ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ КАЗЕННОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ ЮРИДИЧЕСКИЙ ИНСТИТУТ
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ»

ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Уфа 2022

УДК 351.74.07:002:004(470)(075.8)
ББК 67.401.133-9(2Рос)с51ф1я73-1
О-75

Рекомендовано к опубликованию
редакционно-издательским советом Уфимского ЮИ МВД России

Рецензенты:
кандидат экономических наук, доцент О. Л. Морозов
(Нижегородская академия МВД России);
кандидат юридических наук, доцент Е. Ю. Семенов
(Орловский юридический институт МВД России имени В. В. Лукьянова)

Коллектив авторов:
В. В. Антонов – доктор технических наук, профессор;
З. И. Харисова – кандидат технических наук, б/з;
В. Р. Гурьянова – кандидат физико-математических наук, б/з;
Н. Р. Калимуллин – б/с, б/з

О-75 **Особенности информационного обеспечения профессиональной деятельности в органах внутренних дел** : учебное пособие / В. В. Антонов [и др.]. – Уфа : Уфимский ЮИ МВД России, 2022. – 48 с. – Текст : непосредственный.

ISBN 978-5-7247-1107-4

В учебном пособии представлены анализ реализации программы импортозамещения программного обеспечения, особенности и сравнение современного программного обеспечения, входящего в Единый реестр российских программ для электронных вычислительных машин и баз данных, используемых в органах внутренних дел, сформированы рекомендации для эффективной работы с использованием некоторых программ из указанного реестра.

Учебное пособие предназначено для профессорско-преподавательского состава, обучающихся образовательных организаций МВД России.

УДК 351.74.07:002:004(470)(075.8)
ББК 67.401.133-9(2Рос)с51ф1я73-1

ISBN 978-5-7247-1107-4

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Информационное обеспечение профессиональной деятельности в органах внутренних дел – это обеспечение соответствующих подразделений и должностных лиц совокупностью сведений, а также средствами сбора, хранения и обработки информации, необходимых для осуществления возложенных на органы внутренних дел задач и функций. Информационное обеспечение должно удовлетворять множество требований, определенных различными нормативно-правовыми актами.

Реализация информационного обеспечения органов внутренних дел требует системного подхода, включающего различные аспекты, начиная от повышения эффективности работы с информационными системами и заканчивая конкретным программным обеспечением, используемым в профессиональной деятельности.

Используемое в правоохранительных органах программное обеспечение на текущий период времени находится в стадии форсированного обновления, вызванного необходимостью обеспечить информационный суверенитет и требуемый уровень информационной безопасности. На законодательном уровне были утверждены ограничения на использование зарубежного программного обеспечения при осуществлении государственных и муниципальных закупок. Были введены поправки в Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», в частности, ст. 12.1 – «Особенности государственного регулирования в сфере использования российских программ для электронных вычислительных машин и баз данных», в рамках реализации которой был сформирован единый реестр российских программ. Подобный подход дал толчок развитию индустрии разработки отечественного программного обеспечения и замены зарубежных аналогов.

Единый реестр российских программ (далее – реестр) и правила его пополнения требуют анализа ввиду неразрешенности вопроса, связанного с использованием за основу таких разработок свободного программного обеспечения (под различными видами лицензий: GPL, MPL и других). Большая часть отечественных операционных систем, некоторые офисные пакеты программ, системы управления базами данных берут за основу свободное программное обеспечение. Использование свободного программного обеспечения с открытым исходным кодом безусловно представляет интерес как с точки зрения информационной безопасности (можно осуществить верификацию кода программы), так и с экономической точки зрения, поскольку они бесплатны. Ввиду перспектив использования такого класса программного обеспечения они также будут отражены в пособии, несмотря на отсутствие в Едином реестре российских программ и попытки исключить из реестра программы на их основе.

Программы импортозамещения программного обеспечения наталкиваются на ряд трудностей, например, сложность интеграции в существующие информационные системы без нарушения работоспособности; необходимость обучения и переобучения пользователей и администраторов; высокую стоимость и временные затраты на комплекс мероприятий и само программное обеспечение и т. д.

В пособии представлен анализ реализации программы импортозамещения программного обеспечения, особенности современного программного обеспечения, входящего в Единый реестр российских программ для электронных вычислительных машин и баз данных, используемых в органах внутренних дел, формирование рекомендаций для эффективной работы с использованием некоторых программ из Единого реестра российских программ для электронных вычислительных машин и баз данных, а также свободно распространяемых программ с открытым исходным кодом.

Данное учебное пособие предназначено для повышения эффективности работы сотрудников органов внутренних дел отечественным программным обеспечением в профессиональной деятельности, оптимизации реализуемых информационных процессов с использованием новых программных и программно-аппаратных комплексов.

ГЛАВА 1. АНАЛИЗ ТЕКУЩЕГО СОСТОЯНИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ ИМПОРТОЗАМЕЩЕНИЯ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

§ 1. Роль информации и информационного обеспечения в деятельности органов внутренних дел

Любая система для своего функционирования требует определенных ресурсов, а в случае, если это социальная система, то ключевым ресурсом, обеспечивающим организацию и управление, является информация.

Понятие «информация» является одним из фундаментальных в современной науке. Несмотря на сформированные определения в законодательстве и отраслевых стандартах, до сих пор нет определения термина «информация», удовлетворяющего все сферы, где он употребляется. В качестве примера можно привести несколько определений информации, которые встречаются в различных источниках:

Информация – это продукт отражения действительности.

Информация (лат. information – разъяснение, изложение, осведомленность) – одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.

Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления.

