НАСТАВНИК-УЧЕНИК

Вестник Сыктывкарского университета.
Серия 1: Математика. Механика. Информатика.
Выпуск 4 (33). 2019

УДК 004.4

О МЕТОДИКЕ ПЕРЕХОДА ОРГАНИЗАЦИЙ НА НОВОЕ ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ

Ю. В. Гольчевский, В. К. Щукин

Данная работа посвящена проблеме уменьшения рисков, возникающих при переходе организации или предприятия на новое программное обеспечение, на основе выполнения последовательного комплекса мероприятий. Обсуждена необходимость этих шагов. Приведен пример апробации предложенного алгоритма.

Ключевые слова: программное обеспечение, организация, переход на новое программное обеспечение.

Введение Ранее мы уже обсуждали некоторые вопросы, связанные с проблемами информатизации современных организаций и предприятий [1]. ИТ-специалисты подчеркивают, что для современных предприятий характерно достаточно быстрое изменение информационной среды, что вызвано постоянным появлением на рынке множества новых приложений и технологий. При этом остро встает вопрос об обеспечении непрерывного бесперебойного функционирования организации на

этапе замены программных продуктов и уменьшении различных рисков, связанных с данной ситуацией [2]. Конечно, речь здесь идет не о переходе на новый офисный пакет, а о замене ключевых корпоративных систем, например систем, обеспечивающих поддержание основных бизнес-процессов, контроль обеспечения информационной безопасности и подобных.

На первый взгляд процедура замены программного обеспечения (ПО) в организации довольно проста: достаточно купить сертифицированный продукт и отдать приказ на удаление старого и установку нового ПО. На самом деле, при такой организации работы появляются угрозы, которые могут нарушить непрерывность деятельности предприятия, в частности:

– уменьшение скорости работы как отдельного ПО, так и различной вычислительной техники, а также сетевого обмена данными, вплоть до полной остановки;

– частичное или полное блокирование работы системы;

– несовместимость ранее установленного ПО с новым, что также влечет замедление или невозможность дальнейшей работы;

– появление ошибок при установке, что может привести к нарушению принятых правил разграничения доступа, повышению уязвимости системы к различного рода атакам, утечке корпоративной информации и т. п.

Чтобы предотвратить возможность наступления негативных последствий, стоит проводить процедуру замены в соответствии с определенным планом, инструкцией или алгоритмом. Поиск в открытых источниках точных инструкций по порядку перехода на новое ПО не дал

каких-либо результатов, так как данная процедура четко не регламентирована. Это обусловило необходимость самостоятельной разработки рекомендаций по порядку перевода организации на эксплуатацию нового ПО и действий непосредственно в период замены ПО.

Итак, поступает Приказ от вышестоящего должностного лица (либо организации, например для филиалов) на переход от эксплуатации одного программного продукта на другой. Желательно, чтобы в нем указывались причины изменений, сам программный продукт, который следует внедрить в организации, конкретные сроки по реализации перехода и сотрудники, на которых возлагается исполнение и контроль по переходу.

Обсудим основные аспекты методики перехода и опишем комплекс мероприятий, которые должны провести ответственные сотрудники для обеспечения бесперебойного функционирования ИТ-инфраструктуры организации.

1. Организационные мероприятия

Рекомендуется подготовить организационно-распорядительную документацию в целях соблюдения внутренних документов по обеспечению безопасного и бесперебойного функционирования ПО в организации (если, конечно, таковые имеются). Изначально требуется создать план мероприятий по выводу из эксплуатации старых программных продуктов и внедрению новых. В нем нужно описать конкретные меры, которые требуется исполнить для вывода старого ПО. В частности, отмена документов, связанных с эксплуатацией выводимого продукта, изменение настроек сетевого доступа для ПО, изменение конфигурационных файлов, отключение учетных записей и прочее. После плана ме-

роприятий для нового продукта создается новая документация, которая будет регулировать работу сотрудников и самого ПО, взаимодействие сотрудников, их доступ к управлению продуктом, соответствующие руководства и инструкции, необходимые при работе. Примерный перечень выглядит следующим образом:

– приказ о назначении администраторов и контролеров ПО в данной организации;

– акт установки и ввода в эксплуатацию ПО;

– конфигурация ПО;

– матрица доступа к ПО;

– руководство по установке и настройке ПО применительно к средствам вычислительной техники (СВТ) данной организации;

– инструкция по проведению контроля;

– инструкция для персонала;

– инструкция по идентификации / аутентификации (создается новая или дорабатывается старая с учетом изменений);

– руководство по настройке дополнительных функций стороннего ПО (при отсутствии использования на каких–либо СВТ данного продукта);

– перечень СВТ, на которых необходимо осуществить переход на новое ПО, с отметками о выполнении.

