

Министерство внутренних дел Российской Федерации

**Федеральное государственное казенное
образовательное учреждение высшего образования
«Орловский юридический институт
Министерства внутренних дел Российской Федерации
имени В.В. Лукьянова»**

**ТЕКУЩЕЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ
ВНЕДРЕНИЯ ОБЛАЧНЫХ ОФИСНЫХ
РЕШЕНИЙ В ДЕЯТЕЛЬНОСТИ ОВД**

Учебно-практическое пособие

**Орёл
ОрЮИ МВД России имени В.В. Лукьянова
2021**

УДК 004
ББК 32.97
Т30

Рецензенты:

В.Б. Гунько, кандидат технических наук, доцент
(Ростовский юридический институт МВД России);
А.Т. Белоусов
(ЦАФАПОДД ГИБДД УМВД России по Орловской области)

Т30 **Текущее состояние и перспективы внедрения облачных офисных решений в деятельности ОВД : учебно-практическое пособие / Л.Д. Матросова [и др.]. – Орел : ОрЮИ МВД России имени В.В. Лукьянова, 2021. – 45, [1] с. – 40 экз. – Текст : непосредственный.**

В работе проанализированы инструменты, позволяющие организовать совместную работу над документами в режиме реального времени. Внедрение подобных инструментов позволит значительно повысить эффективность коллективной работы в деятельности органов внутренних дел.

В условиях импортозамещения и перехода на свободное программное обеспечение необходимо внедрять современные офисные решения, которые включают в себя облачные технологии. Для этого в учебно-практическом пособии предложен необходимый методический инструментарий, позволяющий осуществлять развертывание подобных решений в масштабе МВД России.

Учебно-практическое пособие предназначено для сотрудников МВД России, преподавателей, курсантов, слушателей, адъюнктов.

Издание представлено в авторской редакции.

УДК 004
ББК 32.97

© ОрЮИ МВД России имени В.В. Лукьянова, 2021

Оглавление

Введение	4
1. Развитие свободного программного обеспечения и совершенствование системы электронного документооборота в системе МВД России.....	5
2. Анализ возможностей офисных онлайн-редакторов.....	14
3. Развертывание облачного офисного решения на базе ведомственной сетевой инфраструктуры	26
Заключение	44
Список используемой литературы	45

Введение

Развитие современных информационных и телекоммуникационных технологий направлено на создание новых возможностей и подходов к доступу и обработке информации. В последнее время объемы создаваемой, обрабатываемой и передаваемой информации растут в геометрической прогрессии. Новые инструменты и возможности диктуют и новые требования, предъявляемые к процессам документирования управленческой деятельности. Практически во всех сферах государственного управления отмечается значительный рост документопотоков, что создает дополнительную нагрузку на исполнителей.

В органах внутренних дел постоянно осуществляется внедрение новых информационных технологий, а профессиональная деятельность уже в достаточно высокой степени автоматизирована. Одним из последних значительных шагов по информатизации явилось внедрение сервиса электронного документооборота (СЭД). Основной сложностью, которая возникла при внедрении, была необходимость использования достаточно большого количества вычислительных ресурсов, т.к. поток обрабатываемой органами внутренних дел документации предполагает сложную организацию информационной системы обеспечивающей электронный документооборот. Отдельной задачей являлось обеспечение безопасного хранения документов и одновременной комфортной работы большого количества пользователей.

Внедрение СЭД – это важный шаг, который еще раз доказывает преимущества информационных систем, построенных на базе облачных технологий. Доступ к системе осуществляется через веб браузер, которые установлены на всех современных компьютерах, таким образом для обеспечения работы системы не требуется установка и регулярные обновления программного обеспечения на клиентских компьютерах.

Однако СЭД в системе МВД России обеспечивает только регистрацию, движение и хранение документов, а работы по их созданию и редактированию осуществляются средствами Microsoft Office или иных установленных офисных пакетов.

При подготовке учебно-практического пособия авторы преследовали цель составить целостное представление о современных возможностях офисных программных решениях использующих облачные технологии, их возможностях и перспективах и специфике внедрения в практическую деятельность МВД России.

1. Развитие свободного программного обеспечения и совершенствование системы электронного документооборота в системе МВД России

В настоящее время большая часть создаваемых и обрабатываемых в органах внутренних дел документов осуществляется в электронном виде. Это значительно сокращает количество времени, необходимое на их подготовку, и позволяет осуществлять более удобное хранение. Однако вместе с внедрением новых технологий и достаточно высокой степенью информатизации профессиональной деятельности изменились и требования, предъявляемые к документированию управленческой деятельности в МВД России, что привело к значительному росту документооборота в целом.

Началось обсуждение вопросов и перспективных возможностей внедрения электронного документооборота (ЭДО). Основной сложностью была необходимость использования достаточно большого количества вычислительных ресурсов, т.к. поток обрабатываемой органами внутренних дел документации предполагает сложную организацию информационной системы электронного документооборота. Кроме того, отдельной задачей являлось обеспечение безопасного хранения документов и одновременной комфортной работы большого количества пользователей.

Основным толчком к централизованному созданию СЭД стало Постановление Правительства РФ от 06.09.2012 № 890 «О мерах по совершенствованию электронного документооборота в органах государственной власти», которое предусматривало завершить в 2015 году переход на обмен электронными документами при взаимодействии федеральных органов исполнительной власти между собой и с Правительством Российской Федерации. В связи с этим в МВД России в 2014–2016 годах осуществлялись работы по внедрению и пилотные запуски СЭД в субъектах Российской Федерации, а фактическое внедрение системы состоялось в конце 2016 года с внесением изменений и дополнений в Приказ МВД России от 20.06.2012 № 615 «Об утверждении Инструкции по делопроизводству в органах внутренних дел Российской Федерации», которые установили основные положения, касающиеся особенностей работы с электронными документами в системе МВД России.

Внедрение СЭД было направлено на реализацию ряда организационно-управленческих задач, большая часть которых была успешно решена. В настоящий момент можно уже с уверенностью говорить о положительном эффекте от внедрения СЭД в части, касающейся сокращения сроков обмена документами между подразделениями МВД России, так как теперь документы оперативно поступают в отделения делопроизводства и режима (ОДиР), что позволяет организовать их более качественное и своевременное исполнение. Значительно упростился процесс поиска документов по различным реквизитам в базе данных системы, кроме того, данная функ-

ция теперь доступна для самостоятельного выполнения большому количеству пользователей. Улучшились и логистические процессы в удаленных подразделениях, где отсутствуют собственные ОДиР. Теперь в большинстве случаев исполнителю не нужно расходовать дополнительное время на физическую доставку документа.

Также в положительную сторону следует выделить механизм согласования документа, который позволяет сократить время, обычно затрачиваемое на ожидание рассмотрения руководителями. Подписание документов электронной подписью гарантирует достоверность и целостность документа в течение всего маршрута его прохождения, а хранение в электронном виде фактически решает проблему утери документа и делает документооборот более прозрачным. Одной из важных положительных сторон создания СЭД на федеральном уровне является его доступность из любого подразделения или региона, где есть доступ к Единой системе информационно-аналитического обеспечения деятельности (ИСОД) МВД России, что в ряде случаев позволяет быстро решать оперативные задачи и применять новые подходы к организации работы.

Помимо положительных сторон процесс внедрения СЭД в профессиональную деятельность региональных подразделений МВД России выявил и ряд проблем как организационного характера, так и в построении самой системы. Так, в настоящее время ОДиР региональных подразделений органов внутренних дел фактически осуществляют дублирование документооборота в бумажном и электронном виде.

Это происходит по следующим причинам:

- недоверие руководителей и сотрудников ОДиР к надежности и стабильности работы системы. Высокая степень ответственности за сроки исполнения документов и периодические задержки в работе сервиса пока не дают достаточной уверенности в целесообразности полного перехода на обработку документов в электронном виде.

- отсутствие у некоторых исполнителей автоматизированных рабочих мест (АРМ) и доступа к ИСОД МВД России. Выполнение работ по исполнению осуществляется в традиционном бумажном виде, а ОДиР уже принимают, сканируют и регистрируют документы в СЭД.

Следует отметить, что эти проблемы носят общий характер и присущи не только системе МВД России. Так, отдельные авторы отмечают, что развитие федеральной законодательной базы в области электронного документооборота пока явно недостаточное, что сдерживает переход к широкому использованию электронных документов. Для текущей работы в организации используются электронные версии документов, а для рассылки и передачи в архивное хранение – их бумажные подлинники.

По мнению С.И. Конева, основная проблема оборота электронных документов заключается в том, что в российских подзаконных актах в настоящее время сохраняются и прямые требования, предписывающие ис-

пользование традиционных бумажных документов, целесообразность которых объясняется только тем, что бумажный документ может быть прочитан без использования дополнительной техники, а с сообщениями, полученными при помощи электронной связи, можно ознакомиться лишь на экране компьютера или после распечатки на бумаге.

Кроме того, Е.К. Волчинская выделяет следующие проблемы, присущие хранению данных в целом:

1. Срок действия ключа электронной подписи (ЭП). Для того, чтобы электронный документ, подписанный ЭП, сохранил юридическую силу в течение срока действия электронного документа, необходимо нормативно закрепить правила оценки юридической силы электронного документа при недействительном сертификате ключа проверки подписи.

2. Изменение программно-технических средств воспроизведения электронных документов. Документы, созданные с использованием устаревшего программного обеспечения, если и возможно будет воспроизвести и прочитать, то не любыми средствами и с существенными искажениями. Средства создания, обработки, хранения информации активно модифицируются, поэтому проблемы технической несовместимости форматов, кодировок и иных элементов электронных документов (электронной информации) отнюдь не надуманы.

Ряд авторов считает, что только полноценное архивное образование может обеспечить адекватное взаимодействие с этой средой. Архивное знание уже не национальное, оно носит глобальный характер и становится все более зависимым от направлений развития технологий и требований рынка.

Таким образом, поверхностный взгляд на положительные стороны внедрения ЭДО в большинстве случаев не учитывает указанные выше проблемы, препятствующие полному переходу на создание и обработку документов исключительно в электронной форме. Для их решения необходимо принимать ряд мер организационного характера и требуется внесение изменений в действующие нормативно-правовые акты, регламентирующие порядок и механизмы работы с документами.

Представляется, что продолжить совершенствование управленческой деятельности в подразделениях МВД России и оптимизацию процессов решения практических задач необходимо по следующим направлениям:

1. Сокращение объема обрабатываемых документов. Так, по мнению А.А. Гостева, единственным существенным ресурсом сокращения объемов переписки остается общее делопроизводство, то есть число организационно-распорядительных документов, возникающих в ходе документационного обеспечения отдельных элементов управленческого цикла (планирования, организации, анализа, контроля, оценки, работы коллегиальных органов). По разным причинам не все документы в данной сфере подготовлены исходя из объективной необходимости и обладают должным управленче-

ским эффектом. Н.С. Шамков отмечает, что проблема сокращения внутренней переписки путем использования только одних электронных технологий без оптимизации действующих механизмов осуществления управленческих функций трудно разрешима, поскольку, как представляется, простая замена бумажного носителя на электронный может повысить оперативность взаимодействия структурных подразделений, однако не сможет оказать существенного влияния ни на сокращение объема документооборота (в том числе электронного), ни на высвобождение работников от излишних затрат служебного времени, являющихся основными показателями повышения эффективности системы управления. Одним из решений данной проблемы может послужить автоматизация создаваемых отчетов, которые сотрудники вышестоящих органов внутренних дел могут формировать самостоятельно с использованием существующих автоматизированных информационных систем, а не запрашивать с территориальных подразделений.

2. Необходимо провести работу по организации ведения ряда журналов и учетов полностью в электронном виде. До сих пор в практических подразделениях существует большое количество подобного рода бумажных документов. Многие носят формальный характер, но отказаться от их ведения невозможно, так как это регламентировано соответствующими нормативными документами. Целесообразно перевести такие документы полностью в электронный вид, т.к. даже перебои в работе сервиса не будут оказывать существенного влияния на данную работу.

3. При дальнейшем развитии СЭД МВД России необходимо учитывать специфику перехода органов государственной власти на использование свободного программного обеспечения и на формат хранения данных в соответствии с ГОСТ Р ИСО/МЭК 26300-2010 «Информационная технология. Формат Open Document для офисных приложений (OpenDocument) v1.0», который описывает формат хранения документов, образующихся и используемых в деятельности органов государственной власти.

4. Организовать использование веб-приложений, осуществляющих функции онлайн редакторов документов. Внедрение подобного программного обеспечения в состав СЭД позволит решить сразу несколько задач. Во-первых, задачу унификации хранения и объема хранимого содержимого. В настоящий момент большинство передаваемых документов хранятся в виде изображений и занимают гораздо больше места, чем если бы они хранились в текстовом формате. Это создает дополнительную нагрузку на каналы связи и систему в целом. Во-вторых, задачу создания и хранения типовых форм и бланков документов, которые будут сразу доступны сотрудникам (сейчас многие приходится составлять самостоятельно). После заполнения таких документов целесообразно внедрение логического контроля в целях избежания типичных ошибок и их автоматизированной проверки на соответствие нормативным документам. В-третьих, данные си-

стемы позволяют организовать и внедрить новые формы совместной работы над документами в режиме реального времени. Такие технологии в настоящий момент в системе МВД России практически не применяются, но при правильном использовании могут в несколько раз повысить время подготовки документа. Если сейчас при необходимости совместной работы создание документов происходит последовательно, и одному исполнителю приходится ждать, пока закончит работу другой, то при использовании данной функции система позволит производить работу параллельно.