Термин «информация» стал использоваться в начале XIX века в Европе как составное слово in form и трактовался как нечто упорядочивающее, оформляющее для обозначения некоторого ученья, наставленья (информации), которым делился наставник (информатор). Затем смыслы, вкладываемые в это слово, стали стремительно расширяться. Наиболее часто под информацией понимают: сведения; сообщения о чем-либо, которыми обмениваются люди; сигналы; импульсы; образы, циркулирующие в технических (кибернетических) устройствах; количественную меру устранения неопределенности (энтропии); меру организации системы; отражение разнообразия в любых объектах и процессах неживой и живой природы. Есть и другие определения информации, но все они зачастую несовместимы друг с другом. Например, информацией именуются: абстрактный концепт, физическое свойство, функция самоуправляемых систем. Информация может быть: объективной и субъективной, материальной и идеальной. Информация – это и вещь, и свойство, и отношение.

В настоящее время с целью определения качественных характеристик информации привлекают специалистов в области информационных технологий, инженеров, а также профессиональных психологов, лингвистов и экономистов.

Качество информации является сложной характеристикой, основу которой может составлять система показателей, включающая свойства вы-

дачи, обработки и защиты информации, своевременность выдачи информации, ее достоверность, целостность и безопасность.

Информация играет главенствующую роль в процессе эволюции и развития цивилизации. Владение информационными ресурсами и рациональное их использование создают условия для оптимального управления обществом. И, напротив, искажение информации, блокирование ее получения, использование недостоверных данных ведут к ошибочным решениям.

Информация с высоким темпом общественного и научно-технического развития является важнейшим ресурсом человечества. Потоки информации неисчерпаемы, так как в совокупности «информация» и «знание» появляются новые информационные потоки.

Систематическое научное познание окружающего мира сводится к накоплению информации в форме знаний. По этой причине со стороны процесса познания информация может рассматриваться как знание.

В кибернетике понятие «информация» используется для описания процессов управления в сложных системах. Жизнедеятельность любого организма или нормальное функционирование технического устройства связано с процессами управления, благодаря которым поддерживаются в необходимых пределах значения его параметров.

При рассмотрении процесса управления имеет место взаимодействие управляющего и управляемого объектов, которые связаны между собой каналами прямой (для передачи управляющих сигналов) и обратной (для передачи информации о состоянии управляемого объекта) связи. Таким образом, информация прежде всего является смысловой, т. е. перерабатываемой человеческим сознанием и реализуемой в его деятельности. Она обусловлена потребностями и интересами индивида, социальных групп, классов, находящихся в постоянном общении между собой, в процессе материального и духовного производства и организации всей общественной жизни.

В деятельности органов внутренних дел преобладает особый вид информации под названием социальная, которая является основным предметом деятельности, характеризует ее результаты, благодаря чему органы внутренних дел способны осуществлять взаимодействие с действительностью, координировать деятельность структур, их функционирование.

Для осуществления процесса управления в органах внутренних дел оперируют системой информации – совокупностью сведений о социально-правовых явлениях и процессах. В специальной литературе систему информации именуют понятием «оперативная обстановка».

Компоненты оперативной обстановки образуют информацию, характеризующую органы внутренних дел как систему решения поставленных задач, информацию об объекте воздействия и элементах среды функционирования иных объектов воздействия.

Существует несколько разновидностей классификаций информации, используемой в органах внутренних дел. Как правило, принято подразделять информацию на оперативно-справочную, оперативно-разыскную, криминалистическую, статистическую или управленческую, производственно-экономическую, архивную и научно-техническую. Обычно в организациях мы встречаемся с такой общей классификацией, когда информация подразделяется на входящую, исходящую и внутреннюю.

Наиболее часто применяемыми методами получения информации в органах внутренних дел (далее – ОВД) служат наблюдение (непосредственное, включенное или косвенное); опросы (беседы, анкетирование или интервьюирование); изучение официальных и неофициальных документов; эксперименты лабораторные, полевые, а также специальные методы – от тестовых испытаний до экспертных оценок.

В соответствии со сложившимися информационными связями в ОВД движутся потоки информации, под которыми принято понимать совокупность отдельных сообщений по определенным направлениям. Практика показывает, что отсутствие рациональных схем организации информационных потоков приводит к огромным издержкам и затратам на поддержание необходимой полноты, достоверности и своевременности предъявления информации.

Поступающие в органы внутренних дел данные должны представлять собой именно многомерные распределения, так как только они позволяют проводить сравнения, сопоставления тех или иных индикаторов преступности и правонарушений в соотношении с их качественными и количественными признаками.

На основе сведений о преступлениях и лицах, причастных к их совершению, создаются специализированные базы данных: по выявленным, раскрытым, нераскрытым преступлениям, по делам с законченным расследованием, по ущербу от преступлений, по их участникам и т. д.

Статистические данные о преступности служат основой для выработки многих управленческих решений, при этом методика и техника статистического анализа в управлении практически совпадает с методикой и техникой статистического анализа в криминологии.

Информационное обеспечение управления в органах внутренних дел должно обеспечивать ввод, обработку, хранение и получение необходимой информации и только тех сведений, которые необходимы и достаточны субъекту управления определенного уровня для эффективной организации его работы. Эти сведения должны быть предоставлены в нужный момент и в необходимом объеме.

В требованиях к информации, используемой в управлении ОВД, указывается, что информация должна отражать все основные характеристики изучаемой совокупности явлений (т. е. быть репрезентативной), обеспечивать изучение объекта во всем многообразии его проявлений и взаимосвя-

зей (быть комплексной), относиться к объекту изучения (релевантность), а также быть объективной и достоверной.

Информационное обеспечение любого из направлений деятельности ОВД должно состоять из организации сбора информации субъектами управления, взаимодействия технических средств, позволяющих организовать доступ к информации из всего массива данных и поддержки принимаемых решений субъектом управления.

