ИССЛЕДОВАНИЕ

«Использование электронной почты в государственной инфраструктуре РФ»

Государственные учреждения в России находятся под угрозой взлома почтовых аккаунтов

78% государственных учреждений не используют **специальные** ведомственные **почтовые сервисы.**

Органы и учреждения, имеющие прямое отношение к проблематике информатизации представляют контраст по отношению к прочим: здесь этот показатель составляет 17%.

Содержание

1. Введение 4

2. Оценка уровня информационной безопасности государственных структур 8

3. Анализ базы официальных контактов государственных и муниципальных органов власти и бюджетных учреждений 10

4. Анализ сайтов федеральных органов исполнительной власти 14

5. Отношение к вопросам информационной безопасности в различных структурах 16

6. Заключение 21

7. Приложения 23

   7.1 Методология исследования 24

   7.2 База исследования. Статистические таблицы 31

1 Введение

Способы обмена электронными письмами начали разрабатываться в 1960-х гг. в Массачусетском технологическом институте: первая почтовая программа была написана в 1965 г. и позволяла пересылать электронные сообщения между двумя удаленными компьютерами, связанными посредством телефонной сети. К концу 1971 г. программист Рэй Томлисон создал уже полноценную почтовую программу, использующую систему персональных адресов в их современном виде, с литерой @ в середине.

С развитием сети Интернет в 1990-х гг. сервисы электронной почты начали массово использоваться в сети. Уже к 2011 г.[1] число учетных записей электронной почты составляло более 3 млрд. 25% из них приходилось на долю юридических лиц, причем число входящих и исходящих сообщений достигало 107 триллионов сообщений в день. К концу минувшего 2015 г. число почтовых аккаунтов достигло 4,1 млрд, причем в течение 2016 г. прогнозируется 7%-й прирост.

Масштаб охвата пользовательской аудитории почтовыми сервисами и необходимость соблюдения национальных интересов России вызвали к жизни новые правила, регулирующие использование этого типа связи. 31 декабря 2014 года был принят федеральный закон № 531-ФЗ «О внесении изменений в статьи 13 и 14 Федерального закона “Об информации, информационных технологиях и о защите информации” и Кодекс Российской Федерации об административных правонарушениях», согласно которому технические средства информационных систем, используемых государственными органами, органами

> “...технические средства информационных систем, используемых государственными органами ... должны размещаться на территории Российской Федерации.”

1 http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf

местного самоуправления, государственными и муниципальными унитарными предприятиями или государственными и муниципальными учреждениями, должны размещаться на территории Российской Федерации.

Реальные риски, связанные с использованием "небезопасных" сервисов и средств передачи информации, сегодня осознаются на самом высшем уровне руководства России. 26 августа 2015 г. Секретарь Совета Безопасности РФ на совещании с главами регионов Дальневосточного федерального округа и представителями федеральных министерств и ведомств, посвящённом вопросам защиты информации в информационных системах органов государственной власти и органов местного самоуправления, критически высказался в отношении использования органами власти таких зарубежных сервисов, как Google, Yahoo и WhatsApp.

При этом в части использования отечественных публичных почтовых сервисов, как, например, Mail.ru, Yandex и т.п., никакой регулирующей конкретизации на уровне нормативных правовых актов нет и не может быть, так как существующие нормативно-правовые акты такие регламенты не устанавливают. Также можно отметить, что правоустанавливающие документы в области информационной безопасности, принятые в ряде регионов России, не менялись с 2000 года, когда была утверждена Доктрина информационной безопасности РФ. Положения этих документов повторяют положения Доктрины.

При этом электронная почта играет важную роль в оптимизации работы государственных организаций. Специфика онлайн-коммуникации госучреждений состоит в том, что они, в силу своих полномочий и обязанностей, регулярно имеют дело с данными, не подлежащими разглашению. Это может быть личная информация о гражданах, конфиденциальная информация и, наконец, секретные данные. Особое внимание к обеспечению безопасности переписки государственных структур видится в этом свете чрезвычайно важным, так как массовые утечки персональных данных и другой информации стали сегодня практически повседневным явлением. Достаточно вспомнить масштабную утечку персональных данных 4 миллионов госслужащих в США[2].

> **Подавляющее большинство учреждений, в том числе федерального уровня используют небезопасные публичные почтовые сервисы.**

2 https://www.washingtonpost.com/world/national-security/chinese-hackers-breach-federal-governments-Ц-office/2015/06/04/889c0e52-0af7-11e5-95fd-d580f1c5d44e_story.html

Вопрос информационной безопасности государственных структур России стал предметом данного исследования.

В рамках исследования было проанализировано использование почтовых сервисов федеральными органами исполнительной власти на основе данных из открытых источников, в том числе официальных сайтов ФОИВ, Bus.gov.ru и Budget.gov.ru. Разумеется, исследовались исключительно головные организации, так как их информационная политика является направляющей для подчиненных структур, а проявления хаотических тенденций (допустимых с точки зрения руководства структур нарушений политики информационной безопасности, недостаточно ответственного отношения к служебной и секретной информации и пр.) нарастают по мере расширения системы. Иными словами, по положению дел в министерстве можно судить о положении дел в большинстве организационно подчиненных ему структур, принимая во внимание «организационную энтропию» - рост числа нарушений по мере удаления от руководящего центра.

Также для целей данного исследования использовались контактные данные, предоставляемые учреждением в системе государственных закупок. Можно допустить, что для более ответственных задач учреждения используют более безопасные инструменты связи. Однако при наличии собственного надежного почтового сервиса следовало бы ожидать, что учреждение или структура будет пользоваться для решения всех своих официальных задач именно этим инструментом. Использование же публичных почтовых сервисов говорит об отсутствии собственной внутренней почты и об отношении к политике информационной безопасности в целом: при применении «небезопасной» почты в сфере закупок в случае взлома может произойти утечка не только персональной информации о служащем, создавшем аккаунт, но и материалов, содержащих коммерческую тайну – заявок от поставщиков и запросов от них, информации о конкурентах, о распределении бюджета государственной структуры и пр.

Таким образом базовыми материалами данного исследования стали:

- официальные адреса электронной почты государственных структур (были проанализированы официальные почтовые адреса 72-х федеральных органов исполнительной власти),
- наиболее активно использующиеся адреса электронной почты государственных структур (259 750 организаций различного уровня).

Данная выборка не покрывает всей совокупности адресов электронной почты государственных структур Российской Федерации, однако является достаточно репрезентативной для того, чтобы делать

серьезные организационные выводы и планировать расширение и продолжение исследовательской работы в данном направлении.

Наше исследование, несмотря на его масштаб, безусловно, не является всеобъемлющим и охватывает лишь видимую часть айсберга неурегулированной ситуации в области государственной информатизации и нерегулируемого использования внешних сервисов. За его пределами остаются: использование адресов электронной почты чиновников не в рамках госзаказа, размещение официальных веб-серверов и почтовых серверов органов власти и госучреждений за границей, использование персональных облачных сервисов обмена файлами составляющими служебную тайну[3] и многое другое.

Прежде, чем перейти к описанию результатов исследования, необходимо подчеркнуть, что во-первых, на данном этапе исследования не оценивалась техническая резистентность сервисов к кибератакам, которая может варьироваться в зависимости от оператора, а во-вторых, базовые материалы собирались исключительно из открытых источников, так как отслеживание использования бесплатных адресов электронной почты другими способами относится к сфере методов, применение которых невозможно без санкции соответствующих силовых органов.

Подробная методология исследования вынесена в Приложение 1.

3 О безопасности информации при использовании облачных сервисов органами государственной власти см.: https://www.hse.ru/data/2014/09/03/1316486220/%D0%A2%D0%B5%D1%80%D0%B5%D1%89%D0%B5%D0%BD%D0%BA%D0%BE.pdf

2 Оценка уровня информационной безопасности государственных структур

Под безопасностью в данном исследовании понимается соответствие следующим критериям:

1. Данные переписки хранятся на сервере, управление которого гарантированно заинтересовано в том, чтобы эти данные организаций оставались сохранными и конфиденциальными (в случае с публичными почтовыми сервисами такой гарантии, в принципе, быть не может).

2. В случае использования почтовых сервисов вне собственного сервера доступ к персональной, коммерческой и конфиденциальной информации строго регламентирован, и в случае нарушения регламента оператор почтового сервиса несет ответственность.