Переход на новое ПО также требует выделения дополнительных ресурсов (финансовых, людских, технических и т. д.), что необходимо тщательно спланировать.

2. Обучение сотрудников

Для повышения качества и безопасности перехода в организации и

расширения осведомленности ее сотрудников о вводе нового ПО следует проводить соответствующее обучение.

Для администраторов и контролеров ПО рекомендуется проводить обучение в части установки, настройки и администрирования продукта в специализированных учебных центрах. Причем провести обучение таких сотрудников следует максимально оперативно, по возможности еще до активного внедрения нового продукта, когда исполнители только начинают разрабатывать организационно-распорядительную документацию и могут после обучения внести корректировки. В общем случае рекомендуется выделить на это не более двух недель.

Для остальных сотрудников, которые выполняют роль пользователей ПО, можно проводить обучающие мероприятия в форме презентации или видеокурсов на самом предприятии. Также полезно создать отдельную памятку или инструкцию по правилам пользования ПО. Данное мероприятие следует проводить с сотрудниками, у которых планируется замена ПО за несколько дней, при этом само обучение в организации длится на всем этапе перехода частями.

3. Технические мероприятия

Для понимания того, как интегрируется новое ПО в корпоративные системы, какие проблемы при этом возникают и каковы пути их решения, а также для дальнейшей подготовки таких организационно–распорядительных документов, как «Конфигурация ПО», «Матрица доступа к ПО», доработки «Руководства по установке и настройке», «Инструкции по проведению контроля» и т. д., требуется создать тестовый стенд, моделирующий инфраструктуру предприятия. На таком стенде можно провести испытание нового продукта в инфраструктуре

предприятия. На его развертку требуется выделить необходимое оборудование и сотрудника из числа исполнителей проекта перехода, который производит сборку, первоначальную установку и настройку нужных компонентов инфраструктуры и ПО.

Стенд позволяет еще до ввода продукта в эксплуатацию предварительно выявить и решить появившиеся проблемы, провести проверку совместимости ПО, интеграции с другими системами, продумать возможности передачи данных между внедряемой и функционирующими системами, подготовить файлы–шаблоны, которые могут понадобиться для проведения контроля и т. д.

В организации может эксплуатироваться достаточно большое количество различных вычислительных устройств, для которых следует провести описанные мероприятия. Это обусловливает необходимость отслеживания информации о них, что может быть достаточно трудоемко. К тому же новая информация о них может фигурировать и в других документах в организации. Для решения этой проблемы можно порекомендовать исследовать вопрос выполнения автоматизации таких процедур. Проведение процесса следует проводить с использованием ПО, установленных на СВТ ранее, либо с установкой нового ПО, если это не противоречит внутренним организационно–распорядительным документам в части безопасности СВТ.

С учетом вышеизложенных рекомендаций примерное планирование процесса перехода может выглядеть так, как представлено на рис. 1.

Резюмируя, представить рекомендуемый метод перехода можно в виде SADT-диаграммы, показанной на рис. 2.

