УДК 519.711 *2.3.7.*

ОСОБЕННОСТИ РАЗРАБОТКИ СПЕЦИАЛЬНОГО МАТЕМАТИЧЕСКОГО И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ ДЛЯ ОРГАНОВ УПРАВЛЕНИЯ СИЛОВЫХ СТРУКТУР

Л.Х. Сафиуллина[1], О.В. Красильников[2], А.А. Алексеева[1]

[1] Казанский национальный исследовательский технологический университет КНИТУ
Российская Федерация, 420015, г. Казань, ул. К. Маркса, д. 68

[2] Михайловская военная артиллерийская академия
Российская Федерация, 195009, г. Санкт-Петербург, ул. Комсомола, д. 22

Аннотация. В статье рассматриваются вопросы разработки специализированного программного и математического обеспечения для автоматизированной системы управления в силовых структурах. Приведен краткий анализ отечественного программного обеспечения в силовых ведомствах и структурах, который показывает, что наиболее оптимальным для создания автоматизированной системы управления в силовых структурах с высоким уровнем безопасности и механизмами разграничения доступа будет является программное обеспечение на основе ядра Linux. Для разработки качественно нового специализированного математического и программного обеспечения, позволяющего повысить результаты работы должностных лиц органов управления силовых структур и обеспечить сохранность циркулирующей в автоматизированных системах информации предложена структура программного обеспечения и головного модуля автоматизированной системы. Представленное решение позволяет перестраивать состав автоматизированной системы управления силовых структур в целом и каждого автоматизированного рабочего места в отдельности.

Ключевые слова: информационная безопасность; разработка ПО; база данных; силовые структуры; Astra Linux.

Введение

Активное развитие информационных технологий и цифровизации привело к использованию средств автоматизации в различных сферах производства и общества. Так, по данным отчета Industry 4.0 Market [1] размер финансовых вложений российской промышленности в массовое внедрение информационных технологий и масштабную автоматизацию бизнес-процессов с элементами искусственного интеллекта составил более 400 млрд. руб. При этом динамика затрат российских предприятий в данной сфере выше мирового показателя. Большие объёмы финансирования наблюдаются и в государственном управлении – федеральный проект «Цифровое государственное управление» выполнен на 92,5%: из предусмотренных на него 75 млрд рублей израсходовано примерно 69,4 млрд рублей. Проекты «Кадры для цифровой экономики» и «Информационная безопасность» проработаны на 99,8% [2,3]. Однако, внедрение программных средств цифровизации и автоматизации в определённые сферы государственного управления требует особого внимания. К таким сферам относятся силовые структуры: Министерство обороны, Министерство внутренних дел, МЧС России, Федеральная служба войск национальной гвардии, Следственный комитет и др. Можно сказать, что цифровизация и информатизация на сегодняшний день являются одними из основополагающих векторов развития современных общественных отношений, оказывающих непосредственное влияние на все сферы жизни человека, в том числе и силовые структуры, среди которых особое место занимают правоохранительные органы. Наряду с этим, следует отметить

особенности совершенствования управленческой деятельности силовых структур России с использованием инновационных технологий. К таким особенностям можно отнести внедрение, использование и постоянное совершенствование современных систем связи, аналитики, координации и контроля.

Актуальное состояние информационных технологий позволяет решать многие задачи на новом, более качественном уровне, но в тоже время вызывает необходимость разработки специального математического и программного обеспечения для органов управления различных отраслей и ведомств. Цифровизация процессов управления в данных областях требует внедрения отечественного программного обеспечения (ПО), отвечающего задачам каждого из ведомств, способного осуществлять взаимосвязь между структурами. Помимо того, при разработке и внедрении необходимо выполнять соответствующие требования нормативно-правовой базы России в области обеспечения безопасности информации. Наиболее остро стоит вопрос, связанный с программным обеспечением, специализированным под определенные запросы силовых структур. В решении данного вопроса необходим научный подход с анализом потребностей, проведением научных исследований, последующим проектированием, созданием прототипа для возможности тестирования и оценки функциональности.