Основные задачи информационного обеспечения конкретного направления деятельности органов внутренних дел заключаются в проектировании информационных систем с созданием распределенных баз данных, оперативном получении пользователями информации, необходимой для решения конкретной задачи, реализации математических методов анализа информации и создании на их основе систем поддержки управленческого решения, а также в организации функционирования и постоянного совершенствования самого информационного обеспечения, организационных процессов и информационных систем.

Для эффективного управления необходима рациональная организация информационных процессов. В этих целях создаются системы сбора, хранения, обработки и передачи информации, необходимой для удовлетворения потребностей управления. Основная задача данных систем заключается в том, чтобы соответствующий субъект мог в нужный момент получить из определенных источников систематизированную и должным образом обработанную информацию по интересующему его вопросу. Информационная система служит своего рода посредником между пользователем и источником тех или иных сведений.

Компонентами информационных систем являются: люди (персонал), обеспечивающие функционирование названных систем; информация, которая в них собирается, систематизируется, хранится и обрабатывается; используемые здесь технические средства; методы, процедуры сбора и преобразования информации.

Совокупность информационных систем органа управления образует систему информации, в которой первые выделяются по какому-либо основанию (виду собираемой информации, функциям управления и т. п.) в качестве подсистем. Таким образом, если понятием «система информации» охватывается вся информация органа управления, то понятием «информационная система» – лишь часть этой информации.

Объективная необходимость создания не одной, а многих информационных систем обусловливается тем, что информация, используемая в органе управления, различается по своему содержанию, предназначению, по методам, средствам сбора, передачи и обработки. Наличие специализированных информационных систем позволяет субъекту управления осуществлять различные подходы к решению возникающих задач. Поэтапное же проектирование, внедрение и совершенствование локальных информаци-

онных систем являются реальной основой для последующего создания единой системы информации.

§ 2. Основные направления повышения эффективности информационного обеспечения в органах внутренних дел

Одним их наиболее актуальных направлений совершенствования информационного обеспечения в ОВД является использование информационных технологий в деятельности сотрудников, а также формирование единой актуальной базы данных оперативно-служебной деятельности.

Использование информационных технологий предполагает реализацию межведомственного взаимодействия, использования данных, размещенных в телекоммуникационных системах, сети Интернет. В настоящее время использование информационных технологий в решении оперативных задач набирает все большую популярность, а в некоторых областях, например, в области компьютерной криминалистики, является их неотъемлемой частью. Это открывает новые горизонты и способствует повышению уровня эффективности управления.

Основными критериями эффективности использования информационных технологий в информационном обеспечении служебной деятельности являются:

– использование современных информационных технологий, программного и аппаратного обеспечения;

– подготовка квалифицированных кадров;

– долгосрочный характер развития и использования информационных систем;

– общая техническая оснащенность.

Совершенствование информационных систем должно быть направлено на ликвидацию задержек поступления и обработки информации; фактов ее избытка, несопоставимости сообщений, дублирования данных; низкого коэффициента использования информации. В современных условиях, открывающих возможность использования достижений научно-технического прогресса, первоочередной задачей в рассматриваемой сфере деятельности становится создание на базе электронно-вычислительных машин (далее – ЭВМ) и других технических средств информационно-телекоммуникационной системы (далее – ЕИТКС).

Так, в 2004 году была образована Дирекция Программы МВД России, а уже к концу года была утверждена сама Программа МВД России «Создание единой информационно-телекоммуникационной системы органов внутренних дел», целью которой являлось повышение эффективности деятельности ОВД, обеспечение законности, правопорядка и общественной безопасности путем совершенствования информационного обеспече-

ния ОВД на основе реконструкции и оборудования объектов ОВД новыми и перспективными телекоммуникационными и программно-техническими комплексами с использованием современных телекоммуникационных, информационных и биометрических технологий.

В 2012 году МВД России утвердило новую концепцию создания единой системы информационно- аналитического обеспечения деятельности (далее – ИСОД) МВД России, которая заключалась в комплексном использовании в министерстве новейших информационных систем, телекоммуникационного оборудования, программно-аппаратных комплексов и систем связи, что являлось крайне необходимым условием качественного обеспечения служебной деятельности.

Разработка системы ИСОД МВД России стала продолжением проекта развития ЕИТКС ведомства.

Разрабатываемая система должна была так же решить проблему отсутствия единого подхода в использовании архитектурных решений и комплексного подхода во внедрении информационных систем в ОВД, использовании банка данных для решения оперативных задач.

В настоящее время деятельность ОВД немыслима без использования современных телекоммуникационных технологий, позволяющих обеспечить оперативный обмен информацией и эффективное взаимодействие различных подразделений МВД России. Именно эти обстоятельства обусловили потребность в создании единой информационно-телекоммуникационной системы ОВД.

Введение в эксплуатацию системы ИСОД МВД России было осуществлено в 2015 году. На тот момент к интегрированной мультисервисной системе было подключено порядка 25 000 автоматизированных рабочих мест. На сегодняшний день насчитывается порядка 350 000 пользователей ИСОД МВД России. На данный момент представлено около 130 программно-технических комплексов системы, которые успешно функционируют, эксплуатируются в повседневной деятельности сотрудников и направлены на повышение эффективности информационного обеспечения в ОВД.

Планово проводятся мероприятия по увеличению мощностей центра обработки данной системы, совершенствованию коммуникационного оборудования и технических средств, реорганизации и повышению пропускной способности каналов связи. В круглосуточном режиме осуществляется техническая поддержка пользователей ИСОД МВД России, что способствует эффективному информационному обмену данными.