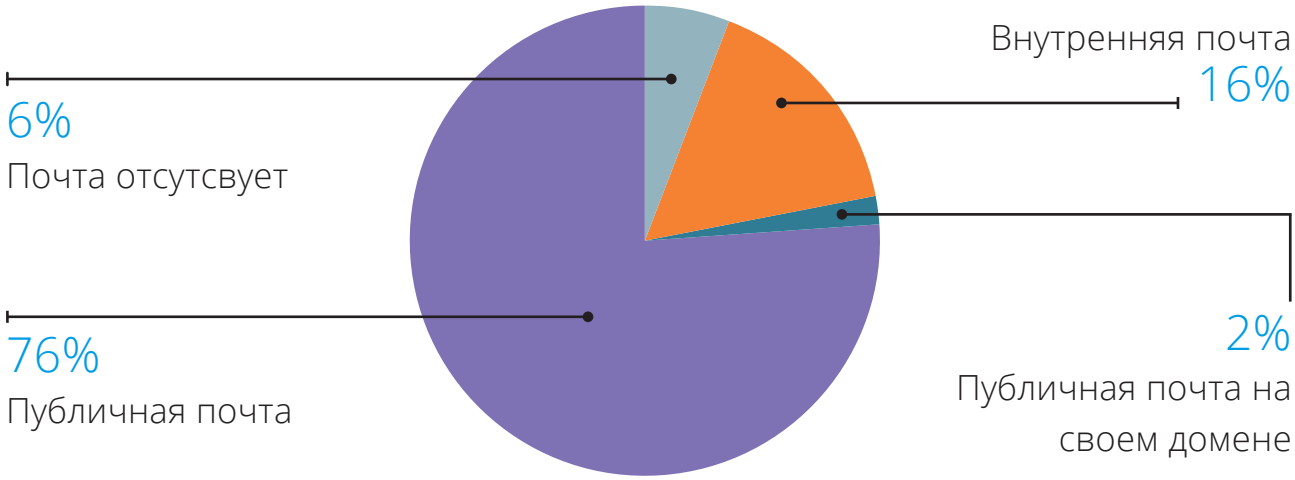
Под гарантиями сохранности мы понимаем условия, в которых данные переписки гарантированно не разглашаются, а поставщик услуг несет ответственность за нарушение конфиденциальности.

С этой точки зрения, публичные почтовые сервисы представляются заведомо небезопасными для официальных государственных структур, так как они не отвечают, как минимум, двум из трех характеристик. Конечно, любой публичный почтовый сервис обязуется сохранять конфиденциальность и защищать персональные данные, но никаких гарантий при этом не предоставляется. Мотивация к выполнению обязательств в таких случаях, прежде всего, репутационная. Однако юридической ответственности за утечку данных переписки оператор публичного почтового сервиса не несет.

Таким образом, приходится констатировать, что публичные почтовые сервисы принципиально небезопасны.

Вывод: Согласно результатам исследования, 78% государственных структур находятся в зоне риска

Процент используемых почтовых сервисов в рассмотренных ФОИВ



Под публичной веб-почтой понимаются общедоступные почтовые веб-сервисы, на которых любой пользователь может создать себе почтовый аккаунт. Известные примеры таких сервисов - Mail.ru, Yandex.ru, Rambler.ru, Gmail.com, а также многие другие.

Как видно из таблицы, публичной веб-почтой пользуется подавляющее количество организаций (почти 76%).

К “внутренним” почтовым сервисам относятся все прочие виды указанных действительных адресов, которые не относятся к публичным. Это могут быть хостинги, собственные серверы, сервисы, предоставляемые интернет-провайдером. В каждом конкретном случае могут быть свои изъяны, однако их объединяет то, что им необязательно присущи те изъяны безопасности, которые неизбежно характеризуют публичные сервисы.

Тем не менее, такими почтовыми сервисами пользуются всего 16% рассмотренных организаций.

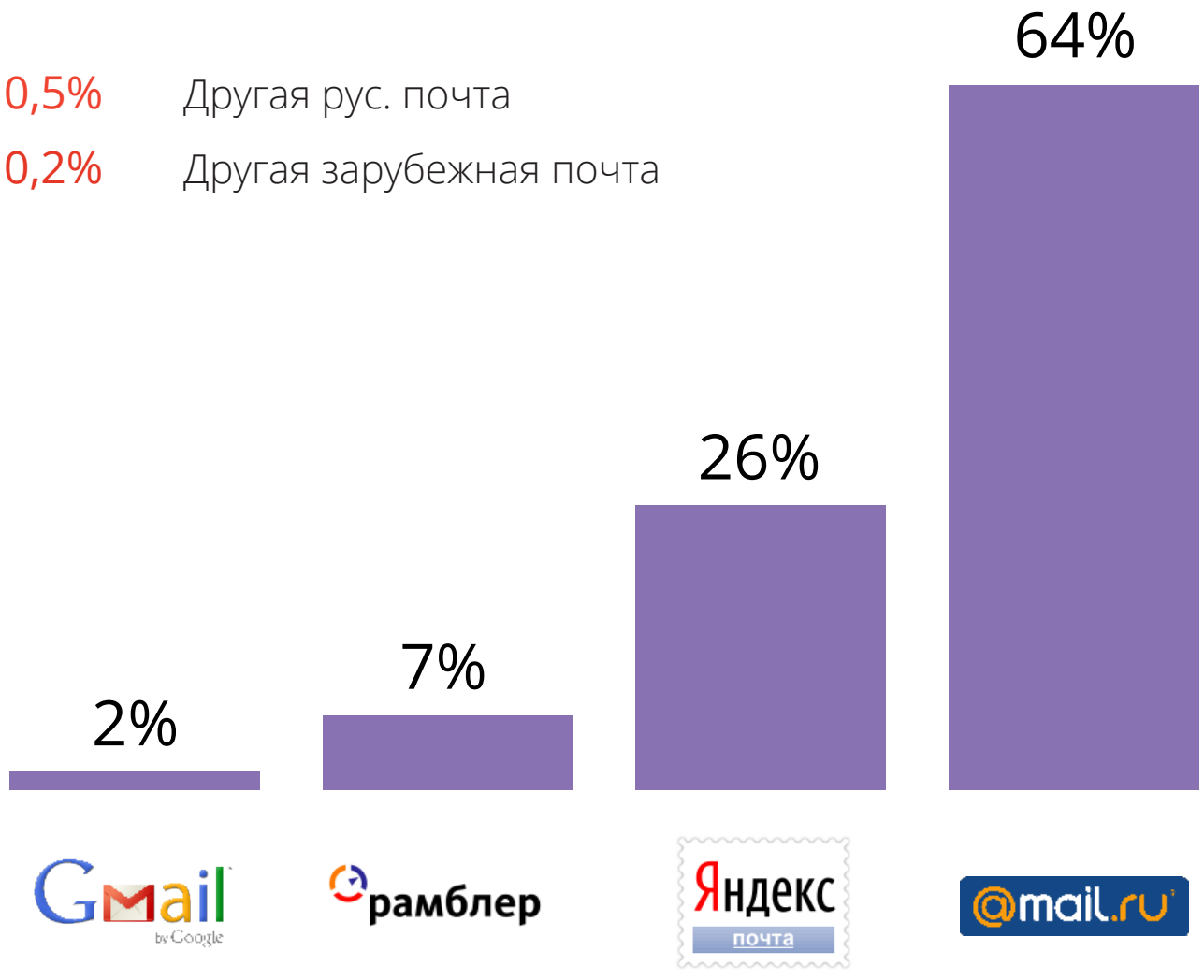
Еще 2% организаций используют публичную почту с привязкой к собственному домену[1]. Привязка к своему домену делает электронный адрес более “официальным” и имиджевым, но фактически условия предоставления услуг (и, следовательно, уровень безопасности) - те же, что и в случае с публичной веб-почтой. Таким образом, мы можем констатировать, что 78% государственных организаций использует публичную почту.

1 Например, адрес, указанный Муниципальным учреждением "Совет депутатов городского округа Электрогорск Московской области" выглядит так: sovet@elgorsk-adm.ru. На самом деле для домена elgorsk-adm.ru почтовым сервером служит alt1.aspmx.l.google.com.

3 Анализ базы официальных контактов государственных и муниципальных органов власти и бюджетных учреждений

Наиболее полный материал для анализа использования публичной почты предоставляет база государственных закупок. Как показывают данные, наибольшей популярностью пользуется публичный почтовый сервис Mail.ru. Также мы видим, что зарубежные почтовые сервисы (например, Google) существенно менее популярны. Между тем, как видно из таблицы 2, разнообразие публичных веб-сервисов очень невелико. 97% организаций, использующих веб-почту (то есть почти все эти организации), распределены между круп-