Для улучшения управления и оперативного реагирования в силовых структурах с использованием инновационных технологий необходимо учитывать правовые нормы, стандарты управления, а главное – новые модели математического программного обеспечения, которые будут рассмотрены далее. Изменение правовых норм должно отражать потребность в адаптации к новым технологическим возможностям и требованиям современной управленческой практики. Целью работы является разработка подхода к проектированию автоматизированных систем управления силовых структур (АСУ СС). Для достижения цели авторами был проведен анализ текущего состояния программного обеспечения.

Анализ существующего отечественного ПО для силовых структур

В качестве приоритетных задач в нормативно-правовых документах, определяющих использование программного обеспечения, указаны следующие [4,5]:

- использование государственными органами управления различных ведомств, органами местного самоуправления и организациями преимущественно отечественного программного обеспечения;
- создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств;
- обеспечение безопасности информационных систем различного уровня на основе отечественных разработок;
- создание сквозных цифровых технологий преимущественно на основе отечественных разработок.

Использование отечественного программного обеспечения особенно актуально для силовых структур, работающих с конфиденциальной информацией и сведениями, составляющими государственную тайну, поскольку в данном случае у АСУ СС увеличивается надежность, гибкость, а главное, уменьшается вероятность наличия в ПО так называемых «бэкдоров».

Сегодня на рынке отечественного ПО безусловным лидером является семейство операционных систем (ОС) Astra Linux. ОС Astra Linux Special Edition подходит для создания защищённых автоматизированных рабочих мест (АРМ) и АСУ любой сложности, обрабатывающих информацию ограниченного доступа. Astra Linux Special

Edition оснащена развитыми средствами обеспечения информационной безопасности обрабатываемых данных, механизмами мандатного разграничения доступа, контроля замкнутости программной среды и защиты адресного пространства системных процессов, встроенными инструментами маркировки документов, регистрации событий, контроля целостности данных, а также прочими обеспечивающими защиту информации компонентами. ОС Astra Linux Special поддерживает работу с различным аппаратными платформами и может функционировать на системах с отечественными процессорами «Эльбрус», «Байкал-Т1» и «Комдив». На сегодняшний день это единственная платформа, сертифицированная одновременно в системах ФСТЭК России, ФСБ, Минобороны РФ [6]. Помимо Astra Linux Special Edition в российский реестр ПО включены следующие ОС:

- Alt Linux производства (ООО «Базальт СПО»);
- РЕД ОС (РЕДСОФТ);
- «РОСА» производства (ООО «НТЦ ИТ РОСА»).

Каждая из вышеперечисленных ОС имеет сертификат ФСТЭК или ФСБ [7], помимо этого, они подходят для оснащения АРМ. Однако, применение данных ОС в силовых структурах логически не обоснованно, т.к. они не полностью отвечают специальным требованиям, предъявляемым к ИБ АСУ СС [8].

Что касается ПО, которое позволяло бы безопасно обрабатывать сведения, составляющие государственную тайну (в т.ч. степень секретности «совершенно секретно»), то среди прочих следует выделить ПО «Мобильная система Вооружённых сил» (МСВС) на базе ядра Linux Red Hat. В основу МСВС положены разграничения доступа к информации, дополненные дискреционной, мандатной и ролевой моделями, а также развитыми средствами аудита (протоколирования событий). Другим специализированным ПО для АСУ СС можно считать такие, как ОС «Заря», защищенная ОС реального времени «Нейтрино», СЭД «ИВК Бюрократъ» и др. Все перечисленные программные продукты имеют сертификат ФСТЭК и/или ФСБ и предназначены, в основном, для ведомственных структур Министерства обороны РФ. Тем не менее, остаётся актуальной задача разработки ПО, в котором выполнялись бы все нижеперечисленные требования:

- возможность применять специальное математическое и программное обеспечение (СМиПО);
- высокий уровень обеспечения ИБ;
- наличие механизмов мандатного разграничения доступа, контроля замкнутости программной среды и защиты адресного пространства системных процессов встроенными инструментами маркировки документов;
- возможность выбора соответствующей ОС;
- регистрация событий ИБ, контроль целостности данных и пр. компоненты, которые обеспечивают защиту информации [9].

