НКК40/2010
Внутренний номер: 335349 Карточка документа
Varianta în limba de stat

Республика Молдова

СЧЕТНАЯ ПАЛАТА

ПОСТАНОВЛЕНИЕ Nr. 40
от 08.06.2010

по Отчету аудита Информационной системы “Менеджмент и финансовый анализ публичного долга”, внедренной в Министерстве финансов

Опубликован : 23.07.2010 в Monitorul Oficial Nr. 126-128 статья № : 21

Счетная палата в присутствии г-жи Е.Сахарнян – администратора ГП “Fintehinform”, г-жи О.Мереуцэ – заместителя начальника управления Министерства финансов по внешнему финансированию и задолженностям, г-на В.Спыну, руководителя специализированной группы по управлению серверами и базами данных Министерства финансов, руководствуясь ст.2 (1) и ст.4 (1) а) Закона о Счетной палате № 261-XVI от 5.12.2008 г.[1], рассмотрела Отчет аудита Информационной системы “Менеджмент и финансовый анализ публичного долга”, внедренной в Министерстве финансов.

[1] ОМ, 2008 г., № 237-240, ст.864.

Аудиторская миссия была проведена в соответствии с Программой аудиторской деятельности Счетной палаты на 2010 год, задача которой состояла в получении компетентных и достоверных доказательств, подтверждающих аудиторские констатации и выводы, указанные в аудиторском отчете.

Аудит был запланирован и проведен в соответствии со стандартами аудита Счетной палаты, а также пособием аудита эффективности, разработанным Счетной палатой на основании Международных стандартов аудита.

При проведении данного аудита областью применения была оценка общих контролей ИТ в Министерстве финансов и прикладных контролей в рамках Информационной системы “Менеджмент и финансовый анализ публичного долга” (далее – ИС “МФАПД”).

Рассмотрев результаты аудита, заслушав представленный отчет и объяснения должностных лиц, присутствующих на заседании, Счетная палата у с т а н о в и л а:

Некоторые общие контроли ИТ, существующие в рамках Министерства финансов, недостаточно развиты, чтобы обеспечить безопасность и доступность ИС “МФАПД”. Это не представляет серьезную озабоченность в отношении ИС “МФАПД”, так как последняя не считается критической, используясь главным образом как средство для хранения информации и анализа данных, вместе с тем информация, хранящаяся в ней, имеет

большое значение и требует надлежащего управления.

Были выявлены и некоторые недостатки в прикладных контролях приложения, которые не оказывают существенного влияния на целостность, доступность и конфиденциальность данных. Тем не менее общие контроли ИТ влияют на всю инфраструктуру организации.

В рамках данного аудита не были установлены документы, подтверждающие стоимость системы и право собственности на нее, ИС "МФАПД" не была отражена в бухгалтерском учете Министерства финансов и ГП "Fintehinform".

Исходя из вышеизложенного, на основании ст.7 (1) a), ст.15 (2) и (4), ст.16 c), ст.34 (3) Закона о Счетной палате № 261-XVI от 05.12.2008 г. Счетная палата ПОСТАНОВЛЯЕТ:

1. Утвердить отчет аудита Информационной системы "Менеджмент и финансовый анализ публичного долга", внедренной в Министерстве финансов, приложенный к настоящему постановлению.

2. Настоящее постановление и приложенный отчет направить:

2.1. Министерству финансов для принятия необходимых мер по выполнению рекомендаций аудита, изложенных в отчете;

2.2. Правительству Республики Молдова для информации и принятия к сведению.

3. О предпринятых мерах по исполнению п.2 настоящего постановления проинформировать Счетную палату в течение 3 месяцев.

4. Настоящее постановление опубликовать в Официальном мониторе Республики Молдова в соответствии со ст.34 (7) Закона о Счетной палате № 261-XVI от 5.12.2008 г.

Председатель Счетной палаты Ала ПОПЕСКУ

№ 40. Кишинэу, 8 июня 2010 г.

