Оригинальная статья / Original article

https://doi.org/10.21869/2223-1560-2019-23-6-99-114

Эффективность централизованного использования цифровых технологий, информационных ресурсов и средств защиты информации в органах власти на примере республики Тыва

Б.С. Донгак [1] ✉, А.С. Шатохин [1], Р.В. Мещеряков [2]

[1] ФГБОУ ВО «Алтайский государственный технический университет им. И.И. Ползунова»
пр. Ленина, 46, г. Барнаул, 656038, Российская Федерация

[2] ФГБУН «Институт проблем управления им. В.А. Трапезникова РАН»
ул. Профсоюзная, 65, г. Москва, 117997, Российская Федерация

✉ e-mail: d_n_buyan@list.ru

Резюме

Цель исследования. *Целью данного исследования является оценка возможности применения методики централизованного управления системами и информационными рисками на примере информатизации органов государственной власти Республики Тыва, в целях оптимизации затрат на приобретение технических, программных и программно-аппаратных средства защиты информации, а также фонда оплаты труда обслуживающего технического персонала.*

Методы. *Одним из главных методов исследования является создание экспериментальной модели механизма единой информационно-вычислительный сети, объединяющей различные ведомства государственной власти, находящиеся в пределах одного административного здания, позволяющего одновременно работать с распределенными или централизованными приложениями, базами данных и другими сервисами, а также централизованное управления рисками информационной безопасности. Следующим методом исследования является анализ и изучение принципа работы информационных ресурсов, информационных систем, базы данных, и увеличение количества доменных пользователей в случае объединения их в единую сеть передачи данных. Взаимодействие и эффективность персонала, специализированного подразделения на базе одного государственного учреждения, обеспечивающие штатное функционирование сети и необходимый уровень информационной безопасностью для всех ведомств государственной власти.*

Результаты. *В результате получен экономический эффект за счет исключения приобретения дублирующих программно-аппаратных средств защиты информации, повышения эффективности использования единых информационных сервисов, а также создания централизованного структурного подразделения, которое использует в работе инструменты регулирования рисков и принимает управленческие решения информационной безопасности, основанные на принципах системного анализа, метода структуризации и методов экспертного опроса. Результаты исследования нашли применение при решении задач совершенствования системы управления информационной безопасностью органов власти Республики Тыва.*

Заключение. *Для органов государственной власти Республики Тыва разработана оригинальная информационно-технологическая архитектура системы управления информационной безопасностью и централизованное использование информационных технологий. Отличительными особенностями структуры программных средств централизованного подхода являются мультиагентная реализация управляющих элементов системы поддержки принятия решений и интеграция различных типов моделей управления безопасностью в единый комплекс.*

Ключевые слова: *информационные риски; информационная безопасность; органы государственной власти; централизованное управление; мультиагентный подход.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Донгак Б.С., Шатохин А.С., Мещеряков Р.В. Эффективность централизованного использования цифровых технологий, информационных ресурсов и средств защиты информации в органах власти на примере республики Тыва // Известия Юго-Западного государственного университета. 2019; 23(6): 99-114. https://doi.org/10.21869/2223-1560-2019-23-6-99-114.

Поступила в редакцию 30.09.2019 *Подписана в печать 16.10.2019* *Опубликована 23.12.2019*

The effectiveness of the Centralized Use of Digital Technologies, Information Resources and Information Protection Tools in Government by the Example of the Republic of Tyva

Buyan S. Dongak [1] ✉, Alexander S. Shatokhin [1], Roman V. Mescheryakov [2]

[1] Altai State Technical University named after I.I. Polzunova
46 Lenin Avenue, Barnaul 656038, Russian Federation

[2] Institute of Control Science of RAS
65 Profsoyuznaya str., Moscow 117997, Russian Federation

✉ e-mail: d_n_buyan@list.ru

Abstract

Purpose of research*. The purpose of this study is to assess the possibility of applying the methodology for centralized management of systems and information risks using the example of informatization of public departments of Republic of Tyva in order to optimize the cost of purchasing technical, software and hardware-software means of protecting information, as well as the payroll of maintenance technical personnel.*

Methods*. One of the main research methods is the creation of an experimental model of the mechanism of a single information and computing network, combining various government departments located within the same administrative building, which allows working simultaneously with distributed or centralized applications, databases and other services, as well as centralized information risk management security. The next research method is the analysis and study of the principle of operation of information resources, information systems, databases, and the increase in the number of domain users if they are combined into a single data transfer network. The interaction and effectiveness of personnel, a specialized unit based on one government agency, ensuring the regular functioning of the network and the necessary level of information security for all government departments.*

Results. *As a result, an economic effect is achieved by eliminating the acquisition of duplicate software and hardware information protection, increasing the efficiency of using unified information services, and creating a centralized structural unit that uses risk management tools and makes information security management decisions based on the principles of system analysis , structuring method and expert survey methods. The results of the study*

have been used in solving problems of improving the information security management system of the authorities of Republic of Tyva.

***Conclusion**. We have developed the original information technology architecture of the information security management system and centralized use of information technologies for the government of Republic of Tyva. The distinctive features of the structure of software tools for the centralized approach are the multi-agent implementation of the control elements of the decision support system and the integration of various types of security management models into a single complex.*

***Keywords:** information risks; information security; government departments; centralized management; multi-agent approach.*

***Conflict of Interest:** The authors declare the absence of overt and potential conflicts of interest related to the publication of this article.*

For citation: Dongak B. S., Shatokhin A. S., Mescheryakov R. V. The effectiveness of the centralized use of digital technologies, information resources and information protection tools in government by the example of the Republic of Tyva. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2019, 23(6): 99-114 (In Russ.). https://doi.org/ 10.21869/2223-1560-2019-23-6-99-114.

