DOI: 10.55648/1998-6920-2023-17-4-74-88 УДК 004.9

Опыт организации информационной инфраструктуры Правительства Алтайского края в ответ на вызовы угроз безопасности

В. В. Снесарь, Е. А. Зрюмов, Д. Ю. Илли,
Е. М. Янкин, О. В. Чумак, С. О. Вольвач

Министерство цифрового развития и связи Алтайского края

Аннотация: Рассмотрены вопросы организации комплексной информационной инфраструктуры Правительства Алтайского края. Описаны этапы построения информационной инфраструктуры Правительства Алтайского края, которые включают определение требований, проектирование и внедрение информационной инфраструктуры, заключающееся в централизации каналов связи и цифровых сервисов, построении регионального центра обработки и хранения данных, установке системы мониторинга сетевого трафика и управления средствами антивирусной защиты.

Ключевые слова: информационная инфраструктура, корпоративная компьютерная сеть, цифровое государственное управление.

Для цитирования: Снесарь В. В., Зрюмов Е. А., Илли Д. Ю., Янкин Е. М., Чумак О. В., Вольвач С. О. Опыт организации информационной инфраструктуры Правительства Алтайского края в ответ на вызовы угроз безопасности // Вестник СибГУТИ. 2023. Т. 17, № 4. С. 73–88. https://doi.org/10.55648/1998-6920-2023-17-4-73-88.

Статья поступила в редакцию 14.11.2022;
переработанный вариант – 07.12.2022;
принята к публикации 18.07.2023.

1. Введение

Информационные технологии стирают границы между государствами и становятся неотъемлемой частью практически всех сфер деятельности человека и общества. Эффективное применение цифровых решений является приоритетным фактором ускорения экономического развития государства и значимым конкурентным преимуществом на глобальных рынках [1, 2].

Глобализация информационной сферы предоставляет широкие возможности для обеспечения реализации стратегических национальных приоритетов Российской Федерации, но при этом несет и угрозы суверенитету, независимости, защите традиционных духовно-нравственных основ российского общества, обеспечению обороны и безопасности [3].

Возможности трансграничного оборота информации и глобальных цифровых экосистем всё чаще используются для достижения геополитических, противоречащих международному праву, а также террористических, экстремистских и криминальных целей в ущерб международной безопасности и стратегической стабильности [1].

Расширяются масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере, возрастает количество атак на российские информационные ресурсы с территорий иностранных государств с целью блокировки работы государственных организаций, увеличивается число преступлений, связанных с нарушением конституционных прав и свобод человека, в том числе в части неприкосновенности частной жизни, личной и семейной тайны, при обработке персональных данных с использованием информационных технологий и методов социальной инженерии [1].

Ежедневно фиксируются факты DDoS-атак на различные государственные информационные сервисы, рассылки спам-сообщений на электронную почту организаций, распространения вредоносного программного обеспечения. Это приводит в ряде случаев к непоправимым последствиям: потере конфиденциальной информации, обрабатываемой в государственных информационных системах, скрытому майнингу криптовалют на рабочих местах сотрудников, несанкционированному управлению автоматизированных систем, в том числе относящихся к объектам критической информационной инфраструктуры.

Исходя из вышесказанного, информационная безопасность является одним из важнейших стратегических национальных приоритетов [4].

Первичный теоретический анализ проблем контроля безопасности на объектах коммуникационных систем, функционирующих в органах государственной власти субъектов Российской Федерации, содержит описание объекта защиты информации, угроз безопасности информации, общей структуры системы безопасности [5]. Однако при практической организации информационной инфраструктуры в высших органах исполнительной власти субъектов Российской Федерации нет единых подходов к обеспечению информационной безопасности. Например, оценка возможности применения методики централизованного управления системами и информационными рисками в органах государственной власти Республики Тыва произведена лишь в четырех органах власти, размещенных в одном здании, где основной целью является оптимизация затрат на приобретение средств защиты информации, а также фонда оплаты труда обслуживающего технического персонала [6].

Зачастую отсутствие централизованной политики обеспечения информационной безопасности на уровне региона приводит к потере управляемости мониторингом инцидентов информационной безопасности и невозможности оперативно устранять или купировать последствия атак на информационную инфраструктуру, использованию конфликтующих между собой программных и аппаратных средств защиты информации.

Целью статьи является формирование универсальных подходов к организации комплексной информационной инфраструктуры Правительства Алтайского края, которые могут быть использованы при централизации обеспечения информационной безопасности во всех субъектах Российской Федерации [7, 8].

Для организации комплексной информационной инфраструктуры Правительства Алтайского края были пройдены стадии, характерные для создания инфраструктурного объекта в области цифровизации [9] в соответствии с моделью жизненного цикла системы защиты информации[10]. Рассмотрим каждый из них более подробно.

2. Определение требований к информационной инфраструктуре

На первом этапе проведен анализ нормативных правовых актов [11–13], методических документов, национальных стандартов и приказов регуляторов [14–16], которым должна соответствовать информационная инфраструктура Правительства Алтайского края. Проведенное исследование позволило выявить и классифицировать государственные информационные системы, информационные системы персональных данных, каналы связи, средства криптографической защиты информации, используемые в информационной инфраструктуре Правительства Алтайского края. На основе этого определены угрозы безопасности информации, реализация которых может привести к нарушению работоспособности. Среди самых значимых проблем можно выделить следующие:

- самостоятельное обеспечение доступа в сеть Интернет каждым органом исполнительной власти Алтайского края;
- отсутствие в органах исполнительной власти Алтайского края контроля доступа в сеть Интернет;
- использование устаревших, зачастую не сертифицированных, устройств маршрутизации;
- большое количество вредоносных и спам-сообщений электронной почты на рабочих местах государственных гражданских служащих;
- вирусная (вредоносная) активность на компьютерах государственных гражданских служащих;
- отсутствие надлежащего контроля и мониторинга доступа государственных гражданских служащих к собственным информационным системам на уровне межсетевого экранирования и средств обнаружения вторжений;
- самостоятельная закупка каждым органом исполнительной власти Алтайского края программных и аппаратных средств преимущественно иностранного производства;
- отсутствие регламентов реагирования на возникающие события, связанные с нарушением информационной безопасности и порядка действий по их устранению (предотвращению);
- низкий уровень подготовки специалистов в сфере информационной безопасности.