ОТЧЕТ
аудита Информационной системы "Менеджмент и финансовый анализ публичного долга", внедренной в Министерстве финансов

СПИСОК АББРЕВИАТУР

ИС "МФАПД"	Информационная система "Менеджмент и финансовый анализ публичного долга"
БД	база данных
Стандарт COBIT 4.1	Control Objectives for Information and Related Technology (Стандарт по Задачам информационных и смежных технологий)
COSO	Committee of Sponsoring Organizations of the Treadway Commission (Комитет спонсорских организаций Комиссии Тредуэя)
IFAC	International Federation of Accountants (Международная федерация бухгалтеров)
IIA	The Institute of Internal Auditors (Институт внутренних аудиторов)
INTOSAI	International Organization of Supreme Audit Institutions (Международная организация высших органов финансового контроля)
ISACA	Information Systems Audit and Control Association (Ассоциация Аудита и Контроля Информационных Систем)
ISACF	The Information Systems Audit and Control Foundation (Фонд Аудита и Контроля Информационных Систем)
ISO	International Organization for Standardization (Международная организация по стандартизации)
ITGA	Informational Technology Governance Association (Ассоциация по управлению ИТ)

ИТ	информационные технологии
ИС	информационная система
ОС	операционная система

СУММАРНЫЙ ИТОГ

1. ГП “Fintehinform” управляет всеми активами ИТ Министерства финансов (в том числе и ИС “МФАПД”). От качества общих контролей ИТ напрямую зависит возможность обеспечения целостности, надежности и доступности всех информационных систем.

2. В ходе аудиторской миссии были рассмотрены общие контроли ИТ, констатируя, что на данный момент времени некоторые из них являются недостаточными, а другие отсутствуют. Это может повлиять как на существующие информационные системы, так и на внедрение и развитие Интегрированной системы финансового менеджмента.

3. ИС “МФАПД” была разработана и внедрена при поддержке Конференции Организации Объединенных Наций по торговле и развитию и используется более чем в 60 странах. Будучи приложением для эффективного управления и анализа данных о публичном долге, ИС была разработана и развита с четко определенным набором контролей. В основном прикладные контроли являются надежными и обеспечивают достаточную уверенность в надежности, точности и целостности данных ИС “МФАПД”.

4. Для обеспечения развития и надлежащего управления потребностями в области ИТ, исключения рисков в доступности и надежности информационных ресурсов предлагаем Министерству финансов:

a) выполнить рекомендации, изложенные в данном отчете;

b) провести анализ затрати выгод для оценки полученных выгод в результате возможного перехода на новую версию ИС “МФАПД”.

Общая информация об организации и информационной системе

В соответствии с Законом №419-XVI от 22.12.2006[2] управление государственным долгом и государственными гарантиями, отчетность и мониторинг публичного долга осуществляет Министерство финансов. Политика в области управления публичным долгом в 2008-2010 гг. была установлена Постановлением Правительства № 756 от 2.02.2007[3].

[2] Закон о публичном долге, государственных гарантиях и государственном рекредитовании № 419-XVI от 22.12.2006 (с последующими изменениями и дополнениями; далее – Закон № 419-XVI).

[3] Постановление Правительства № 756 от 2.07.2007 „О среднесрочном прогнозе расходов (2008-2010)”(с последующими изменениями).

В целях учета всех прямых и условных обязательств Республики Молдова, предоставляемых из средств, полученных по внутренним или внешним государственным займам, Министерство финансов является единственным органом, уполномоченным создавать и вести следующие государственные регистры:

a) Государственный регистр государственного долга;

b) Государственный регистр государственных гарантий;

c) Государственный регистр государственного рекредитования.

Указанные государственные регистры ведутся в электронной форме Министерством финансов и являются единственными официальными записями о прямых и условных обязательствах Республики Молдова, а также и о государственном рекредитовании.

В Государственном регистре государственного долга в хронологическом и систематическом порядке регистрируется информация о прямых обязательствах государства, вытекающих из внутренних и внешних государственных займов, о динамике государственных займов, идентификационном номере долга, дате заключения договора о

долге, дате наступления срока погашения, общей сумме долга. Регистр государственного долга содержит следующие подрегистры:

a) подрегистр внутреннего государственного долга;

b) подрегистр внешнего государственного долга.