Очевидно, что для создания АРМ в силовых структурах наиболее приемлемыми будут являться компоненты и ядро Linux. Имеющиеся и создаваемые органы управления силовыми структурами, как правило, применяют в своей работе автоматизированные рабочие места (АРМ), и являются по своей сути автоматизированными системами специального назначения, имеющими все присущие для АСУ элементы (АСУ СС).

Модель АСУ силовых структур

В составе АСУ СС следует различать его обеспечивающую часть и АРМ пользователей. Обеспечивающая часть включает в себя технические и программные компоненты, гарантирующие функционирование системы управления средствами связи

(серверная инфраструктура, коммутационное оборудование, сетевые устройства) и ПО (базы данных, ОС, специализированное функциональное ПО). Обеспечивающие подсистемы являются системами управления, но может быть произведена их декомпозиция по входимости в различные функциональные подсистемы. АРМ пользователей в составе АСУ включают:

- графические интерфейсы (элементы управления, отображение данных в графическом формате);
- прикладные программы (программы мониторинга и управления, аналитические инструменты);
- средства взаимодействия (коммуникационные средства, системы уведомлений);
- системы аутентификации и безопасности (шифрование, аутентификации).

Структура и состав АСУ включают различных блоки обеспечения (рис. 1).
Здесь:

- МО – математическое обеспечение, которое представляет комплекс программ, управляющих работой технических средств, функционированием информационной базы и обеспечивающих взаимодействие человека с техническими средствами АСУ. МО строится таким образом, чтобы в случае необходимости можно было изменять не только отдельные программы, но и критерии, по которым ведётся управление;
- ПО – программное обеспечение т.е. комплекс программных средств (системных и прикладных программ), который решает конкретные функциональные задачи и обеспечивает функционирование всех средств АСУ;
- ТО – техническое обеспечение, т.е. комплекс технических средств, с помощью которых выполняются функции АСУ. В состав технического обеспечения включают: средства сбора информации, исполнительные устройства, устройства распределенного ввода-вывода и др.;
- ЛО – лингвистическое обеспечение т.е. совокупность средств и правил для формализации естественного языка, используемых при общении пользователей и эксплуатационного персонала АСУ;
- ИО – информационное обеспечение т.е. совокупность форм документов, классификаторов, нормативной базы и реализованных решений по объемам, размещению и формам существования информации, применяемой в АСУ при ее функционировании;
- Орг. О – организационное обеспечение т.е. совокупность документов, устанавливающих организационную структуру, права и обязанности пользователей и эксплуатационного персонала АСУ в условиях функционирования, проверки и обеспечения работоспособности АСУ;
- Мет. О – методическое обеспечение т.е. совокупность документов, описывающих технологию функционирования АСУ, методы выбора и применения пользователями технологических приемов для получения конкретных результатов при функционировании АСУ;
- Пр. О – правовое обеспечение т.е. совокупность правовых норм, регламентирующих правовые отношения при функционировании АСУ и юридический статус результатов ее функционирования [10].