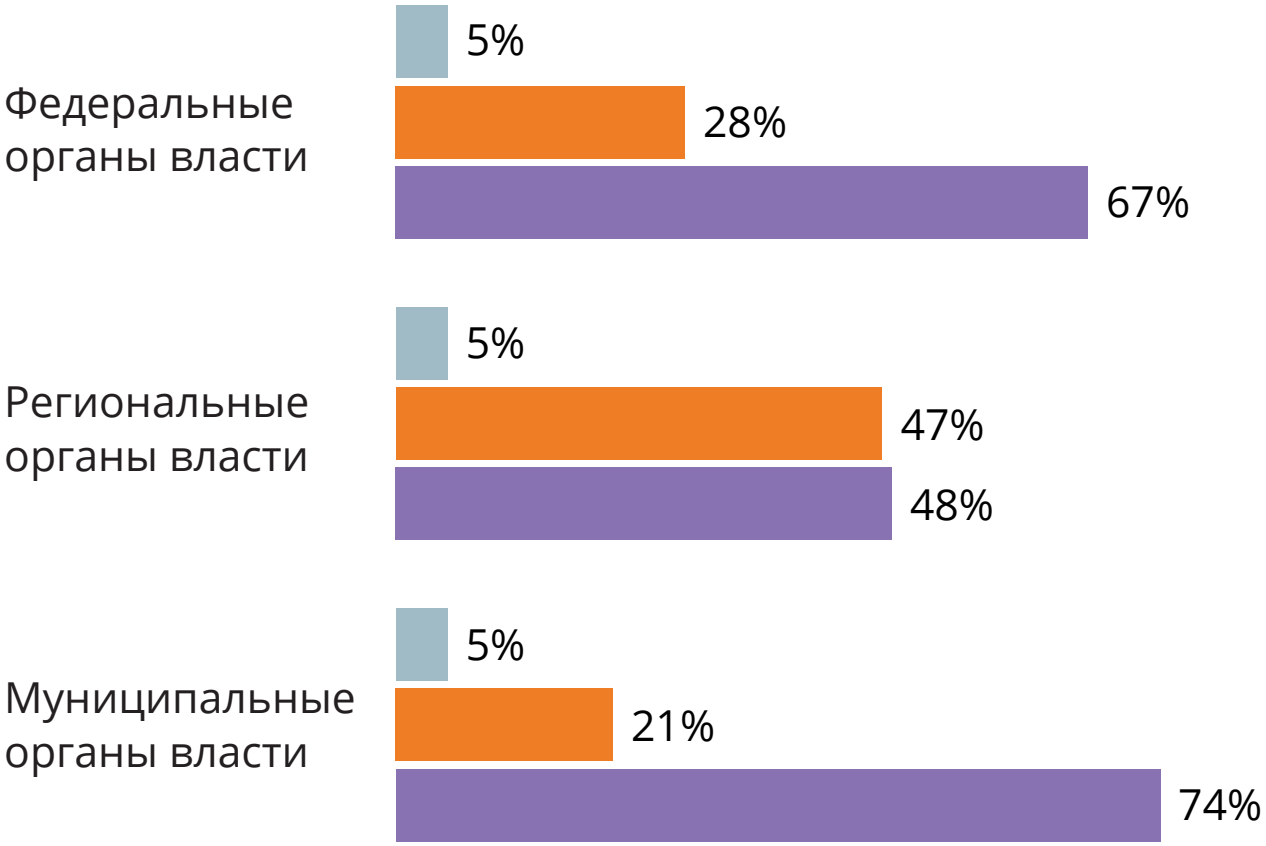
Распределение используемых публичных почтовых сервисов по провайдерам услуг



нейшими российскими провайдерами публичных почтовых услуг: Mail.ru, Yandex.ru и Rambler.ru. Эти сервисы уже в силу масштаба своей аудитории постоянно подвергаются хакерским атакам. Это значит, что, помимо целенаправленых кибератак, государственные организации, использующие публичные сервисы, рискуют стать жертвами общих атак. Из-за их масштабности, они постоянно подвергаются хакерским атакам.

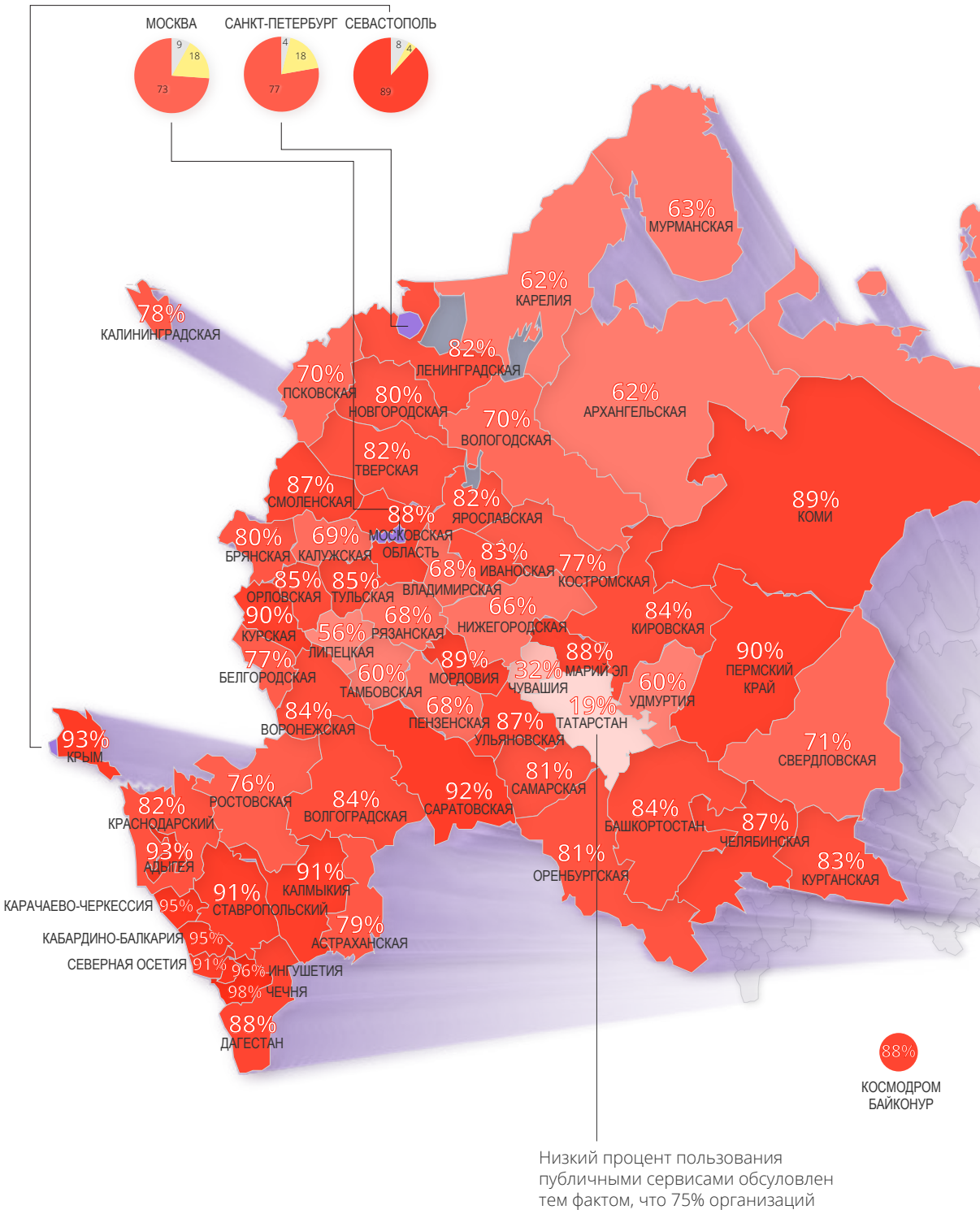
В этом смысле российские публичные сервисы не более безопасны, чем зарубежные. 97% государственных организаций используют публичные сервисы, а значит, рискуют стать жертвами кибератак. Эти данные основаны на контрактных данных, но здесь можно вспомнить о том, что почти 70% от ФОИВ, по которым были доступны данные об использовании почтовых сервисов из других открытых источников, используют почту Microsoft.