5. Совершенствование системы организации и контроля за исполнением документов. В целях избежания проблемы несвоевременной передачи документа исполнителю требуется совершенствование организации работы с документами. Нередко возникают ситуации, когда документ отписывается уже после окончания срока его исполнения, и сотрудник оказывается виновным в несвоевременном исполнении. Кроме того, необходима более тесная интеграция контрольных функций в интерфейс делопроизводителя, автоматическое снятие документов с контроля после их исполнения и подписи руководителя.

6. Урегулировать порядок действий исполнителей и ОДиР в случаях отказа работы системы. Одной из главных причин, по которой отделения делопроизводства продолжают осуществлять ведение ряда документов в бумажном виде, является отсутствие регламентации и порядка их действий в случае сбоя системы. В настоящий момент, если произошел сбой, и сотрудник несвоевременно исполнил документ, вина фактически ложится на него. Во избежание этого ОДиР продолжают осуществлять ведение документации на бумажном носителе, а работа в СЭД во многих случаях просто является дополнительной нагрузкой. Необходимо определить порядок действий сотрудников и перечень ситуаций, при которых сбои являются удовлетворительной причиной несвоевременного выполнения отдельных функций.

7. Произвести более тесную интеграцию отдельных функций СЭД в другие информационные системы МВД России. В настоящее время осуществляется ведение большого количества учетов и баз данных. При добавлении и изменении сведений в подобных системах в большинстве случаев не осуществляется применение ЭП, а аутентичность предоставляемых сведений имеет критическое значение, например, при необходимости ответа на запрос о предоставлении физическому лицу какой-либо информации. Так, по мнению В.Ф. Макарова и Б.А. Торопова, проблема заключается в том, что этот ответ не может быть подписан юридически значимой электронной подписью. Ведь такая подпись неотъемлема от конкретного физического лица. Сложно требовать, например, от администратора базы данных подписания всего ее содержимого, т.е. принятия на себя ответственности за достоверность содержащихся в базе сведений.

Таким образом, когда обсуждаются вопросы информатизации, всегда находятся как сторонники, так и противники данных решений, потому что в некоторых ситуациях какие-то процессы улучшаются, а другие приходится перестраивать или ломать. Представляется, что при внедрении и дальнейшем развитии СЭД, необходимо сначала обратить внимание на процессы, требующие оптимизации, а уже потом переходить к автоматизации более сложных управленческих задач. Кроме того, больше внимания следует уделять обучению сотрудников и разработке максимально точных инструкций и методических указаний, которые будут помогать в работе и не будут оставлять сотрудника один на один с возникшей проблемой.

Свободное программное обеспечение представляет собой достаточно безопасную, надежную и финансово-привлекательную платформу для построения информационных систем. Использование свободного программного обеспечения позволяет:

- обеспечить технологическую независимость разработки и использования программного обеспечения независимо от аппаратной платформы;
- снизить начальную стоимость оборудования;
- сократить время необходимое для исправления выявленных дефектов, а также плату за использование программных продуктов.

Идеологию открытых систем реализуют в своих последних разработках все ведущие фирмы-поставщики средств вычислительной техники, передачи информации, программного обеспечения и разработки прикладных информационных систем. В настоящее время принцип использования открытых систем является одним из основных направлений развития в области информационных технологий. Кроме того, данный процесс оказывает существенное влияние на средства вычислительной техники и поддерживающей инфраструктуры.

В то же время СПО не является заменой для проприетарного программного обеспечения и может широко использоваться для государственных, региональных и муниципальных нужд наряду с ним. При этом одним из основных условий является доступность исходного текста программы и возможность внесения в него, при необходимости, модификаций и исправлений

Цели создания и применения СПО направлены на формирование рынка программного обеспечения со свободной контрактацией двух сторон - поставщика и приобретателя таких услуг как копирование, тиражирование, модификация, добавление функциональности и т.п. При этом не участники рынка не апеллируют к третьей стороне.

Разрабатываемое СПО должно соответствовать таким критериям как:

- возможность свободного использования пользователем в любых, не запрещенных законом Российской Федерации целях;
- возможность изучения программного кода и его последующей переработки пользователем для достижения своих целей;

– возможность свободного распространения переработанной версии.

Примерами самых известных свободных программ являются: широко распространенный веб-сервер Apache, развивающаяся операционная система GNU/Linux, полнофункциональный офисный пакет OpenOffice.org, браузер Mozilla Firefox, операционная система FreeBSD. На свободном программном обеспечении работают поисковые системы Google и Yandex. В таких странах как Франция, Бразилия, Испания, Китай и др. свободное программное обеспечение используют также на государственном уровне.

Для большинства пользователей привычной и стандартной является схема использования несвободного или как еще его называют – проприетарного ПО (англ. proprietary software): на каждую устанавливаемую копию программного продукта приобретается лицензия, часто также ограниченная по сроку действия. СПО предоставляет пользователям право устанавливать сколько угодно большое число копий программы, работать с ней без каких-либо ограничений, без необходимости платить при этом за лицензии. Такой порядок использования СПО является вполне легальным и регулируется специальными свободными лицензиями.

Вариантов свободных лицензий великое множество, но наиболее распространенной и широко используемой из них является GNU General Public License (GNU GPL). Именно ее мы проанализируем с точки зрения соответствия российскому законодательству.

Использование свободного программного обеспечения наряду с отечественным проприетарным программным обеспечением – наиболее эффективный путь создания российской программной платформы, которая может стать основой возрождения отечественной отрасли программирования.

Использование программного обеспечения как объекта авторского права регулируется в четвертой части ГК РФ. В частности, в ст. 1286 ГК РФ раскрывается понятие лицензионного договора: «Заключение лицензионных договоров о предоставлении права использования программы для ЭВМ или базы данных допускается путем заключения... договора присоединения, условия которого изложены на приобретаемом экземпляре... программы... либо на упаковке этого экземпляра. Начало использования такой программы... означает его согласие на заключение договора».

Лицензия GPL соответствует определению договора присоединения, данному в ГК РФ. В этом смысле порядок ее использования аналогичен привычному нам лицензионному соглашению с конечным пользователем (End-User License Agreement (EULA)) на несвободное программное обеспечение. Таким образом, порядок применения свободной лицензии мы можем описать в терминах российского законодательства. Для подтверждения законности использования СПО необходимо, чтобы свободная лицензия соответствовала требованиям к лицензионному договору, опреде-

ленным в ГК РФ. И тут возникает ряд неоднозначностей, которые, тем не менее, не являются неразрешимыми.

Использование свободного программного обеспечения с соблюдением условий соответствующей версии лицензии GNU GPL соответствует требованиям законодательства Российской Федерации об авторском праве и является правомерным. Разработка пакета свободного отечественного программного обеспечения является одной из центральных задач, которая необходима для обеспечения информационной безопасности России.

С 1 января 2012 года вступил в силу ГОСТ Р 54593-2011 «Информационные технологии. Свободное программное обеспечение. Общие положения».

В феврале 2015 года на конференции разработчиков свободной СУБД PostgreSQL Минкомсвязи сообщило о планах финансово поддержать миграцию российских госорганов на свободное ПО. «Мы будем поддерживать грантами НИР (научно-исследовательские работы – прим. CNews), которые позволяют осуществлять переход на СПО», – сказал министр связи Николай Никифоров.

Вскоре был утвержден приказ Минкомсвязи России от 19.08.2015 № 305 «Об утверждении Методических рекомендаций по использованию свободного программного обеспечения в деятельности федеральных органов исполнительной власти, включая критерии определения государственных информационных систем, при создании которых необходимо использовать свободное программное обеспечение, в том числе государственных информационных систем, предназначенных для оказания государственных и муниципальных услуг в электронном виде».

Отечественная компания НПО «РуБИТех» осуществила работы по созданию специализированного и «защищенного» дистрибутива на базе Linux, ориентированного на использование в государственных организациях и силовых структурах. Данный продукт получил название Astra Linux. Дистрибутив версии Special Edition позволяет работать со сведениями под грифом «совершенно секретно», а также имеет на это сертификаты Минобороны, ФСБ и ФСТЭК.

Свободное программное обеспечение способно решать задачи государственного масштаба.

Яркими примерами корпоративных пользователей свободного программного обеспечения могут служить Министерство обороны, Федеральная служба охраны, Федеральная служба судебных приставов, государственные корпорации Ростех и Росатом, где планомерно внедряется программное обеспечение на основе открытого ПО.

Опыт внедрения решений на базе ОС Astra Linux показывает, что зависимость от зарубежных проприетарных продуктов обусловлена в первую очередь требованиями ведомственных и отраслевых стандартов. Внесение изменений в эти стандарты и приобретение организациями необ-

ходимых компетенций позволит широко использовать свободное и отечественное программное обеспечение, что позволит существенно снизить долю зарубежного проприетарного ПО.

Система Astra Linux представляет собой целое семейство операционных систем предназначенных для различных аппаратных платформ, а также инфраструктуру программного и аппаратно-программного обеспечения, которое для этих операционных систем разрабатывают отечественные компании и независимые разработчики. Например, такие релизы как «Орел» (x86-64), «Смоленск» (x86-64), «Новороссийск» (ARM), «Мурманск» (Z/Architecture), «Керчь» (Power) и «Севастополь» (MIPS).

Система Astra Linux представляет собой яркий пример импортозамещения «снизу», так как формирование требований и выделение ресурсов производится исключительно коммерческими компаниями без привлечения государственных средств. При этом стоит обратить внимание на тот факт, что пользователи Astra Linux применяют как результаты труда огромного количества независимых разработчиков СПО в мире и в России, так и продукцию отечественных компаний.

В настоящее время компания разработчик предлагает доступную для скачивания и использования пользователями бесплатную версию ОС Astra Linux Common Edition, которая практически полностью соответствует платной ОС Astra Linux Special Edition за исключением некоторых встроенных средств информационной защиты, предназначенных для обработки информации ограниченного доступа, применение которых требует сертификации. В случаях неудовлетворенности программами входящими в состав дистрибутива пользователь может легко подключить огромный репозиторий Debian, совместимость с которым обеспечивается производителем в целях расширения функциональных возможностей.

2. Анализ возможностей офисных онлайн-редакторов

В настоящее время идет процесс активного развития программного обеспечения для создания и работы с документами. Помимо традиционных офисных пакетов, включающих в себя текстовый редактор, табличный процессор и приложение для создания презентаций, все большую популярность начинают приобретать приложения, построенные на базе современных веб-технологий. Главное преимущество подобных решений заключается в том, что они доступны со всех компьютеров в рамках единой сети, а для работы не требуется предустановка специального программного обеспечения. Доступ к приложениям осуществляется через обычный веб-браузер, который входит в состав практически любой современной операционной системы.

В зависимости от аппаратных возможностей и специфики построения облачного приложения, фактические вычисления могут производиться как на удаленном сервере, так и непосредственно на клиентском компьютере. Это позволяет интегрировать веб-приложения в практически любые сложные системы. Кроме того, преимущество подобного подхода заключается в том, что для внесения изменений в само приложение достаточно обновить его на сервере и все пользователи при следующем запуске будут работать уже в новой версии. Это значительно сокращает издержки, связанные с распространением и установкой обновлений программных модулей.

Использование облачных приложений в системе МВД России уже активно ведется и продолжает развиваться в рамках реализации программы по созданию и развитию Единой системы информационно-аналитического обеспечения деятельности (ИСОД) МВД России. Практически все существующие в настоящий момент сервисы обеспечения повседневной и оперативно-служебной деятельности разработаны как веб приложения.

Важной особенностью такого подхода является независимость программного обеспечения от аппаратно-программной платформы. Так, например, в рамках программы по импортозамещению, осуществляется поэтапный переход на использование свободного программного обеспечения (СПО) и в перспективе на процессоры отечественного производства.

Использование программного обеспечения, предназначенного для работы в операционной системе Windows, на других рабочих станциях будет невозможно. Даже в случае использования программного обеспечения для операционных систем, построенных на базе ядра Linux, оно должно быть специальным образом скомпилировано для поддержки соответствующей архитектуры процессора (MIPS или ARM для процессоров «Байкал», Эльбрус для процессоров «Эльбрус»). Работа с веб приложениями на по-

добных специализированных рабочих станциях будет осуществляться в привычном пользователю режиме.

Таким образом, отсутствие необходимости в дополнительной подготовке программного обеспечения и дополнительных затрат ресурсов на его установку и своевременное обновление является важнейшим фактором, которым следует руководствоваться при выборе программной платформы в пользу веб-приложений.

