предполагаемой даты полной реализации SID, в том числе для внутренних секьюритизированных долгов. |
| * Назначение Управляющего по информационной безопасности и коммуникациям и Комитета по информационной безопасности. |
| * Документальное оформление BCP. |
| * Документальное оформление плана обеспечения непрерывности ИТ-услуг. |
| * Создание группы реагирования на происшествия в компьютерных сетях. |
| * Оценка и минимизация рисков в сфере ИТ. |
| * Проверка ежедневного автоматического регламентного обслуживания базы данных пользователей SID. |
| * Проверка процедуры пересмотра доступов для пользователей SID. |
| * Проверка процедуры предоставления доступов для основных пользователей SID. |
| * -Установление процедур для периодического обзора данных аудиторского следа, формируемого SID. |
| * Обеспечение внесения записей SID в журнал приложений. |
| * Обзор сообщений об ошибках SID. |
| * Разработка Руководства пользователя для SID. |
| * Обзор порядка предоставления отчетности в SID. |

|  |
| --- |
| Рисунок 2. Аудиторские проверки государственного долга, выполняемые ВОА: Молдавский случай |
| **Оценка контрольных процедур приложения, выполненная Судом счетов Республики Молдова** |
| Приложение ДМФАС имеет надлежащие интегрированные контрольные процедуры, которые автоматически проверяют, правильно ли введены данные. Однако, есть некоторые аспекты, которые вызывают опасения, и которые необходимо урегулировать: операторы могут вводить данные в классификаторы системы и другие системные таблицы, что может повлиять на точность и целостность данных путем дублирования или удаления внесенных данных. |
| Рекомендация 15 (b) Пересмотреть права операторов на ввод, изменение или удаление данных в классификаторе базы данных ДМФАС или выявить такие операции, которые приводят к дублированию данных или неправильному вводу данных. |
| Помимо имеющихся стандартных отчетов в приложении ДМФАС, многие общие отчеты были разработаны в Excel, в том числе по большинству важных вопросов. Не все виды отчетов используются систематически. Большинство необходимых отчетов формируются в Excel. Однако, есть определенные отчеты, формируемые вручную на основании данных, полученных из других отчетов. Проблемным моментом является обновление данных в отчетах Excel. Формирование отчетов является сложной процедурой, на которую могут сильно повлиять ошибки, вызванные человеческим фактором. Кроме того, сформированные отчеты могут быть изменены без разрешения, и эти ошибки могут возникнуть в других важных итоговых отчетах, которые должны иметь максимальный уровень безопасности и представлять собой основной вид деятельности Общего отдела по вопросам государственного долга. |
| В результате некоторые незначительные недостатки могут существенно повлиять на надежность и точность данных в важных отчетах о деятельности Общего отдела по вопросам государственного долга. |
| Рекомендация 16 (b) Рассмотреть возможность оптимизации и автоматизации процесса изменения формируемых отчетов. Определить способ автоматического создания сводных отчетов, исключая возможность возникновения ошибок, вызванных человеческим фактором. Рассмотреть возможность перехода на версию 6.0. |

БИБЛИОГРАФИЯ

Азиатская организация высших органов аудита **Научно-исследовательские проекты:** Руководство по аудиту ИТ - 6-е издание.(2003 сентября 2016 года)

Гальегос, Фредерик, Сандра Сенфт, Дэниэл П. Мэнсон и Кэрол Гонсалес. *Контроль и аудит информационных технологий* Издательство «Ауэрбах Пабликейшнс» (Auerbach Publications). США

Управление ревизора генерального аудитора Индии *Аудит информационных технологий - Общие принципы* (Серия монографий по аудиту ИТ -т. 1.)

Международный валютный фонд и Всемирный банк. *Руководство по управлению государственным долгом.* 1 апреля 2014 г.

Международная организация высших органов аудита. ISSAI 5440 «Руководство по проведению аудита государственного долга - применение теста на существенность в финансовых проверках».2007 ноября 2015 г.:

Международная организация высших органов аудита. Стандарт ISSAI 3000 «Стандарты и руководящие принципы аудита эффективности, основанные на стандартах аудита ИНТОСАИ и практическом опыте».2004 июля 2016 г.:

Международная организация высших органов аудита. ISSAI 5310, *Методика проверки безопасности информационных систем.* 1995 октября 2015 г.:

Инициатива развития ИНТОСАИ Рабочая группа по аудиту ИТ, *Руководство IDI по аудиту ИТ для высших органов аудита* 2014 февраля 2016 г.:

Паркер, Ксения Лэй. Информационные технологии Издательство CCH Incorporated. США

Веб-сайт Министерства внутренней безопасности США: [http://www.dhs.gov.](http://www.dhs.gov/)

Главное контрольное управление Соединенных Штатов Руководство по аудиту средств управления федеральных информационных систем (FISCAM). Государственное управление общего учета США (GAO)-09-232 G. 2009 февраля 2016 г.:

1. Электронный учебный курс Инициативы развития ИНТОСАИ (IDI) по проведению аудита управления государственным долгом, Занятие 6: Выполнение аудита Информационной системы управления государственным долгом. [↑](#footnote-ref-1)
2. Ксения Лэй Паркер, Аудиторские проверки информационных технологий, CCH Incorporated, США, 2006 г. [↑](#footnote-ref-2)
3. Паркер, Аудиторские проверки информационных технологий. [↑](#footnote-ref-3)
4. Управление Контролера и Генерального аудитора Индии, Аудит информационных технологий - Общие принципы, Серия монографий по аудиту ИТ т. 1. [↑](#footnote-ref-4)
5. Фредерик Гальегос, Сандра Сенфт, Дэниэл П. Мэнсон и Кэрол Гонсалес, Контроль и аудит информационных технологий - издание второе, издательство «Ауэрбах Пабликейшнс» (Auerbach Publications), США, 2004 г. [↑](#footnote-ref-5)
6. Гальегос, Контроль и аудит информационных технологий. [↑](#footnote-ref-6)
7. Гальегос, Контроль и аудит информационных технологий. [↑](#footnote-ref-7)
8. Гальегос, Контроль и аудит информационных технологий. [↑](#footnote-ref-8)
9. Гальегос, Контроль и аудит информационных технологий. [↑](#footnote-ref-9)
10. Азиатская организация высших органов аудита, Руководство по аудиту ИТ - 2003-е издание, Сентябрь 2003 г. [↑](#footnote-ref-10)
11. Управление Контролера и Генерального аудитора Индии, Аудит информационных технологий - Общие принципы. [↑](#footnote-ref-11)
12. Управление Контролера и Генерального аудитора Индии, Аудит информационных технологий - Общие принципы. [↑](#footnote-ref-12)
13. Управление Контролера и Генерального аудитора Индии, Аудит информационных технологий - Общие принципы. [↑](#footnote-ref-13)