Для управления государственным долгом и ведения упомянутых государственных регистров Министерство финансов использует приложение программного обеспечения (software) "МФАПД", которое было установлено весной 1998 года и внедрено при поддержке Конференции Организации Объединенных Наций по торговле и развитию в рамках технической помощи по применению прикладной программы "МФАПД".

Программа технической помощи по применению ИС „МФАПД" внедрена в ряде стран и предоставляет им ряд решений, которые уже доказали свою способность по администрированию публичного долга и получению надежных данных для управления и мониторинга государственного долга. К программе технической помощи относятся как сама прикладная программа по управлению долгом "МФАПД", которая облегчает работу в области администрирования государственным долгом, так и предоставление консультаций и подготовка кадров в области менеджмента долгов.

ИС „МФАПД" используется для администрирования, анализа и предоставления информации о государственном долге. Эта информация не используется для осуществления платежей или для финансового управления. Исходя из своего назначения и аналитико-консультативного аспекта, можем считать ИС „МФАПД" некритической системой, так как в случае остановки ее функционирования она не повлечет за собой остановку основной деятельности организации.

ИС „МФАПД" используется и Национальным банком Молдовы. Для этих целей установлена другая копия системы. Министерство финансов еженедельно получает от Национального банка данные по обменному курсу валют. Посредством телекоммуникационных систем органов публичной власти, другие органы центрального публичного управления могут получить доступ к данной системе. Таким образом, был организован доступ для одной рабочей станции Правительства (Приложение №1).

Администрирование и техническое обслуживание ИС „МФАПД" осуществляется Г.П. "Fintehinform" на основе договора №34 от 1.01.2010, заключенного с Министерством финансов.

ГП "Fintehinform" осуществляет свою деятельность на основе принципа самофинансирования и было учреждено в соответствии с Постановлением Правительства N 516 от 2.06.2005[4] в результате упразднения главного управления информационных технологий Министерства финансов.

[4] Постановление Правительства N 516 от 2.06.2005 „О структуре и предельной численности центрального аппарата Министерства финансов" (с последующими изменениями). Утратил силу: 21.11.2008. Постановление Правительства N 1265 от 14.11.2008.

В соответствии с положениями устава ГП "Fintehinform" **основные задачи** предприятия заключаются в администрировании, поддержании, развитии и обеспечении функционирования информационной системы управления публичными финансами Министерства финансов, представлении его в вопросах, касающихся информационных технологий и их продвижении как в рамках министерства, так и вне него. **Основными видами деятельности** являются: оказание услуг по разработке, содержанию и внедрению программных продуктов, информационных технологий и систем; оказание услуг по проектированию, разработке, внедрению автоматизированных информационных систем государственного значения и обеспечению их деятельности.

Цель аудита

Обеспечивают ли общие контроли ИТ, существующие в рамках Министерства финансов, и прикладные контроли ИС „МФАПД" точность, сохранность и надежность данных, а также безопасность и эффективность системы?

ВЫВОДЫ

Аудиторская группа рассмотрела прикладные контроли методом тестирования в главном управлении государственного долга Министерства финансов и существующие общие контроли ИТ путем непосредственного наблюдения в ГП"Fintehinform", поскольку последняя несет ответственность за управление, техническое обслуживание и эксплуатацию ИС „МФАПД". В основном прикладные контроли являются кредитоспособными и обеспечивают достаточную уверенность в надежности, точности и целостности данных ИС „МФАПД".

Некоторые общие контроли ИТ, существующие в рамках ГП "Fintehinform", недостаточно развиты, чтобы обеспечить безопасность, доступность и досягаемость ИС "МФАПД". Это не приводит к серьезной озабоченности в отношении ИС "МФАПД", так как последняя не считается критической, используясь главным образом как средство для хранения информации и анализа данных. Тем не менее общие контроли ИТ влияют на всю инфраструктуру организации. ГП "Fintehinform" является ответственной за администрирование и контроль всех информационных систем Министерства финансов, в том числе Интегрированной системы финансового менеджмента (в настоящее время в процессе реализации), которая имеет большое значение не только для министерства, но и для Правительства Республики Молдова.