Received 28.06.2019 *Accepted 15.08.2019* *Published 25.10.2019*

***

Введение

В соответствии со Стратегией национальной безопасности Российской Федерации, утвержденной Указом Президента Российской Федерации от 31 декабря 2015 г. № 683, одним из главных направлений обеспечения национальной безопасности в сфере информационных технологий (далее – ИТ) является повышение уровня технологической безопасности, в том числе в информационной сфере. ИТ приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития региона и формирования информационного общества. В соответствии с Указом Президента Российской Федерации от 7 мая 2018 г. № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года» Правительству Российской Федерации при реализации совместно с органами государственной власти субъектов Российской Федерации национальной программы «Цифровая экономика Российской Федерации» необходимо обеспечить в 2024 году достижение основных целей и целевых показателей, таких как: создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи данных, обработки и хранения больших объемов данных, доступной для всех организаций, и использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями. Однако существует и ряд вопросов, которые необходимо решить для обеспечения функционирования систе-

мы. Основным и наиболее важным вопросом при создании и эксплуатации информационных систем является обеспечение информационной безопасности. Она достигается путем применения последовательных, взаимосвязанных действий, направленных на обеспечение конфиденциальности, целостности и доступности информации в системах.

В данной статье рассмотрена методика централизованного управления системами и информационными рисками на примере органов государственной власти Республики Тыва в целях оптимизации затрат на приобретение технических, программных и программно-аппаратных средства защиты информации, а также фонда оплаты труда обслуживающего технического персонала, явившаяся результатом применения мультиагентного подхода в имитационной модели [1].

Материалы и методы

Специфика объекта исследования. Методы и подходы

Исследование и апробация результатов проводились на примере информационно-телекоммуникационной инфраструктуры региональных органов государственной власти Республики Тыва. Ключевыми недостатками существующей системы являются: 1) отсутствие целостной информационной инфраструктуры управления информационной безопасностью органов власти; 2) несогласованность децентрализованного принятия решений на разных уровнях управления информационной безопасностью. Децентрализованный подход к управлению информационной безопасностью малоэффективен в реальных условиях работы органов государственной власти. В каждом из регионов существуют свои особенности, повышающие информационные риски. Такими специфическими особенностями Республики Тыва, требующими совершенствования системы управления информационной безопасностью органов власти, являются географическое положение, неразвитость инфраструктуры, удаленность от федерального центра. Эти факторы в совокупности препятствуют достижению таких основных целей и целевых показателей, как создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций, и использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями [2]. Это обусловливает необходимость перехода на модель централизованного управления информационной безопасностью органов власти. Таким образом, технологическая реализация и взаимодействие органов власти должны осуществляться в рамках современного централизованного подхода. Централизованное управле-

ние информационной безопасностью заключается в реализации сетевой структуры организационного управления, взаимодействие между которыми осуществляется на базе их интеграции в единое региональное информационное пространство [3]. Эффективным средством реализации централизованной системы управления информационной безопасностью в данных условиях являются мультиагентные технологии. Это обусловлено двумя решающими факторами: высокой динамичностью среды функционирования субъектов управления и необходимостью координации принятия решений, и учета человеческого фактора в процессе управления. Комбинированное применение программных агентов и проблемно-ориентированных имитационных моделей обеспечивает адаптивное моделирование поведения субъектов управления с учетом их активности и кооперативности в условиях различных нештатных ситуаций [4].

Структура и состав информационно-телекоммуникационной сети

В пятиэтажном административном здании размещены четыре органа государственной власти Республики Тыва. Информационная инфраструктура каждого органа власти разграничена на логическом уровне, но используется единая, физическая структурированная кабельная сеть (СКС), спроектированная и введенная в эксплуатацию в 2007 году.

С помощью системного анализа эффективности применяемых мер защиты информации [5] в каждом органе государственной власти, а также финансовых затрат на обслуживание и сопровождение информационных ресурсов, систем и телекоммуникационной сети выявлен ряд вопросов, требующих дополнительного внимания при применении новой политики информационной безопасности. Так, например, каждый орган государственной власти осуществляет закупку технических, программных и программно-аппарат-ных средств защиты информации, а также средств вычислительной техники. Это приводит к неэффективному расходованию средств, нарушению политики информационной безопасности, снижению возможности управления информационными рисками, повышению уровня внутренних и внешних угроз [6]. Структурная схема существовавшей информационно-телекоммуникационной сети и информационных ресурсов органов государственной власти (рис. 1) демонстрирует эти проблемы.

Авторами проведены исследования, целью которых являлось изучение подходов построения эффективной системы защиты информации для всех органов государственной власти, при этом финансовые средства не должны превышать общий объем предусмотренных лимитов. Иными словами, без дополнительных средств на приобретение программно-аппаратных комплексов.