В рамках исполнения данного этапа зафиксировано отсутствие единой политики обеспечения информационной безопасности на уровне Правительства Алтайского края, что создавало предпосылки для деструктивного воздействия на существующую информационную инфраструктуру. На основе выявленных недостатков сформированы требования к системе защиты информации информационной инфраструктуры Правительства Алтайского края.

3. Проектирование информационной инфраструктуры

На этапе проектирования построена архитектура информационной инфраструктуры Правительства Алтайского края, которая включает профессиональные высокопроизводительные и сертифицированные отечественные решения по обеспечению информационной безопасности. Выделим основные результаты, достигнутые при реализации этого этапа:

- централизация каналов доступа в сеть Интернет для всех органов исполнительной власти Алтайского края;
- создание единой точки доступа и обеспечение надлежащего контроля доступа к информационным системам и в сеть Интернет;
- мониторинг единой точки доступа с использованием средств обнаружения вторжений (IDS) и анализа событий информационной безопасности (TIAS) и последующее подключение информационной инфраструктуры каждого органа власти к системе мониторинга средствами обнаружения вторжений;
- централизация системы электронной почты Правительства Алтайского края;
- ввод в эксплуатацию специализированного программного обеспечения для анализа и проверки всех сообщений электронной почты, приходящих в адрес органов исполнительной власти Алтайского края;
- централизация размещения информационных систем и ресурсов органов исполнительной власти Алтайского края в региональном центре обработки и хранения данных (ЦОД);
- централизация средств антивирусной защиты с внедрением единой системы управления средствами антивирусной защиты вплоть до конкретного рабочего места государственного гражданского служащего;
- контроль процесса импортозамещения посредством централизации закупок отечественного программного и аппаратного обеспечения для нужд органов исполнительной власти Алтайского края;

- создание проекта регионального закона о государственных информационных системах в Алтайском крае;
- разработка регламента взаимодействия при возникновении событий, связанных с нарушением информационной безопасности;
- создание межведомственной рабочей группы по решению вопросов в сфере информационной безопасности;
- выстраивание системы повышения квалификации специалистов органов исполнительной власти Алтайского края, в том числе и по образовательным программам в сфере информационной безопасности, сертифицированным ФСТЭК России.

Создание единой политики обеспечения информационной безопасности на уровне Правительства Алтайского края базировалось на централизации практически всех функций в области информационной безопасности на органе исполнительной власти Алтайского края, уполномоченном в организации и координации мероприятий по совершенствованию систем защиты информации в информационных системах и информационных ресурсах – Министерстве цифрового развития и связи Алтайского края [17], что позволило:

- обеспечить единое управление политикой безопасности при работе государственных гражданских служащих в сети Интернет, а также при их доступе к информационным системам и ресурсам, размещённым в центре обработки и хранения данных;
- обеспечить контроль и фильтрацию трафика, мониторинг активности вредоносного программного обеспечения и оперативную реакцию на события информационной безопасности;
- обеспечить более высокий уровень защиты за счет использования эффективных средств информационной безопасности;
- увеличить степень внедрения отечественного программного и аппаратного обеспечения в органах исполнительной власти Алтайского края;
- снизить, а в ряде случаев полностью исключить, финансовые затраты органов исполнительной власти Алтайского края на самостоятельное обеспечение информационной безопасности, приобретение аппаратно-программных средств, каналов доступа в сеть Интернет, ведомственных каналов связи и эксплуатационные расходы на обеспечение работоспособности информационных систем и ресурсов, размещенных в региональном центре обработки и хранения данных.

Исходя из принципа реализации «практической безопасности», централизация является основой построения эффективной системы информационной безопасности.

4. Внедрение информационной инфраструктуры

Для внедрения спроектированной архитектуры информационной инфраструктуры Правительства Алтайского края были решены следующие задачи:

- проведение работ по централизации каналов связи и цифровых сервисов;
- формирование единой системы электронной почты;
- создание регионального центра обработки и хранения данных и обеспечение его средствами защиты для размещения государственных информационных систем;
- реализация системы мониторинга сетевого трафика и управления средствами антивирусной защиты.

Для реализации поставленных задач был организован центр компетенций, в который вошли специалисты отдела по администрированию информационной инфраструктуры и отдела информационной безопасности Министерства цифрового развития и связи Алтайского края, а также отдела импортозамещения подведомственного Министерству КГБУ «Оператор электронного правительства Алтайского края». Текущий статус выполнения работ рассматривался на заседаниях межведомственной рабочей группы по решению оперативных задач в обла-

сти информационной безопасности, в состав которой входят уполномоченные специалисты из каждого органа исполнительной власти Алтайского края. Общая координация работ осуществлялась Советом по защите информации при Губернаторе Алтайского края.

4.1. Централизация каналов связи

Сначала была произведена централизация каналов связи и доступа в сеть Интернет (рис. 1), которая включала в себя [18]:

- создание корпоративной сети передачи данных (КСПД) уровня L2 на базе одного из региональных провайдеров;
- приобретение автономной системы и блока независимых от провайдера IP-адресов;
- установку в каждый орган исполнительной власти Алтайского края оборудования, обеспечивающего криптографическую защиту канала связи и маршрутизацию (точка подключения);
- организацию и обеспечение доступа в сеть Интернет с помощью основного и резервного каналов, которые обеспечивают два провайдера с собственными магистральными каналами связи;
- организацию и обеспечение доступа в корпоративную сеть передачи данных.