Рекомендуем рассмотреть выводы данного отчета в более широком контексте, а именно с точки зрения влияния на все информационные системы Министерства финансов, находящиеся в управлении ГП "Fintehinform".

Хотя аудиторская группа была проинформирована, что готовится к сдаче в эксплуатацию новое помещение для хранения всех существующих и будущих систем, чрезвычайно важно, чтобы Министерство финансов проанализировало рекомендации этого отчета в ходе оснащения нового помещения. Если информационные системы по-прежнему будут находиться в том же помещении, придется вносить значительные изменения, чтобы обеспечить безопасность и доступ к информационным системам. Кроме того, Министерству финансов необходимо разработать, утвердить и ввести в действие ряд стратегических документов, политик и процедур в области управления и развития информационных технологий.

КОНСТАТАЦИИ

Внедрение ИС "МФАПД"

Согласно утверждениям руководства главного управления государственного долга и ГП "Fintehinform" проект по внедрению ИС "МФАПД", финансированный Программой развития Организации Объединенных Наций, стартовал в 1998 году и был завершен в 2001 году, стоимость проекта составляла 327,5 тыс. долл. США, из которых Правительство Республики Молдова оплатило 158,5 тыс. леев. В настоящее время используется версия 5.3 ИС "МФАПД", которая была запущена 8 апреля 2005. Ответственный за внедрение версии 5.3, техническое обслуживание и разработку отчетов был проект «Поддержка управления государственным долгом в Молдове», который в сентябре 2005 передал на баланс ГП "Fintehinform" сервер для работы с базой данных ИС "МФАПД" (акт приема-передачи от 15.09.2005), а на баланс Министерства финансов - 8 компьютеров и 4 принтера. Связь с приложением по учету внутреннего долга стала

возможной после запуска версии 5.3 ИС “МФАПД”, что и сделало доступным обмен информацией и регистрацию соглашений по внутреннему долгу.

В период проведения аудиторской миссии не были выявлены документы, определяющие стоимость системы и право собственности на нее, также установлено, что ИС “МФАПД” не была отражена в бухгалтерском учете министерства или ГП “Fintehinform”.

Рекомендация 1: *Предпринять меры с целью отражения в бухгалтерском учете ИС “МФАПД”.*

ПРЕДСТАВЛЕНИЕ КОНТРОЛЕЙ ИТ

Несмотря на то, что ИС “МФАПД” не является критической для деятельности Министерства финансов, все же информация, хранящееся в ней, имеет большое значение и требует надлежащего управления.

Для оценки информационных систем существуют множество различных руководств, инструкций, стандартов и наилучших практик. Они не являются обязательными, но имеют схожие принципы и если на национальном уровне не утверждены некоторые из них, то могут быть использованы те, которые лучше соответствуют потребностям. Таким образом, существуют инструкции, стандарты, прочие публикации INTOSAI (в частности Постоянного комитета по аудиту ИТ) и региональных рабочих групп. Стандарты аудита INTOSAI не являются обязательными, поскольку они отражают выбор наилучшей практики.

Соответствующие документы:

• Стандарты аудита ИТ ISACA и стандарт COBIT ITGA;

• Отчеты IIA;

• Стандарты, разработанные специализированными организациями, такими как ISACF или IFAC, COSO;

• Международные стандарты ISO, разработанные для отдельных отраслей ИТ;

• Стандарты аудита информационных технологий, утвержденные Постановлением Счетной палаты № 54 от 22.12.2009.

Общие контроли

Политики, процедуры, стандарты и организационные структуры разработаны с целью обеспечения гарантии того, что все задачи, цели и задания бизнес-процессов будут достигнуты и вместе с тем какие-либо нежелательные события будут предотвращены, исправлены или удалены. Пересмотр общих контролей ИТ представляет особый интерес, поскольку их наличие и качество непосредственно влияет на все активы, находящиеся в администрировании.