Идея создания «облачного» офисного решения не нова. Активные разработки в данном направлении ведутся с начала 2000-х годов, и офисные веб-приложения уже прошли достаточно длинный путь от простейших веб-редакторов текстов до полноценных функциональных решений, способных полностью выполнять любые профессиональные задачи. В настоящее время все крупные IT-компании, такие как Google, Microsoft, Apple представляют пользователям бесплатные облачные продукты для личного пользования, которые также имеют более функциональные коммерческие версии, предназначенные для коммерческого применения.

В соответствии с Федеральным законом от 29 июня 2015 года № 188 «О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации» и статью 14 Федерального закона «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» был создан Единый реестр российских программ для электронных вычислительных машин и баз данных (реестр отечественного ПО), который предназначен для расширения использования отечественной IT-продукции в органах государственной власти РФ, а также в целях оказания правообладателям ПО мер государственной поддержки. Реестр содержит перечень российского ПО, отечественное происхождение которого было подтверждено и для которого предусмотрена преференция при государственных и муниципальных закупках.

Таким образом, в качестве объектов потенциального внедрения целесообразно рассматривать решения, включенные в реестр. В настоящий момент в нем содержатся два офисных продукта отечественного происхождения, которые предоставляют функции онлайн редакторов документов, это «МойОфис Частное Облако» и «Р7-Офис. Профессиональный (серверная версия)».

МойОфис Частное Облако представляет собой набор сертифицированных приложений для безопасной обработки конфиденциальной информации, облачного хранения данных и коллективной работы над документами в режиме реального времени.

МойОфис Документы – это продукт для совместного редактирования текстовых документов и электронных таблиц. В продукт входят редакторы Текст и Таблица, созданные на базе единого программного ядра, приложение для просмотра презентаций, а также средство доступа к документам на

серверах компании. Доступ к документам и совместная работа над ними возможна с любого устройства.

МойОфис Текст обеспечивает удобное и быстрое создание документов с использованием шаблонов, стилей и средств форматирования текста. Функции совместного редактирования обеспечивают эффективную совместную работу сотрудников.

МойОфис Таблица – это приложение для быстрой и удобной работы с электронными таблицами и анализа данных. Продукт поддерживает расширенный набор формул и средств для обработки данных. Совместное редактирование на любой из поддерживаемых платформ обеспечивает быстрый анализ и подготовку документов группой сотрудников.

МойОфис Презентация – приложение с полным набором инструментов для просмотра графических презентаций.

Вход в МойОфис Документы осуществляется посредством главной страница авторизации [https://auth.{\\$DOMAIN}](https://auth.{$DOMAIN}). На указанной странице необходимо ввести логин и пароль пользователя, затем нажать кнопку «Войти». Во время первого входа в систему необходимо ознакомиться и согласиться с условиями пользовательского соглашения.

Особенности веб-интерфейса МойОфис Документы

На стартовой странице МойОфис Документы предоставлены (см. рисунок 1):

- поля для ввода логина (email) и пароля (для зарегистрированных в МойОфис Документы пользователей),
- гиперссылка на механизм восстановления забытого пароля,
- кнопка «Войти»,
- копирайт и название компании-разработчика,
- гиперссылка на блок информации о политике конфиденциальности,
- гиперссылка на блок информации об условиях использования продукта,
- гиперссылка на блок информации о программе,
- переключатель языковых версий продукта,
- пиктограмма для обращения в службу поддержки.

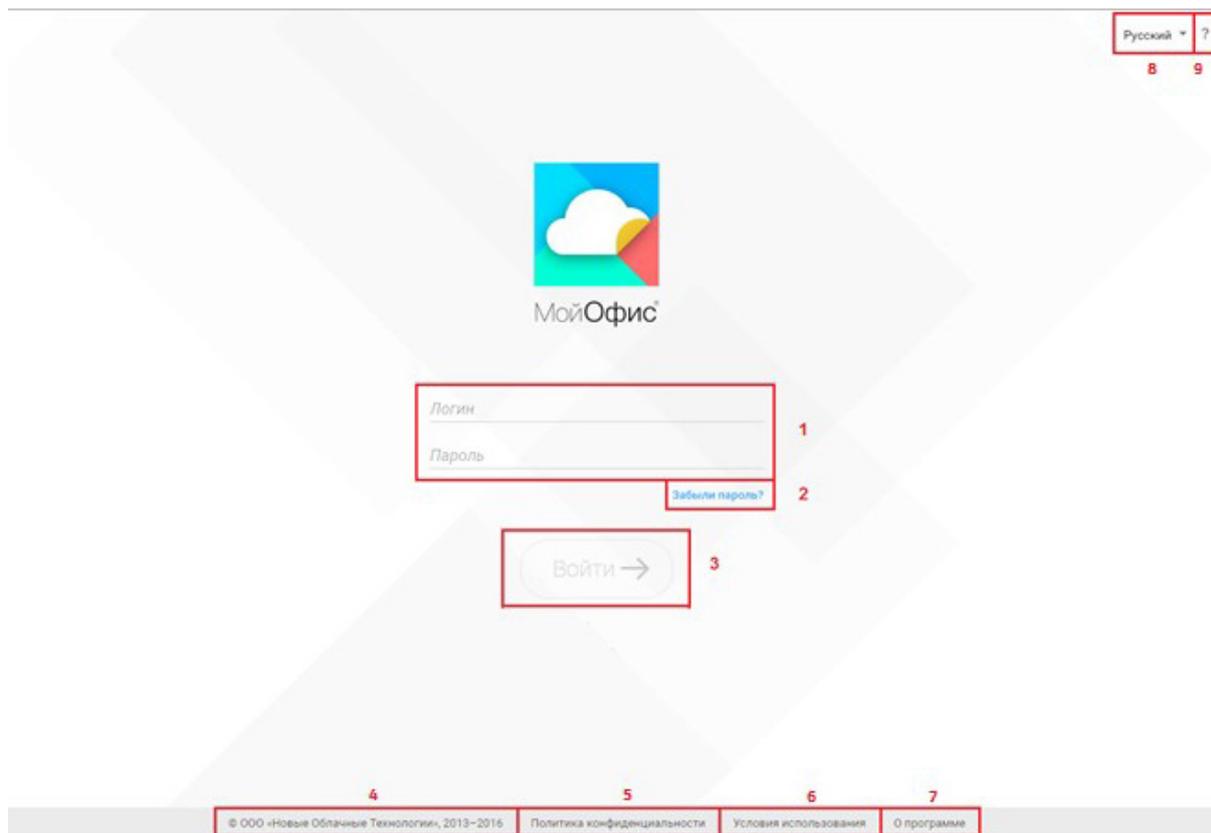


Рисунок 1. Стартовая страница МойОфис Документы.

При входе в МойОфис Документы отображается главная страница, которая представлена следующими элементами (см. рисунок 2):

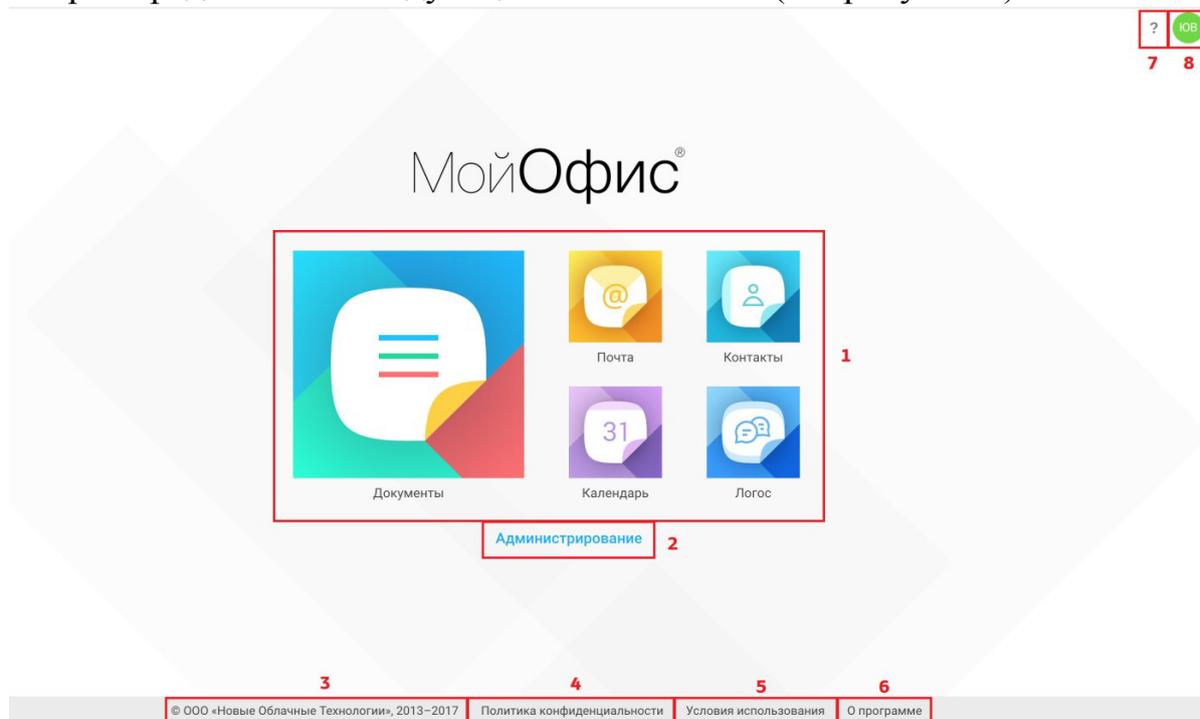


Рисунок 2. Интерфейс главной страницы МойОфис Документы.

- 1) блок пиктограмм для перехода к:
 - хранилищу документов («Документы»),
 - электронной почте («Почта»),
 - приложению «Контакты»,
 - приложению «Календарь»,
 - приложению «Логос»,
- 2) гиперссылка «Администрирование» (только для пользователей с правами администратора) для перехода к административной панели (МойОфис Администрирование),
- 3) копирайт и название компании-разработчика,
- 4) гиперссылка на блок информации о политике конфиденциальности,
- 5) гиперссылка на блок информации об условиях использования продукта,
- 6) гиперссылка на блок информации о программе,
- 7) пиктограмма для обращения в службу поддержки,
- 8) панель информации об активном пользователе МойОфис Документы по умолчанию отображает уникальную пиктограмму, присвоенную данному пользователю в МойОфис Документы; при нажатии на панель открывается окно дополнительной информации (см. рисунок 3), включающее следующие элементы:

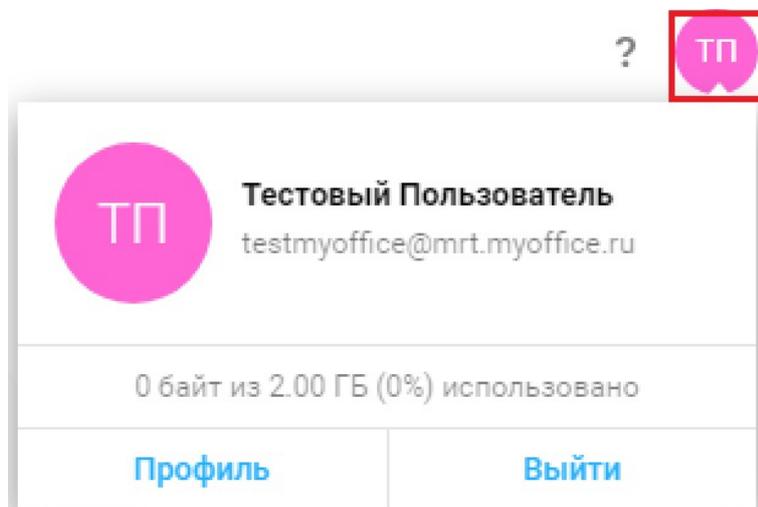


Рисунок 3. Панель информации об активном пользователе МойОфис Документы.

- имя пользователя,
- электронный адрес пользователя,
- информация о размерах имеющегося и используемого дискового пространства,
- кнопка «Профиль» для перехода к профилю пользователя,
- кнопка «Выйти» для выхода из активной учетной записи.