Отдельным аспектом является повышение уровня информационной безопасности системы, для чего был разработан комплекс организационно-технических мер по повышению культуры информационной безопасности при работе в системе, в том числе реализована масштабная антивирусная инфраструктура.

Основными структурными компонентами ИСОД МВД России являются: центр обработки данных, интегрированная телекоммуникационная сеть, сервисы обеспечения повседневной служебной деятельности сотрудников ОВД, системы межведомственного взаимодействия и подсистема обеспечения информационной безопасности.

Прикладные сервисы обеспечения деятельности сотрудников ОВД представлены следующим перечнем:

– сервис электронного документооборота;
– сервис электронной почты;
– ведомственный информационно-справочный портал;
– система видео-конференц-связи.

Прикладные сервисы обеспечения оперативно-служебной деятельности подразделений МВД России на сегодняшний день представлены следующим перечнем:

– Следопыт-М – информационно-поисковый сервис;
– СООП – сервис обеспечения охраны общественного порядка;
– СОДЧ – сервис обеспечения деятельности дежурных частей;
– СОМТО – сервис обеспечения деятельности подразделений материально-технического обеспечения МВД;
– ГИБДД-М – федеральная информационная система ГИБДД;
– СОЭБ – сервис обеспечения экономической безопасности;
– СОДИ – сервис НЦБ Интерпола;
– ЕАИС ЭКП – сервис экспертно-криминалистической деятельности;
– СУОГЗ – сервис обеспечения государственной защиты лиц;
– СОПС – сервис оформления проезда сотрудников;
– СОПД ГУСБ – сервис ГУ собственной безопасности МВД;
– МОСТ – сервис статистической отчетности;
– ЦИАДИС – банк отпечатков пальцев.

Из числа подсистем межведомственного взаимодействия и поддержки взаимодействия с населением в том числе выделяют:

– СПГУ – сервис предоставления государственных услуг;
– СЦУО – систему централизованного учета оружия;
– Ретроспективу – единый банк данных архивной информации;
– интегрированный банк данных.

Таким образом, программно-технические комплексы системы ИСОД МВД России являются одним из ключевых компонентов повышения эффективности информационного обеспечения в ОВД и позволяют:

– интегрировать разрозненные информационные ресурсы ОВД в единый банк данных;

– организовать эффективное информационное взаимодействие информационных систем органов внутренних дел;

– обеспечить оперативный и безопасный доступ сотрудников ОВД к интегрированному банку данных, в том числе в режиме удаленного доступа.

В настоящее время в сервисе управления доступом к информационным ресурсам и системам ИСОД МВД России имеется порядка 350 000 учетных записей пользователей, разработано около 40 прикладных сервисов, что является показателем востребованности системы, являющейся ключевым элементом повышения эффективности информационного обеспечения.

§ 3. Анализ программы импортозамещения программного обеспечения

Сбор, обработка, хранение и эффективное использование информации возможно лишь с применением соответствующего требованиям программного обеспечения. Специфика и направления деятельности ОВД требуют ответственного подхода к выбору и выработке правил работы с программным обеспечением. Сложившаяся ситуация, когда все государственные и муниципальные органы были вынуждены закупать и использовать зарубежное программное обеспечение, требовало решительных и оперативных мер государственного реагирования. Ситуация усложнилась санкционной политикой стран-импортеров программного обеспечения (далее – ПО), ставшей угрозой национальной безопасности России. Многие организации, оказавшиеся в зависимости от ненадежной политики зарубежных партнеров, были вынуждены идти на большие издержки для обеспечения функционирования и безопасности информационных систем.

Для реализации Доктрины информационной безопасности Российской Федерации[1], обеспечения государственного суверенитета и безопасности информационной инфраструктуры Российской Федерации, был разработан комплекс мероприятий по стимулированию отечественных разработчиков и формированию базы надежных российских программ – Единый реестр российских программ для электронных вычислительных машин и баз данных (далее – реестр). Реестр создан как реализация статьи 12.1 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [2] в целях расширения использования российских программ для электронных вычислительных машин и баз данных, подтверждения их происхождения из Российской

[1] Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646. – URL: http:// www.pravo.gov.ru (дата обращения: 11.01.2022).

[2] Об информации, информационных технологиях и о защите информации : федеральный закон от 27 июля 2006 г. № 149-ФЗ. – URL: http:// www.pravo.gov.ru (дата обращения: 11.01.2022).

Федерации, а также в целях оказания разработчикам и правообладателям мер государственной поддержки. Реестр формируется на основании решений Экспертного совета по российскому программному обеспечению. Экспертный совет принимает заявления от правообладателей, затем рассматривает эти заявления в соответствии с утвержденным регламентом и принимает решение о включении соответствующего ПО в реестр.

Реализация поставленных задач осуществляется также Указом Президента Российской Федерации от 9 мая 2017 года № 203 « О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы»[1], предписывающим заменить импортное программное обеспечение российскими аналогами, обеспечить технологическую, производственную независимость и информационную безопасность. Стратегия определяет порядок формирования банка безопасного и технологически независимого программного обеспечения, различных сервисов и обосновывает необходимость создания российского системного и прикладного ПО для широкого использования гражданами, субъектами малого, среднего и крупного предпринимательства, государственными органами и органами местного самоуправления и обеспечения использования российских информационных и коммуникационных технологий в органах государственной власти РФ, компаниях с государственным участием, органах местного самоуправления.

В Указе Президента Российской Федерации от 7 мая 2018 года № 204 «О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года»[2] предписано, чтобы в России к 2024 году было осуществлено достижение цели по использованию преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями (п. 11). Кроме того, указ устанавливает, что создание глобальной конкурентоспособной инфраструктуры передачи, обработки и хранения данных, обеспечение информационной безопасности, а также создание сквозных цифровых технологий должно осуществляться преимущественно на основе отечественных разработок (п. 11).