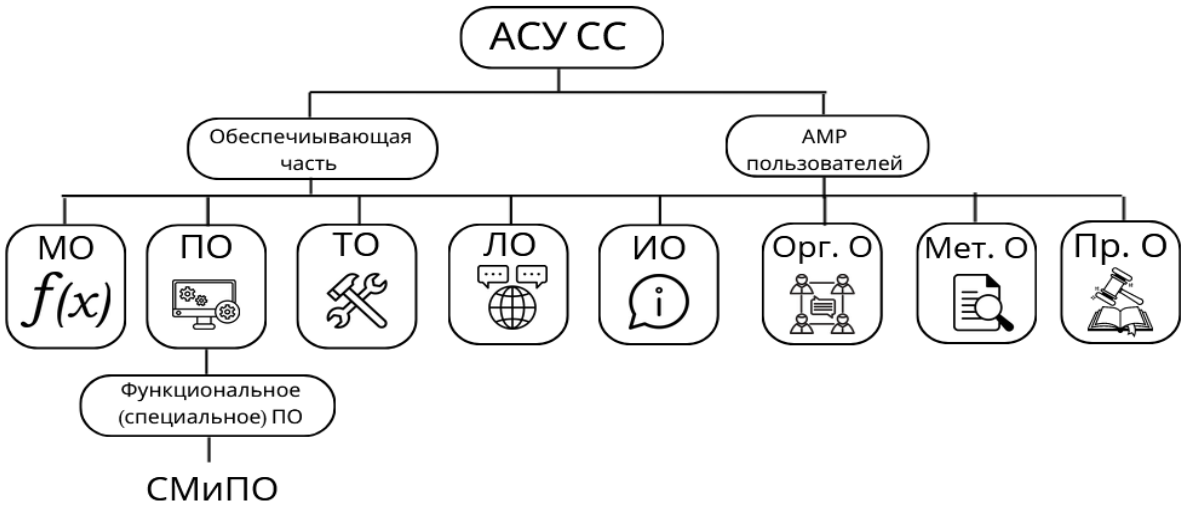

Рис.1. Состав АСУ СС

Важнейшей составляющей АСУ СС, ее интеллектуальной основой является специальное математическое и программное обеспечение (СМиПО), которое имеет сложную структуру, и в этом контексте является ключевым элементом, обеспечивающим интеллектуальные функции и эффективное управление в разнообразных сценариях.

В жизненном цикле разработки ПО, в том числе СМиПО для силовых структур, можно выделить следующие основные этапы:

- анализ,
- составление требований к ПО,
- планирование и проектирование,
- разработка,
- тестирование,
- развертывание,
- эксплуатация.

Построение СМиПО и организация его функционирования в структурных подразделениях силовых структур осуществляются исходя из задач, решаемых АСУ СС. Эти задачи могут быть трансформированы в требования к СМиПО, основными из которых являются [10]:

1) соответствие основным этапам информационной, аналитической и распорядительной деятельности должностных лиц АСУ СС (сбор информации, ее анализ, принятие управленческого решения);
2) объективность и достоверность результатов его функционирования (валидация данных, проверка моделей);
3) разработка СМиПО на основе единого сценария действий (унификация алгоритмов, адаптивность);
4) соответствие состава и степени детализации информации, обрабатываемой и формируемой средствами СМиПО, иерархическому уровню органа управления (иерархическая структура, кастомизация информации);
5) своевременность получения результатов применения средств СМиПО (оптимизация и повышение производительности, получение информации в режиме рольного времени);
6) удобство практического применения средств СМиПО должностными лицами АСУ СС (интуитивно удобные интерфейсы, обучение и поддержка).

Состав компонентов СМиПО будет определяться перечнем задач, которые необходимо решать в соответствующем органе управления, и особенностей, выполняемых функций.

Оценка проводимых опытно-конструкторских работ (ОКР) по созданию АСУ СС показывает, что чаще всего возникает ситуация, когда принимаемые на эксплуатацию компоненты из состава СМиПО создаваемых АСУ СС оказываются малопригодными ввиду:

- морального и технологического устаревания;
- изменения требований стандартов и законодательства;
- изменений в методологии и подходах к управлению;
- недостаточной гибкости и адаптивности СМиПО;
- отсутствия планов обслуживания и модернизации [11].