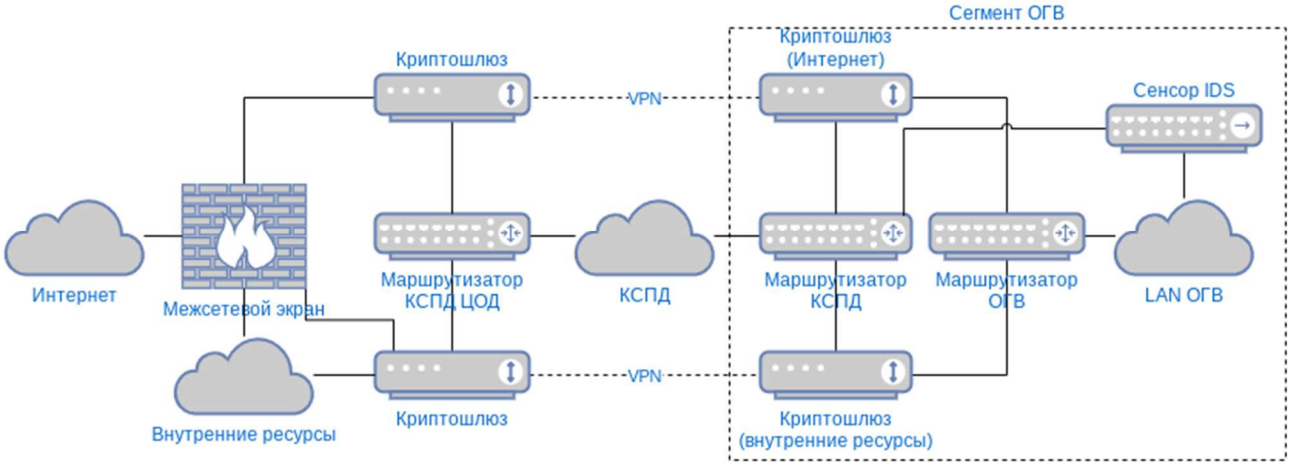

Рис. 1. Типовая схема подключения органов исполнительной власти Алтайского края

Эффект от централизации каналов связи оказался значительным. Если до этого каждый орган исполнительной власти Алтайского края самостоятельно приобретал каналы связи с пропускной способностью до 100 Мбит/с, что в совокупности предполагало использование канала с пропускной способностью 2.5 Гбит/с, то после проведенных мероприятий был сформирован единый канал связи для всех органов власти (основной и резервный с пропускной способностью 1 Гбит/с) при средней нагрузке от 300 до 550 Мбит/с при соотношении входящего и исходящего трафика – 80/20 процентов и 4000 рабочих мест (рис. 2 и 3).

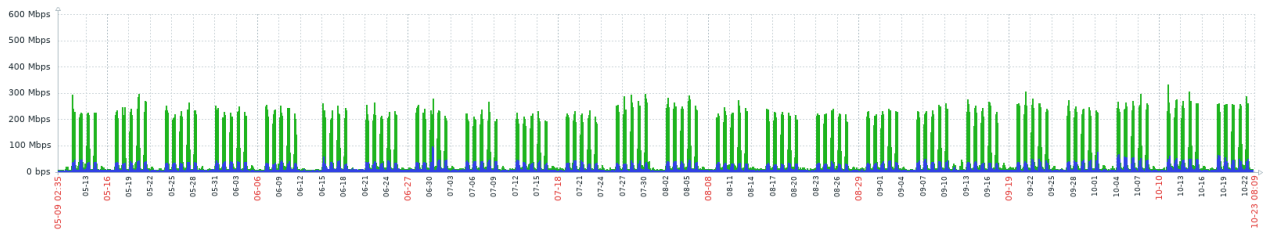

Рис. 2. Нагрузка на каналы связи в течение месяца

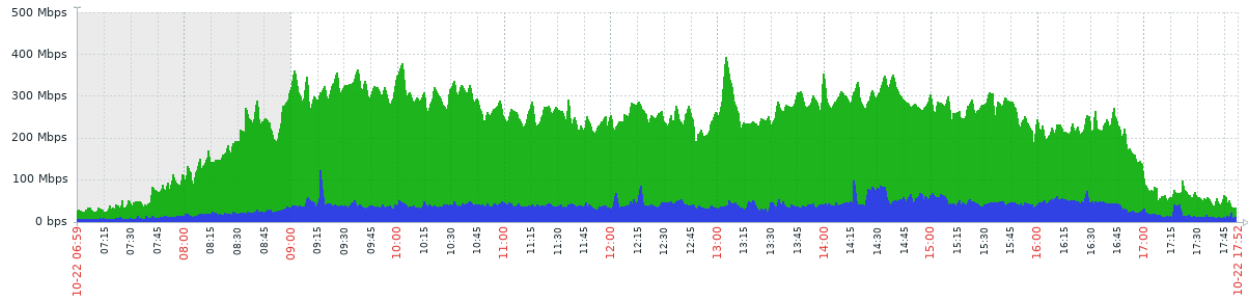

Рис. 3. Нагрузка на каналы связи в течение рабочего дня

После централизации каналов связи и доступа в сеть Интернет органы исполнительной власти Алтайского края перестали самостоятельно оплачивать услуги по доступу к корпоративной сети передачи данных, эта работа была организована на базе Министерства цифрового развития и связи Алтайского края.

4.2. Централизация системы электронной почты

Далее проводилась работа по централизации системы электронной почты как для серверов электронной почты органов исполнительной власти Алтайского края, так и для их подведомственных учреждений в виде сервиса. Для этого был сформирован шлюз безопасности, на основе решения «Kaspersky Security Mail Gateway», через который проходят все сообщения электронной почты и после необходимых проверок на спам и вредоносное программное обеспечение доставляются в почтовые ящики государственных гражданских служащих (рис. 4).