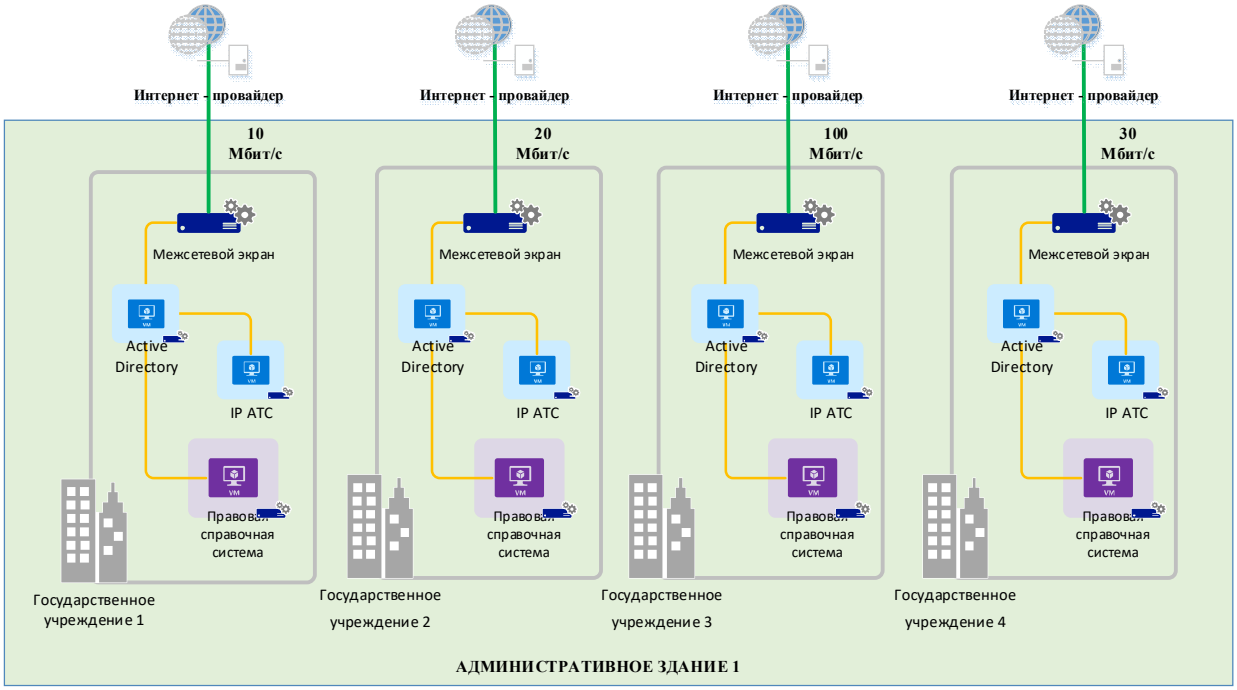

Рис. 1. Структурная схема информационно-телекоммуникационной сети и информационных ресурсов государственных учреждений, расположенных в пределах одного административного здания

Fig. 1. Structural diagram of the information and telecommunications network and information resources of government agencies located within the same administrative building

Для решения данного вопроса требовалось решить две задачи: техническую и организационную. В технической части приведен механизм создания единой информационно-вычислительный сети, объединяющей в единую систему различные ведомства государственной власти, находящиеся в пределах одного административного здания, позволяющий одновременно работать с распределенными или централизованными приложениями, базами данных и другими сервисами, а также централизованное управления рисками информационной безопасности [7]. В организационной части приводится взаимодействие персонала, формирование небольшого специализированного подразделения на базе одного государственного учреждения, обеспечивающие штатное функционирование сети и необходимый уровень информационной безопасности для всех ведомств государственной власти. Одним из главных преимуществ создания централизованного управления системами и обеспечения необходимого уровня защищенности таких сетей является процесс управления рисками, который позволяет направить все усилия на защиту от наиболее вероятных угроз [8].

В результате проведенных авторами исследований разработана методика централизованного управления системами и информационными рисками на примере органов государственной власти Республики Тыва. Применение разработанной методики позволит усовершенствовать систему управления информационной безопасностью, обеспе-

чить экономию финансовых средств на покупку программно-аппаратных средств защиты информации, повысить эффективность использования единых информационных сервисов. Реализация методики требует создания централизованного структурного подразделения, использующего в своей работе инструменты регулирования рисков и принимающего управленческие решения в области информационной безопасности, основанных на принципах системного анализа, метода структуризации и методов экспертного опроса [9].

Информационная инфраструктура (единая корпоративная сеть)

На первом этапе была проведена работа по логическому объединению информационно-телекоммуникационной сети органов государственной власти и метода мультиагентной реализации (Active Directory), построена на базе сервис-ориентированной архитектуры [10]. Интеграция сервисов агентов позволяет субъектам управления совместно использовать современные когнитивные информационные технологии и инструменты моделирования для выработки и реализации согласованных стратегий и управленческих решений в условиях неопределенности и риска [11].

В мультиагентной модели (Active Directory) каждой сущности реального мира ставится в соответствие программный агент, который представляет интересы данной сущности и может согласовывать свои решения с другими агентами.

Такой подход позволил создать единый центр управления и мониторинга коммуникационной сети и небольшой штат технических специалистов, осуществляющих работу по единой политике информационной безопасности [12] (рис. 2).

Единый выход в сеть интернет

Благодаря созданию единой корпоративной сети появилась возможность отказаться от других точек подключения к сети Интернет, что позволило сэкономить финансовые средства, использовать систему контроля доступа и учета интернет трафика [13], использовать системы защиты информации для всех органов власти, а также повысить скорость передачи информации.

Единые информационные системы

Отказ от дублирующих информационных систем общего пользования, например, справочные правовые системы, чаты, доска объявлений, локальное хранилище документов, система тестирования сотрудников и т.д., использование, в том числе, единой системы защиты информации для всех органов власти, например, межсетевой экран на границе сети Интернет, позволили существенно сократить затраты [14].