Политики и стандарты

Из политик и стандартов, используемых в соответствии с передовой международной практикой в области ИТ, Министерство финансов не обладает утвержденными следующими стратегическими документами:

• Стратегия развития ИТ;

• Оценка и управление рисками;

• План по возмещению в случае бедствий и план непрерывности действий;

• Не существует политика резервного копирования, хотя для ИС “МФАПД” резервное копирование осуществляется, используя инструкции из документации системы;

• Регистр и процедуры управления инцидентами;

• Регистр управления изменениями. Хотя с момента перехода в управление ГП “Fintehinform” ИС “МФАПД” не понесла значительные изменения, такой регистр необходим для управления любой системой;

• Некоторые требования Положения «Об обеспечении информационной безопасности в Министерстве финансов», утвержденного Приказом министра финансов №460-С от

20.08.2009, не могут быть применены в рамках ИС “МФАПД” вследствие функциональных ограничений.

После делегирования ГП “Fintehinform” полномочий и ответственности по управлению, эксплуатации и развитию всех информационных систем, эффективность общих контролей ИТ является важным фактором для Министерства финансов в обеспечении непрерывности и безопасности информационных активов. Отсутствие или недостаток некоторых стратегических документов, ненадлежащее их соблюдение или применение, представляет собой существенный риск для существующих информационных систем в процессе их развития или внедрения.

Рекомендация 2: *Разработать и утвердить необходимые политики и стратегии, а существующие пересмотреть и актуализировать.*

Отсутствуют процедуры, изложенные в письменной форме, в которых было бы указано, что требования пользователей выполнялись бы посредством закупок, разработок и системных изменений. Вместе с тем, заявления пользователей рассматриваются в соответствующем порядке.

Отсутствует письменная процедура, предусматривающая, что эффективность и производительность ИТ подлежали бы измерению, составлялась бы отчетность и рассматривались бы руководством для обеспечения своевременного исполнения, полной обработки и доступности данных. Несмотря на то, что до настоящего времени не были задокументированы случаи превышения возможностей оборудования, их появление может быть неизбежным.

Рекомендация № 3: *Разработать и ввести в действие некоторые операционные процедуры, а именно:*

• процедуры менеджмента изменений в приложениях и оборудовании, которые гарантировали бы, что любое изменение системы мониторизировано, утверждено, внедрено и может быть удалено в случае необходимости;

• процедуры адресации и решения запросов пользователей.

Рекомендация №4**:** *Для обеспечения непрерывности работы оборудования периодически пересматривать его потенциал, а в соответствии с этим анализом разработать среднесрочный и долгосрочный план по переоборудованию и закупкам.*

Физические контроли и контроли окружающей среды

Доступ в здание ограничен, на входе находится охранник. Другие физические защиты и среда находятся на низком уровне. Отсутствует система видеонаблюдения, не все необходимые окна имеют решетки, регистр посетителей ведется нерегулярно и т.д. Серверное помещение имеет много недостатков с точки зрения обеспечения физической защиты.

Посетив серверную комнату, были отмечены следующие недостатки:

- входная дверь – не металлическая, лишь покрыта жестью;
- входная дверь защищена только простым замком;
- в данном помещении проходят трубы отопления;
- отсутствуют сенсоры влажности или система анти-наводнение;
- отсутствует ложный пол, оборудование не поднято на 15-20 см от пола;
- помещение не обеспечено подачей электроэнергии от двух независимых источников из-за ограничений поставщика электроэнергии;
- отсутствуют дымовые сенсоры;
- отсутствует система видеонаблюдения;
- на окнах не установлены решетки.

Согласно утверждениям руководства ГП “Fintehinform” сетевое оборудования и сервера скоро будут переведены в новое помещение, которое отвечает всем требованиям безопасности и защиты.