При входе в приложение «Документы» (по умолчанию вход осуществляется в директорию хранилища документов «Мои документы») на главной странице хранилища документов представлены следующие основные области (см. рисунок 4):

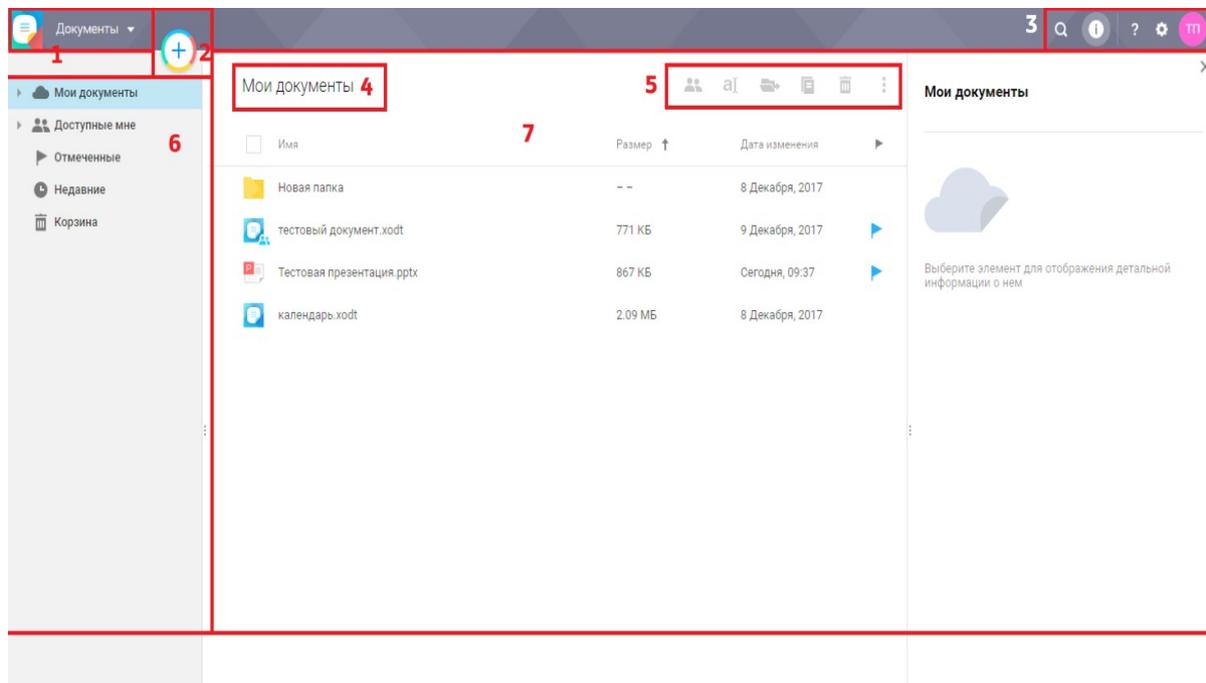


Рисунок 4. Интерфейс хранилища документов.

1) панель активного приложения. При раскрытии выпадающего списка открывается дополнительная навигационная панель (см. рисунок 5), предоставляющая возможность перехода к:

- главной навигационной странице МойОфис Документы («Приложения»),
- почте,
- приложению «Календарь»,
- приложению «Контакты»,
- приложению «Логос»,

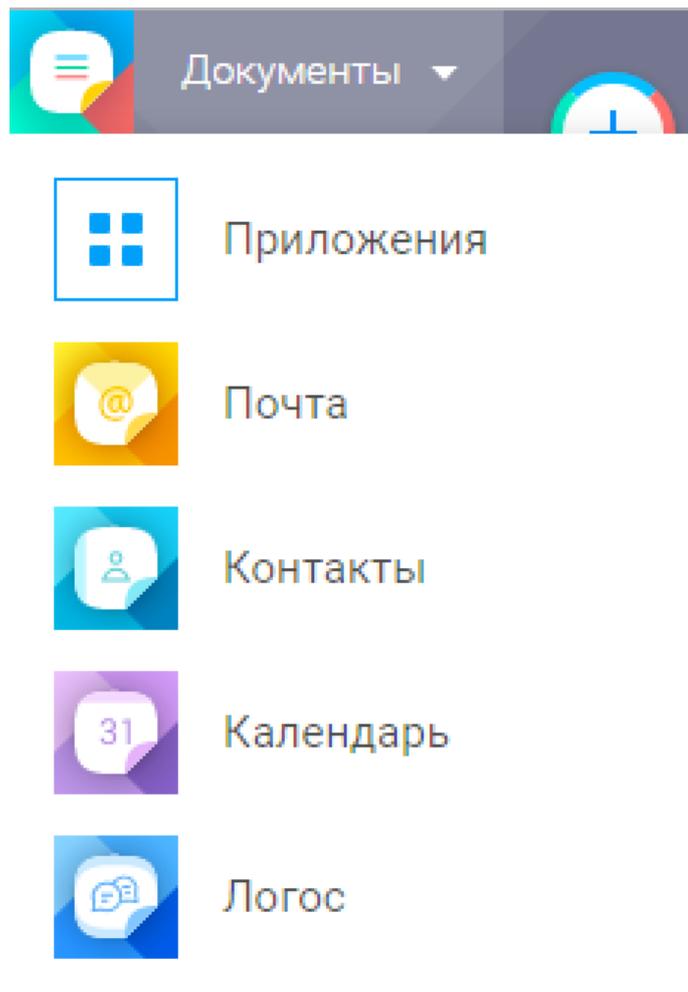


Рисунок 5. Дополнительная навигационная панель.

2) инструмент «Добавить» предназначен для создания/загрузки нового документа или папки. При активации данной пиктограммы открывается дополнительная панель (см. рисунок 6) выбора создаваемого/загружаемого объекта:

3) панель инструментов, в состав которой входят:

- пиктограмма «Последние операции» – для включения/отключения отображения панели «Последние операции» на месте панели свойств,
- пиктограмма «Поиск»,
- пиктограмма «Свойства» – для включения/отключения отображения панели свойств папки/документа,

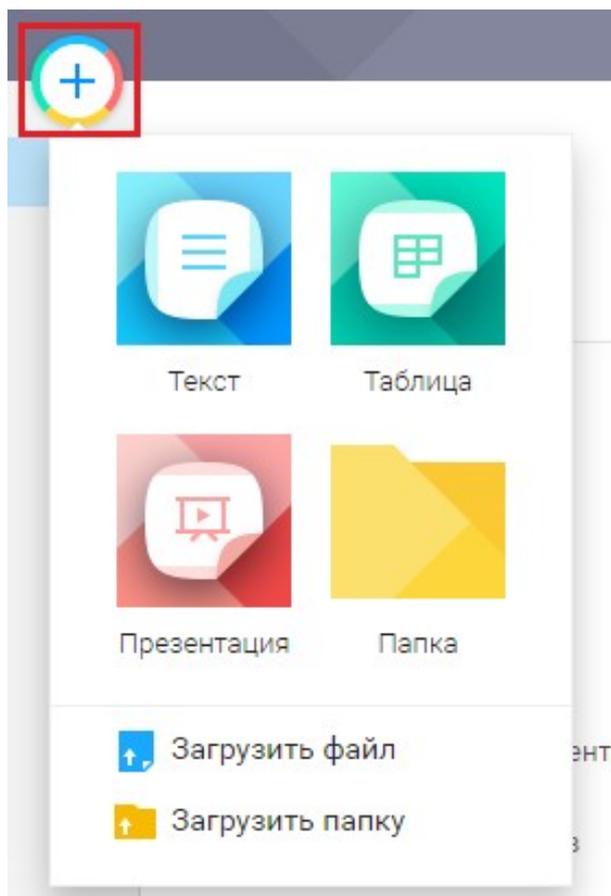


Рисунок 6. Инструмент «Добавить».

- пиктограмма «Помощь» – для обращения в службу поддержки,
- пиктограмма «Настройки» – для настройки параметров конвертации во внутренний формат МойОфис Документы загружаемых документов. Настройка осуществляется путем проставления знака в поле однозначного выбора и нажатия на кнопку «Сохранить» (см. рисунок 7),
- пиктограмма панели информации об активном пользователе МойОфис.

Настройки

Конвертация файлов во внутренний формат во время загрузки (когда возможно)

- Всегда с конвертацией
- Всегда без конвертации
- Спрашивать во время загрузки

Отмена

Сохранить

Рисунок 7. Настройки конвертации документов.

4) строка заголовка отображает наименование активной папки/подпапки,

5) панель инструментов для работы с отмеченными документами и папками хранилища. Панель включает в себя следующие элементы (см. рисунок 8):

- «Общий доступ»,
- «Переименовать»,
- «Переместить»,
- «Создать копию»,
- «Удалить»,
- «Скачать»,
- «Поделиться ссылкой»,
- «Отправить по почте».

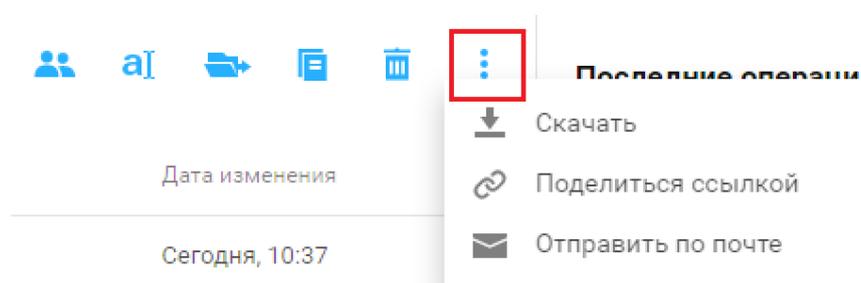


Рисунок 8. Панель инструментов для работы с документами и папками.

6) панель навигации по каталогам и подкаталогам хранилища документов. В состав элементов панели по умолчанию входят следующие каталоги:

- «Мои документы» – содержит документы владельца учетной записи, недоступные прочим пользователям МойОфис Документы,
- «Доступные мне» – содержит документы, доступ к которым был предоставлен их авторами/владельцами одному или нескольким другим пользователям МойОфис Документы (в данном каталоге пользователю доступны документы, доступ к которым был предоставлен ему автором/владельцем документа),
- «Отмеченные» – содержит документы, отмеченные пользователем,
- «Недавние» – содержит последние редактированные документы,
- «Корзина» – содержит документы, удаленные пользователем,

7) рабочая область. В рабочей области представлены в виде списка документы и папки активного каталога хранилища,

8) панель свойств активного каталога или документа – содержит информацию о:

- размере (только для документа),
- датах создания и последнего изменения документа или каталога,
- размере всех версий (только для документа),

- дате и времени создания текущей версии (только для документа),
- ссылку на журнал версий (только для документа, открывается на месте панели свойств). Включение/отключение отображения панели свойств осуществляется при помощи пиктограммы «Свойства».

Интерфейс текстового редактора МойОфис Документы представлен следующими элементами (см. рисунок 9):

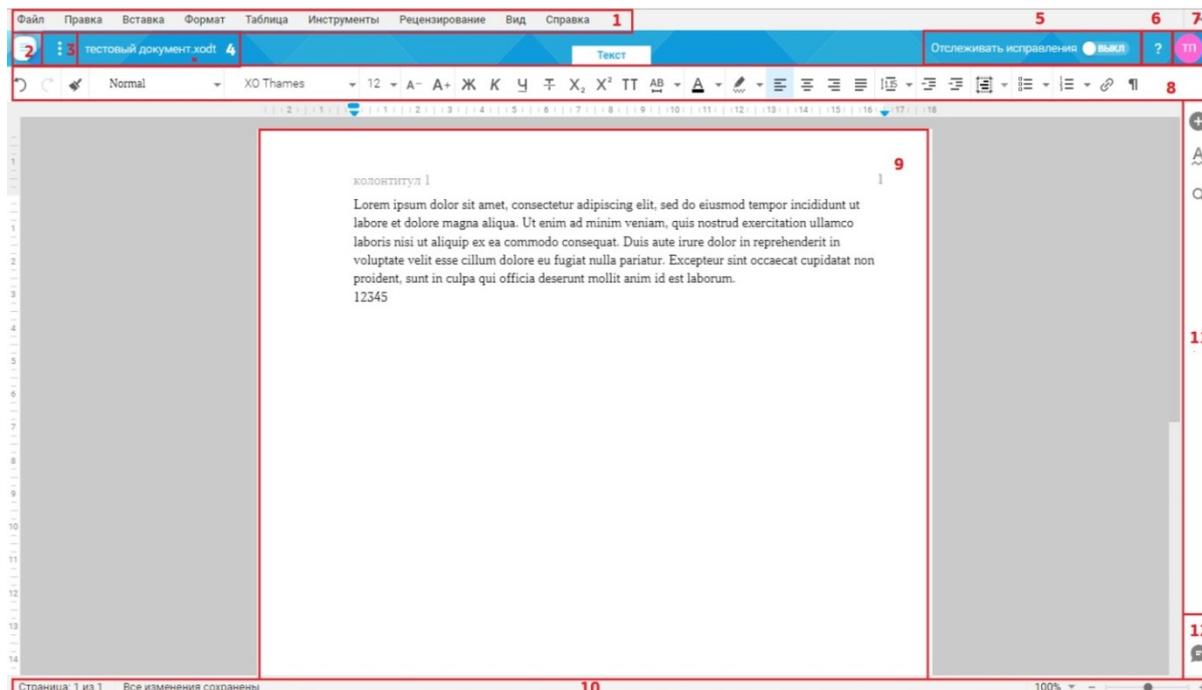


Рисунок 9. Интерфейс текстового редактора МойОфис Документы.

- 1) командное меню,
- 2) пиктограмма панели приложений,
- 3) кнопка вызова меню,
- 4) имя файла с расширением,
- 5) переключатель «Отслеживать исправления»,
- 6) кнопка «Помощь»,
- 7) аватар пользователя,
- 8) панель инструментов,
- 9) область редактирования,
- 10) панель состояния,
- 11) боковая панель инструментов,
- 12) панель совместной работы.