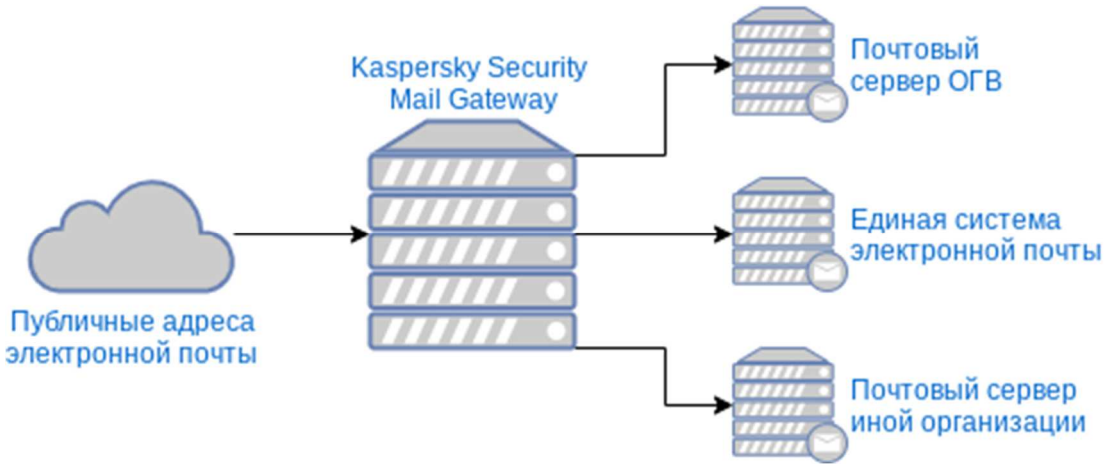

Рис. 4. Схема работы шлюза безопасности электронной почты

Единая система электронной почты Алтайского края была создана на базе двух отечественных продуктов – «CommuniGate Pro» и «Почта Mail.Ru», включенных в реестр отечественного программного обеспечения. Обе системы электронной почты размещены в центре обработки и хранения данных Алтайского края, что исключает доступ к почтовым сообщениям третьей стороны и обеспечивает надлежащий контроль пересылаемых электронных писем и вложений.

4.3. Региональный центр обработки и хранения данных

Далее были проведены работы по созданию регионального центра обработки и хранения данных, которые включали следующие этапы:

- обследование информационных систем органов исполнительной власти Алтайского края для определения потребности в вычислительных ресурсах и объемах хранения информации с учетом резервирования вычислительных ресурсов, резервного копирования информации и планируемого роста нагрузки на инфраструктуру в ближайшие три года;
- подготовка специализированных помещений для размещения серверного оборудования и систем хранения данных с учетом обеспечения гарантированного электроснабжения, надежного охлаждения и пожаротушения;
- создание инфраструктуры размещения информационных систем и ресурсов с использованием передовых технологий виртуализации аппаратных ресурсов и резервного копирования информации;
- формирование единой системы информационной безопасности в части защиты размещаемых информационных систем и ресурсов и обеспечения доступа к ним;
- создание многоуровневой распределенной автоматизированной системы мониторинга, обеспечивающей контроль состояния и управление оборудованием инфраструктуры размещения информационных систем, а также климатических параметров помещений;
- принятие закона Алтайского края от 24.12.2019 № 120-ЗС «О государственных информационных системах Алтайского края»;
- закрепление нормативно-правовым актом регионального центра обработки и хранения данных как приоритетной инфраструктуры для размещения информационных систем органов исполнительной власти Алтайского края.

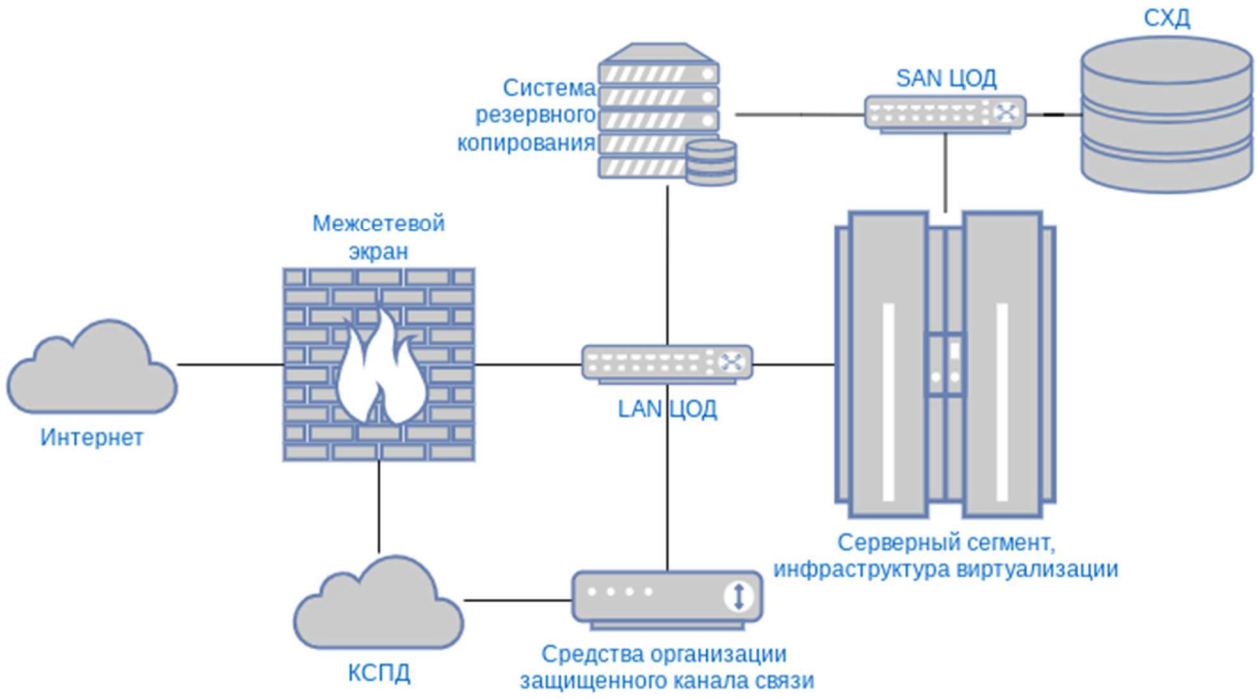

Рис. 5. Схема центра обработки и хранения данных

Созданный региональный центр обработки и хранения данных (рис. 5) обеспечен ресурсами в объеме: 1200 vCPU, 10.5 ТБ оперативной памяти, 167 ТБ емкости для хранения данных (50 ТБ – SSD, 88 ТБ – SAS, 29 ТБ – NLSAS), 370 ТБ – для хранения ежесуточных резервных копий в течение минимум тридцати дней.