Распределение в различных уровнях органов власти



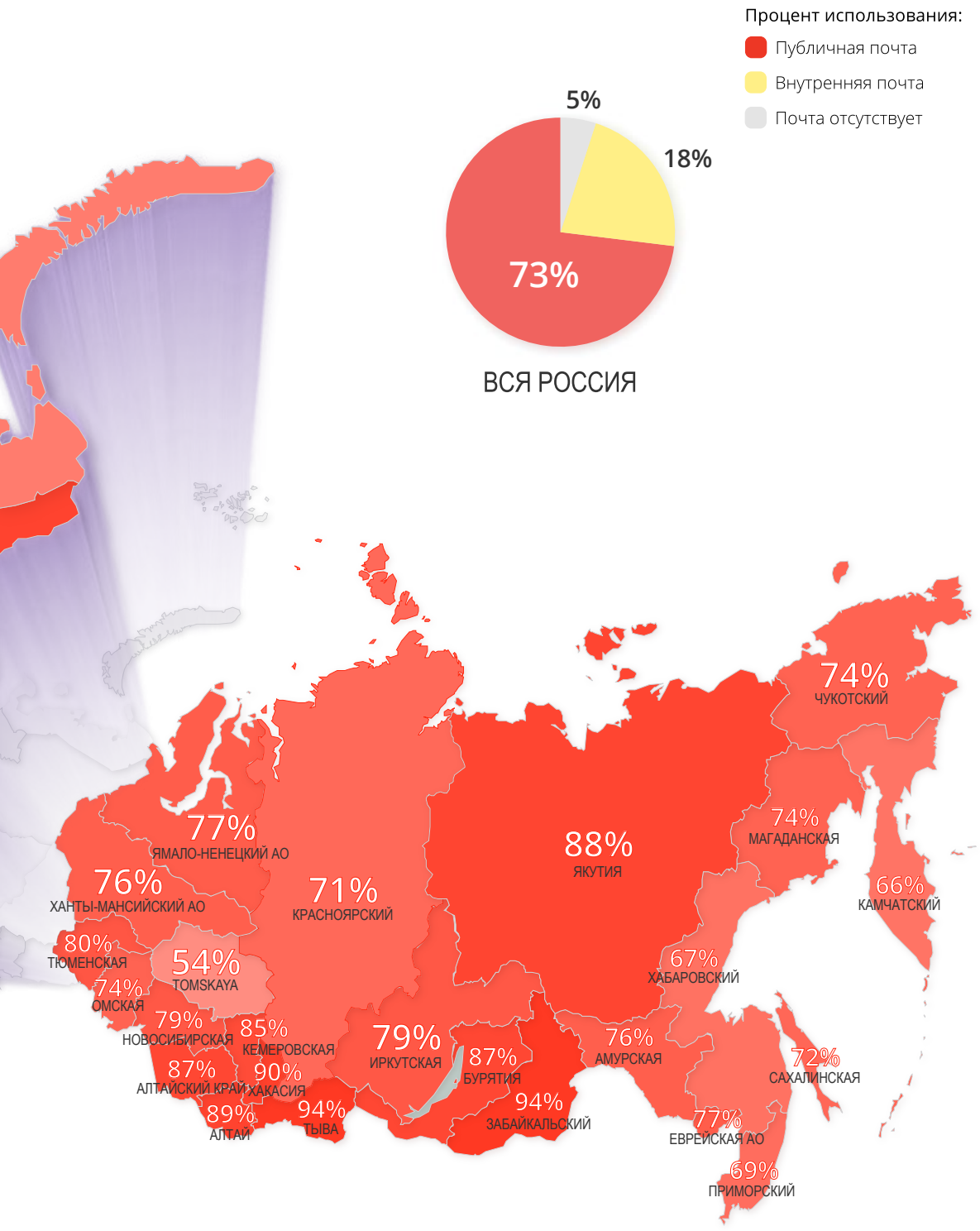
На всех уровнях доля организаций, использующих публичную почту, составляет, как минимум, около 50%.

Использование почтовых сервисов по регионам РФ



Низкий процент пользования публичными сервисами обусловлен тем фактом, что 75% организаций

Использование почтовых сервисов по регионам РФ



4 Анализ сайтов федеральных органов исполнительной власти

В рамках исследования был проведен анализ почтовых серверов 72 федеральных органов исполнительной власти (ФОИВ). Данные были собраны из открытых источников, в частности, использовались почтовые адреса, размещенные на официальных сайтах организаций. У 43 из рассмотренных организаций были найдены веб-интерфейсы для почтовых серверов (Таблица 1).

Таблица 1: Анализ почтовых серверов ФОИВ

Почтовые сервисы по видам	Число организаций	% от общего числа
Microsoft	30	41,6(7)
CommuniGate	3	4,16(7)
Zenon	3	4,16(7)
Почта для домена	3	4,16(7)
Неизвестные	17	23,6(1)
Остальные	16	22,2(2)

> Это значит, что его сервисы неизбежно становятся мишенью для целенаправленного взлома, и методы взлома постоянно совершенствуются.

Анализ показал, что наибольшей популярностью пользуются почтовые сервисы Microsoft, их использует более 30 ведомств, в основном с организацией доступа через интернет (Outlook Web App). Это составляет 42% от числа всех рассмотренных организаций и почти 70% от организаций, по которым были доступны данные об использовании почтовых серверов.

Остальные службы гораздо менее популярны. 3 федеральные службы (ФСТЭК, Росавиация и ФАДН) используют сервисы почты для доменов Mail.ru, Nic.ru и Yandex'a соответственно. Одно федеральное агентство (Ростуризм) использует почту своего интернет-провайдера.

Наконец, некоторые ведомства, например Росслесхознадзор[1], продолжают указывать в качестве контактных адреса на сервисах бесплатной почты например на доменах bk.ru, gmail.com, yandex.ru.

Ситуация с преобладанием Microsoft, вероятно, объясняется тем, что Microsoft - ведущий игрок на рынке. Проблема массового использования услуг Microsoft связана с тем же. Это значит, что его сервисы неизбежно становятся мишенью для целенаправленного взлома, и методы взлома постоянно совершенствуются. Косвенно это подтверждается тем, что в Сети при обсуждениях способов взлома почты особо оговариваются методы взлома почты Microsoft.

Таким образом, анализ официальных адресов ФОИВ дает основания для тех же выводов, что и анализ контактных данных из базы госзакупок: в каждом случае не менее 70% государственных организаций, данные по которым были доступны, используют почтовые сервисы, либо не имеющие формальных договоров с органами власти (бесплатные сервисы почты), либо созданные на базе ПО и услуг зарубежных вендоров.

1 http://www.rosleshoz.gov.ru/media/contact%20details

5 Отношение к вопросам информационной безопасности в различных структурах

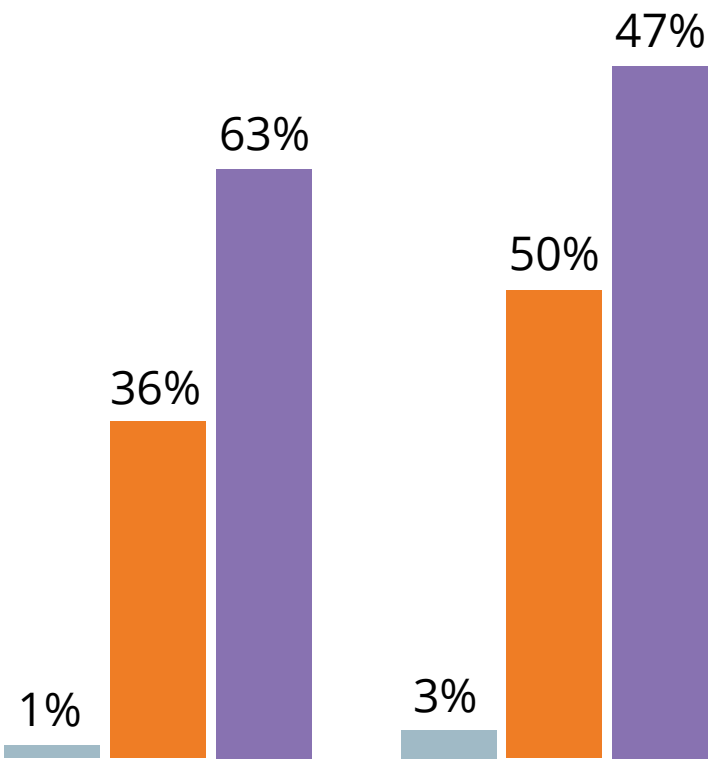
Уровень ответственности и секретности информации может иметь корреляты на уровне выбора почтового сервиса. Так, например, 70% судебных организаций использует внутренние почтовые серверы. Впрочем, среди судов тоже нет однородности. Арбитражные суды в наибольшей степени склонны использовать внутренний почтовые сервисы: публичными пользуются всего 11% учреждений. При этом 75% военных судов, наоборот, предпочитают публичные сервисы. В остальных типах судов использование публичных и внутренних сервисов распределяется примерно поровну. Обобщая, можно заключить, что многие суды не пренебрегают принципами кибербезопасности, однако существенная их доля использует «небезопасные» сервисы (либо не имеющие официальных договоров с органами власти, такие, как сервисы бесплатной электронной почты, либо созданные на базе ПО зарубежных коммерческих вендоров).

Также можно отметить, что подавляющее большинство отделов ОВД (81%), от которых тоже можно было бы ожидать повышенного внимания к цифровой безопасности, использует публичную почту.

“Обобщая, можно заключить, что многие суды не пренебрегают принципами кибербезопасности, однако существенная их доля использует небезопасные сервисы.