По состоянию на конец февраля 2021 года в реестр включено более 9 000 программ, при этом было подано более 10 000 заявлений. Все ПО в реестре разделено на 22 класса.

---

[1] О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента Российской Федерации от 9 мая 2017 г. № 203. – URL: http:// www.pravo.gov.ru (дата обращения: 11.01.2022).

[2] О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 года : указ Президента Российской Федерации от 7 мая 2018 г. № 204. – URL: http:// www.pravo.gov.ru (дата обращения: 11.01.2022).

Классы ПО в Реестре[1]:

1. BIOS и иное встроенное программное обеспечение.
2. Библиотеки подпрограмм (SDK).
3. Информационные системы для решения специфических отраслевых задач.
4. Лингвистическое программное обеспечение.
5. Операционные системы.
6. Офисные приложения.
7. Поисковые системы.
8. Прикладное программное обеспечение общего назначения.
9. Серверное и связующее программное обеспечение.
10. Системы анализа исходного кода на закладки и уязвимости.
11. Системы мониторинга и управления.
12. Системы сбора, хранения, обработки, анализа, моделирования и визуализации массивов данных.
13. Системы управления базами данных.
14. Системы управления проектами, исследованиями, разработкой, проектированием и внедрением.
15. Системы управления процессами организации.
16. Средства версионного контроля исходного кода.
17. Средства виртуализации и системы хранения данных.
18. Средства обеспечения информационной безопасности.
19. Средства обеспечения облачных и распределенных вычислений.
20. Средства подготовки исполнимого кода.
21. Среды разработки, тестирования и отладки.
22. Утилиты и драйверы.

Правила формирования реестра утверждены постановлением Правительства Российской Федерации от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск иностранного программного обеспечения при закупках для государственных и муниципальных нужд», вводящим с 1 января 2016 года ограничение для государственных заказчиков на закупку ПО, отсутствующего в реестре[2]. Сам сайт реестра начал функционировать в России с начала 2016 года. Распоряжением Правительства Российской Федерации от 26 июля 2016 года № 1588-р «Об утверждении плана перехода органов исполнительной власти и государственных внебюджетных фондов на использование отечественного программного обеспечения» принят план перехода на российское ПО.

---

[1] Единый реестр российских программ для электронных вычислительных машин и баз данных. – URL: https://reestr.digital.gov.ru/reestr/ (дата обращения: 20.01.2022).

[2] Фролов А. Минкомсвязи включило первые приложения в реестр российского программного обеспечения. – URL: https://reestr.digital.gov.ru/reestr/ (дата обращения: 11.01.2022).

К программному обеспечению, допускаемому к включению в реестр, относят программные продукты, удовлетворяющие следующим условиям:

1. Российское юридическое лицо с российским контролем (более 50 %).

2. Исключительные права на составное произведение из:

2.1.Лицензированных компонентов с исходными кодами и правом на модификацию и распространение.

2.2.Заимствованных открытых (open-source) компонентов.

2.3.Собственных разработок.

3. Отчисления зарубежным бенефициарам не более 30 % выручки.

4. Технологическая независимость ПО (суверенитет разработки).

5. Наличие полных исходных кодов в России.

6. Локальная инфраструктура разработки и сборки.

7. Локальные специалисты, исследования и разработка (R&D) и техническая поддержка.

8. Защита информации (суверенитет безопасности).

9. Контроль «закладок», утечек данных, устойчивости к взломам и других уязвимостей.

10. Доработки и сертификация продуктов по требованиям Федеральной службы по техническому и экспортному контролю России (далее – ФСТЭК), Федеральной службы безопасности России (далее – ФСБ) и др.

Регулирование деятельности организаций с критической информационной инфраструктурой (далее – КИИ) также требует внедрения и российского оборудования и элементной базы.

Согласно первому документу владельцы КИИ смогут использовать только ПО, которое включено в реестр российского ПО или единый реестр евразийского ПО, и (или) в единый реестр российской радиоэлектронной продукции (далее – РРП).

Сформированы исключения для следующих категорий ПО:

– отсутствие в российском ПО или в реестре российских программ (далее – РРП) соответствующего класса (типа), являющегося аналогом иностранного ПО, используемого субъектом КИИ;

– отсутствие в реестре сведений о телекоммуникационном оборудовании и радиоэлектронной продукции, являющейся аналогом иностранного оборудования, используемого субъектом КИИ;

– наличие сведений о телекоммуникационном оборудовании и радиоэлектронной продукции в реестре российского ПО, не позволяющей по своим техническим характеристикам достичь определенных законодательством целей и задач субъекта КИИ.

Согласно плану перехода владельцы КИИ должны будут провести аудит своего ПО и оборудования и утвердить план действий до 1 июля 2021 года.

Использование зарубежного ПО необходимо будет согласовать с Министерством цифрового развития, связи и массовых коммуникаций Российской Федерации и Министерством промышленности и торговли Российской Федерации.

Таким образом, переход на отечественное ПО и оборудование обеспечит технологически независимую информационную среду таких стратегически важных объектов, как органы государственной власти, нефтепроводы и газопроводы, атомные электростанции, больницы, воздушный и железнодорожный транспорт, объекты оборонного комплекса.

Если управление этими объектами будет перехвачено извне с помощью недекларированных возможностей зарубежного программного обеспечения, возникнут недопустимые риски. Также, если санкционная политика иностранных производителей приведет к отзыву лицензий на используемое ПО и оборудование, объекты критической информационной инфраструктуры не смогут функционировать, поэтому переход на российскую программно-аппаратную платформу должен быть стремительным.