В части информационной безопасности региональный центр обработки и хранения данных Алтайского края обеспечен сертифицированными средствами:

- организации защищенного канала связи (ViPNet CUSTOM 4.x, ViPNet TLS Gateway);
- межсетевого экранирования;
- межсетевого экранирования уровня приложений («Positive Technologies Application Firewall»);
- защиты среды виртуализации от несанкционированного доступа («vGate»);
- обнаружения вторжений (ViPNet IDS, ViPNet TIAS);
- анализа уязвимостей («Сканер-ВС»);
- доверенной загрузки (ПАК «Соболь»).

Доступ к информационным системам и ресурсам органов исполнительной власти Алтайского края обеспечен защитой от DDoS-атак на канальном уровне с использованием центров очистки трафика, расположенных на территории Российской Федерации.

На текущий момент в региональном центре обработки и хранения данных размещено 80 % информационных систем органов исполнительной власти Алтайского края, включая государственные системы и ресурсы, в абсолютном выражении это порядка двухсот виртуальных серверов.

4.4. Система мониторинга сетевого трафика и управления средствами антивирусной защиты

Следующий блок работ был посвящен выстраиванию системы мониторинга событий информационной безопасности в органах исполнительной власти Алтайского края и на рабочих местах государственных гражданских служащих и включал следующие этапы:

- создание единой системы управления средствами антивирусной защиты, вплоть до конкретного рабочего места государственного гражданского служащего;
- создание системы мониторинга сетевого трафика локальной инфраструктуры каждого органа исполнительной власти Алтайского края с использованием средств обнаружения вторжений и хранения журналов подключения к ресурсам сети Интернет;
- создание системы анализа событий информационной безопасности на основе баз экспертных данных;
- подключение информационной инфраструктуры к внешнему центру мониторинга информационной безопасности (Security Operations Center, SOC) компании «ИнфоТеКС» для обеспечения наиболее качественной экспертизы событий информационной безопасности и получения рекомендаций по их устранению (предотвращению);
- ежемесячное направление в адрес органов исполнительной власти Алтайского края бюллетеней об информационной безопасности, подготовленных сотрудниками Министерства на основе получаемой информации из центра мониторинга «СОПКА» об актуальных уязвимостях в оборудовании и программном обеспечении, банка данных угроз безопасности информации ФСТЭК России «bdu.fstec.ru» и собственных систем мониторинга;
- принятие Постановления Правительства Алтайского края от 19.11.2020 № 497 «Об утверждении Порядка взаимодействия органов исполнительной власти Алтайского края с Министерством цифрового развития и связи Алтайского края в части реагирования на инциденты информационной безопасности».

Система мониторинга трафика (рис. 6) на первый взгляд кажется сложной в реализации. Однако выбор решений, зарекомендовавших себя при эксплуатации во многих субъектах Российской Федерации, позволил создать единую точку регистрации и анализа событий с разграничением доступа для каждого органа исполнительной власти Алтайского края. К таким решениям относятся:

- средства обнаружения вторжений – ViPNet IDS;
- средства анализа событий информационной безопасности – ViPNet TIAS;
- средства управления поверхности внешней атаки – Attack Surface Management компании Group-IB.

Единый сервис журналирования и хранения данных о подключениях, как часть системы мониторинга, был реализован на базе стандартного протокола netflow.

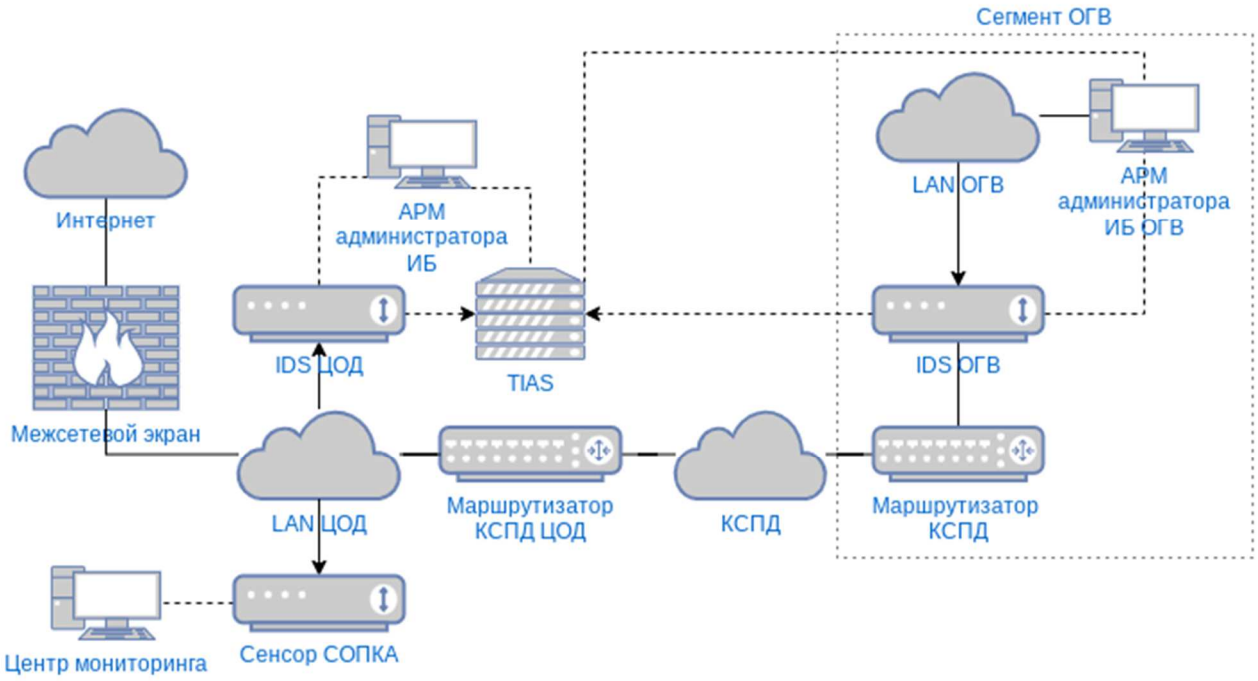

Рис. 6. Схема мониторинга событий информационной безопасности

Сформированная схема управления средствами антивирусной защиты позволила оперативно выявлять конкретное рабочее место – источник вредоносной активности (рис. 7), своевременно его блокировать и предотвращать распространение вредоносного воздействия на объекты информационной инфраструктуры Правительства Алтайского края.