Примеры использования публичных почтовых сервисов в разных организациях

Использование электронной почты силовыми структурами



Силовые структуры (ФСБ, ФСО, ФСКН, Следственный. Комитет, фельдъегерская служба)

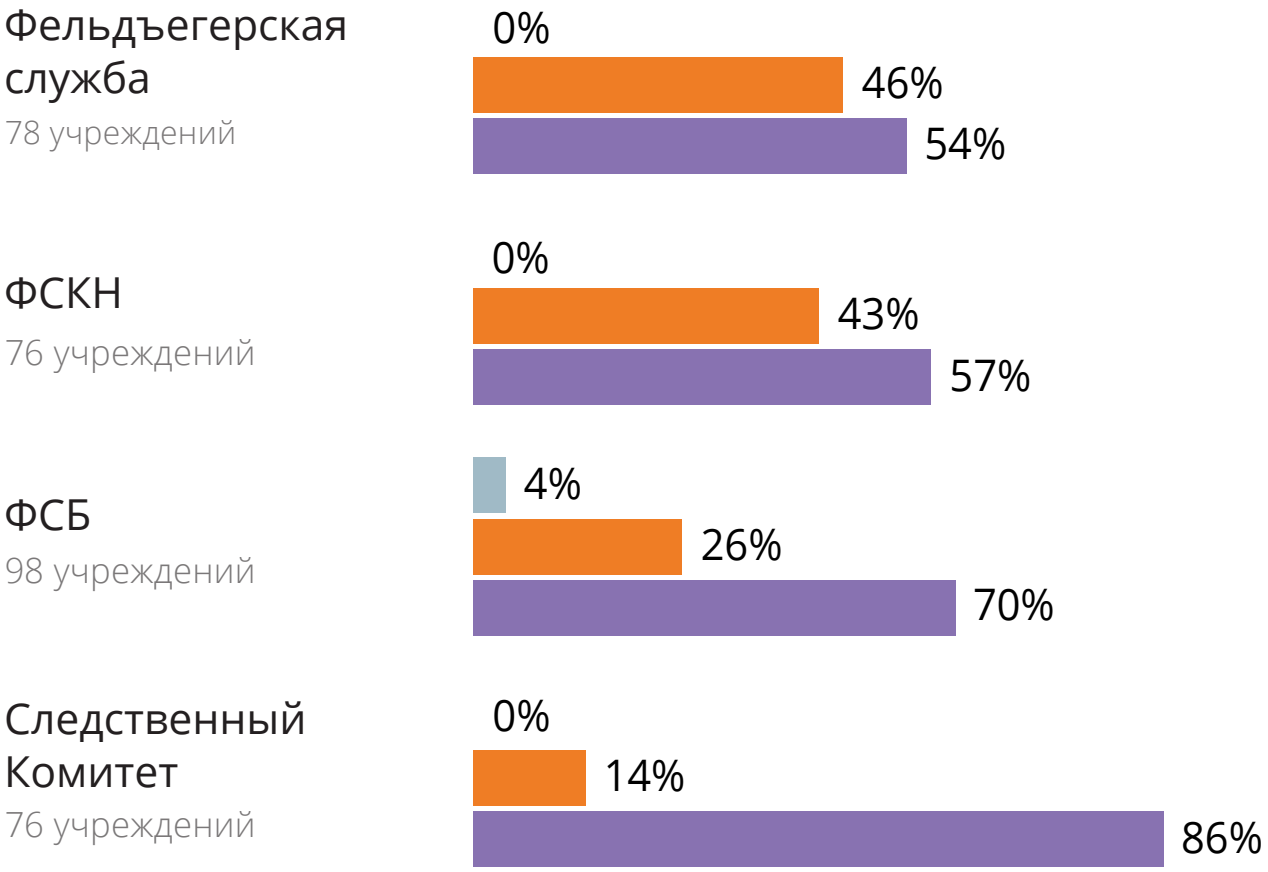
Центры специальной. связи и информации ФСО

Отдельный интерес представляет использование электронной почты силовыми структурами, которым по долгу службы необходимо соблюдать секретность: ФСБ, ФСО, Следственным комитетом, ФСКН и Фельдъегерской службой.

63% этих организаций используют публичную веб-почту. Несмотря на доступ к средствам специальной связи и режим повышенной секретности, почти половина центров спецсвязи ФСО использует публичную почту для контакта с поставщиками. Это может быть чревато, как минимум, утечкой личных данных сотрудников.

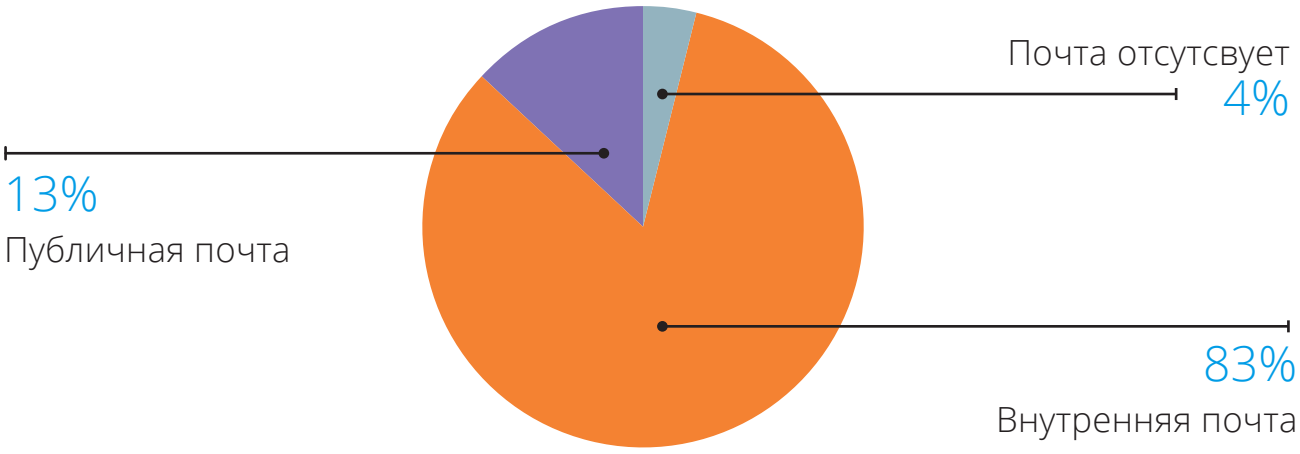
Мы также приводим детализацию по ФСБ, ФСКН, Следственному комитету, Фельдъегерской службе. Мы видим, что у всех этих служб доля использования публичных сервисов превышает долю внутренних сервисов. Особенно это касается ФСБ (70% использует публичные сервисы) и Следственный комитет (86% использует публичные сервисы).

Использование электронной почты некоторыми силовыми структурами



В связи с этим интересно посмотреть на распределение использования публичных и внутренних сервисов IT-службами, которые в силу своей специализации должны быть наиболее компетентными в вопросах кибербезопасности, и их предпочтения в плане использования почтовых технологий.

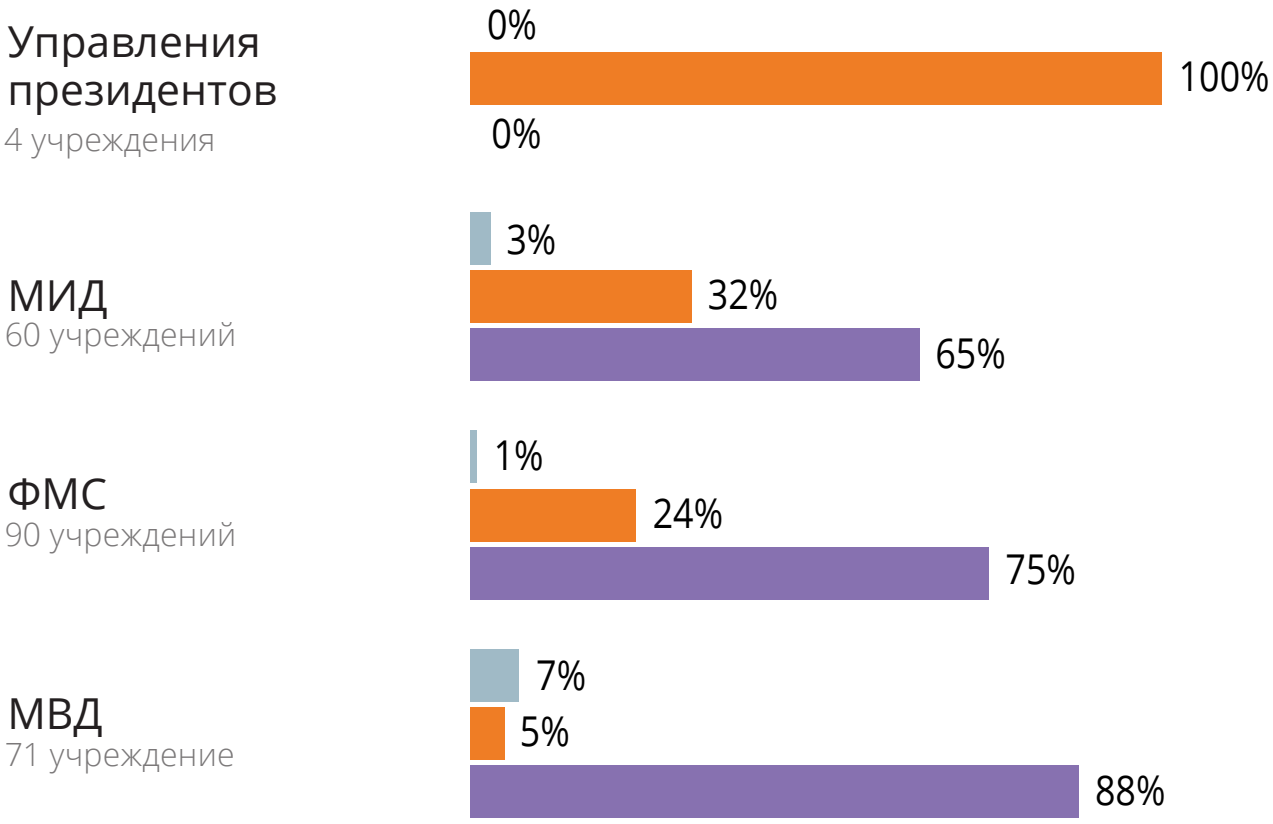
Использование электронной почты IT-службами



Здесь можно сделать два наблюдения. Во-первых, показательно, что 83% IT-департаментов используют внутренние сервисы. Во-вторых, приходится констатировать, что 13% таких организаций всё же используют публичную почту.