Рекомендация №5: *Для улучшения ситуации, рекомендуем:*

• пересмотреть все документы по внутреннему регламентированию физической защиты и среды;

• разработать и утвердить политику в области физической безопасности среды (с соответствующими процедурами);

• устранить все недостатки и нарушения с целью обеспечения соответствующей физической безопасности и адекватной среды.

Безопасность системы и внутренний аудит

Периодический контроль регистров безопасности и регистров деятельности. Для обеспечения безопасности на всех уровнях используется различное оборудование, программы и методы: брандмауэр, антивирусная программа, ограничения доступа к сетевым приложениям и т.д.

Журналы операций используются для слежения обработки в системе, и для проверки авторизации и целостности обработки.

Средства защиты информации не настроены и не активизированы для представления событий безопасности (например, отчеты о нарушении безопасности, попытки несанкционированного доступа к информационным ресурсам). Отсутствуют автоматически или периодически сгенерированные отчеты, которые должны регулярно рассматриваться.

Для приложения "МФАПД" и ее платформы Oracle не хранятся журналы активности (логи). Тогда, когда деятельность не документирована, трудно проследить, если эта деятельность ведется согласно намерениям руководства и когда изменяется порядок осуществления деятельности. Отсутствие документации может привести к путанице и задержке в выполнении процессов. В частности, мониторинг журналов безопасности является критической деятельностью по обеспечению информационной безопасности. Если эти журналы не отслеживаются в полном объеме и в срок, могут возникнуть серьезные нарушения информационной безопасности. Согласно утверждениям ответственных лиц журналы активности не хранятся из-за низкого потенциала серверов.

Рекомендация №6: *Рекомендуем Министерству финансов идентифицировать и документировать вместе с ГП "Fintehinform" все процессы обеспечения информационной безопасности. На этой основе рекомендуем для каждого процесса, определить, какие события должны регистрироваться в системе, место хранения журналов, кем и как часто проводится мониторинг, как управлять и отслеживать любые проблемы или попытки несанкционированного доступа.*

Резервные копии. Для ИС "МФАПД" резервное копирование производится ежедневно автоматически (экспорт на сервер резервного копирования), ежемесячно производятся копии БД Oracle с архивированием и копированием в другое местоположение. Не используется процедура проверки, тестирования и утверждения резервных копий. Резервные копии хранятся около месяца.

Рекомендация №7: *Проводить периодические процедуры тестирования, проверки и утверждения резервных копий, в соответствии с установленным графиком. Резервные копии хранить в соответствии с передовой практикой в данной области.*

Политики паролей. Несмотря на то, что Положение «Об обеспечении информационной безопасности в Министерстве финансов» предусматривает ряд требований к сложности паролей, периодичности изменения и их формат, большинство пользователей ИС "МФАПД" не соблюдают эти требования. Таким образом, существуют пользователи, которые никогда не изменяли пароль к доступу, или он совпадает с именем пользователя. Были выявлены случаи, когда несколько пользователей используют одну и ту же учетную запись или один пользователь использует учетную запись другого. Такая ситуация возникает из-за невозможности установить ограничения в ИС "МФАПД" и вследствие

того, что пользователи не соблюдают требования этого положения.

***Рекомендация №8*: *Проинструктировать всех пользователей по вопросам политики безопасности и, в частности, требований к паролям. Довести до сведения «Положение по обеспечению информационной безопасности в Министерстве финансов» и осуществлять мониторинг за его соблюдением.*

Оценка информационных систем. **Департаментом внутреннего аудита не были оценены информационные системы Министерства финансов. Не оценено и не мониторизировано соблюдение политик, стандартов и процедур, что представляет собой мотив для беспокойства в части их применения.**

***Рекомендация №9**: Рекомендуем разработать и внедрить внутренние стратегические документы, с последующим их соблюдением, а на основе существующих провести оценку информационных систем.*

Отбор, рассмотрение и обучение персонала

Для доступа к ИС “МФАПД” определены три типа ролей:

• Администратор (3 сотрудника- специалисты IT);

• Оператор ввода данных (8 сотрудников- работники Главного управления государственного долга);

• Оператор-консультант, просмотр данных и свод отчетов (один сотрудник Главного управления государственного долга).