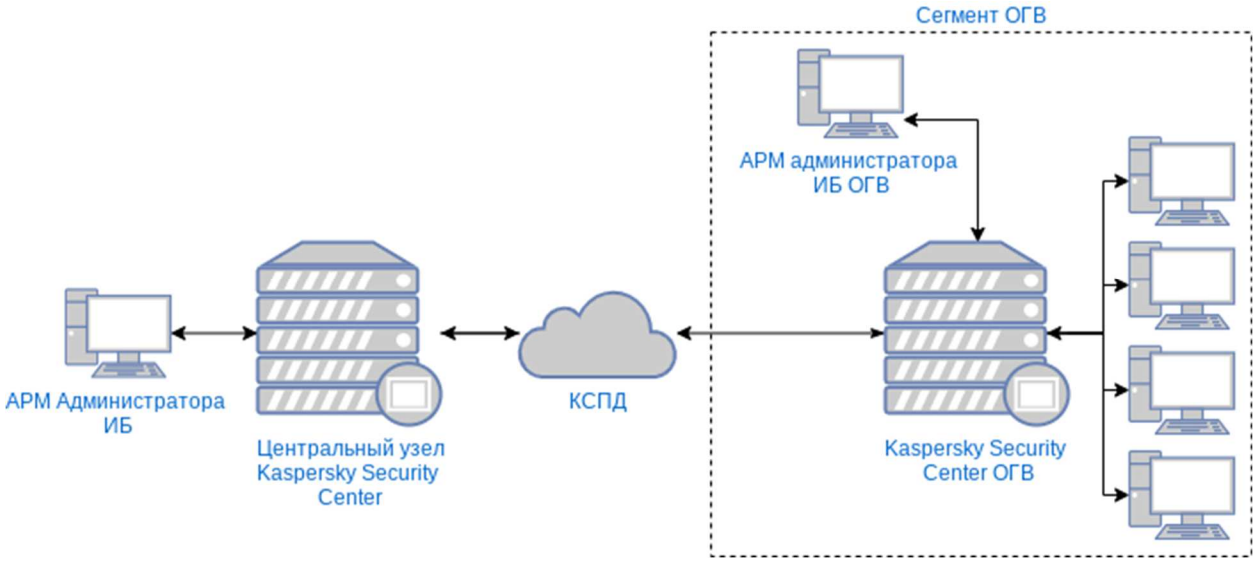

Рис. 7. Схема управления средствами антивирусной защиты

Важно отметить, что вместе с собственными системами мониторинга повысить эффективность выявления вредоносной активности позволяет подключение центрального узла доступа в сеть Интернет к центру мониторинга «СОПКА» и дальнейшее оперативное взаимодействие с сотрудниками центра.

5. Повышение компетенций в области информационной безопасности

Не менее важной задачей при выстраивании информационной инфраструктуры является подготовка и переподготовка кадров, которые в дальнейшем должны ее сопровождать и использовать, так как фиксируется недостаточное кадровое обеспечение в области информационной безопасности, а также низкая осведомленность граждан в вопросах обеспечения личной информационной безопасности. Начиная с 2020 года проведены:

- очное обучение тридцати специалистов органов исполнительной власти Алтайского края, отвечающих за развитие информационных технологий, по сертифицированной ФСТЭК России программе повышения квалификации «Обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных» (72 часа);
- очное обучение пятидесяти муниципальных служащих по программе «Обеспечение защиты информации в органах местного самоуправления Алтайского края» (24 часа);
- краевой конкурс профессионального мастерства «Лучший по профессии» в номинации «Лучший системный администратор», включающий раздел, посвященный обеспечению информационной безопасности;
- тренировка в области информационной безопасности с органами исполнительной власти Алтайского края, в рамках которой на официальные адреса электронной почты государственных гражданских служащих были направлены спам-сообщения, содержащие ссылку для перехода на условно «зараженный» ресурс;
- обучение учителей общеобразовательных организаций Алтайского края по дополнительной профессиональной программе повышения квалификации «Кибербезопасность школ и профилактика правонарушений в сфере информационных технологий», разработанной Министерством цифрового развития и связи Алтайского края, Министерством образования и науки Алтайского края и компанией «Акронис-Инфозащита»;
- занятия со школьниками по теме информационной безопасности в рамках всероссийского образовательного проекта «Урок цифры» Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации, Министерства просвещения Российской Федерации и АНО «Цифровая экономика».

6. Централизованное обеспечение компьютерной техникой

В рамках унификации подходов к обеспечению информационной безопасности Министерством цифрового развития и связи Алтайского края проводятся единые закупочные процедуры преимущественно отечественного программного обеспечения и аппаратных средств для нужд органов исполнительной власти Алтайского края на средства краевого бюджета. Типовое автоматизированное рабочее место государственного гражданского служащего состоит из:

- операционной системы «Astra Linux» или «ALT Linux»;
- офисного пакета «Р7-офис»;
- справочно-правовой системы «Консультант+» или «Гарант»;
- криптопровайдера для работы с электронной подписью и приложениями через протокол TLS «Крипто ПРО» или «ViPNet CSP»;
- браузера от компании «Yandex» или «Chromium GOST»;
- средства антивирусной защиты «Kaspersky» или «Dr.Web»;
- средства защиты от несанкционированного доступа «Secret Net» или «Dallas Lock»;
- средства доверенной загрузки ПАК «Соболь» (в случае необходимости).

7. Заключение

Проведенная в течение трех лет работа по организации комплексной информационной инфраструктуры Правительства Алтайского края показала свою эффективность как в организационном плане при реагировании на инциденты информационной безопасности, так и в финансовом плане при оптимизации расходов на приобретение программно-аппаратных комплексов.