Управления делами президентов, представленные в базе, вообще не используют публичные сервисы. Одновременно с этим мы наблюдаем заметное преобладание публичных сервисов над внутренними в таких крупных и ответственных федеральных службах, как МИД, ФМС и МВД.

Использование электронной почты некоторыми ведомствами



6 Заключение

В ходе исследования обнаружен исключительно высокий уровень использования публичной веб-почты среди органов власти всех уровней, включая федеральный. Доля организаций, использующих публичные сервисы, составила 78% от числа всех рассмотренных организаций и более 80% от числа организаций, предоставивших валидные электронные адреса.

На этом фоне можно выделить ряд ведомств и министерств, у которых использование внутренних почтовых сервисов, наоборот, преобладает над использованием публичных сервисов. К числу таких институтов относится Министерство финансов, Министерство экономического развития, департаменты по информатизации. С одной стороны, это закономерно, с точки зрения того, что именно от такого рода ведомств следует ожидать большого внимания к вопросам информационной безопасности. С другой стороны, приходится отметить, что даже у организаций, относящихся к таким ведомствам, зачастую доля использования публичных сервисов не ниже 15%.

В то же время было установлено, что ряд ведомств, от которых можно было бы ожидать особой бдительности в плане интернет-безопасности, тем не менее предпочитает использовать публичные сервисы. Речь идет, прежде всего, о силовых структурах, где доля организаций, использующих публичную почту, может достигать и даже существенно превышать 50%. В частности, доля использования публичных сервисов у ФСБ составляет 70%, а у Следственного комитета - 86%.

Эти наблюдения подтверждаются исследованием использования почтовых серверов федеральными органами государственной власти на основе контактных данных, предоставляемых, в частности, на официальных сайтах. 70% организаций, релевантные данные по которым оказались доступны, используют почтовые серверы Microsoft, что делает их потенциальной мишенью для целенаправленных кибератак.

На основе ранее публиковавшихся исследований 2012[1] и 2014 годов можно заключить, что отсутствие защищённых почтовых сервисов у органов государственной власти является повсеместным и неизменным.

1 Roem.ru: “Половина госучреждений сидит на почте Mail.Ru” https://roem.ru/03-09-2012/131458/begtin-polovina-gosuchrejdeniy-sidit-na-pochte-mailru/

Подводя итоги исследования, можно сделать следующие краткие выводы

Государственные учреждения в России находятся под угрозой взлома и утечки информации, являющейся служебной тайной.

Почти 80% учреждений использует неподконтрольные публичные почтовые сервисы.

Подавляющее большинство учреждений, в том числе федерального уровня, использует «небезопасные» публичные почтовые сервисы (не имеющие официальных договоров с органами власти).

Только 7% государственных организаций пользуется специальными ведомственными почтовыми сервисами.

Приложения

Приложение 1

Методология исследования

Анализ использования почтовых сервисов федеральными органами исполнительной власти (ФОИВ)

При анализе ФОИВ использовались данные из открытых источников, в первую очередь ресурсов Bus.gov.ru[1] и Budget.gov.ru[2], а также официальных сайтов ФОИВ. Список сайтов приводится в Приложении.

Всего было проанализировано 72 организации. Целью анализа было определение типа используемого сервиса электронной почты. Информация, необходимая для этого анализа была обнаружена по 43 из рассмотренных организаций.Определение типа сервиса проводилось на основе:

- анализа официальных контактов на официальном сайте (выявление базового домена для электронной почты);
- анализа почтовых серверов домена с помощью публичных онлайн-баз данных, таких как censys.io, scans.io и других;
- анализа DNS/MX записей домена, используемого данным органом власти в качестве основного;
- непрямого анализа сертификатов SSL/TLS, ассоциированных с данным доменом, на основании базы censys.io.

По результатам анализа была разработана система классификации веб-серверов и идентификации их вендоров.

Описание выборки из базы государственных закупок

Анализ использования электронной почты также проводился на основе данных из реестра организаций с Официального портала государственных закупок. В основу выборки легли организации, закупающиеся в соответствии с 44-ФЗ3, то есть финансирующиеся из бюджета РФ. На момент 31 марта 2016 г. в реестре было представлено 269 619 организаций. Так как ФЗ-44 был введен в 2014 году, мы анализируем только те контактные данные организаций, которые используются с 2014 и по настоящее время.

Далее выборка была отфильтрована по типу организации. В ней были оставлены:

- органы государственной власти;

1 http://bus.gov.ru/

2 http://budget.gov.ru/

3 44-ФЗ - Федеральный закон о контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: https://www.consultant.ru/document/cons_doc_LAW_144624/

- органы управления государственными фондами (пенсионным и ОМС);
- бюджетные, казенные и автономные госучреждения.

Из выборки были удалены унитарные предприятия, предприятия, имеющие долю с государственным участием, естественные монополии и иные предприятия. Также из выборки удалено 628 дублированных записей (в случаях, когда у организации поменялся только КПП, но название и адрес электронной почты не изменились, эта запись оказывалась в первоначальной выборке дважды).

Финальная выборка в разбивке по типам организаций общим числом 259 750 выглядит так (Таблица 1).

Электронная почта, доменные имена и почтовые сервисы

Использование учреждением электронной почты определялось по адресу электронной почты, указанному в контактах учреждения на Официальном портале госзакупок.

Электронная почта почта всегда состоит из двух частей: имя_пользователя@имя_домена.

Следует различать имя домена, указанное в электронной почте и имя почтового сервера, обрабатывающего этот домен. Почтовый сервер определяется при запросе к специальной DNS-службе[4] по имени домена и может отличаться от имени домена в адресе. Далее почтовые серверы были классифицированы на разные группы в зависимости типа сервиса и владельца домена. Владелец домена определялся с помощью сервиса Whois[5], выдающего информацию о регистрации домена.

Подход к классификации проиллюстрирован на следующем примере (Таблица 2).

4 DNS-сервер, name server — приложение, предназначенное для ответов на DNS-запросы по соответствующему протоколу. Также DNS-сервером могут называть хост, на котором запущено приложение. https://ru.wikipedia.org/wiki/DNS-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80

5 http://www.whois-service.ru/

Таблица 1

Категория	Число организаций
Органы государственной власти	52 949
Органы управления государственными фондами	2 287
Бюджетные учреждения	143 217
Казенные учреждения	54 330
Автономные учреждения	6 968
Всего	259 750

Таблица 2

	Организация	Email	Имя домена	Почтовый сервер	Классификация
1	ОБЛАСТНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ УЧРЕЖДЕНИЕ «ТОМСКОЕ УПРАВЛЕНИЕ ЛЕСАМИ»	elena@les.tomsk.gov.ru	les.tomsk.gov.ru	mail.les.tomsk.gov.ru	Собственный сервер
2	Комитет по образованию Администрации Омского муниципального района Омской области	zakupkiobraz@yandex.ru	yandex.ru	mx.yandex.ru	Публичная веб-почта
3	Муниципальное учреждение Совет депутатов городского округа Электрогорск Московской области	sovet@elgorsk-adm.ru	elgorsk-adm.ru	alt1.aspmx.l.google.com	Публичная веб-почта
4	ОБЛАСТНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ «БОРОВИЧСКАЯ МЕЖРАЙОННАЯ ВЕТЕРИНАРНАЯ ЛАБОРАТОРИЯ»	vetlabbor@novgorod.net	novgorod.net	mx1.novgorod.net	Интернет-провайдер “Ростелеком”

Таблица 2

	Организация	Email	Имя домена	Почтовый сервер	Классификация
5	МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ КУЛЬТУРЫ ЛЕНИНСКОГО СЕЛЬСКОГО ПОСЕЛЕНИЯ «ЛЕНИНСКИЙ СЕЛЬСКИЙ ДОМ КУЛЬТУРЫ»	Lenbibl@aksay.ru	aksay.ru	mx-first.donpac.ru	Интернет провайдер “Ростелеком”
6	Управление Министерства внутренних дел Российской Федерации по закрытому административно-территориальному образованию город Озерск Челябинской области	uvd2@ozersk.ru	ozersk.ru	mx1.ozersk.ru	Портал / Хостинг
7	МУНИЦИПАЛЬНОЕ БЮДЖЕТНОЕ УЧРЕЖДЕНИЕ ОЗЁРСКОГО ГОРОДСКОГО ОКРУГА «ГОРОДСКОЙ МУЗЕЙ»	0o0@adm.ozersk.ru	adm.ozersk.ru	mx.adm.ozersk.ru.	На субдомене портала/ провайдера

Таблица 2

	Организация	Email	Имя домена	Почтовый сервер	Классификация
8	ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ГОРОДА МОСКВЫ ДЕТСКИЙ САД № 2435	skazka2435@mosuzedu.ru	mosuzedu.ru	mx.ekis.ru.	Другое (другая коммерческая структура)
9	АДМИНИСТРАЦИЯ МУНИЦИПАЛЬНОГО РАЙОНА ШЕНТАЛИНСКИЙ САМАРСКОЙ ОБЛАСТИ	econom@shentala.ru	shentala.ru	mail.shentala.ru.	Другое (контроль утрачен)

В случае 1 почтовый сервер был расположен на официальном государственном портале Томской области. Почтовый сервер явным образом принадлежит государственному учреждению (причем, как в этом случае, это может и быть сервер вышестоящего учреждения). В таких случаях мы относим почту к категории «собственный сервер».