«Р7-Офис. Профессиональный» – редакторы документов, таблиц и презентаций для госучреждений и образования. «Р7-Офис» предлагает широкий набор инструментов для создания документов со сложным форматированием, а также множество возможностей для совместной работы,

включая рецензирование, комментирование и совместное редактирование в режиме реального времени.

В онлайн-редакторе документов Р7-Офис используется вкладочный интерфейс, в котором команды редактирования сгруппированы во вкладки по функциональности.

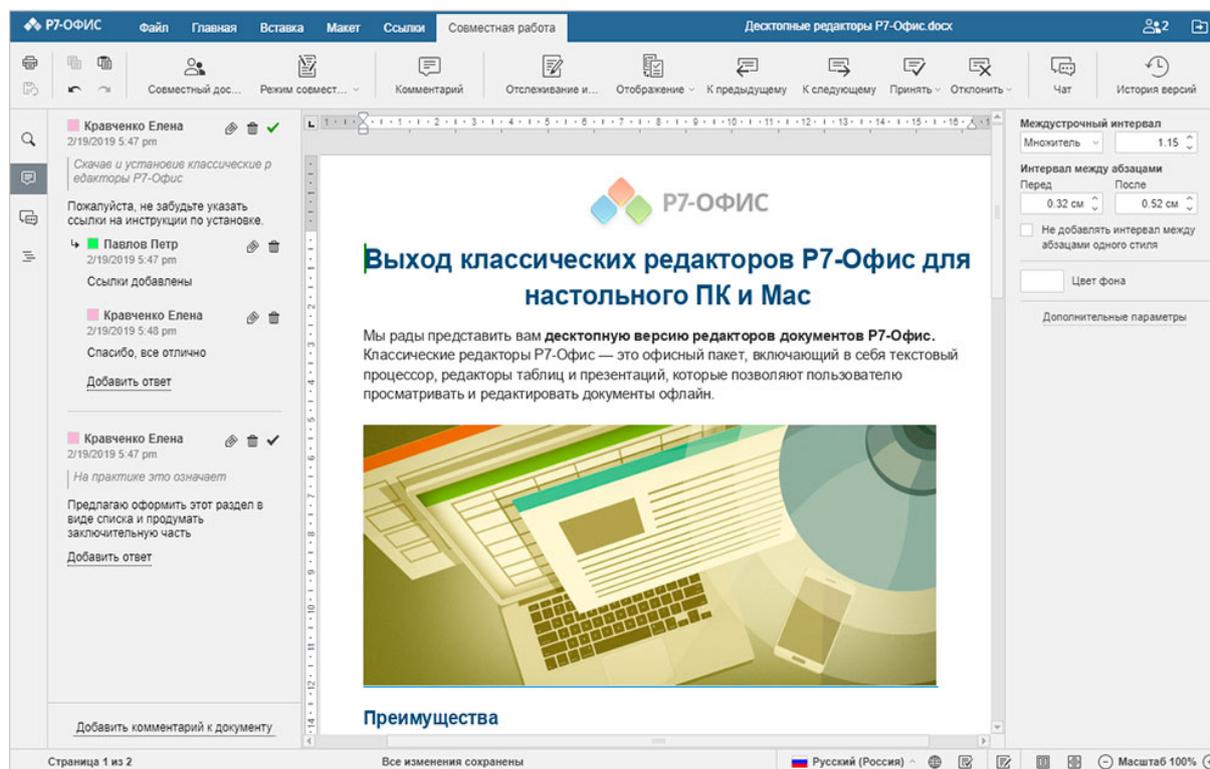


Рисунок 10. Окно онлайн-редактора документов.

Используя веб-версию редактора, вы можете работать над документом совместно с другими пользователями. Эта возможность включает в себя следующее:

- одновременный многопользовательский доступ к редактируемому документу,
- визуальная индикация фрагментов, которые редактируются другими пользователями,
- мгновенное отображение изменений или синхронизация изменений одним нажатием кнопки,
- чат для обмена идеями по поводу отдельных частей документа,
- комментарии, содержащие описание задачи или проблемы, которую необходимо решить.

Совместное редактирование. В редакторе документов можно выбрать один из двух доступных режимов совместного редактирования:

- быстрый используется по умолчанию, в нем изменения, вносимые другими пользователями, отображаются в реальном времени,

– строгий режим позволяет скрывать изменения, внесенные другими пользователями, до тех пор, пока вы не нажмете значок «Сохранить» чтобы сохранить ваши изменения и принять изменения, внесенные другими.

Режим можно выбрать в «Дополнительных настройках». Нужный режим также можно выбрать, используя значок «Режим совместного редактирования» на вкладке «Совместная работа» верхней панели инструментов.

Когда документ редактируют одновременно несколько пользователей в «Строгом режиме», редактируемые фрагменты текста помечаются пунктирными линиями разных цветов. При наведении курсора мыши на один из редактируемых фрагментов отображается имя того пользователя, который в данный момент его редактирует.

В «Быстром режиме» действия и имена участников совместного редактирования отображаются непосредственно в процессе редактирования текста. Количество пользователей, которые в данный момент работают над текущим документом, отображается в правой части шапки редактора. Чтобы увидеть, кто именно редактирует файл в настоящий момент, можно щелкнуть по соответствующему значку или открыть панель Чата с полным списком пользователей.

Права доступа также можно задать, используя значок «Совместный доступ» на вкладке «Совместная работа» верхней панели инструментов. Как только один из пользователей сохранит свои изменения остальные увидят в строке состояния примечание, которое сообщает о наличии обновлений.

3. Развертывание облачного офисного решения на базе ведомственной сетевой инфраструктуры

В МВД России функционирует облачная инфраструктура программно-технических комплексов единого информационного пространства (ОИ ПТК ЕИП) МВД России, которую можно использовать для размещения различных сервисов.

Назначением ОИ ПТК ЕИП является:

- предоставление вычислительных ресурсов для размещения общесистемных сервисов МВД России в виде единого пула ресурсов;
- предоставление централизованного средства управления ОИ ПТК ЕИП;
- предоставление администраторам системы средств организации масштабирования и перераспределения ресурсов инфраструктуры;
- автоматизация выполнения процессов масштабирования и перераспределения ресурсов инфраструктуры;
- предоставление доступа к общесистемным сервисам сотрудникам МВД России;
- автоматизация эксплуатационных процессов подсистем ОИ.

Условия функционирования ОИ ПТК ЕИП:

- ОИ ПТК ЕИП предназначена для функционирования в условиях МВД России;
- необходимо наличие оборудования ОИ ПТК ЕИП, его функционирование в штатном режиме;
- необходимо функционирование ИМТС;
- необходимо наличие обслуживающего персонала в соответствии схеме организационной структуры;
- необходимо наличие канала связи между подключаемой к ОИ ПТК ЕИП площадкой и основной площадкой ОИ ПТК ЕИП;
- необходимо наличие комплекта запасных частей для оборудования ОИ ПТК ЕИП;
- наличие канала связи между ОИ ПТК ЕИП и СУДИС МВД России;
- наличие защищенного канала подключения к интернет (в случае размещения в ОИ ПТК ЕИП систем, имеющих соответствующее требование).

Рассмотрим порядок действий для выделения виртуальных мощностей в облачной инфраструктуре ИСОД МВД России.

1. Направить в адрес эксплуатирующей организации ИСОД МВД России официальное письмо о необходимости выделения виртуальных мощностей в ОИ ИСОД МВД России, приложив следующую информацию:

- количество vCPU создаваемого виртуального центра обработки данных (ВЦОД).

- объем RAM (Гбайт) создаваемого ВЦОД.
- объем дискового пространства (Гбайт) создаваемого ВЦОД.
- количество ip-адресов в ИМТС создаваемого ВЦОД.
- Ф.И.О. ответственного за создаваемый ВЦОД сотрудника.

Архитектура создаваемого ВЦОД. Пример архитектуры создаваемого ВЦОД:

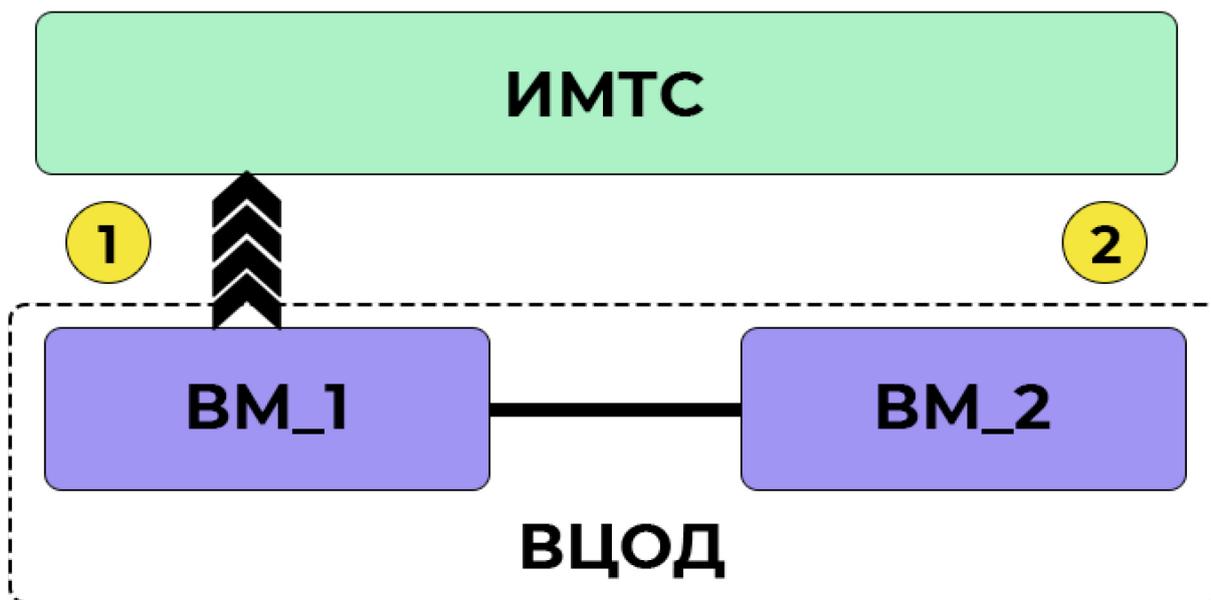


Рисунок 11. Архитектура ВЦОД.

где:

1 – виртуальная машина с ip-адресом в ИМТС; 2 – локальная виртуальная машина в рамках ВЦОД.

Архитектура создаваемого ВЦОД должна быть представлена в формате «.xls» или «.xlsx». При этом необходимо учитывать, что каждая виртуальная машина, создаваемая на вычислительных мощностях ВЦОД, имеет следующие ограничения по максимальным вычислительным мощностям:

- vCPU: 8.
- RAM: 64 Гбайт.
- HDD/SSD: 100 Гбайт.

2. После обработки обращения на выделение виртуальных мощностей направляется номер созданного ВЦОД.

Для получения доступа к веб-интерфейсу панели администрирования Вашего ВЦОД необходимо:

- пройти авторизацию в сервисе «ОИ ПТК ЕИП» по адресу «cloud.mvd.ru» под учетной записью СУДИС, с которой будет происходить администрирование созданного ВЦОД. Условие является обязательным,

поскольку сервис «ОИ ПТК ЕИП» осуществляет выборку учетных записей СУДИС, прошедших авторизацию по адресу «cloud.mvd.ru».

- направить заявку в ЕЦЭ ИСОД МВД России. Заявка должна содержать следующую информацию:

1. Номер созданного ВЦОД, полученного после выполнения шага 1.
2. Логин/логины учетных записей СУДИС, прошедших авторизацию по адресу «cloud.mvd.ru», с которых будет осуществляться администрирование созданного ВЦОД.

После выполнения данной заявки будет получен доступ к виртуальным машинам только по VNC. Доступ по SSH и/или RDP на данном этапе отсутствует.

3. Произвести создание и конфигурирование виртуальных машин созданного ВЦОД, обязательно назначив ip-адрес ИМТС хотя бы одной из виртуальных машин. Доступ по SSH и/или RDP происходит по назначенному ip-адресу ИМТС. Осуществление указанных действий изложено в разделе 2 настоящей инструкции.

4. Для получения доступа к виртуальным машинам по SSH и/или RDP необходимо произвести конфигурирование аппаратного сетевого экрана, расположенного в ЦОД ИСОД МВД России. Для этого необходимо направить заявку в ЕЦЭ ИСОД МВД России, выбрав в качестве сервиса «Подсистема ОИБ», следующего содержания:

Src ip (адрес источника)	Dst ip (адрес назначения)	Порты	Протоколы
11.xx.xx.xx	172.xx.xx.xx	22, 3389	SSH, RDP

где:

Src ip – ip-адрес АРМ, с которого будет осуществляться доступ по SSH и/или RDP. Чтобы узнать данный ip-адрес необходимо:

1. Пройти авторизацию по адресу «it.mvd.ru».
2. Перейти по адресу «it.mvd.ru/ip».
3. Необходимый ip-адрес указан в графе «ip».