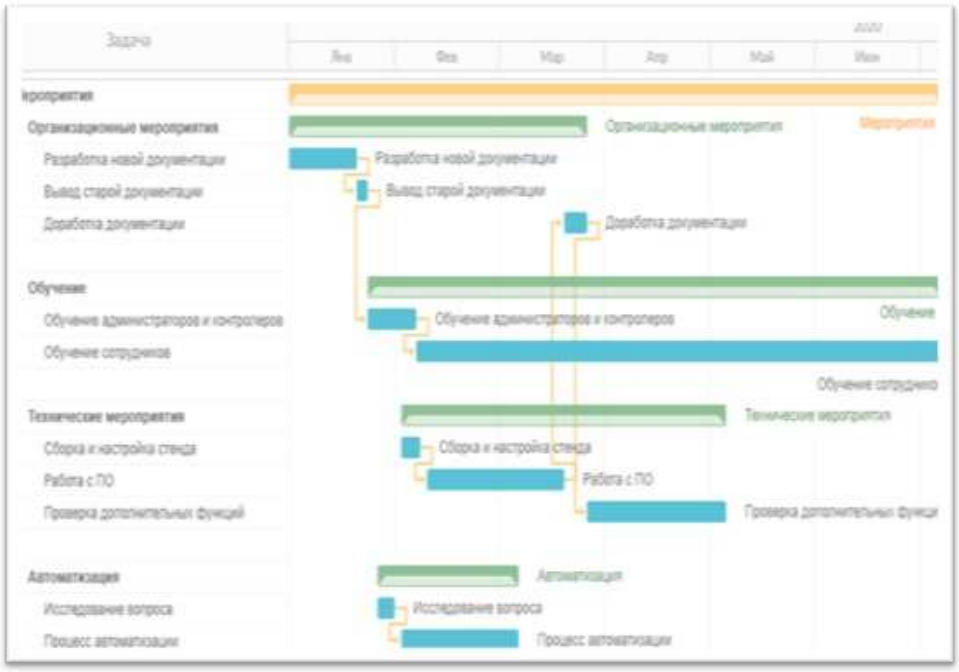

Рис. 1. График перехода на новое программное обеспечение

Апробация

В соответствии с изложенным выше алгоритмом была проведена апробация некоторых мероприятий на примере отказа от DLP DeviceLock, СЗИ от НСД Secret Net и Паспорт АРМ и перевод на эксплуатацию Secret Net Studio — комплексное решение для защиты рабочих станций и серверов на уровне данных, приложений, сети, операционной системы и периферийного оборудования [3] и дополнительные функции для антивируса Kaspersky Endpoint Security в одной из достаточно крупных организаций Республики Коми, имеющей в своей структуре пятнадцать подразделений и свыше четырехсот различных вычислительных средств.

Апробация проводилась в очередности, отличающейся от представ-

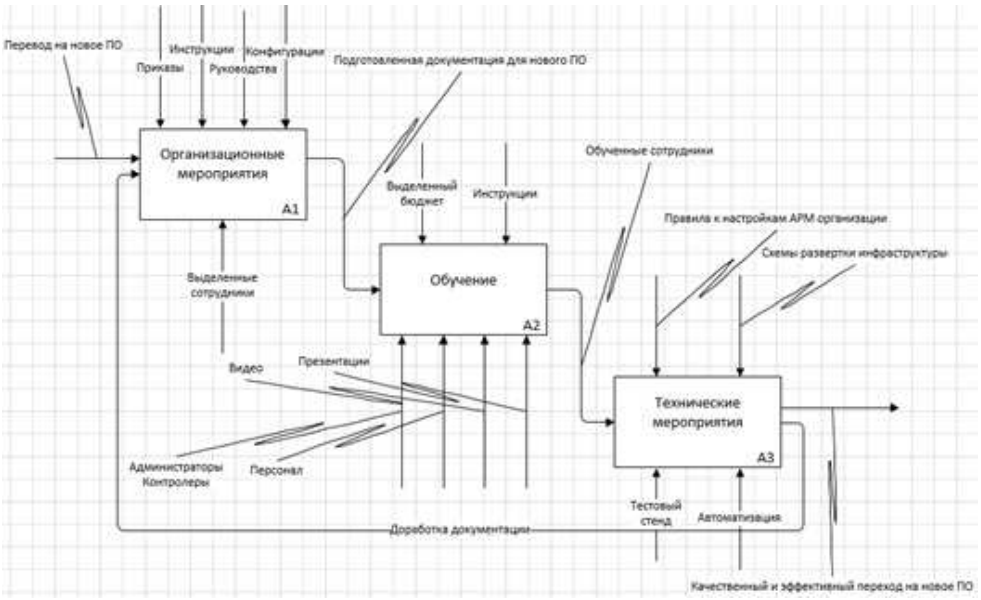

Рис. 2. SADT-диаграмма, представляющая переход организации на новое ПО

ленной выше, так как в описываемом случае ключевыми были именно технические мероприятия и затем уже остальные. Остановимся более подробно на некоторых результатах.

Тестовый стенд был создан на базе двух компьютеров и коммутатора: первый компьютер имитировал пользователя на базе операционной системы семейства Windows, на втором средствами виртуализации были развернуты два сервера под управлением операционной системы Windows Server 2012 (рис. 3).

На одном сервере была добавлена роль контроллера домена и с помощью служб Active Directory созданы пользователи, необходимые в дальнейшем для отработки сценариев работы нового программного продукта в корпоративной сети. На другом сервере были установлены компоненты Net Framework, реляционная база данных SQL Server 2012 и

Рис. 3. Схема тестового стенда

развернут Сервер безопасности Secret Net Studio.

Далее была произведена удаленная установка агентов и настроены Политики безопасности в соответствии с внутренними документами организации. На компьютере пользователя было установлено необходимое ПО, которое используется на каждом рабочем месте (каждой роли) в организации, и проверена корректность работы с новым ПО. Дополнительно были добавлены и настроены различные электронные идентификаторы и устройства, которые используются при работе на предприятии.

После выполнения описанных выше действий на стенде появляется возможность выполнять ряд процедур, которые нужно протестировать перед вводом в эксплуатацию Secret Net Studio. Таким образом были

отработаны типовые ситуации в части «Администрирования», «Журналирования» и «Проведения аудита» для раздела Контроль устройств, а также проведено тестирование функции Паспорт ПО.

Данная отработка сценариев позволила еще на этапе ввода в эксплуатацию нового ПО заранее проверить, насколько оно удовлетворяет потребностям организации и превосходит (либо не превосходит) уже имеющееся и эксплуатируемое на данный момент ПО. Это позволило определиться с правами для контролеров, подготовить файл-выборки при проведении внутреннего контроля с использованием ПО, заранее продумать и решить проблемы тех сценариев, которые оно выполнять не может.