В случае 2 для почтового сервера использовалась публичная веб-почта Яндекса.

В случае 3, хотя имя домена выглядит как сервер администрации, на самом деле

этот адрес обслуживается публичным почтовым сервером Google.com.

В случаях 4 и 5 почтовый сервис был предоставлен местным провайдером интернета.

В случае 6 почтовый ящик размещен на сайте негосударственного развлекательного портала ozersk.ru. Такие случаи мы объединяем со случаями, когда почтовый сервис предоставлен провайдерами хостинга сайтов.

Случай 7 отличается тем, что для почтового сервера используется субдомен портала: adm.ozersk.ru.

Использование субдоменов на серверах провайдера и хостинга говорит о том, что учреждение использует отдельный почтовый сервер с большей степенью

контроля. Эти случаи мы тоже выделяем в особую группу.

В случаях 8 и 9 почтовый сервер принадлежит другой коммерческой структуре, не относящейся к упомянутым категориям, либо контроль администрации над сервером был утрачен, и сервером владеет другое лицо. Такие случаи, а также случаи, когда нам не удалось достоверно определить владельца почтового сервера были объединены в категорию «другое/не определено». В них попало 929 организаций, что составляет 0.35% от общего числа организаций.

Интерпретация результатов

При интерпретации полученных нами результатов следует учитывать, что для анализа брались контактные данные с портала госзакупок, а не, например, с собственного сайта учреждения. Таким образом, если мы фиксируем, что учреждение использовало публичную веб-почту на сайте госзакупок, это не обязательно означает, что учреждение не пользуется собственным почтовым сервером для приема обращений граждан или для внутренней переписки. Это значит лишь, что для контакта с поставщиками ответственное лицо в учреждении предпочло использовать личную или общественную web почту. Тем не менее этот факт тоже является самодостаточным для вывода об IT-инфраструктуре учреждения.

Также следует учитывать, что, хотя в отдельных случаях мы фиксировали, что контроль учреждения над сервером был утрачен, в общем случае мы не проверяли указанные электронные адреса на валидность и актуальность. Это может являться предметом отдельного исследования.

> Использование субдоменов на серверах провайдера и хостинга говорит о том, что учреждение использует отдельный почтовый сервер с большей степенью контроля.

Приложение 2

База исследования. Статистические таблицы.

Таблица А1

Распределение организаций по типу использования почтовых сервисов

Классификация почтового сервиса, по типу			
	Число организаций	% от числа организаций, указавших валидный электронный адрес	% от всех организаций
Публичная веб-почта	196 854	81	76
Публичный веб-сервис на своем домене	5 144	2	2
Собственный сервер	19 055	8	7
Почта интернет провайдера	18 044	7	7
Хостинг	1 164	0	0
На субдомене (провайдер, портал, хостинг)	3 099	1	1
Другое/ не определено	8989	0	0
Всего	244 258	100	94

В этой таблице подсчитано распределение организаций по типу используемой почты. Процент высчитывается относительно двух параметров с учетом того, что 6% от общего числа организаций, фигурирующих в данных, либо не указывают электронный адрес, либо указанный ими адрес невалиден (некорректен; недоступен; сервис, размещавший почту, перестал существовать или сменил специализацию). Таким образом, процент рассчитывался, с одной стороны, для тех организаций, которые указали валидную почту; и с другой стороны, для общего числа организаций.

Таблица А2

Распределение почтовых сервисов по видам власти и типам учреждений

	Публичная веб-почта	Публичный веб-сервис на своем домене	Собственный сервер	Почта интернет-провайдера	Хостинг	На субдомене (провайдер, портал, хостинг)	Другое/ не определено
Федеральные органы власти	68%	2%	19%	8%	1%	2%	1%
Региональные органы власти	47%	3%	32%	10%	1%	5%	1%
Муниципальные органы власти	76%	2%	9%	10%	1%	2%	0%
Федеральные учреждения (казен., бюдж., автоном.)	78%	4%	7%	7%	1%	1%	2%
Региональные учреждения (казен., бюдж., автоном.)	78%	3%	8%	9%	1%	1%	1%
Муниципальные учреждения (казен., бюдж., автоном.)	86%	2%	5%	6%	0%	1%	0%
Органы ОМС	16%	3%	60%	11%	2%	6%	2%
Отделения Пенсионного фонда	24%	3%	61%	4%	0%	8%	0%

Таблица А3

Распределение почтовых сервисов по видам судов

Суды	Публичная веб почта	Публичный веб сервис на своем домене	Собственный сервис на своем домене	Почта интернет провайдера	Хостинг	На субдомене (провайдер, портал, хостинг)	Другое/ не определено
Арбитражные суды	11%	0%	82%	5%	0%	1%	1%
Конституционные суды РФ и республик	53%	7%	27%	13%	0%	0%	0%
Областные управления судебным департаментом	44%	4%	26%	21%	0%	5%	0%
Областные суды и верховные суды республик	37%	7%	24%	18%	5%	7%	1%
Военные суды	67%	8%	25%	0%	0%	0%	0%

Таблица A4

Распределение почтовых сервисов среди законодательных собраний

	Публичная веб почта	Публичный веб сервис на своем домене	Собственный сервис на своем домене	Почта интернет провайдера	Хостинг	На субдомене (провайдер, портал, хостинг)	Другое/ не определено
Законодательные собрания	16%	6%	43%	10%	6%	12%	7%

Таблица A5

Распределение почтовых сервисов среди региональных администраций

	Публичная веб почта	Публичный веб сервис на своем домене	Собственный сервис на своем домене	Почта интернет провайдера	Хостинг	На субдомене (провайдер, портал, хостинг)	Другое/ не определено
Региональные правительства и администрации	16%	1%	67%	7%	1%	7%	0%

Таблица А6

Распределение по министерствам и ведомствам (исполнительная власть)

Федеральные и региональные министерства	Публичная почта	Внутренние почтовые сервисы	Отсутствует	Число учреждений
Министерство финансов	19%	80%	1%	70
Министерство транспорта	23%	72%	4%	47
Министерство экономического развития	28%	69%	3%	61
Министерство энергетики	34%	59%	7%	74
Министерство промышленности и торговли	35%	65%	0%	34
Министерство сельского хозяйства	36%	58%	6%	64
Министерство здравоохранения и социального развития	37%	59%	4%	76
Министерство труда и социальной защиты	38%	54%	8%	52
Министерство природных ресурсов и экологии	41%	58%	2%	66
Министерство юстиции	42%	55%	2%	92
Министерство образования и науки	45%	52%	3%	73
Министерство строительства и жилищно-коммунального хозяйства	47%	49%	4%	57
Министерство культуры	49%	47%	4%	75
Министерство спорта, туризма и молодежной политики	57%	42%	1%	74

Федеральные и региональные министерства	Публич-ная почта	Внутренние почтовые сервисы	Отсутствует	Число учреждений
Министерство иностранных дел	65%	32%	3%	62
Министерство по делам граж-данской обороны и чрезвы-чайным ситуациям	76%	22%	2%	97
Министерство внутренних дел	88%	6%	6%	81
Всего	47%	50%%	4%	100

Таблица А7

Силовые структуры

	Публичная веб почта	Публичный веб сервис на своем домене	Собственный сервис на своем домене	Почта интернет провайдера	Хостинг	На субдомене (провайдер, портал, хостинг)	Другое/ не определено	Число учреждений
ФСБ	70%	3%	9%	17%	0%	0%	1%	94
ФСКН	53%	4%	16%	24%	3%	1%	0%	76
Следственный Комитет	86%	3%	9%	1%	0%	1%	0%	76
Фельдъегерская служба	53%	1%	29%	17%	0%	%	0%	78
Федеральная служба судебных приставов	38%	1%	49%	6%	0%	3%	3%	79
Федеральная служба по оборонному заказу	67%	0%	17%	17%	0%	0%	0%	6

	Публичная веб почта	Публичный веб сервис на своем домене	Собственный сервис на своем домене	Почта интернет провайдера	Хостинг	На субдомене (провайдер, портал, хостинг)	Другое/ не определено	Число учреждений
Федеральное агентство по обустройству границы	26%	0%	54%	3%	17%	0%	0%	35
Министерство обороны	0%	0%	100%	0%	0%	0%	0%	1
Центры спец. связи ФСО	46%	1%	43%	6%	1%	0%	2%	84
Всего	55%	2%	28%	11%	2%	1%	1%	100