Dst ip – ip-адрес ИМТС, назначенный виртуальной машине в процессе конфигурирования.

По умолчанию аппаратный сетевой экран ЦОД ИСОД МВД России «пропускает» весь сетевой трафик только по 80-ому порту. «Открывать» 80-ый порт не требуется.

IP-адрес источника «связан» с dst-файлом владельца и является статическим.

IP-адрес ИМТС резервируется за конкретным ВЦОД до момента его удаления администратором ВЦОД. Даже в случае отвязки IP-адреса ИМТС

от виртуальной машины, IP-адрес сохраняется за конкретным ВЦОД, т.е. фактически IP-адрес ИМТС резервируется за конкретным ВЦОД при первом назначении для виртуальной машины.

Порядок создания и настройки виртуальной машины в ОИ ИСОД МВД России

1. Перейти в раздел «Виртуальные ЦОДы» по адресу «cloud.mvd.ru» и ввести полученный номер ВЦОД.

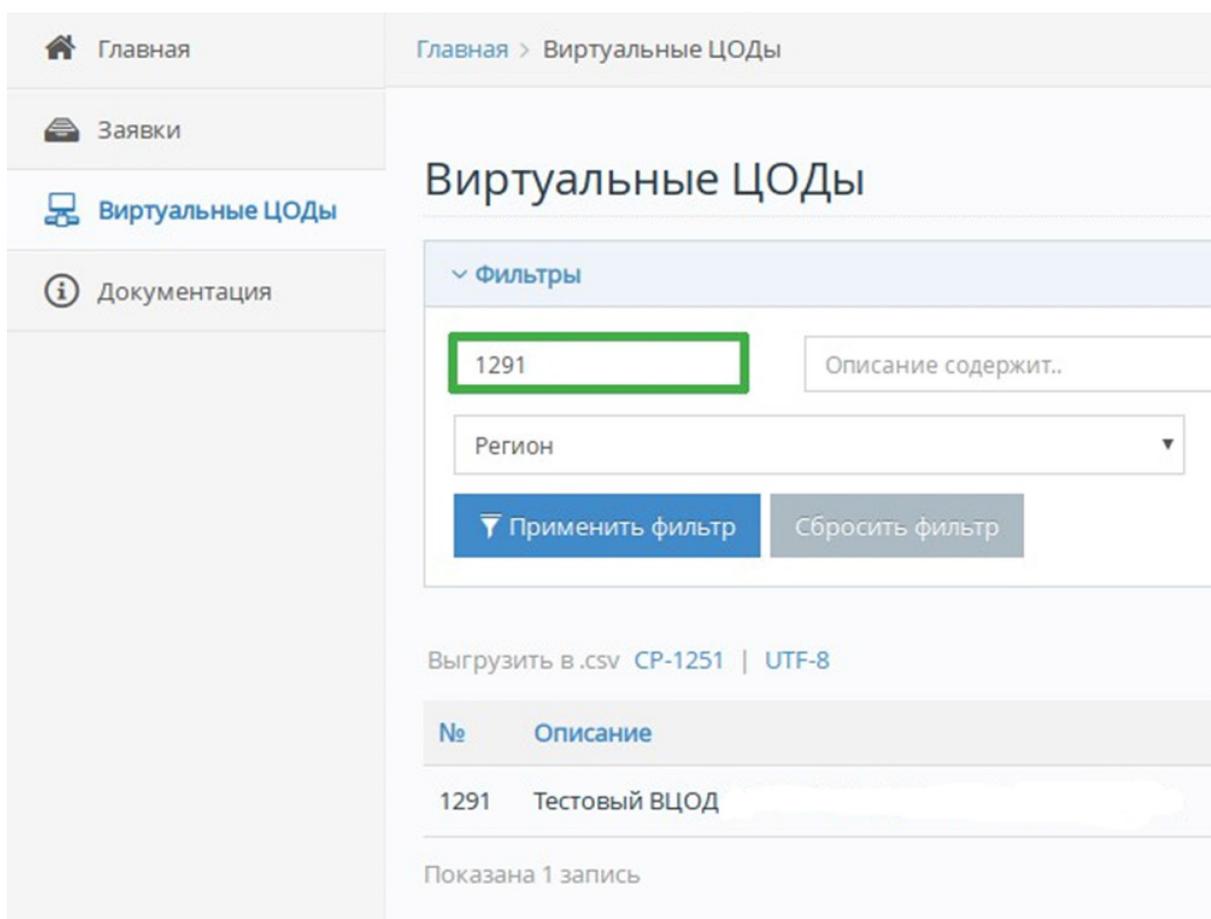


Рисунок 12. Виртуальные ЦОДы.

2. Перейти в панель администрирования ВЦОД.

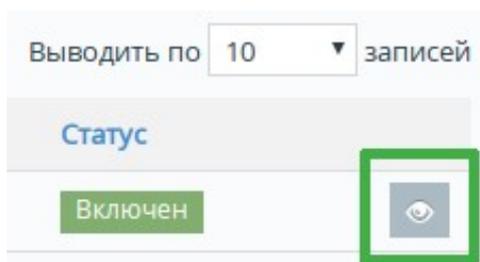


Рисунок 13. Панель администрирования ВЦОД.

3. Добавить конфигурацию вычислительных мощностей для виртуальных машин с учетом ограничений, нажав на элемент «Добавить конфигурацию».

Виртуальный ЦОД № 1291 > dc1-ditsizi-test

Общая информация | Управление | Заявки по этому ВЦОД

Перенести VM в другой ВЦОД | Удалить Виртуальный ЦОД

Виртуальные сети

No Networks

Конфигурации виртуальных машин

Добавить конфигурацию

Новая конфигурация

vCPU	<input type="text" value="8"/>	?
RAM	<input type="text" value="64"/> GB	?
HDD	<input type="text" value="100"/> GB	?

Сохранить | Отменить

Рисунок 14. Добавление конфигурации ВЦОД.

4. В панели администрирования ВЦОД указаны идентификационные данные для авторизации в панели конфигурирования виртуальных машин ВЦОД.

5. Пройти авторизацию в панели конфигурирования виртуальных машин ВЦОД, перейдя по адресу, указанному в п. 4. По умолчанию ВЦОД не имеет настроек сети, в том числе сетевого оборудования, доступа и безопасности.



Войти

Имя пользователя

dc1

Пароль

.....

Подключиться

Рисунок 15. Добавление конфигурации ВЦОД.

6. Настроить сеть ВЦОД, перейдя в раздел «Сети» строго в соответствии со скриншотами за исключением наименования сети и подсети:

- «Проект» => «Сеть» => «Сети» => «Создать сеть».

Создать сеть

Сеть

Подсеть

Детали подсети

Название сети

network

Создайте новую сеть. Дополнительно на следующих шагах мастера можно создать подсеть, связанную с сетью.

Административное состояние ⓘ

UP

Общая ⓘ

Создать подсеть

Отмена

« Назад

Следующий »

Рисунок 16. Создание сети ВЦОД.

Создать сеть



Сеть

Подсеть

Детали подсети

Название подсети

network_subnet

Сетевой Адрес

192.168.0.0/24

Версия IP

IPv4

IP шлюза

Запретить шлюз

Создает подсеть, связанную с сетью. Необходимо указать правильные "Сетевой адрес" и "IP-адрес шлюза". Если не указан IP-адрес шлюза, то по умолчанию присваивается первое значение сети. Для того чтобы не использовать шлюз, включите опцию "Выключить шлюз". Дополнительные параметры доступны на вкладке "Сведения о подсети".

Отмена

« Назад

Следующий »

Рисунок 17. Создание подсети ВЦОД.

Создать сеть



Сеть

Подсеть

Детали подсети

Разрешить DHCP

Указать дополнительные атрибуты для подсети.

Выделение пулов

Сервера DNS

172.26.236.36
172.26.238.38

Маршруты узла

Отмена

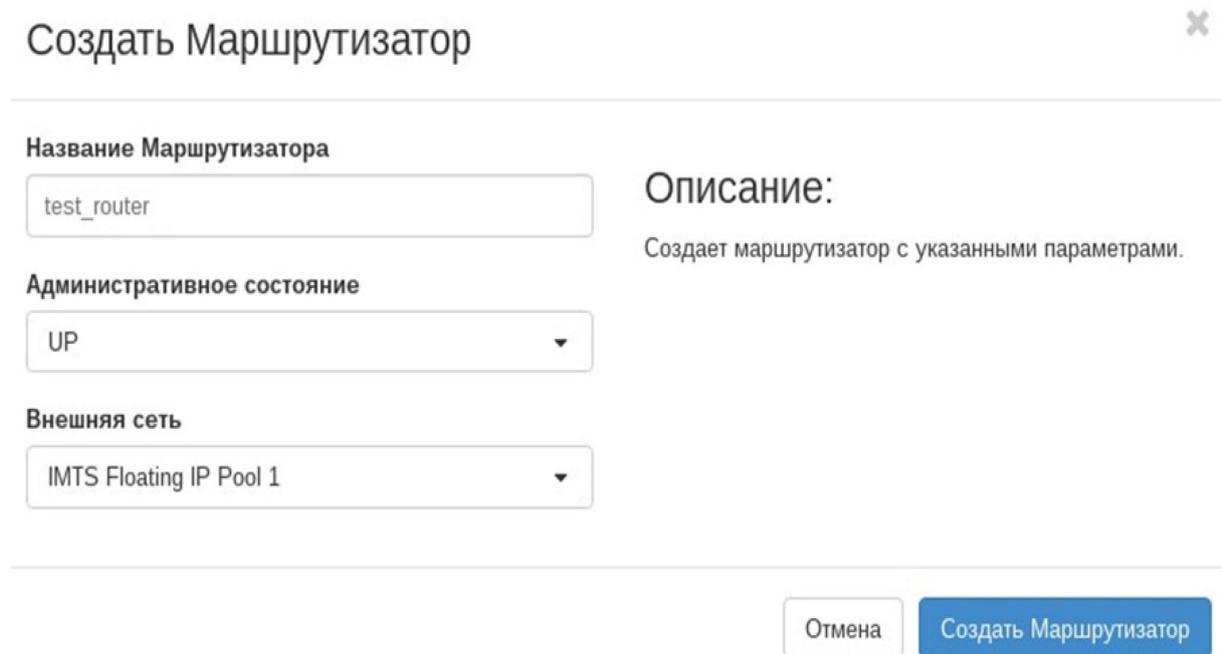
« Назад

Создать

Рисунок 18. Детали подсети ВЦОД.

7. Добавить маршрутизатор ВЦОД, перейдя в раздел «Маршрутизаторы» (наименование маршрутизатора не имеет значения):

- «Проект» => «Сеть» => «Маршрутизаторы» => «Создать маршрутизатор».



Создать Маршрутизатор

Название Маршрутизатора

test_router

Описание:

Создает маршрутизатор с указанными параметрами.

Административное состояние

UP

Внешняя сеть

IMTS Floating IP Pool 1

Отмена Создать Маршрутизатор

Рисунок 19. Добавление маршрутизатора ВЦОД.

8. Добавить интерфейс к созданному маршрутизатору:

- «Проект» => «Сеть» => «Маршрутизаторы» => «Кликнуть по наименованию маршрутизатора» => «Интерфейсы» => «Добавить интерфейс».

9. По умолчанию весь входящий трафик на ВЦОД заблокирован. Для «пропуска» входящего трафика необходимо добавить следующее правило:

- «Проект» => «Вычислительные ресурсы» => «Доступ и безопасность» => «Группы безопасности» => «Кликнуть по наименованию уже существующей группы правил» => «Добавить правило».

Правило *

Другой Протокол ▼

Направление

Входящий трафик ▼

IP протокол ?

Удаленный адрес * ?

CIDR ▼

CIDR ?

0.0.0.0/0

Рисунок 20. Добавление правила маршрутизации.

10. Для организации доступа по SSH необходимо создать пару ключей. Если доступ по SSH не требуется, указанный шаг возможно пропустить. На данном шаге создается открытый ключ, хранимый на ВЦОД, и закрытый ключ, который будет предложено сохранить на APM администратора. Наименование созданной пары будет указано при создании виртуальной машины. Для доступа по SSH может быть использована одна ключевая пара для всех машин или уникальная для каждой виртуальной машины. Закрытая часть ключевой пары сохраняется в формате «.pem».

- «Проект» => «Вычислительные ресурсы» => «Доступ и безопасность» => «Пары ключей» => «Создать пару ключей».

Создать пару ключей ✕

Название пары ключей *

ssh

Описание:

Пары ключей это учетные данные SSH, которые вводятся в образ при запуске. Создание новой пары регистрирует публичный ключ и загружает частный ключ (файл .pem).

Храните и используйте ключ, как любой обычный закрытый ключ ssh.

Отмена **Создать пару ключей**

Рисунок 21. Создание ключей.

11. Создать виртуальную машину:
- Перейти в «Проект» => «Вычислительные ресурсы» => «Инстансы» => «Запустить машину».