Несмотря на все инициативы государства по поддержке российских разработчиков и правообладателей ПО, замещение иностранных программных и аппаратно-программных продуктов осуществляется медленнее, чем ожидалось. Тем не менее результаты ощутимы, особенно в области критической информационной инфраструктуры и системного программного обеспечения в правоохранительных органах и оборонной инфраструктуре.

Зависимость крупных заказчиков от программных продуктов западных поставщиков сформировалась исторически в течение десятилетий. Она является сложностью отказа от используемых годами решений, особенно отказа от класса сложных программных комплексов, служащих для автоматизации бизнес-процессов (ERP/HRM). Кроме того, ПО западных производителей поставлялось в виде интегрированных продуктов как законченные «стековые» решения, что само по себе имело конкурентные преимущества. И сегодня предприятия вынуждены искать не просто альтернативную замену требуемой функциональности ПО, но и замену всего комплекта оборудования и программ, начиная от операционной системы и заканчивая офисным ПО. Такие задачи сложны и требуют системного подхода и глубокого анализа всех информационных процессов организации.

Довольно серьезной проблемой было то, что многим компаниям приходилось самостоятельно разрабатывать для себя стратегии импортозамещения.

Комплекс мер по импортозамещению несомненно должен был включать в себя и изменение учебных программ, поскольку весь цикл обучения, начиная от среднего образования и заканчивая высшим профессиональным, был составлен для проприетарного ПО. Это можно объяснить активной маркетинговой политикой: учебные заведения снабжались проприе-

тарными программными продуктами западных корпораций бесплатно либо по сниженной стоимости.

Еще одним ограничением является то, что далеко не все западные продукты можно заменить решениями с открытым кодом или отечественным ПО: на создание многих продуктов были потрачены многие тысячи человеко-лет, и даже на простое копирование функциональности существующих продуктов нужны огромные ресурсы – а значит, нужны масштабные инвестиции: либо через выделение бюджетов потребителям, либо через финансирование производителей.

Тем не менее за прошедшие годы российские прикладные информационные ресурсы и IT-решения существенно нарастили свои возможности и повысили конкурентоспособность. Изменилось и отношение заказчиков к российским разработкам – чувствуя недостаток в отраслевых решениях, они стали все чаще выбирать российских разработчиков для сотрудничества и создания нужных им продуктов. Многие противники импортозамещения перестали искать аргументы против перевода своих IT-инфраструктур на отечественные программные продукты, приступили к формированию корпоративных программ технологической независимости и начали выбирать российские продукты для автоматизации тех или иных процессов.

Тенденция на импортозамещение усиливается с каждым годом, темпы в IT отрасли растут. Процессы импортозамещения привели к тому, что ассортимент IT-продуктов расширился: на рынке теперь есть и западные, и азиатские, и отечественные производители, решения которых можно сравнивать как с точки зрения технологий, так и с точки зрения цены и экономии. Появляется все больше успешных российских IT-решений, отношение к отечественным разработкам улучшается. Заказчики уже в состоянии подбирать комплекты отечественного ПО для оптимального решения типовых задач – и учатся анализировать экономическую эффективность перехода на отечественные продукты[1].

§ 4. Использование отечественного программного обеспечения в органах внутренних дел

Во исполнение п. 3 распоряжения Правительства Российской Федерации о переходе на отечественное программное обеспечение органов муниципальной власти, государственных внебюджетных фондов и исполни-

[1] Морозов И. Импортозамещение в ИТ-отрасли. Взгляд из 2020. – URL: https://www.it-world.ru/cio№ews/busi№ess/153205.html (дата обращения: 12.01.2022).

тельной власти[1], МВД России опубликовало ведомственный приказ[2], утверждающий план-график перехода ОВД на использование отечественного программного обеспечения на 2018 год и на плановый период до 2020 года, согласно которому антивирусы и справочно-правовые системы должны были стать на 100 % российскими уже в 2018 году, а операционные системы и офисные пакеты – на 80 % в 2020 году. Однако, по ряду позиций допускалось изменение индикатора эффективности перехода на использование отечественного офисного программного обеспечения с учетом использования программного обеспечения, требующегося для работы с информационной системой и несовместимого с операционной системой отечественного производства.

Используемое в ОВД программное обеспечение, в случае работы с информацией ограниченного доступа, должно соответствовать руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденному решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года, а также Методическому документу, утвержденному ФСТЭК России 5 февраля 2021 года «Методика оценки угроз безопасности информации», в соответствии с которыми, установлено девять классов защищенности автоматизированных систем от несанкционированного доступа к информации. Каждый класс характеризуется определенной минимальной совокупностью требований по защите. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в автоматизированной системе. В пределах каждой группы соблюдается иерархия требований по защите в зависимости от ценности (конфиденциальности) информации и, следовательно, иерархия классов защищенности автоматизированных систем.

Третья группа включает автоматизированные системы, в которых работает один пользователь, допущенный ко всей информации автоматизированной системы, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает автоматизированные системы, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей ин-

---

[1] Об утверждении плана перехода в 2016–2018 годах федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения : распоряжение Правительства Российской Федерации от 26 июля 2016 г. № 1588-р. – URL: http:// www.pravo.gov.ru (дата обращения: 13.01.2022).

[2] Об утверждении плана-графика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года : приказ МВД России от 10 мая 2018 г. № 284. – URL: http:// www.pravo.gov.ru (дата обращения: 13.01.2022).

формации автоматизированной системы, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса – 2Б и 2А.

Первая группа включает многопользовательские автоматизированные системы, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации автоматизированной системы. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Следует отметить, что классы 3А, 2А, 1А, 1Б и 1В присваиваются автоматизированным системам, обрабатывающим информацию, содержащую сведения, составляющие государственную тайну (секретная – С, совершенно секретная – СС и особой важности – ОВ).