IP-телефония

За последние годы IP-телефония активно вытесняет традиционную телефонную связь по всем направлениям. Потенциал IP-телефонии намного шире, чем традиционная телефонная связь,

например, существует возможность интеграции с компьютером, доступ к разным голосовым терминалам, короткие номера для внутреннего использования, автоответчик, конференцсвязь и т.д. IP-телефония на сегодняшний день успешно используется в государственном секторе.

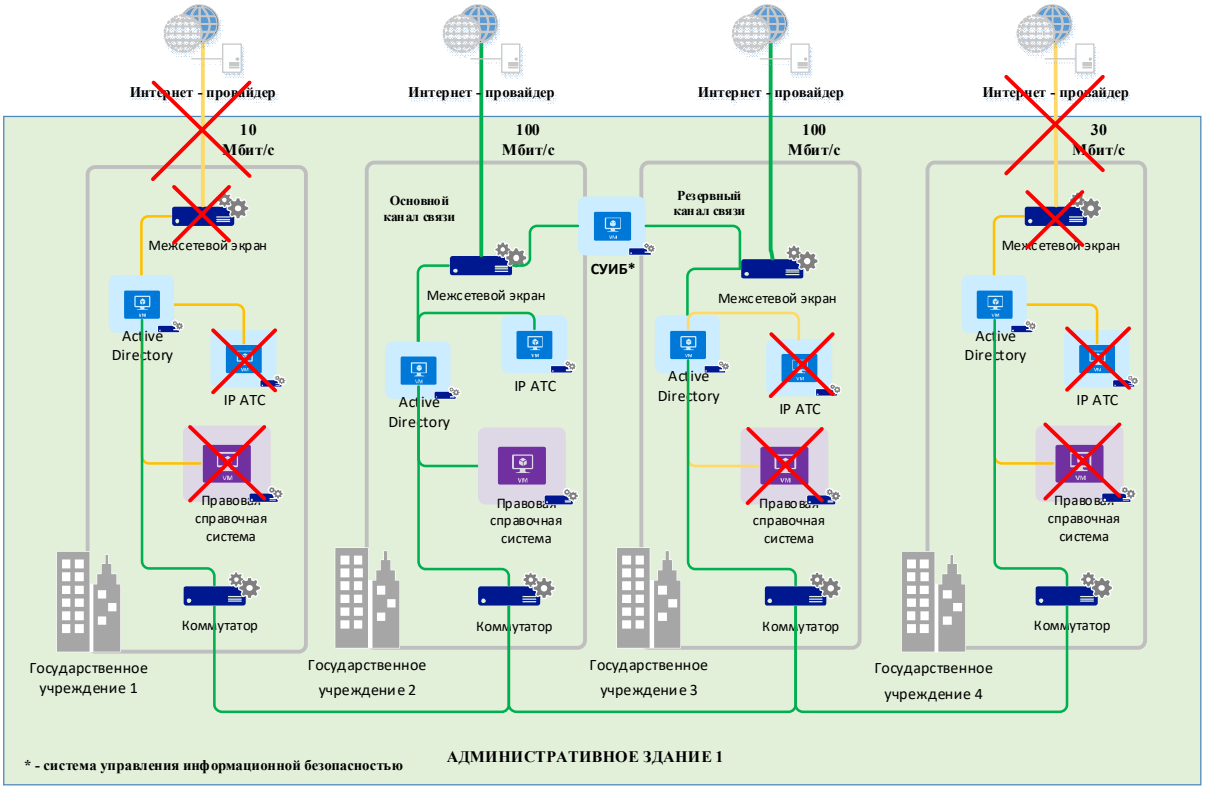

Рис. 2. Централизованный подход организации информационно-телекоммуникационной сети и информационных ресурсов государственных учреждений, расположенных в пределах одного административного здания

Fig. 2. Centralized approach to organizing an information and telecommunication network and information resources of state institutions located within the same administrative building

Существует два подхода к использованию IP-телефонии. Первый – полный отказ от традиционной телефонии. В этом случае для соединения абонентов используется локальная сеть. Второй подход подразумевает сохранение традиционной телефонной инфраструктуры, но с установленным новым оборудованием [22]. Поскольку реализация первого подхода требует определенной издержки по времени, реализация не представляется возможной. Таким образом, было принято решение использовать частично оба подхода, оставить традиционную телефонную инфраструктуру для непрерывности работы телефонной связи и модернизировать существующую локальную сеть для применения IP-телефонии. Выбранное решение, в свою очередь, может существенно расширить функционал телефонии. Необходимо отметить, что для корпоративных пользователей IP-телефония является не только эффективным средством опти-

мизации расходов на междугородные и международные телефонные переговоры, но и представляет возможность реализации на базе технологий IP-телефонии качественно новых сервисов [22] (рис. 3).

Переход на новую систему IP-телефонии позволил не только сэкономить финансовые средства на абонентские платы традиционных телефонных номеров, а также на IP-инфраструктуру, поскольку не потребовалось развертывания локальной сети. Существующая информационно-телекоммуникационная сеть позволяет передавать и голосовой, и компьютерный трафик. При использовании IP-телефонии органы власти также избавились от необходимости оплаты аренды городских линий. IP-телефония обеспечивает бесплатную связь между органами власти и предоставляет все преимущества мобильности при перемещении сотрудников.