Для предотвращения подобных ситуаций, при проведении опытно-конструкторских работ следует уделять внимание не только текущим требованиям, но и возможным изменениям в будущем. Также важно регулярно проводить обзор и модернизацию компонентов СМиПО, чтобы они оставались актуальными и эффективными в течение всего срока службы АСУ СС

Достаточно часто практическая работа должностных лиц в соответствующем органе управления заставляет сотрудников разрабатывать ПО, которое используется ими повседневно, но оно не адаптировано под возможности штатных программных средств (особенно ориентированных на решение задач защиты информации), а это, в свою очередь, создаёт возможность утечки информации. Всё это обусловливает необходимость разработки качественно нового СМиПО, позволяющего повысить результаты работы должностных лиц органов управления силовых структур и обеспечить сохранность циркулирующей в АСУ информации [11].

С учётом сказанного структура ПО АСУ СС будет иметь вид (рис.2)

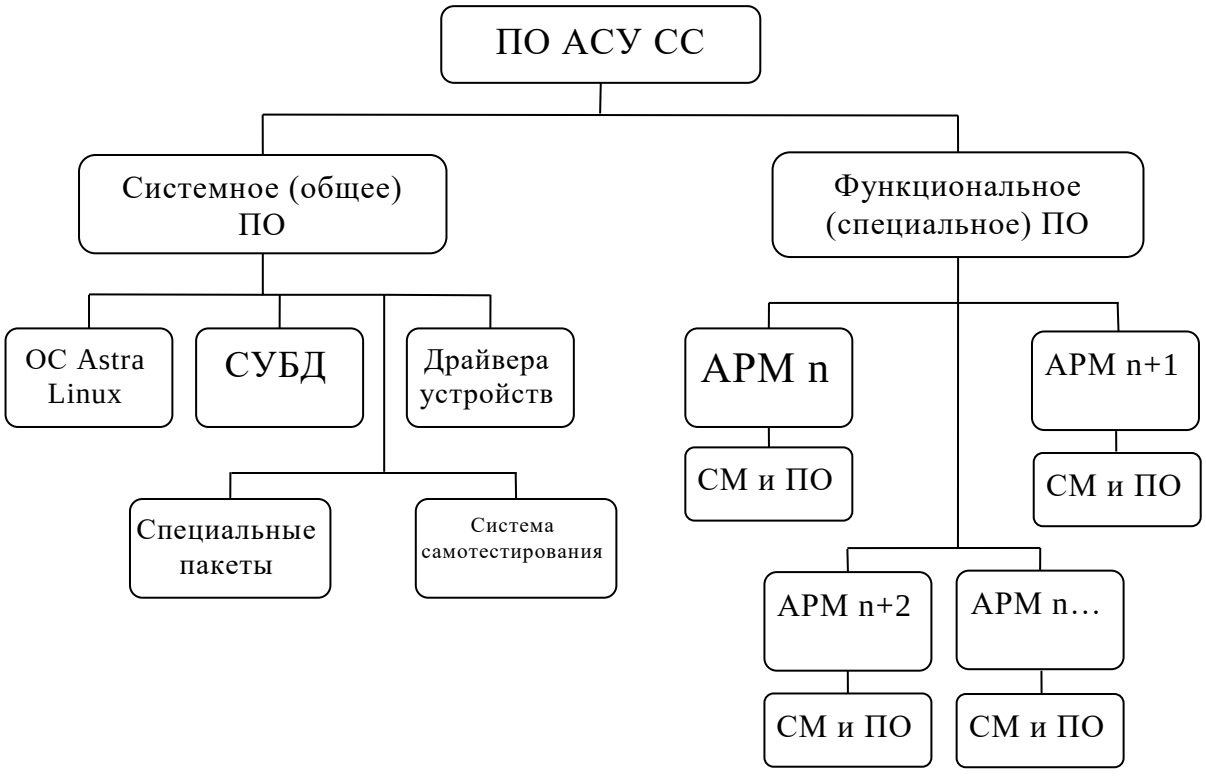

Рис. 2. Структура ПО АСУ СС

Проблемным в настоящее время остаётся вопрос выбор СУБД для АСУ СС. Так, СУБД «Линтер Бастион 6.0» прошла сертификацию в Министерстве обороны и ФСТЭК. Многоуровневая защита позволяет строить информационные системы, в частности, предназначенные для обработки и хранения секретной информации. СУБД «Заря» обладает сертификатом Министерства обороны и предназначена для обработки и хранения информации, составляющей государственную тайну не выше уровня «совершенно