Как сотрудники, которые используют ИС “МФАПД”, так и те, которые вовлечены в администрирование системы, соответствуют должностным инструкциям и регламентам подразделений, в которых они работают. Сотрудники ГП “Fintehinform”, ответственные за администрирование и обслуживание ИС “МФАПД”, обладают знаниями, достаточными для обеспечения беспрерывной функциональности системы. В ходе внедрения ИС “МФАПД” были проведены несколько курсов обучения по использованию и управлению системой (последний курс был организован в 2007). В результате опроса лиц, которые обслуживают ИС “МФАПД” (раздел “Обучение”), четверо из опрошенных пользователей системы ответили, что не прошли обучение. Как руководство Главного управления государственного долга, так и его сотрудники проявили заинтересованность в переходе к версии 6.0 ИС “МФАПД”, которая уже доступна и предлагает больше возможностей.

***Рекомендация №10**: *Проводить периодическое обучение пользователей, с анализом существующих проблем и оказание помощи в устранении недостатков в использовании ИС “МФАПД”.*

Доступ к сети и операционной системе

Права и обязанности пользователей в сети распределяются по другому и отличаются от прав по использованию приложения. В частности, ИС “МФАПД” не интегрирована в Active Directory. Так, все рабочие станции подключены к сети и зарегистрированы в Active Directory. Это позволяет администратору управлять и осуществлять мониторинг прав каждого пользователя или групп пользователей. Как правило, пользователи имеют соответствующе ограниченные права, но существуют случаи необоснованного предоставления привилегированных прав (некоторые пользователи имеют права администратора на рабочих станциях). Вместе с тем, существуют некоторые недостатки, которые могут повлиять на информационную безопасность:

- привилегированные права, предоставленные в несоответствующем порядке *(пользователи могут инсталлировать и удалять программы, могут изменять настройки и местные политики)*. Ответственные лица ГП “Fintehinform” предприняли меры по решению данной проблемы, однако некоторые случаи еще встречаются;

- наличие сетевых ресурсов, других, кроме как папки с обменными файлами (папки с системными файлами, приложения и базы данных), с полным доступом для всех пользователей;

- часто для рабочих станций не проводится систематическое обновление ОС, тем самым не устранена уязвимость ОС, а в этом случае компьютеры находятся в непосредственной опасности заражения вирусом.

Рекомендация №11*: Пересмотреть необходимость предоставления привилегированных прав для пользователей и ограничить их адекватно.*

Рекомендация №12*: Ограничить доступ пользователей к сетевым ресурсам, пересмотреть предоставление привилегированных прав или порядка функционирования приложений для исключения их создания.*

Рекомендация №13*: Провести повторный анализ программного обеспечения, установленного на рабочих станциях, удалить пиратские версии или те, которые могут представлять риск для информационной безопасности.*

Рекомендация №14*: Предпринять необходимые действия для систематического обновления ОС на рабочих станциях.*

Прикладные контроли

Прикладные контроли являются неотъемлемой частью системы внутреннего контроля, и их наличие гарантирует, что все операции являются действительными, авторизированными и зарегистрированными. Они являются автоматизированными и характерными определенному приложению и имеют прямое воздействие на обработку отдельных операций. Основные задачи контроля достигаются в том случае, если существуют процедуры для проведения контроля полноты и точности ввода, обработки и вывода данных из системы.

Аудиторская группа проанализировала прикладные контроли ввода, обработки и вывода данных, существующие в ИС “МФАПД”, путем непосредственного наблюдения в Главном управлении государственного долга.

Контроли ввода (внесения) в систему данных предполагают рассмотрение процедур и контролей, обеспечивающих авторизацию, полноту, недублирование, аккуратность и своевременность ввода данных.

На этапе введения данных, в ходе ознакомления с ИС “МФАПД”, аудиторами были выявлены следующие контроли:

• Создание информационных сообщений о существовании кредитного идентификационного номера. Система отмечает наличие идентификационного номера.