Разработанные универсальные подходы к организации комплексной информационной инфраструктуры Правительства Алтайского края позволили:

- организовать централизованную защиту от DDoS-атак государственных информационных систем и ресурсов;
- обеспечить постоянный мониторинг, выявление и устранение уязвимостей в публичных информационных ресурсах;
- блокировать доступ к информационным системам с вредоносных IP-адресов (ресурсов), в том числе иностранных.

Описанный практический опыт построения информационной инфраструктуры Правительства Алтайского края является универсальным и может быть использован во всех субъектах Российской Федерации для обеспечения информационной безопасности государственных информационных систем и ресурсов с помощью отечественных программных и аппаратных средств.

Литература

1. Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации».
2. Указ Президента РФ от 09.05.2017 № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017 – 2030 годы».
3. Указ Президента Российской Федерации от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации».
4. Выписка из Основных направлений научных исследований в области обеспечения информационной безопасности Российской Федерации (утв. Секретарем Совета Безопасности Российской Федерации Н.П. Патрушевым 31.08.2017).
5. *Демидов А. А.* Проблемы контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления: учебное пособие. СПб.: Университет ИТМО, 2015. 70 с.
6. *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. Т. 23, № 6. С. 99–114.
7. Паспорт национальной программы «Цифровая экономика Российской Федерации» (утв. президиумом Совета при Президенте Российской Федерации по стратегическому развитию и национальным проектам протокол от 24 декабря 2018 г. № 16).
8. Постановление Правительства Алтайского края от 24 января 2020 г. № 25 «Об утверждении государственной программы Алтайского края «Цифровое развитие экономики и информационной среды Алтайского края».
9. Постановление Правительства РФ от 06.06.2015 № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации».

10. *Соловьев М. Л., Минеева Т. Е., Конев А. А., Буинцев Д. Н.* Модель угроз безопасности, возникающих при управлении системой защиты информации // Доклады Томского государственного университета систем управления и радиоэлектроники. 2019. Т. 22, № 3. С. 31–36.
11. Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
12. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
13. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры».
14. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну».
15. Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».
16. Приказ ФСТЭК от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».
17. Указ Губернатора Алтайского края от 6 декабря 2018 г. № 194 «Об утверждении Положения о Министерстве цифрового развития и связи Алтайского края».
18. Указ Президента Российской Федерации от 22.05.2015 № 260 «О некоторых вопросах информационной безопасности Российской Федерации».

Снесарь Виталий Владимирович
заместитель председателя Правительства Алтайского края – руководитель Администрации Губернатора и Правительства Алтайского края (656049, Барнаул, пр. Ленина, 59), e-mail: snesar@alregn.ru.

Зрюмов Евгений Александрович
д.т.н., доцент, министр цифрового развития и связи Алтайского края (656038, Барнаул, ул. К. Маркса, д. 1), e-mail: eaz@alregn.ru.

Илли Денис Юрьевич
начальник отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края (656038, Барнаул, ул. К. Маркса, д. 1), e-mail: iden@alregn.ru.

Янкин Евгений Михайлович
к.т.н., заместитель начальника отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края, e-mail: yankin@alregn.ru.

Чумак Олег Владимирович
консультант отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края, e-mail: ov.chumak@alregn.ru.

Вольвач Сергей Олегович
консультант отдела информационной инфраструктуры Министерства цифрового развития и связи Алтайского края, e-mail: volvach@alregn.ru.

Авторы прочитали и одобрили окончательный вариант рукописи.
Авторы заявляют об отсутствии конфликта интересов.
Вклад соавторов: *Каждый автор внес равную долю участия как во все этапы проводимого теоретического исследования, так и при написании разделов данной статьи.*

Experience in Organizing the Information Infrastructure of the Government of the Altai Region in Response to Security Threats

Snesar Vitaly V., Zryumov Evgeny A., Illi Denis U.,
Yankin Evgeny M., Chumak Oleg V., Volvach Sergey O.

Ministry of Digital Development and Communications of the Altai Region

Abstract: In this paper, complex information infrastructure of the government of the Altai Region is considered. The authors identify three possible stages of information infrastructure development of the government of the Altai Region, such as requirements definition, design, and implementation.

Keywords: information infrastructure, corporate network, digital public administration.

For citation: Snesar V. V., Zryumov E. A., Illi D. U., Yankin E. M., Chumak O. V., Volvach S. O. Experience in Organizing the Information Infrastructure of the Government of the Altai Region in Response to Security Threats (in Russian). *Vestnik SibGUTI*, 2023, vol. 17, no. 4, pp. 74-88. https://doi.org/10.55648/1998-6920-2023-17-4-74-88.

The article was submitted: 14.11.2022;
revised version: 07.12.2022;
accepted for publication 18.07.2023.

References

1. *Ukaz Prezidenta Rossiiskoi Federatsii «Ob utverzhdenii Doktriny informatsionnoi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation “On approval of the Information Security Doctrine of the Russian Federation”]. 5 December, 2016, no. 646.
2. *Ukaz Prezidenta RF «O Strategii razvitiya informatsionnogo obshchestva v Rossiiskoi Federatsii na 2017 - 2030 gody»* [Decree of the President of the Russian Federation “Strategy of the Information Society Development in the Russian Federation for 2017 – 2030”]. 9 May, 2017, no. 203.
3. *Ukaz Prezidenta Rossiiskoi Federatsii «O Strategii natsional'noi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation “On the National Security Strategy of the Russian Federation], 2 July, 2021, no. 400.
4. *Vypiska iz Osnovnykh napravlenii nauchnykh issledovanii v oblasti obespecheniya informatsionnoi bezopasnosti Rossiiskoi Federatsii (utv. Sekretarem Soveta Bezopasno-sti Rossiiskoi Federatsii N.P. Patrushevym)* [Extract from the Main Directions of Scientific Research in the Field of Ensuring Information Security of the Russian Federation]. 31 August, 2017.
5. Demodov A. A. *Problemy kontrolya bezopasnosti informatsii na ob"ektakh telekommunikatsionnykh sistem organov gosudarstvennogo upravleniya* [Problems of Information Security Control at the Objects of Telecommunication Systems of Government Bodies]. Saint Petersburg, ITMO University, 2015, 70 p.
6. Dongak B. S., Shatokhin R. V., Mescheryakov R. V. Effektivnost' tsentralizovannogo ispol'zovaniya tsifrovykh tekhnologii, informatsionnykh resursov i sredstv zashchity informatsii v organakh vlasti na primere respubliki Tyva [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]. *Proceedings of the Southwest State University*, 2019, vol.23 no. 6, pp. 99-114.