1. «Подробности» – изменять только наименование.

2. «Источник» – элементом «+» выбрать необходимый дистрибутив операционной системы.

3. «Тип инстанса» – элементом «+» выбрать необходимую конфигурацию вычислительных мощностей, созданную в п. 3.

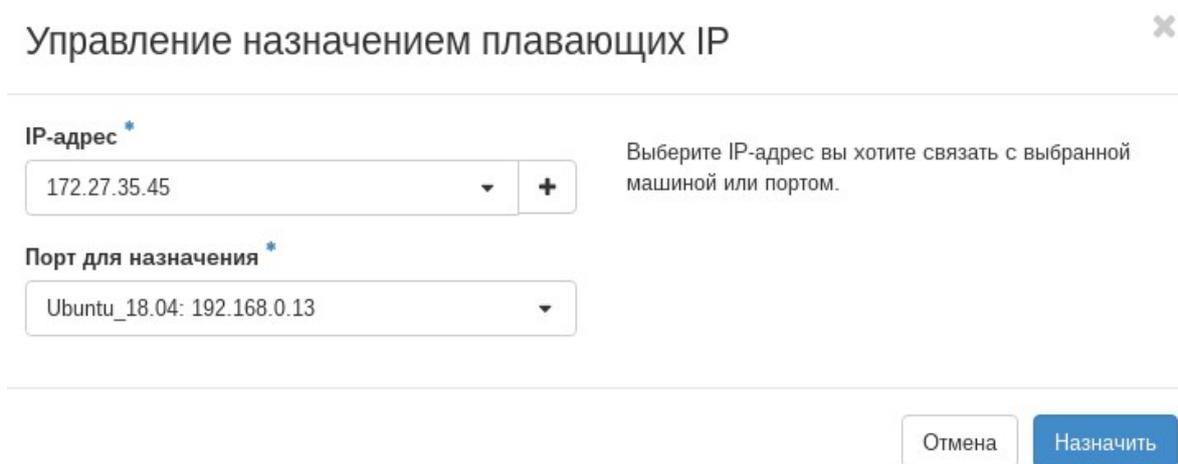
4. «Ключевая пара» – элементом «+» выбрать необходимую ключевую пару для доступа по SSH, созданную в п. 10.

Нажать на элемент «Запустить инстанс».

12. Чтобы «привязать» ip-адрес ИМТС к созданной в п. 11 виртуальной машины, необходимо:

- Перейти в «Проект» => «Вычислительные ресурсы» => «Инстансы».

Выделив созданную виртуальную машину, нажать на элемент «Ещё действия». Выбрать элемент «Связать ip-адрес» (ip-адрес ИМТС и порт назначения будет отличаться):



Управление назначением плавающих IP ✕

IP-адрес *
172.27.35.45 +

Выберите IP-адрес вы хотите связать с выбранной машиной или портом.

Порт для назначения *
Ubuntu_18.04: 192.168.0.13

Отмена Назначить

Рисунок 22. Управление диапазоном адресов.

Порядок настройки доступа к виртуальной машине в ОИ ИСОД МВД России посредством протокола SSH

Доступ по SSH к виртуальной машине уже настроен, в случае создания ключевой пары в панели конфигурирования ВЦОД и «привязки» созданной ключевой пары к конкретной виртуальной машине.

Все действия в терминале выполнять под учетной записью администратора или «root». Открыть терминал на АРМ администратора ВЦОД

(ip-адрес АРМ является ip-адресом источника в заявке, указанной в шаге 1.4. настоящей инструкции).

При первом подключении по SSH с АРМ под управлением операционных систем семейства «Unix» прописать следующие команды:

```
ssh-keygen -f "/root/.ssh/known_hosts" -R 172.27.35.45
```

где вместо «172.27.35.45» - ip-адрес ИМТС, привязанный к виртуальной машине, созданной на шаге 2.12. настоящей инструкции.

Ввести в терминале «yes» и нажать «Enter».

Прописать следующую команду:

```
ssh -i /home/tkachenko/ssh.pem cloud@172.27.35.45
```

где:

1. «/home/tkachenko/ssh.pem» - путь к закрытой части ключевой пары, создаваемой на шаге 2.10. настоящей инструкции.

2. «172.27.35.45» - ip-адрес ИМТС, привязанный к виртуальной машине, созданной на шаге 2.12. настоящей инструкции.

Порядок установки

1) Подготовка Astra Linux.

Рекомендуется использовать дистрибутив без графического окружения и других предлагаемых дополнений. Для работы сервисов рекомендуется использовать локальный сервис разрешения имён (например, dnsmasq из состава защищённой ОС), в таком случае первым nameserver в файле /etc/resolv.conf должен быть либо 127.0.0.1. Для обеспечения этого может быть настроен файл конфигурации сетевого интерфейса, клиента dhcp или сервиса NetworkManager. Набор доменов и имен для конфигурирования сервиса dnsmasq устанавливается в ходе развертывания скриптом на основании переменных из файла конфигурации.

2) Подготовка ALT Linux.

В случае необходимости установки изделия в среде операционной системы Astra Linux, предварительно необходимо сделать следующее:

2.1 установить менеджер инициализации systemd: apt-get install systemd,

2.2 в файл /etc/sysconfig/grub2 к переменной GRUB_CMDLINE_LINUX_DEFAULT добавить init=/lib/systemd/systemd,

2.3 применить новую конфигурацию загрузчика: update-grub.

3) Управление конфигурацией установки.

Перед началом установки изделия рекомендуется создать файл /etc/sysconfig/myoffice, содержащий параметры развёртывания «МойОфис Защищённое Облако». Переменные устанавливаются следующим образом: ИМЯ_ПЕРЕМЕННОЙ=ЗНАЧЕНИЕ.

Если указанный файл недоступен или переменная не задана явным образом, в процессе установки будут использованы значения по умолчанию. Используются следующие переменные:

3.1 MYOFFICE_DOMAIN – доменное имя «МойОфис Защищённое Облако», по умолчанию – myoffice.demo,

3.2 RELEASE_VERSION – версия изделия, по умолчанию – 6.07,

3.3 INTERNAL_DOMAIN – внутреннее доменное имя, используемое службами изделия, по умолчанию - internal.demo,

3.4 PGSRV – имя сервиса PostgresPRO; по умолчанию postgrespro-9.5,

3.5 PGDATA – путь к базе данных PostgresPRO, по умолчанию “/var/lib/pgpro/9.5/data”,

3.6 PGENGINE – путь к исполняемым файлам PostgresPRO; /usr/pgpro9.5/bin,

3.7 PGINITDB — команда инициализации базы данных; по умолчанию “/usr/pgpro9.5/bin/pg-setup initdb”,

3.8 SSLPATH—путь к SSL-сертификатам, по умолчанию – /etc/co/nginx/conf/ssl.

4) Установка изделия.

Установка изделия производится автоматически посредством сценариев, поставляемых на диске. Также в процессе требуется работающее соединение с сетью интернет для загрузки части сторонних зависимостей. Со стороны администратора необходимо выполнить следующие действия:

4.1 вставить диск «МойОфис Защищённое Облако» в устройство чтения; если операционная система не поддерживает автоматическое монтирование съёмных носителей, выполнить операцию вручную:

```
mount -o exec /media/cdrom
```

```
запустить установку: /media/cdrom/scripts/setup-distrow.sh.
```

5) Запуск изделия.

Для нормальной работы на серверной части «МойОфис Защищённое Облако» должны быть открыты порты 53 и 443. Данная операция должна быть выполнена в соответствии с инструкциями используемого межсетевого экрана.

Процесс запуска изделия может различаться в зависимости от менеджера инициализации операционной системы.

В случае использования upstart (в таких дистрибутивах, как CentOS 6), необходимо выполнить команду:

```
start myoffice
```

В случае использования systemd (в таких дистрибутивах, как ALT Linux, Astra Linux), команда примет вид:

```
systemctl enable nct-myoffice.target
```

```
# разрешить автозагрузку служб
systemctl start nct-myoffice.target
# запустить службы
```

Проверить корректность запуска служб изделия можно следующим образом:

```
curl -s http://127.0.0.1:8888/api/manage/core/status | python -m json.tool | grep all
```

В случае отсутствия ошибок, в консоли будет напечатано: "all": "ОК"

б) Проверка корректности установки.

Сравнить значения контрольных сумм установленных файлов МойОфис Защищённое облако с зафиксированными в документе «Программное обеспечение «МойОфис Защищённое облако». Формуляр» RU.2914487.501.490.001 30 значениями.

Установка серверной версии Р7-Офис. Сервер. Профессиональный с помощью скрипта для ОС Astra Linux

Р7-Офис. Сервер. Профессиональный – это система для совместной работы, централизованного управления документами и электронной перепиской.

Р7-Офис. Сервер. Профессиональный поставляется как скрипт автоматической установки для операционной системы Astra Linux. Скрипт автоматически установит и настроит все необходимые зависимости, а также компоненты Р7-Офис. Сервер. Профессиональный (Сервер документов, Панель управления и Сервер совместной работы), скрипт также можно использовать для обновления серверной версии.

Системные требования:

- поддерживается только 32- и 64-битная архитектура,
- процессор: двухъядерный с тактовой частотой 2 ГГц или лучше,
- оперативная память: не менее 6 Гб.
- свободное место на жестком диске: не менее 40 Гб,
- операционная система: Astra Linux Special Edition (релиз Смоленск версия 1.6).

Для корректной работы Сервера документов требуется Node.js версии 8.12.0 или выше. Нет необходимости устанавливать этот компонент вручную, так как все зависимости автоматически устанавливаются с помощью скрипта. Но в том случае, если у вас в системе уже установлена платформа Node.js более ранней версии, пожалуйста, обновите версию Node.js, прежде чем начинать установку Р7-Офис. Сервер. Профессиональный. Хотя запуск Р7-Офис. Сервер. Профессиональный – это очень

ресурсоемкая операция, вам не придется выделять пространство подкачки (swap) перед началом установки. При запуске скрипта установки автоматически создается swap-файл размером 6 Гб.

Шаг 1. Получение скрипта Р7-Офис. Сервер. Профессиональный
Скачайте файл скрипта Р7-Офис. Сервер. Профессиональный для Astra Linux. Это можно сделать на странице загрузок нашего сайта. Вы также можете выполнить следующую команду: `wget https://download.r7-office.ru/repo/install-AstraLinux.sh`

Шаг 2. Добавление репозитория
Перед установкой Р7-Офис. Сервер. Профессиональный потребуется добавить репозиторий Debian. После того как вы добавите репозиторий, можно начинать установку.

Шаг 3. Установка Р7-Офис. Сервер. Профессиональный
Все действия по установке должны выполняться с правами пользователя root. Чтобы установить все компоненты и модули Р7-Офис. Сервер. Профессиональный, выполните следующую команду: `bash install-AstraLinux.sh`

Когда установка завершится, можно убедиться в корректной работе Р7-Офис. Сервер. Профессиональный. Для этого откройте браузер и введите в адресной строке IP-адрес компьютера в локальной сети (пожалуйста, не используйте ни localhost, ни сетевой адрес 127.0.0.1 того компьютера, на котором установлена серверная версия Р7-Офис. Сервер. Профессиональный, а используйте вместо этого его IP-адрес в локальной сети). Серверная версия Р7-Офис. Сервер. Профессиональный должна работать, что свидетельствует об успешной установке.

Требования к интеграции с СУДИС

Требования по идентификации и аутентификации для сервисов ИСОД, которые интегрируются по протоколу SAML:

Взаимодействие между сервисом ИСОД и Сервисом управления доступом в процессе прохождения пользователем процедуры идентификации и аутентификации должно быть реализовано с использованием протокола SAML 2.0 поверх протокола HTTP.

При попытке доступа неавторизованного пользователя к сервису, сервис ИСОД должен перенаправлять пользователя на страницу авторизации Сервиса управления доступом для прохождения процедуры идентификации и аутентификации.

После процедуры успешной аутентификации:
сервис управления доступом возвращает сервису ИСОД следующие атрибуты: Ф.И.О., email, ID пользователя в сервисе управления доступом.

сервис ИСОД должен обеспечить разграничение доступа пользователя к функциям сервиса.

В случае неуспешной аутентификации сервис управления доступом потребует повторной попытки аутентификации.

При выходе пользователя из сервиса ИСОД необходимо использовать функцию завершения пользовательской сессии протокола SAML 2.0.

Механизмы взаимодействия на основе протокола SAML 2.0 уточняются на этапе разработки конструкторской документации.

Требования по управлению учетными записями (ведению пользователей)

Управление учетными записями пользователей сервиса ИСОД должно осуществляться с использованием API создания, редактирования, блокирования, активации учетной записи Сервиса управления доступом.

При создании пользователя в Сервисе ИСОД необходимо вызвать метод Сервиса управления доступом «Создать пользователя» передав следующие параметры (Логин, Пароль, Фамилия, Имя, Отчество, email). В случае успешного выполнения Сервис управления доступом возвращает (Id пользователя в Сервисе управления доступом), либо возвращается (код ошибки, текст ошибки). После создания пользователя администратор Сервиса ИСОД должен установить права доступа к функциям в сервисе ИСОД.