В ходе замены программного продукта возникла потребность во внесении достаточно значительных изменений в работу компьютеров, которые не подключены к централизованной системе. Отказ от одного продукта не подразумевает обязательной установки другого. В таком случае дополнительно должны быть предусмотрены сценарии для решения подобного рода проблем. В описанном случае потребовалось включить дополнительные функции на Kaspersky Endpoint Security [4]. И в связи с этим потребовалось разработать инструктивно-методический материал — «Руководство для администраторов информационной безопасности по настройке блокировки доступа к устройствам». Данное руководство включает в себя полное описание общей настройки Контроля устройств, настройки журналирования и создания «белого» списка.

Для организации и планирования перехода на новое программное обеспечение необходимо обладать актуальной информацией об используемых технических средствах и статусе их перевода на новое ПО.

В ходе выполнения описываемых мероприятий возникла необходимость реализовать автоматизированный сбор данных об используемых технических средствах. Был создан Справочник типизируемых данных, который позволяет сотрудникам вносить данные, которые при последующем использовании удобно фильтровать и сортировать. Добавлены функции условного форматирования и логические правила, позволяющие уменьшить вероятность ошибки при заполнении документов и наглядно показать, где информация еще не введена. Также была доработана система сбора и обобщения информации о технических средствах через соответствующие настройки запросов и генерации сводных таблиц.

Заключение

Предложенная методика зарекомендовала себя как практически полезная при организации перевода достаточно большого предприятия на эксплуатацию нового программного продукта. Ее применение позволило обеспечить в организации высокий уровень безопасности функционирования структурных подразделений организации на этапе перехода, наладить и сделать более эффективным сам процесс перехода при помощи автоматизации, решить появившиеся в ходе апробаций проблемы.

Список литературы

1. **Гольчевский Ю. В., Малдрик А. В.** Пять шагов на пути к эффективной информатизации предприятия // *Прикладная информатика. 2013. № 3(45). С. 23–35.*

2. **Торосян Е. К., Торопчинова А. Д.** Вопросы управления рисками IT-проектов при переходе на новое программное обеспечение в современных условиях // *Петербургский экономический журнал. 2018. № 3. С. 105–109.*

3. Secret Net Studio [Электронный ресурс] «Код безопасности» URL: https://www.securitycode.ru/products/secret–net–studio/ (дата обращения: 16.06.2019).

4. Kaspersky Endpoint Security for Windows [Электронный ресурс] «Энциклопедия фан–клуба Лаборатории Касперского». URL: https://forum.kasperskyclub.ru/wiki/Kaspersky_Endpoint_Security_for_Windows (дата обращения: 16.06.2019).

Summary

Golchevskiy Yu. V., Schukin V. K. The enterprise transition method to new software operation

The paper is devoted to the problem of reducing risks arising during the enterprise transition to new software operation, based on the implementation of a consistent set of measures. The necessity of these steps is discussed. An example of testing the proposed algorithm is given.

Keywords: software, organization, transition, product, enterprise transition to new software operation.

References

1. **Golchevskiy Yu. V., Maldrik A. V.** Pyat' shagov na puti k effektivnoy informatizatsii predpriyatiya (Five steps to effective

enterprise informatization), *Prikladnaya informatika (Applied Informatics)*, 2013, No 3(45), pp. 23–35.

2. **Torosyan Ye. K., Toropchinova A. D.** Voprosy upravleniya riskami IT-proyektov pri perekhode na novoye programmnoye obespecheniye v sovremennykh usloviyakh (Risk management issues of IT-projects during the transition to new software in modern conditions), *Peterburgskiy ekonomicheskiy zhurnal (Petersburg Economic Journal)*, 2018, No 3, pp. 105–109.

3. Secret Net Studio. URL: https://www.securitycode.ru/products/secret–net–studio/ (date of the application: 16.06.2019).

4. Kaspersky Endpoint Security for Windows. URL: https://forum.kasperskyclub.ru/wiki/Kaspersky_Endpoint_ Security_for_Windows (date of the application: 16.06.2019).

Для цитирования: Гольчевский Ю. В., Щукин В. К. О методике перехода организаций на новое программное обеспечение // *Вестник Сыктывкарского университета. Сер. 1: Математика. Механика. Информатика. 2019. Вып. 4 (33). С. 55–67.*

For citation: Golchevskiy Yu. V., Schukin V. K. The enterprise transition method to new software operation, *Bulletin of Syktyvkar University. Series 1: Mathematics. Mechanics. Informatics*, 2019, 4 (33), pp. 55–67.

СГУ им. Питирима Сорокина *Поступила 08.11.2019*