В начале 2020 года МВД России закупило компьютеры на отечественной операционной системе Astra Linux. Данная операционная система прошла необходимые процедуры проверки для работы с информацией ограниченного доступа, в том числе с государственной тайной. Ранее ее уже закупили силовые органы: в ходе нескольких закупок в совокупности 100 000 лицензий приобрело Министерство обороны Российской Федерации и 50 000 лицензий приобрела Федеральная служба войск национальной гвардии Российской Федерации.

ГЛАВА 2. СРАВНЕНИЕ ВНЕДРЯЕМОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ, ВЫЯВЛЕНИЕ ОСОБЕННОСТЕЙ ОТЕЧЕСТВЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ, РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ИСПОЛЬЗОВАНИЮ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

§ 1. Особенности отечественных операционных систем

Операционная система (далее – ОС) – это комплекс взаимосвязанных программ и библиотек, применяемых для управления ресурсами аппаратного обеспечения и организации взаимодействия с пользователем. В логической структуре типичной ЭВМ ОС занимает положение между устройствами с их микроархитектурой, машинным языком и при наличии собственными (встроенными) микропрограммами (драйверами) – с одной стороны – и прикладными программами – с другой.

Большая часть отечественных операционных систем основываются на проектах с открытым исходным кодом. К таким продуктам относятся, к примеру, ОС «Альт» (ранее известная под названием AltLinux), РЕД ОС, «ОСь», а также ROSA и Astra Linux.

«Альт Линукс СПТ» представляет собой унифицированный дистрибутив на базе Linux для серверов, рабочих станций и тонких клиентов со встроенными программными средствами защиты информации, который может быть использован для построения автоматизированных систем по классу 1В включительно и информационных систем персональных данных (ИСПДн) по классу 1К включительно. ОС позволяет одновременно хранить и обрабатывать на одном персональном компьютере или сервере конфиденциальные данные, обеспечивать многопользовательскую работу с разграничением доступа к информации, работать с виртуальными машинами, а также использовать средства централизованной авторизации. Выданный ФСТЭК России сертификат подтверждает соответствие продукта требованиям следующих руководящих документов: «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации» – по 4-му классу защищённости; «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню отсутствия недекларированных возможностей» – по 3-му уровню контроля и технических условий. Техническая поддержка пользователей «Альт Линукс СПТ» осуществляется компанией «Свободные программы и технологии» через партнёра-разработчика «Базальт СПО».

Операционная система «ОСь» представляет собой российский проект по созданию экосистемы программных продуктов на базе дистрибутива Linux, предназначенных для комплексной автоматизации рабочих мест

и IT-инфраструктуры организаций и предприятий, в том числе в дата-центрах, на серверах и клиентских рабочих станциях. Платформа представлена в вариантах «ОСь.Офисная» и «ОСь.Серверная». Они различаются наборами включённого в дистрибутив прикладного ПО. Офисная редакция продукта содержит собственно операционную систему, средства защиты информации, пакет программ для работы с документами, почтовый клиент и браузер. В состав серверной версии включены операционная система, средства защиты информации, инструменты мониторинга и системного управления, сервер электронной почты и СУБД. В числе потенциальных пользователей платформы фигурируют федеральные и региональные органы власти, органы местного самоуправления, компании с государственным участием и государственные корпорации. Предполагается, что экосистема на основе «ОСи» в ближайшем будущем станет полноценной альтернативой западным аналогам[1].

ROSA Linux (раззработчик: ООО «НТЦ ИТ РОСА») представляет собой семейство ОС, который содержит в себе широкий набор решений, предназначенных для домашнего использования (версия ROSA Fresh) и применения в корпоративной среде (ROSA Enterprise Desktop), развёртывания инфраструктурных IT-служб организации (ROSA Enterprise Linux Server), обработки конфиденциальной информации и персональных данных (РОСА «Кобальт»), а также составляющих государственную тайну сведений (РОСА «Хром» и «Никель»). В основу перечисленных продуктов положены наработки Red Hat Enterprise Linux, Mandriva и CentOS с включением большого количества дополнительных компонентов – в том числе оригинальных, созданных программистами научно-технического центра информационных технологий «РОСА». В частности, в составе дистрибутивов ОС для корпоративного сегмента рынка представлены средства виртуализации, ПО для организации резервного копирования, инструменты для построения частных облаков, а также централизованного управления сетевыми ресурсами и системами хранения данных.

ICLinux (разработчик: АО «АйСиЭл-КПО ВС») – сертифицированная и защищённая операционная система, позволяющая обрабатывать информацию в соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных» и реализовывать системы обработки информации ограниченного доступа, не относящейся к государственной тайне. ICLinux включает средства удалённого администрирования, имеет встроенный межсетевой экран, сертифицированный на соответствие РД МЭ по 3-му классу защищённости, поддерживает RDP, X-Windows System, SSH, Telnet, VNC, VPN, NX, ICA и прочие протоколы. Также в активе платфор-

[1] Made in Russia : обзор 20 российских операционных систем. – URL: https://3dnews.ru/958857 (дата обращения: 14.01.2022).

мы значатся совместимость со средствами аутентификации компании «Аладдин Р. Д.» и модульная архитектура, которая позволяет гибко настраивать операционную систему под требования заказчика.