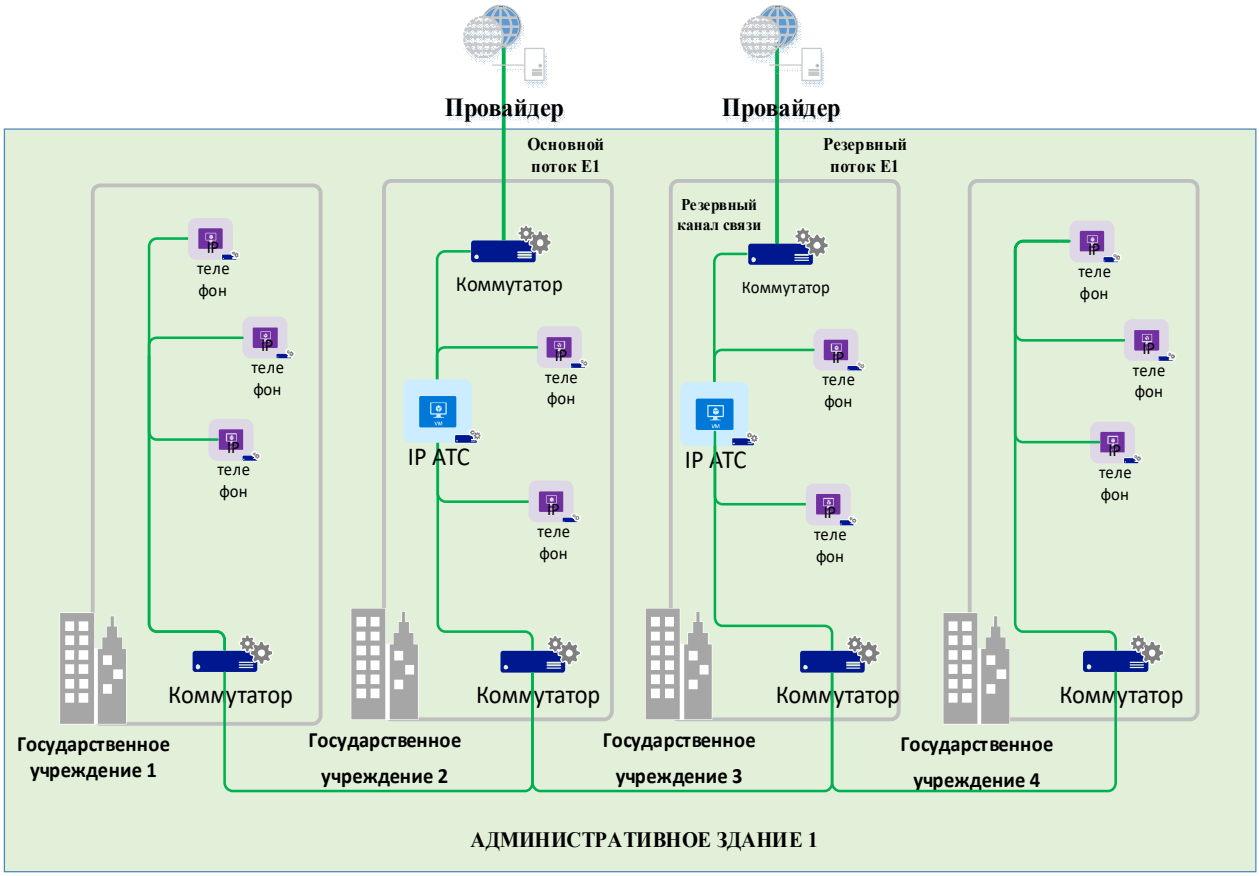

Рис. 3. Структурная схема организации IP-телефонии для государственных учреждений, расположенных в пределах одного административного здания

Fig. 3. Structural diagram of the organization of IP-telephony for public institutions located within the same administrative building

Информационная безопасность

Подсистема обеспечения информационной безопасности и администрирования предназначена для защиты обрабатываемых и передаваемых данных в органах власти и ее программных компонентов от несанкционированного до-

ступа и воздействия вредоносных программ. Такая защита должна обеспечиваться как на уровне операционного ядра и приложений, так и на уровне сторонних платформ [15]. Администрирование заключается в поддержании корректной работы всех функциональных информационных систем и контроле действий пользователей. Коммуникационная подсистема обеспечивает взаимодействие между всеми подсистемами и внешними ведомственными и корпоративными информационными системами на основе современных Интернет-технологий и средств телекоммуникаций [16]. Унифицированная точка доступа к ресурсам и сервисам реализуется в виде портала на основе веб-технологий и построена на базе сервисориентированного подхода. Основными категориями пользователей являются: субъекты управления (лица, принимающие решения), субъекты обеспечения безопасности, системные аналитики, эксперты, разработчики и технический персонал, обслуживающие программную и информационно-коммуникационную структуру [17].

Результаты и их обсуждение. Экономическое моделирование

При анализе затрат рассматривалось соотношение планируемых и непланируемых затрат. Под оптимизацией затрат подразумевается процесс, результатом которого будет не бездумное сокращение статей затрат, а вдумчивое нахождение наилучшего решения, при котором будет возможно достижение заданного результата при минимальных ресурсных затратах [18].

Расходы органов власти Республики Тыва (информационные сервисы, телефонные линии связи и доступ к глобальной сети Интернет) за 2018 год приведены в табл. 1. В целях сохранения конфиденциальности приведены нормированные значения расходов органов власти.