Таблица А8

Департаменты информатизации

	Публичная веб-почта	Публичный веб-сервис на своем домене	Собственный сервис на своем домене	Почта интернет провайдера	Хостинг	На субдомене (провайдер, портал, хостинг)	Число учреждений
ФС по надзору в сфере связи, информационных технологий и массовых коммуникаций	11%	1%	82%	4%	1%	0%	73%
Региональные департаменты и министерства по информатизации и информационным технологиям	15%	4%	65%	6%	1%	10%	82%
ФА по печати и масс. коммуникациям, ФА связи, министерство связи и массовых коммуникаций	0%	0%	100%	0%	0%	0%	3%

Список адресов сайтов ФОИВ

ФОИВ	Адресов сайтов
Министерство внутренних дел Российской Федерации	http://mvd.ru
Министерство Российской Федерации по делам гражданской обороны, чрезвычайным ситуациям и ликвидации последствий стихийных бедствий (МЧС)	http://www.mchs.gov.ru
Министерство иностранных дел Российской Федерации (МИД)	http://mid.ru
Федеральное агентство по делам Содружества Независимых Государств, соотечественников, проживающих за рубежом, и по международному гуманитарному сотрудничеству (Россотрудничество)	http://rs.gov.ru
Министерство обороны Российской Федерации (Минобороны)	http://mil.ru
Федеральная служба по военно-техническому сотрудничеству (ФСВТС)	http://www.fsvts.gov.ru
Федеральная служба по техническому и экспортному контролю Российской Федерации (ФСТЭК)	http://fstec.ru
Федеральное агентство специального строительства (Спецстрой)	http://spetsstroy.ru/
Министерство юстиции Российской Федерации (Минюст)	http://minjust.ru
Федеральная служба исполнения наказаний (ФСИН)	http://fsin.su
Федеральная служба судебных приставов (ФССП)	http://fssprus.ru
Министерство здравоохранения Российской Федерации (Минздрав)	http://www.rosminzdrav.ru
Федеральная служба по надзору в сфере здравоохранения (Росздравнадзор)	http://www.roszdravnadzor.ru
Федеральное медико-биологическое агентство (ФМБА)	http://fmbaros.ru
Министерство культуры Российской Федерации (Минкультуры)	http://www.mkrf.ru
Федеральное агентство по туризму (Ростуризм)	http://www.russiatourism.ru

ФОИВ	Адресов сайтов
Министерство образования и науки Российской Федерации (Минобрнауки)	http://xn--80abucjiibhv9a.xn--p1ai/
Федеральная служба по надзору в сфере образования и науки (Рособрнадзор)	http://obrnadzor.gov.ru
Федеральное агентство по делам молодёжи (Росмолодёжь)	https://fadm.gov.ru
Министерство природных ресурсов и экологии Российской Федерации (Минприроды)	http://www.mnr.gov.ru
Федеральная служба по гидрометеорологии и мониторингу окружающей среды (Росгидромет)	http://www.meteorf.ru
Федеральная служба по надзору в сфере природопользования (Росприроднадзор)	http://rpn.gov.ru
Федеральное агентство водных ресурсов (Росводресурсы)	http://voda.mnr.gov.ru
Федеральное агентство лесного хозяйства (Рослесхоз)	http://www.rosleshoz.gov.ru
Федеральное агентство по недропользованию (Роснедра)	http://www.rosnedra.gov.ru
Министерство промышленности и торговли Российской Федерации (Минпромторг)	http://minpromtorg.gov.ru
Федеральное агентство по техническому регулированию и метрологии (Росстандарт)	http://gost.ru
Министерство Российской Федерации по развитию Дальнего Востока (Минвостокразвития)	http://minvostokrazvitia.ru
Министерство связи и массовых коммуникаций Российской Федерации (Минкомсвязь)	http://minsvyaz.ru
Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор)	http://rkn.gov.ru
Федеральное агентство по печати и массовым коммуникациям (Роспечать)	http://fapmc.ru
Федеральное агентство связи (Россвязь)	http://www.rossvyaz.ru

ФОИВ	Адресов сайтов
Министерство Российской Федерации по делам Северного Кавказа	http://minkavkaz.gov.ru
Министерство сельского хозяйства Российской Федерации (Минсельхоз)	http://mcx.ru
Федеральная служба по ветеринарному и фитосанитарному надзору (Россельхознадзор)	http://www.fsvps.ru
Федеральное агентство по рыболовству (Росрыболовство)	http://fish.gov.ru
Министерство спорта Российской Федерации (Минспорт)	http://minsport.gov.ru
Министерство строительства и жилищно-коммунального хозяйства (Минстрой)	http://www.minstroyrf.ru
Министерство транспорта Российской Федерации (Минтранс)	http://www.mintrans.ru/
Федеральная служба по надзору в сфере транспорта (Ространснадзор)	http://rostransnadzor.ru
Федеральное агентство воздушного транспорта (Росавиация)	http://favt.ru
Федеральное дорожное агентство (Росавтодор)	http://rosavtodor.ru
Федеральное агентство железнодорожного транспорта (Росжелдор)	http://roszeldor.ru
Федеральное агентство морского и речного транспорта (Росморречфлот)	http://www.morflot.ru
Министерство труда и социальной защиты Российской Федерации (Минтруд)	http://rosmintrud.ru
Федеральная служба по труду и занятости (Роструд)	http://www.rostrud.ru
Министерство финансов Российской Федерации (Минфин)	http://minfin.ru
Федеральная налоговая служба (ФНС)	http://www.nalog.ru
Федеральная служба по регулированию алкогольного рынка (Росалкогольрегулирование)	http://www.fsrar.ru
Федеральная таможенная служба (ФТС)	http://customs.ru

ФОИВ	Адресов сайтов
Федеральное казначейство (Казначейство)	http://roskazna.ru
Министерство экономического развития Российской Федерации (Минэкономразвития)	http://economy.gov.ru
Федеральная служба по аккредитации (Росаккредитация)	http://fsa.gov.ru
Федеральная служба государственной регистрации, кадастра и картографии (Росреестр)	https://rosreestr.ru
Федеральная служба по интеллектуальной собственности (Роспатент)	http://www.rupto.ru
Федеральное агентство по государственным резервам (Росрезерв)	http://www.rosreserv.ru
Федеральное агентство по управлению государственным имуществом (Росимущество)	https://www.rosim.ru
Министерство энергетики Российской Федерации (Минэнерго)	http://minenergo.gov.ru
Служба внешней разведки Российской Федерации (СВР)	http://svr.gov.ru
Федеральная служба безопасности Российской Федерации (ФСБ)	http://fsb.ru
Федеральная служба охраны Российской Федерации (ФСО)	http://fso.gov.ru
Федеральная служба по финансовому мониторингу (Росфинмониторинг)	http://www.fedsfm.ru
Федеральное архивное агентство (Росархив)	http://archives.ru
Главное управление специальных программ Президента Российской Федерации (ГУСП)	http://www.gusp.gov.ru
Управление делами Президента Российской Федерации (Управление делами)	http://www.udprf.ru
Федеральная антимонопольная служба (ФАС)	http://www.fas.gov.ru
Федеральная служба государственной статистики (Росстат)	http://www.gks.ru
Федеральная служба по надзору в сфере защиты прав потребителей и благополучия человека (Роспотребнадзор)	http://www.rospotrebnadzor.ru

ФОИВ	Адресов сайтов
Федеральная служба по экологическому, технологическому и атомному надзору (Ростехнадзор)	http://www.gosnadzor.ru
Федеральное агентство научных организаций (ФАНО)	http://fano.gov.ru
Государственная фельдъегерская служба Российской Федерации (ГФС)	http://www.gfs.ru
Федеральное агентство по делам национальностей (ФАДН)	http://fadn.gov.ru

Список источников

1. Портал государственных закупок: http://zakupki.gov.ru/epz/main/public/home.html

2. Определитель владельцев доменов: http://www.whois-service.ru/

3. Официальный интернет – портал правовой информации (Банк данных Законодательство России) http://pravo.gov.ru

4. Регистр правовых актов Министерства юстиции РФ http://zakon.scli.ru

5. Банк документов официального опубликования «Российской газеты» http://rg.ru/doc/

6. Базы правовых документов официальных сайтов исполнительных органов государственной власти субъектов РФ.

7. THE RADICATI GROUP, INC. Email Statistics Report, 2011-2015 http://www.radicati.com/wp/wp-content/uploads/2011/05/Email-Statistics-Report-2011-2015-Executive-Summary.pdf

8. База адресов государственных структур, созданная на основе данных из открытых источников, в том числе - официальных сайтов ФОИВ, bus.gov.ru и budget.gov.ru.

МойОфис®

«Использование электронной почты в государственной инфраструктуре РФ»

Аналитическое исследование проведено компанией «Новые Облачные Технологии» при экспертной поддержке АНО «Информационная культура» в 2016 году.