7. *Pasport natsional'noi programmy «Tsifrovaya ekonomika Rossiiskoi Federatsii» (utv. prezidiumom Soveta pri Prezidente Rossiiskoi Federatsii po strategicheskomu razvitiyu i natsional'nym proektam)* [Passport of the National Program "Digital Economy of the Russian Federation", approved by presidium of Council at the President of the Russian Federation for strategic development and national projects]. 24 December, 2018, no. 16.
8. *Postanovlenie Pravitel'stva Altaiskogo kraya ot 24 yanvarya 2020 g. №25 «Ob utverzhdenii gosudarstvennoi programmy Altaiskogo kraya «Tsifrovoe razvitie ekonomiki i informatsionnoi sredy Altaiskogo kraya»* [Decree of the Government of the Altai Territory "On approval of the state program of the Altai Territory "Digital development of the economy and information environment of the Altai Territory"]. 24 January, 2020, no. 25.
9. Postanovlenie Pravitel'stva RF «O trebovaniyakh k poryadku sozda-niya, razvitiya, vvoda v ekspluatatsiyu, ekspluatatsii i vyvoda iz ekspluatatsii gosudar-stvennykh informatsionnykh sistem i dal'neishego khraneniya soderzhashcheisya v ikh bazakh dannykh informatsii» [Decree of the Government of the Russian Federation "On Requirements for the Procedure for the Creation, Development, Commissioning, Operation and Decommissioning of State Information Systems, and Further Storage of Information Contained in their Databases"]. 6 July, 2015, no. 676.
10. Soloviev M. L., Mineeva T. E., Konev A. A., Buintsev D. N. Model' ugroz bezopasnosti, voznikayushchikh pri upravlenii sistemoi zashchity informatsii [Model of Security Threats Arising from the Management of Information Security Systems]. *Proceedings of the Tusur University*, Tomsk, 2019, vol. 22, no. 3, pp. 31-36.
11. *Federal'nyi zakon «Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii»* [Federal "On information, information technologies and information protection"]. 27 July, 2006, no. 149-FZ.
12. *Federal'nyi zakon «O personal'nykh dannykh»*. [Federal Law "On personal data"]. 27 July, 2006, no.152-FZ.
13. *Federal'nyi zakon «O bezopasnosti kriticheskoi informatsionnoi infrastruktury»* [Federal Law "About safety of critical information infrastructure of the Russian Federation"]. 26 July, 2017, no.187-FZ
14. *Prikaz FAPSI «Ob utverzhdenii instruktsii ob organizatsii i obespechenii bezopasnosti khraneniya, obrabotki i peredachi po kanalam svyazi s ispol'zovaniem sredstv kriptograficheskoi zashchity informatsii s ogranichennym dostupom, ne soderzhashchei svedenii, sostavlyayushchikh gosudarstvennuyu tainu»* [FAPSI Order "On approval of the Instruction on the organization and security of storage, processing and transmission through communication channels using cryptographic protection of information with limited access, which does not contain information constituting a state secret"]. 13 June, 2001, no. 152.
15. *Prikaz FSTEK Rossii «Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personal'nykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personal'nykh dannykh»* [Order of Federal Service for Technical and Export Control OF Russia "About statement of Structure and content of organizational and technical measures for safety of personal data in case of their processing in personal data information systems"]. 18 February, 2013, no. 21.
16. *Prikaz FSTEK «Ob utverzhdenii Trebovanii o zashchite informatsii, ne sostavlyayushchei gosudarstvennuyu tainu, soderzhashcheisya v gosudarstvennykh informatsionnykh sistemakh»* [Order of Federal Service for Technical and Export Control OF Russia "Requirements for the protection of information that does not constitute a state secret contained in State information systems"]. 11 February, 2013, no. 17.
17. *Ukaz Gubernatora Altaiskogo kraya «Ob utverzhdenii Polozhe-niya o Ministerstve tsifrovogo razvitiya i svyazi Altaiskogo kraya»* [Decree of the Governor of the Altai Territory "On approval of the Regulations on the Ministry of Digital Development and Communications of the Altai Territory"]. 6 December, 2018, no. 194.
18. *Ukaz Prezidenta Rossiiskoi Federatsii «O nekotorykh voprosakh informatsionnoi bezopasnosti Rossiiskoi Federatsii»* [Decree of the President of the Russian Federation "On Certain Issues of Information Security of the Russian Federation"]. 22 May, 2015, no. 260.

Vitaly V. Snesar
Deputy Head of the Government of the Altai Region – Head of the Administration of the Governor and the Government of the Altai Region (Lenina av., 59, Barnaul, Russia, 656049), e-mail: snesar@alregn.ru.

Evgeny A. Zryumov
Dr. of Sci. (Engineering), Docent, Minister of Digital Development and Communications of the Altai Region (K. Marksa st., 1, Barnaul, Russia, 656038), e-mail: eaz@alregn.ru.

Denis U. Illi
Head of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Territory, e-mail: iden@alregn.ru.

Evgeny M. Yankin
Cand. of Sci. (Engineering), Deputy Head of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Territory, e-mail: yankin@alregn.ru.

Oleg V. Chumak
Consultant of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Region, e-mail: ov.chumak@alregn.ru.

Sergey O. Volvach
Consultant of Department of Information Infrastructure of Ministry of Digital Development and Communications of the Altai Region, e-mail: volvach@alregn.ru.