Таблица 1. Расходы на 2018 г. с учетом НДС 18%

Table 1. Expenses for 2018, including VAT 18%

Наименование	Информационные сервисы / тыс. руб.	Телефонная связь / тыс. руб.	Доступ к глобальной сети Интернет / тыс. руб.
Орган власти 1	250,0	1 300,0	390,0
Орган власти 2	320,0	970,0	430,0
Орган власти 3	180,0	430,0	170,0
Орган власти 4	640,0	760,0	80,0
ИТОГО	1 390,0	3 460,0	1 070,0

Предложенная авторами методика централизованного управления системами и информационными рисками на примере органов государственной власти Республики Тыва позволила не только сэкономить финансовые средства на покупку программно-аппаратных комплексов (ПАК), но и сократить количество работ, связанных с закупками. Закупочные работы проводятся одним из органов власти для всех, вместо четырех, что существенно облегчает нагрузку хозяйственного отдела. Табл. 2 демонстрирует полученный экономический эффект [19].

Таблица 2. Расходы на 2019 г. с учетом НДС 20%

Table 2. Expenses for 2019, including VAT 20%

Наименование	Информационные сервисы	Телефонная связь	Доступ к глобальной сети Интернет
Орган власти 1	590,0	2 030,0	560,0
Орган власти 2	0,0	0,0	0,0
Орган власти 3	0,0	0,0	0,0
Орган власти 4	130,0	0,0	0,0
ИТОГО	720,0	2 030,0	560,0
ЭКОНОМИЯ:	670,0	1 430,0	510,0

В соответствии с Указом Президента Российской Федерации от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена» выход в глобальную сеть Интернет должен осуществляться только с использованием специально предназначенных для этого средств защиты информации (межсетевые экраны, система обнаружения вторжений и т.д.) [20]. Таким образом, для каждого органа власти необходимо приобрести ПАК и ежегодное продление баз экспертных правил. Табл. 3 демонстрирует необходимые расходы. В случае создания единой информационно-телекоммуникационной сети достаточно использовать имеющиеся ПАК у четвертого органа власти на границе сети Интернет [21, 22]. Таким образом, общая сумма экономии финансовых средств составила около 4,5 млн. руб.

Выводы

Разработанная информационно-технологическая архитектура органов государственной власти призвана обеспечить унификацию форм представления информации и методов ее обработки с целью интеграции средств.

Таблица 3. Экономия средств защиты информации за счет отказа дублирующих программно-аппаратных комплексов защиты информации

Table 3. Savings in information security due to the failure of duplicate software and hardware information security systems

№	Наименование	Межсетевой экран на границе		ПАК для анализа событий информационной безопасности		ПАК для обнаружения вторжений в информационные системы		Расходы каждого органа власти / тыс. руб.	Экономия / тыс. руб.	ИТОГО на ИБ / тыс. руб.
		Затраты на приобретения ПАК / тыс. руб.	Техническая поддержка / тыс. руб.	Затраты на приобретение ПАК, / тыс. руб.	Ежегодное продление баз экспертных правил / тыс. руб.	Затраты на приобретение ПАК, / тыс. руб.	Ежегодное продление баз экспертных правил / тыс. руб.			
1	Орган власти 1	260,0	90,0	800,0	160,0	160,0	30,0	1 500,0	4 500,0	280,0
2	Орган власти 2	260,0	90,0	800,0	160,0	160,0	30,0	1 500,0		
3	Орган власти 3	260,0	90,0	800,0	160,0	160,0	30,0	1 500,0		
4	Орган власти 4	0,0	90,0	0,00 ₽	160,0	0,00 ₽	30,0	280,00		
								4 780,0		

Мультиагентная реализация управляющих элементов системы поддержки принятия решений и интеграция различных типов моделей управления безопасностью в единый комплекс позволили осуществлять совместную логико-аналитическую обработку данных и ситуационный анализ состояния изучаемого объекта с применением экспертных знаний и учетом пространственно-временных зависимостей. В результате получен экономический эффект за счет исключения приобретения дублирующих программно-аппаратных средств защиты информации, повышения эффективности использования единых информационных сервисов, а также создания централизованного структурного подразделения, которое использует в работе инструменты регулирования рисков и принимает управленческие решения информационной безопасности, основанные на принципах системного анализа, метода структуризации и методов экспертного опроса. Вышеуказанные работы будут продолжены с акцентом на два направления:

1. Поэтапное добавление новых органов власти Республики Тыва к разработанной единой информационно-технологической архитектуре.

2. Анализ рабочей нагрузки сотрудников и коммуникационных потоков.

В дальнейших исследованиях планируется постановка экспериментов и анализ полученной информации по указанным направлениям.

Список литературы

1. Волков Д.В. Имитационное мультиагентное моделирование системы связи специального назначения // International Journal of Advanced Studies, 2017. Vol 7, №1-2. С. 31-37.

2. Oleynik A., Fridman A., Masloboev A. Informational and analytical support of the network of intelligent situational centers in Russian Arctic // CEUR Workshop Proceedings. 2018. Vol. 2109. P. 57-64.

3. Oliveira R., Ribeiro M., Vieira A. ELPC-CMAC: An enhanced cooperative mac protocol for broadband plc systems // Computer networks. 2019. Vol. 153. P. 11-22. ISSN: 1389-1286.

4. Mohamad Noor M., Hassan W. Current research on internet of things (IOT) security: A survey // Computer networks. 2019. Vol. 148. P. 283-294. ISSN: 1389-1286.

5. Vyalyi M., Khuziev I. Fast protocols for leader election and spanning tree construction in a distributed network // Problems of information transmission. 2017. Vol. 53, № 3. P. 183-201.