секретно». Таким, образом, в настоящее время отсутствует единое мнение в пользу выбора единой для силовых структур СУБД. В [12] утверждается, что Postgres Pro стала первой отечественной СУБД, сертифицированной по новым требованиям регулятора. Сертификат допускает использование программного комплекса для хранения и обработки данных в критической инфраструктуре первой категории и государственных информационных системах первого класса защищённости.

Реализация требований к АСУ СС возможна только при соблюдении принципа распределенной обработки данных в рамках локальных вычислительных сетей, состав элементов которой и их функциональные возможности позволяют адаптировать её структуру к реальной обстановке без организационной и технической перестройки. Разработка АСУ СС с соблюдением данных принципов будет способствовать выполнению стратегических задачах развития Российской Федерации [4]. Такой подход не только обеспечивает высокую производительность и гибкость системы управления, но также позволяет ей эффективно функционировать в динамичной и изменчивой среде, что особенно важно для силовых структур.

Типовая структура комплекса программ АСУ СС представлена на рис.3.

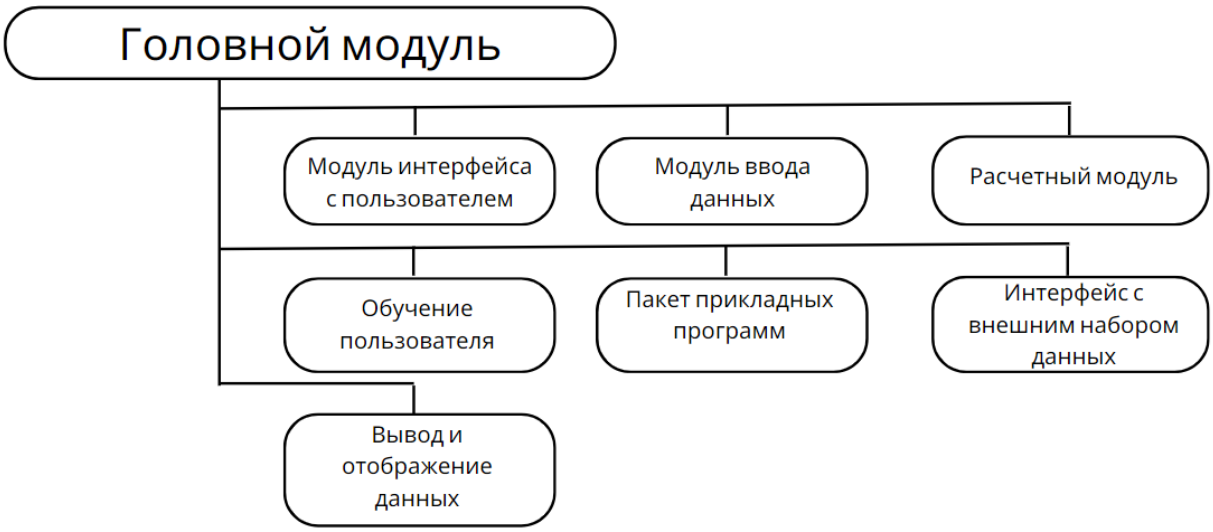

Рис.3. Типовая структура комплекса программ АСУ СС

Для достижения принципа распределенной обработки данных система должна иметь модульную структуру, а состав должностных лиц на АСУ СС и их техническое оснащение средствами автоматизации и связи для каждого модуля соответствовать определенному уровню иерархии [10].