При редактировании пользователя в Сервисе ИСОД необходимо вызвать метод Сервиса управления доступом «Редактировать пользователя» передав следующие параметры (Логин, Пароль, Фамилия, Имя, Отчество, email). В случае ошибки возвращается (код ошибки, текст ошибки).

При блокировании пользователя в Сервисе ИСОД необходимо вызвать метод «Блокировать пользователя» передав следующие параметры (ID пользователя в Сервисе управления доступом).

При активации пользователя в Сервисе ИСОД необходимо вызвать метод «Активировать пользователя» передав следующие параметры (ID пользователя в Сервисе управления доступом).

Для смены пароля пользователем сервиса ИСОД должна использоваться страница смены пароля в веб-интерфейсе Сервиса управления доступом. Сервис ИСОД должен в интерфейсе пользователя сделать переход на URL веб-страницы. Адрес веб-страницы уточняется на этапе разработки конструкторской документации.

В случае наличия накопленной собственной базы пользователей сервиса ИСОД, база пользователей (до ввода в эксплуатацию сервиса ИСОД) должна быть импортирована в Сервис управления доступом. Импорт осуществляется после подготовки файла XML в соответствии с установленным форматом: Ф.И.О., email, логин, пароль, ID пользователя в сервисе

ИСОД. После импортирования сервис ИСОД должен получить и сохранить от сервиса управления доступом информацию в установленном формате: ID пользователя в сервисе ИСОД, ID пользователя в сервисе управления доступом.

Адреса сервисов механизмы взаимодействия на основе протокола SAML 2.0 уточняются на этапе разработки конструкторской документации.

Требования по предоставлению информации о событиях безопасности

Сервис ИСОД должен осуществлять протоколирование событий безопасности с использованием API Сервиса управления доступом:

- при входе пользователя в сервис ИСОД необходимо вызвать метод «Добавить запись в протокол событий» передав следующие параметры (Тип события = «вход в сервис», дата и время события, Id пользователя в сервисе управления доступом).

- при выходе пользователя в сервис ИСОД необходимо вызвать метод «Добавить запись в протокол событий» передав следующие параметры (Тип события = «выход из сервиса», дата и время события, Id пользователя в сервисе управления доступом).

Требования по идентификации и аутентификации для сервисов ИСОД, которые интегрируются по протоколу LDAP

Идентификация и аутентификация пользователей сервиса ИСОД должна быть реализована в соответствии со следующими требованиями:

Взаимодействие между сервисом ИСОД и Сервисом управления доступом в процессе прохождения пользователем процедуры идентификации и аутентификации должно быть реализовано с использованием протокола LDAP. Сервис ИСОД должен обеспечить возможность ввода идентификатора и пароля пользователя в системе и/или работу со средствами электронной подписи;

После процедуры успешной аутентификации:

- сервис управления доступом возвращает сервису ИСОД следующие атрибуты: Ф.И.О., email, ID пользователя в сервисе управления доступом.

- сервис ИСОД должен обеспечить разграничение доступа пользователя к функциям сервиса.

- При выходе пользователя из сервиса ИСОД необходимо использовать функцию завершения пользовательской сессии протокола LDAP.

- Механизмы взаимодействия на основе протокола LDAP уточняются на этапе разработки конструкторской документации.

Для обеспечения возможности эксплуатации должны быть удовлетворены следующие требования к техническим характеристикам и документированию размещаемого сервиса.

Технические требования. На всех серверах, размещаемых в ИСОД, должен быть установлен агент мониторинга системы ЕЦЭ МВД.

Во всех изолированных сетевых сегментах (размещенных за NAT) облачной инфраструктуры KVM должна быть развернута технологическая виртуальная машина системы ЕЦЭ МВД, обеспечивающая проксирование сетевых запросов от систем ЕЦЭ МВД до серверов ИС.

С целью обеспечения мониторинга и автоматического сбора конфигураций ИС на всех серверах должны быть:

- подняты соответствующие сетевые службы;
- разрешен доступ по SNMP read или WMI (в зависимости от ОС) от систем ЕЦЭ или технологических прокси-серверов;
- обеспечено создание технологической учетной записи на серверах ЕЦЭ для обеспечения целей мониторинга и сбора конфигураций.

В БД должна быть создана технологическая учетная запись, обеспечивающая мониторинг БД и других компонентов.

Должны быть созданы технологические учетные записи в ИС МВД для обеспечения возможности подключения к ИС для проверки их работоспособности.

Технологическая учетная запись должна обладать ограниченными, но достаточными правами, чтобы выполнять необходимые действия для проверки работоспособности ИС.

Требования к документированию

В пояснительной записке к сервису должны быть приведены:

- описание программных компонентов, обеспечивающих работу сервиса;
- описание размещения компонентов на виртуальных или физических серверах (например, в виде схемы развертывания);
- описание методов журналирования ошибок функционирования сервиса, возникающих проблем в работоспособности сервиса;
- при наличии количественных показателей, отражающих состояние сервиса, должны быть реализованы внутренние счетчики, предоставляющие информацию о внутренних показателях работы, и предоставлен интерфейс для их опроса (например, веб-сервис, системный скрипт, запрос в базу данных). Пример: счетчик числа неуспешных транзакций к системе межведомственного обмена за последние 5 минут. Наличие такого счетчика покажет проблемы во взаимодействии сервиса и системы межведомственного обмена.

- при возможности должны быть разработаны тестовые процедуры проверки работоспособности компонентов сервиса.

Пример 1: возможность создания тестовой заявки, не влияющей на отчетность ИС, позволит проверить работоспособность внутренней логики ИС, подтвердить работоспособность заявки и не нарушить отчетность, предоставляемую сервисом.

Пример 2: разработка тестового веб-сервиса, возвращающего статус работоспособности внутренних объектов.

Требования к метрикам мониторинга

Должны быть сформированы метрики мониторинга, обеспечивающие проверку работоспособности сервиса, и методы получения значений их статуса (например, системный скрипт или запрос в базу данных).

Описания метрик должны содержать:

1. Наименование (например, доступность базы данных <название>);
2. Уровень влияния на сервис:
 - сервис недоступен;
 - наличие деградации производительности;
 - недоступность отдельных функциональных возможностей.

Пример 1: в случае недоступности базы данных или сервера приложений система электронного документооборота (СЭД) будет недоступна.

Пример 2: падение модуля отправки оповещений о событиях электронного документооборота приводит к деградации функциональных возможностей СЭД, но не к недоступности сервиса в целом.

Пример 3: переполнение очереди отправки почтовых оповещений приводит к деградации почтового сервиса и к задержке в доставке почтовых писем.

Метрики должны отражать состояние доступности и производительности сервиса в момент проверки их состояния.

Требования к описанию сервиса

Должны быть подготовлены краткие описания сценариев работы пользователя с сервисом, позволяющие проверить работоспособность системы эксплуатационным персоналом.

Описания должны содержать скриншоты экранов сервиса, ссылки на веб-страницы (в случае, если пользовательский интерфейс реализован в виде веб-ресурса), соответствующих этим скриншотам.

Должны быть подготовлены требования к квалификации и численности персонала, необходимого для эксплуатации сервиса.

Заключение

Результатом проведенного научного исследования стали выводы, обобщающие теоретические положения, а также предложения и рекомендации по их практическому применению.

Развитие и внедрение офисных облачных технологий – это важный шаг, направленный на дальнейшую модернизацию профессиональной деятельности в системе МВД России, т.к. документирование управленческой деятельности, работа с обращениями граждан, подготовка плановой и отчетной документации занимают достаточно большое количество рабочего времени.

Современные разработки офисного отечественного программного обеспечения могут быть эффективно использованы в деятельности органов внутренних дел. Создание и освоение новых инструментов для совместной работы позволит в ряде случаев значительно усовершенствовать текущие процессы подготовки документов. В случае интеграции сервера документов с СЭД, сотрудники получают удобный инструмент для организации работы.

Программное обеспечение с открытым кодом имеет ряд преимуществ перед проприетарным ПО.

Во-первых, это дешевизна и антикоррупционность. СПО не требует лицензионных выплат за каждый установленный экземпляр программы. Государство может провести открытый конкурс, однократно заплатить фирме-разработчику за поставку программного обеспечения и затем тиражировать его без ограничений. Таким образом, для обычных пользователей оно будет практически бесплатным.

Во-вторых, СПО более безопасно. Многие проприетарные приложения от известных производителей содержат недокументированные функции, что является потенциальной угрозой. Доступ к исходным кодам программы дает возможность контролировать этот аспект.

В-третьих, СПО легко адаптируется: большое количество доступных свободных приложений позволяет приспособливать их под конкретные нужды пользователей и создавать на их основе новые необходимые программы.

В-четвертых, использование СПО учитывает национальные интересы. Несмотря на то, что создание свободных программ неотделимо от мирового сообщества разработчиков, сервисные услуги по их адаптации, внедрению, поддержке и развитию оказывают, как правило, национальные фирмы, что более выгодно государству и обществу.

Список используемой литературы

1. Исаева, Г.Н. Региональные проблемы внедрения и распространения систем защищаемого электронного документооборота / Г.Н. Исаева, Н.Н. Теодорович, С.А. Басова. – Текст : электронный // НАУКОВЕДЕНИЕ. – 2017, т. 9, № 3. – URL: <http://naukovedenie.ru/PDF/54TVN317.pdf> (дата обращения: 11.10.2020).

2. Конев, С.И. Правовая характеристика системы электронного документооборота как ключевого элемента электронного правительства / С.И. Конев. – Текст : электронный // Контуры глобальных трансформаций: политика, экономика, право. – 2011, № 1. – URL: <https://cyberleninka.ru/article/n/pravovaya-harakteristika-sistemy-elektronnogo-dokumentoooborota-kak-klyuchevogo-elementa-elektronnogo-pravitelstva> (дата обращения: 08.10.2020).

3. Волчинская, Е.К. Электронный документооборот: проблемы хранения / Е.К. Волчинская. – Текст : непосредственный // Информационное право. – 2017, № 1. – С. 4–12.

4. Овчинников, С.А. Основные проблемы сохранения цифровых записей при внедрении электронной подписи и юридически значимого электронного документооборота в России / С.А. Овчинников, Е.П. Болдырева, М.Д. Земсков. – Текст : электронный // Вестник Саратовского государственного социально-экономического университета. – 2013, № 4 (48). – URL: <https://cyberleninka.ru/article/n/osnovnye-problemy-sohraneniya-tsifrovyyh-zapisey-pri-vnedrenii-elektronnouy-podpisi-i-yuridicheski-znachimogo-elektronnogo> (дата обращения: 12.10.2020).

5. Гостев, А.А. Оптимизация документооборота в системе МВД России / А.А. Гостев. – Текст : электронный // Профессионал. – 2018, № 6. – С. 2–6. – URL: <http://www.ormvd.ru/pubs/102/optimization-of-workflow-in-the-system-of-the-mia-of-russia> (дата обращения: 11.10.2020).

6. Шамков, Н.С. Организационно-правовые проблемы внедрения системы электронного документооборота (СЭД) в органах государственного управления по материалам Федеральной службы судебных приставов / Н.С. Шамков. – Текст : электронный // Правовая информатика. – 2012, № 3. – URL: <https://cyberleninka.ru/article/n/organizatsionno-pravovye-problemy-vnedreniya-sistemy-elektronnogo-dokumentoooborota-sed-v-organah-gosudarstvennogo-upravleniya-po> (дата обращения: 07.10.2020).

7. Макаров, В.Ф. Вопросы внедрения систем электронного документооборота в деятельность органов внутренних дел. Область применения электронных документов / В.Ф. Макаров, Б.А. Торопов. – Текст : электронный // Труды Академии управления МВД России. – 2012, № 2 (22). – URL: <https://cyberleninka.ru/article/n/voprosy-vnedreniya-sistem-elektronnogo-dokumentoooborota-v-deyatelnost-organov-vnutrennih-del-oblast-primeneniya-elektronnyh> (дата обращения: 12.10.2020).

Учебно-практическое пособие

Авторы:

кандидат юридических наук
Матросова Лидия Дмитриевна;

кандидат юридических наук
Семенов Евгений Юрьевич;

кандидат технических наук
Линьков Вадим Вячеславович;

кандидат педагогических наук
Шумилин Владимир Петрович

**ТЕКУЩЕЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ
ВНЕДРЕНИЯ ОБЛАЧНЫХ ОФИСНЫХ
РЕШЕНИЙ В ДЕЯТЕЛЬНОСТИ ОВД**

Свидетельство о государственной аккредитации
Рег. № 2660 от 02.08.2017.

Подписано в печать 17.06.2021. Формат 60x90¹/₁₆.
Усл. печ. л. – 2,81. Тираж 40 экз. Заказ № 182.

Орловский юридический институт МВД России имени В. В. Лукьянова.
302027, г. Орел, ул. Игнатова, 2.