6. Nazarova Y., Bozhko Y. Development of it-infrastructure for the providing system of educational process in sparsely populated areas of the arctic zone of the Russian Federation// CEUR Workshop Proceedings. 2018. Vol. 2109. P. 49-56.

7. El-Shekeil I, Pal A., Kant K. Precession: Progressive recovery and restoration planning of interdependent services in enterprise data centers // Digital communications and networks. 2019. Vol. 4. P. 39-47. ISSN: 2468-5925.

8. Arutyunov V. Clustering of information-security standards of the Russian Federation // Scientific and technical information processing. 2017. Vol. 44, №2. P. 125-133.

9. Yayla A., Lei Y. Information security policies and value conflict in multinational companies // Information and computer security. 2018. Vol. 26. P. 230-245. ISSN: 2056-4961.

10. Донгак Б.С. Мониторинг сетевой активности автоматизированных рабочих мест сотрудников организации // Безопасность информационных технологий. 2018. С. 71-79. ISSN 2074-7136.

11. Лохин С.В., Семашко А.В. Мониторинг сетевой активности персонала в целях обеспечения информационной безопасности предприятия // Вопросы защиты информации. 2017. №2 (117). С. 53-57.

12. Мещеряков Р.В., Шелупанов А.А. Концептуальные вопросы информационной безопасности региона и подготовки кадров // Труды СПИИРАН. 2014. № 3 (34). С. 136-159.

13. Vasilyev V., Sulavko A., Zhumazhanova S., Borisov R. Identification of the psychophysiological state of the user based on hidden monitoring in computer systems // Scientific and technical information processing. 2018. Vol. 45, №6. P. 398-410.

14. Михайловская Н.Г. Центры управления информационной безопасностью // Безопасность информационных технологий. 2016. № 4. С. 38-51.

15. Jiang J., Wen S., Liu B., Yu S., Zhou W., Xiang Y. Malicious attack propagation and source identification // Advances in information security. 2019. Vol. 73. P. 1-192. ISSN: 1568-2633.

16. Ходашинский И.А., Мещеряков Р.В., Горбунов И.В. Методы нечеткого извлечения знаний в задачах обнаружения вторжений // Вопросы защиты информации. 2012. № 1. С. 45-50.

17. Абросимов М.Б., Камил И.А. Разработка системы предотвращения вторжений с использованием параллельного программирования и системы отказоустойчивости // Безопасность информационных технологий. 2018. № 1 (25). С. 65-73.

18. Filyak P.Y. Information security in the context of the digital economy// CEUR Workshop Proceedings. 2018. Vol. 2109. P. 25-30.

19. Norkin V. B&B Method for discrete partial order optimization // Computational management science. 2019. P. 165-170. ISSN: 1619-697X.

20. Токарева М.В. Мультиагентный подход к планированию ресурсов // Сб. материалов XIX международной научно-методической конференции «Информатика: проблемы, методология, технологии». Воронеж, 2019. С. 1757-1760.

21. Prelov V. On some optimization problems for the renin divergence // Problems of information transmission. 2018. Vol. 54. №3. P. 229-244.

22. Серебряник И.А., Дружинина А.В. IP-телефония для бизнеса: экономический аспект // Актуальные проблемы гуманитарных и естественных наук. 2014. №5-1. С.255-257.

References

1. Volkov D.V. Imitatsionnoe mul'tiagentnoe modelirovanie sistemy svyazi spetsial'nogo naznacheniya [Simulation of multi-agent modeling of a special-purpose communication system"]. *International Journal of Advanced Studies*, 2017, vol. 7, no. 1-2, pp. 31-37 (In Russ.).

2. Oleynik A., Fridman A., Masloboev A. Informational and analytical support of the network of intelligent situational centers in Russian Arctic. *CEUR Workshop Proceedings*, 2018, vol. 2109, pp. 57-64.

3. Oliveira R., Ribeiro M., Vieira A. ELPC-CMAC: An enhanced cooperative mac protocol for broadband plc systems. *Computer networks*, 2019, vol. 153, pp. 11-22. ISSN: 1389-1286.

4. Mohamad Noor M., Hassan W. Current research on internet of things (IOT) security: A survey. *Computer networks*, 2019, vol. 148, pp. 283-294. ISSN: 1389-1286.

5. Vyalyi M., Khuziev I. Fast protocols for leader election and spanning tree construction in a distributed network. *Problems of information transmission*, 2017, vol. 53, no. 3, pp. 183-201.

6. Nazarova Y., Bozhko Y. Development of it-infrastructure for the providing system of educational process in sparsely populated areas of the arctic zone of the Russian Federation. *CEUR Workshop Proceedings*, 2018, vol. 2109, pp. 49-56.

7. El-Shekeil I., Pal A., Kant K. Precession: Progressive recovery and restoration planning of interdependent services in enterprise data centers. *Digital communications and networks*, 2019, vol. 4, pp. 39-47. ISSN: 2468-5925.

8. Arutyunov V. Clustering of information-security standards of the Russian Federation. *Scientific and technical information processing*, 2017, vol. 44, no. 2, pp. 125-133.

9. Yayla A, Lei Y. Information security policies and value conflict in multinational companies. *Information and computer security*, 2018,vol. 26, pp. 230-245. ISSN: 2056-4961.

10. Dongak B.S. Monitoring setevoi aktivnosti avtomatizirovannykh rabochikh mest sotrudnikov organizatsii [Monitoring the network activity of automated workplaces of organization employees]. *Bezopasnost' informatsionnykh tekhnologii = Information Technology Security,* 2018, pp. 71-79. ISSN 2074-7136 (In Russ.).