Важнейшая функция локальной вычислительной сети (ЛВС) (использование которых будет преобладать, очевидно, в ближайшей перспективе в органах управления силовыми структурами) заключается в организации распределенного хранения и распределенной обработки информации в узлах сети, а также учета возможности масштабируемости систем. Необходимо отметить, что информационные ресурсы вооружённых сил РФ сосредоточены в органах управления различного уровня. Вся их

совокупность образует объективно существующее информационное пространство, использование которого в процессах управления при подготовке и принятии обоснованных решений, контроле их выполнения весьма затруднительно по ряду объективных и субъективных причин. При построении АСУ СС используются общие подходы к АСУ общего назначения. При этом учитываются особенности функционирования АРМ должностных лиц (как мобильных, так и стационарных) в жестких условиях их эксплуатации и ограничений на их использование с учётом требований СС. При этом на функционирование данных АРМ накладываются ряд ограничений как по условиям их эксплуатации, так и по защите информации, циркулирующей в них. Проблемным вопросом остаётся правовое регулирование использования СМПО на этих АРМ, так как под требования СС (которые в должной мере не разработаны) они не подходят, а на практике должностными лицами используется данное ПО.

Каждое из АРМ имеет, набор пакета прикладных программ (ППП) из их общего состава СМПО, так и ППП, необходимый на данном АРМ.

При этом необходимо на всех узлах сети использовать совместимые средства программного и информационного обеспечения с тем, чтобы повысить эффективность функционирования сети и её эксплуатационные характеристики, а также снизить затраты на ее создание [10]. Это не только способствует снижению затрат на создание сети, но и обеспечивает ее согласованное и совместное действие.

Создание единого информационного пространства (ЕРИП) в рамках ЛВС является стратегическим шагом и позволит решить задачу обеспечения должностных лиц органов управления нужной информацией, так как они не только могут хранить данные на своей рабочей станции, но и получают доступ к данным, хранимым в любом узле сети.

Важными являются вопросы совместимости для всех ЭВМ (ПЭВМ) сети средств программного и информационного обеспечения, и универсальной доступности программ. Под программной совместимостью понимается возможность переноса любой программы, написанной на исходном алгоритмическом языке, на любую ЭВМ (ПЭВМ) информационной сети без её переделки. Здесь также возникает вопрос правового обеспечения правомерности разработки программного обеспечения с соблюдением требований защиты информации.

Выводы

Рынок ПО в России ежегодно пополняется новыми предложениями. Одни из них разрабатываются с нуля отечественными специалистами, другие создаются на основе заимствованных исходных кодов. Несмотря на это, многие дистрибутивы уже нашли свою нишу и своих постоянных пользователей. Не все продукты из перечня российского ПО совершенствуются и выдерживают конкуренцию, но большинство из них достойно проходят проверку импортозамещением и становятся лидерами в своей отрасли. Анализ состояния программного обеспечения АСУ СС и технических средств органов управления силовых структур указывает на то, что перечень прикладных программ довольно обширен и расширяется постоянно с целью повышения качества организации и управления структурными подразделениями, а разработанные с учетом требований защиты информации и правил организации такой работы в органах управления силовых структур алгоритмы охватывали бы весь перечень решаемых ими задач.

Предложенная в статье структура программного обеспечения и головного модуля автоматизированной системы позволяет перестраивать состав автоматизированной системы управления силовых структур в целом и каждого автоматизированного рабочего места в отдельности с соблюдением представленных выше требований.