• При выходе из интерфейса для ввода данных приложение запрашивает у пользователя подтверждение о сохранении или несохранении произведенных изменений.

• Каждый кредит состоит как минимум из одного транша. При вводе транша приложение предлагает ввести сначала общую сумму кредита. При вводе следующего транша приложение автоматически предлагает оставшуюся сумму.

• При регистрации оплаты система предупреждает, что операция завершена: одна или несколько записей выполнены и сохранены.

• Программа не допускает изменения графика уплаты, если фактические выплаты были произведены.

• Обновление обменного курса валют осуществляется через интерфейс с Национальным банком. Хотя на момент проведения аудита в системе отсутствовали данные по обменному курсу валют более чем за 10 дней, это не является слабостью приложения ИС “МФАПД”, а относится к человеческому фактору, благодаря которому запускается процесс скачивания.

• В случае отсутствия обменного курса на дату осуществления операции, система отказывает в регистрации данных.

• Система не позволяет регистрировать операцию, если некоторые поля не заполнены. Система предупреждает, если какие-то поля не заполнены.

Приложение “МФАПД” располагает достаточными интегрированными контролями,

которые автоматически проверяют, если ввод данных был выполнен аккуратно для последующего его утверждения, вместе с тем существуют некоторые аспекты, которые представляют беспокойство и должны быть удалены: **операторы имеют возможность вводить данные в классификаторы системы и в другие системные таблицы, что может повлиять на точность и сохранность данных путем дублирования или удаления записей.**

Рекомендация №15*: Пересмотреть возможность ограничения предоставления прав операторам вводить, изменять или удалять данные в классификаторах базы данных ИС "МФАПД" или предусмотреть возможность учета таких операций, с тем, чтобы исключить дублирование данных или неправильный ввод.*

Контроли обработки данных являются контролями, обеспечивающими использование правильных приложений и файлов, обработку всех данных и обновление соответствующих файлов.

В этой связи приводим следующие примеры контролей обработки данных:

• Приложение информирует пользователя об успешном выполнении внутреннего процесса.

• Система не допускает применения кредитной ставки до начала действия даты кредита.

• Система автоматически начисляет проценты по кредитам, а при досрочной оплате используется для согласования счет на оплату, выданный международной организацией.

Для имеющегося объема данных приложение "МФАПД" располагает достаточными контролями, чтобы обеспечить полноту и точность данных.

Контроли выхода (отчетности) данных являются контролями, которые обеспечивают соответствующее производство всех выходов (отчетности), их полноту и пересылку по назначению и в установленные сроки.

Кроме существующих стандартных отчетов в приложение к "МФАПД" было разработано большое количество сводных отчетов в „Excel", которые включают в себя большинство необходимых аспектов. Не все виды отчетов используются систематично. Большинство необходимых отчетов производятся в „Excel". Однако существуют некоторые отчеты, которые создаются вручную из данных других отчетов. Порядок обновления данных в отчетах „Excel" представляет беспокойство. Обобщение отчетов является довольно сложной процедурой, которая может пострадать коренным образом от человеческого фактора. Более того, сводные отчеты могут быть несанкционированно изменены, а эти ошибки могут найти отражение и в других важных отчетах, которые должны обладать высоким уровнем доверия и являться основным результатом деятельности Главного управления государственного долга.

В результате некоторые незначительные недостатки могут существенным образом повлиять на достоверность и точность информации или на отчетность, важную для деятельности Главного управления государственного долга.

Рекомендация №16**:** *Проанализировать возможность оптимизирования или автоматизирования процесса изменения отчетов при их обобщении. Предусмотреть возможность автоматизированного свода консолидированных отчетов, исключая человеческий фактор. Своевременно проанализировать возможность перехода к версии 6.0 ИС "МФАПД".*

Аудиторская группа:
руководитель аудиторской группы,
старший государственный контролер,
государственный аудитор **В. Шаргаровский**

член группы,

начальник управления **Г. Анточ**

Приложение №1