11. Lokhin S.V., Semashko A.V. Monitoring setevoi aktivnosti personala v tselyakh obespecheniya informatsionnoi bezopasnosti predpriyatiya [Monitoring network activity of personnel in order to ensure information security of the enterprise]. *Voprosy zashchity informatsii = Issues of information security*, 2017, no. 2 (117), pp. 53-57 (In Russ.).

12. Meshcheryakov R.V., Shelupanov A.A. Kontseptual'nye voprosy informatsionnoi bezopasnosti regiona i podgotovki kadrov [Conceptual issues of information security of the region and training]. *Trudy SPIIRAN = Proceedings of SPIIRAS,* 2014, no. 3 (34), pp. 136-159 (In Russ.).

13. Vasilyev V., Sulavko A., Zhumazhanova S., Borisov R. Identification of the psychophysiological state of the user based on hidden monitoring in computer systems. *Scientific and technical information processing*, 2018, vol. 45, no. 6, pp. 398-410.

14. Mikhailovskaya N.G. Tsentry upravleniya informatsionnoi bezopasnost'yu [Information Security Management Centers]. *Bezopasnost' informatsionnykh tekhnologii = Security of information technology*, 2016, no. 4, pp. 38-51 (In Russ.).

15. Jiang J., Wen S., Liu B., Yu S., Zhou W., Xiang Y. Malicious attack propagation and source identification. *Advances in information security*, 2019, vol. 73, pp. 1-192. ISSN: 1568-2633.

16. Khodashinsky I.A., Meshcheryakov R.V., Gorbunov I.V. Metody nechetkogo izvlecheniya znanii v zadachakh obnaruzheniya vtorzhenii [Fuzzy methods of knowledge extraction in intrusion detection tasks]. *Voprosy zashchity informatsii = Issues of information security*, 2012, no. 1, pp. 45-50 (In Russ.).

17. Abrosimov M.B., Kamil I.A. Razrabotka sistemy predotvrashcheniya vtorzhenii s ispol'zovaniem parallel'nogo programmirovaniya i sistemy otkazoustoichivosti [Development of an intrusion prevention system using parallel programming and a fault tolerance system]. *Bezopasnost' informatsionnykh tekhnologii = Security of information technology*, 2018, no. 1 (25), pp. 65-73 (In Russ.).

18. Filyak P.Y. Information security in the context of the digital economy [Information security in the context of the digital economy]. *CEUR Workshop Proceedings,* 2018, vol. 2109, pp. 25-30.

19. Norkin V. B&B Method for discrete partial order optimization. *Computational management science*, 2019, pp. 165-170. ISSN: 1619-697X.

20. Tokarev M.V. Mul'tiagentnyi podkhod k planirovaniyu resursov [Multi-agent approach to resource planning]. *Sbornik XIX mezhdunarodnoi nauchno-metodicheskoi konferentsii "Informatika: problemy, metodologiya, tekhnologii"* [Collection of the XIX international scientific-methodical conference “Informatics: problems, methodology, technologies”. Voronezh, 2019, pp. 1757-1760 (In Russ.).

21. Prelov V. On some optimization problems for the renin divergence. *Problems of information transmission*, 2018, vol. 54, no. 3, pp. 229-244.

22. Serebrjanik I.A., Druzhinina A.V. IP-telefoniya dlya biznesa: ekonomicheskii aspekt [IP-telefonija dlja biznesa: jekonomicheskij aspekt]. *Aktual'nye problemy gumanitarnykh i estestvennykh nauk = Actual Problems of Humanities and Natural Sciences*, 2014, no.5, pt. 1, pp.255-257 (In Russ.).

Информация об авторах / Information about the Authors

Донгак Буян Станиславович, аспирант, кафедра информатики, вычислительной техники и информационной безопасности, ФГБОУ ВО «Алтайский государственный технический университета им. И.И. Ползунова, г. Барнаул, Российская Федерация, e-mail: d_n_buyan@list.ru

Buyan S. Dongak, Post-Graduate Student, Department of Informatics, Computer Engineering and Information Security, Altai State Technical University named after I.I. Polzunova (AlSTU), Barnaul, Russian Federation, e-mail: d_n_buyan@list.ru

Шатохин Александр Семенович, кандидат технических наук, доцент, кафедра информатики, вычислительной техники и информационной безопасности, ФГБОУ ВО «Алтайский государственный технический университета им. И.И. Ползунова, г. Барнаул, Российская Федерация, e-mail: asshatokhin@gmail.com

Aleksandr S. Shatohin, Cand. of Sci. (Engineering), Associate Professor, Department of Informatics, Computer Engineering and Information Security, Altai State Technical University named after I.I. Polzunova (AlSTU), Barnaul, Russian Federation, e-mail: asshatokhin@gmail.com

Мещеряков Роман Валерьевич, доктор технических наук, профессор РАН**,** главный научный сотрудник лаборатории 80, Федеральное государственное бюджетное учреждение науки Институт проблем управления им. В.А. Трапезникова РАН, Москва, Российская Федерация, e-mail: meshcheryakov.roman@gmail.com

Roman V. Meshcheryakov, Dr. of Sci. (Engineering), Professor, Chief Researcher at Laboratory 80, Russian Academy of Sciences, Institute of Management Problems named after V.A. Trapeznikova RAS, Moscow, Russian Federation, e-mail: meshcheryakov.roman@gmail.com