Список литературы

1. Industry 4.0 Market Size & Share Analysis - Growth Trends & Forecasts (2024 - 2029) [Электронный ресурс]. – Режим доступа: https://www.mordorintelligence.com/industry-reports/industry-4-0-market
2. TAdviser. Национальная программа Цифровая экономика Российской Федерации [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php/
3. На пути к цифровому будущему: о реализации нацпрограммы «Цифровая экономика» [Электронный ресурс]. – Режим доступа: https://telesputnik.ru/materials/gov/article/na-puti-k-tsifrovomu-budushchemu-o-realizatsii-natsprogrammy-tsifrovaya-ekonomika
4. Указ Президента Российской Федерации от 07.05.2018 г. № 204 О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года [Электронный ресурс]. – Режим доступа: http://www.kremlin.ru/acts/bank/43027
5. Приказ Минкомсвязи России «О внесении изменений в приказ Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации от 20.09.2018 № 486 «Об утверждении методических рекомендаций по переходу государственных компаний на преимущественное использование отечественного программного обеспечения, в том числе отечественного офисного программного обеспечения» [Электронный ресурс]. – Режим доступа: https://digital.gov.ru/ru/documents/6458/
6. Обзор ПО для российских военных и силовых структур [Электронный ресурс]. – Режим доступа: https://servernews.ru/968470?ysclid=lsj5l2epsg483565274
7. Официальный сайт единого реестра российских программ для электронных вычислительных машин и баз данных [Электронный ресурс]. – Режим доступа: https://reestr.digital.gov.ru
8. Талашко А. К. Импортозамещение в сфере программного обеспечения //Современное образование: интеграция образования, науки, бизнеса и власти. Трансформация образования, науки и производства - основа технологического прорыва. – 2023. – С. 131-134.
9. Безопасность операционной системы специального назначения Astra Linux Special Edition: Учебное пособие для вузов / П.В. Буренин, П.Н. Девянин, Е.В. Лебеденко, В.Г. Проскурин, А.Н. Цибуля; под редакцией доктора техн. наук П. Н. Девянина. – 2-е изд., стереотип. – Москва: Горячая линия-Телеком, 2018. - 312 с.
10. Переносные комплексы автоматизированного управления огнём артиллерии тактического звена: монография / Моисеев В.С., Козар А.Н., Красильников В.Н, Красильников О.В. - Казанское высшее артиллерийское командное училище (военный институт) имени маршала артиллерии М.Н. Чистякова, 2009. – 144 с.
11. Абросимов, Л. И. Базисные методы проектирования и анализа сетей ЭВМ. Учебное пособие / Л.И. Абросимов. - М.: Университетская книга, 2015. - 248 с
12. Postgres Pro стала первой отечественной СУБД, сертифицированной по новым требованиям ФСТЭК России [Электронный ресурс]. – Режим доступа: https://servernews.ru/1096176

FEATURES OF DEVELOPMENT OF SPECIAL MATHEMATICAL AND SOFTWARE FOR CONTROLS OF POWER STRUCTURES

L.H. Safiullina[1], O.V. Krasilnikov[2], A.A. Alekseeva[1]

[1] Kazan National Research Technological University KNRTU
68, st. K. Marksa, Kazan, 420015, Russian Federation

[2] Mikhailovskaya Military Artillery Academy
22, st. Komsomol, St. Petersburg, 195009, Russian Federation

Annotation. The article discusses the development of specialized software and mathematical support for an automated control system in law enforcement agencies. A brief analysis of domestic software in law enforcement agencies and structures is provided, which shows that the most optimal for creating an automated control system in law enforcement agencies with a high level of security and access control mechanisms will be software based on the Linux kernel. To develop qualitatively new specialized mathematical and software that will improve the performance of officials of law enforcement agencies and ensure the safety of information circulating in automated systems, the structure of the software and the head module of the automated system is proposed. The presented solution allows you to rebuild the composition of the automated control system of law enforcement agencies as a whole and each automated workstation separately.

Key words: information security; software development; database; strong structure; Astra Linux.

Статья представлена в редакцию 29 декабря 2023г.