«Эльбрус» (разработчик: АО «МЦСТ») – это программная платформа, разработанная специально для вычислительных комплексов с архитектурой SPARC и «Эльбрус». Особенностью системы является кардинально переработанное ядро Linux, в котором были реализованы особые механизмы управления процессами, виртуальной памятью, прерываниями, сигналами, синхронизацией, поддержка тегированных вычислений. «Нами была проделана фундаментальная работа по преобразованию ОС Linux в операционную систему, поддерживающую режим работы в реальном времени, для чего были реализованы актуальные оптимизации в ядре. В ходе работы в реальном времени можно устанавливать различные режимы обработки внешних прерываний, планирования вычислений, обменов с дисковыми накопителями и некоторые другие», – поясняют в компании «МЦСТ». Помимо этого, в ядро программной платформы «Эльбрус» встроен комплекс средств защиты информации от несанкционированного доступа, который позволяет использовать ОС для построения автоматизированных систем, отвечающих самым высоким требованиям информационной безопасности. Также в составе системы представлены средства архивации, планирования заданий, разработки ПО и прочие инструменты[1].

KasperskyOS – операционная система, разработанная «Лабораторией Касперского», в которой на уровне архитектуры заложены функции кибербезопасности и превентивной защиты от злоумышленников. KasperskyOS не является производной дистрибутива Linux и полностью создана с чистого листа специалистами «Лаборатории Касперского». ОС является оригинальной разработкой компании и зарегистрирована в реестре российского ПО как рекомендованная для приобретения отечественными организациями и государственными структурами. Впервые идея создания абсолютно безопасной операционной системы, способной противостоять любым типам атак, возникла у команды разработчиков «Лаборатории Касперского» 11 ноября 2002 года. Именно эта дата и определила внутреннее название проекта – Project 11.11.

KasperskyOS построена на базе концепции MILS (Multiple Independent Levels of Security – «множественные независимые уровни защиты/безопасности»), определяющей строгие принципы изоляции системных процессов и политик управления информационными потоками. Одним из наиболее важных компонентов ОС является модуль контроля доступа Kaspersky Security System (далее – KSS), отслеживающий все межпроцессорные взаимодействия и исключающий доступ приложений к защищённым областям памяти с критически важными процессами и данными. KSS

[1] Made in Russia. – Указ. соч.

поддерживает широкий набор правил и политик доступа и может быть настроен в соответствии с конкретными требованиями заказчика. Любое действие, не предусмотренное политиками безопасности, запрещено по умолчанию. И это, пожалуй, самое важное отличие Kaspersky OS от популярных сегодня операционных систем, в которых всё, что не запрещено, по умолчанию разрешено (рисунок 1).

В рамках реализации объявленной программы по развитию экосистемы приложений для KasperskyOS и привлечению к проекту заинтересованных партнёров у операционной системы есть шансы получить статус универсальной ОС.

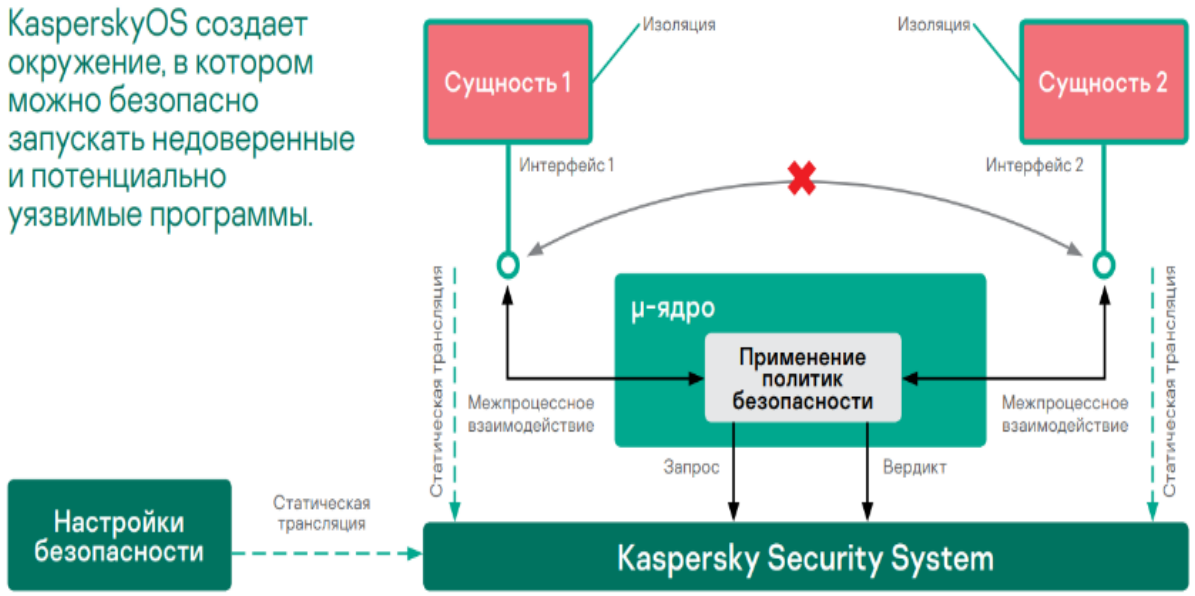

Рисунок 1. Схема работы Kaspersky Security System

ОС Astra Linux предназначена для построения автоматизированных систем в защищенном исполнении, обрабатывающих информацию, содержащую сведения, составляющие государственную тайну с грифом не выше «совершенно секретно». Astra Linux (далее – ОС) предоставляет пользователям широкие возможности в решении задач, связанных с обработкой информации в условиях сохранения государственной тайны. Для этого ОС оснащена защищенной графической оболочкой и, кроме стандартного пакета офисных программ, включает в себя:

– защищенный комплекс программ печати и учета документов;

– защищенную СУБД;

– защищенный комплекс программ гипертекстовой обработки данных;

– защищенный комплекс программ электронной почты.

Стандартная установка ОС включает базовую систему и графический рабочий стол Fly (рисунок 2) с набором административных и пользовательских графических утилит.

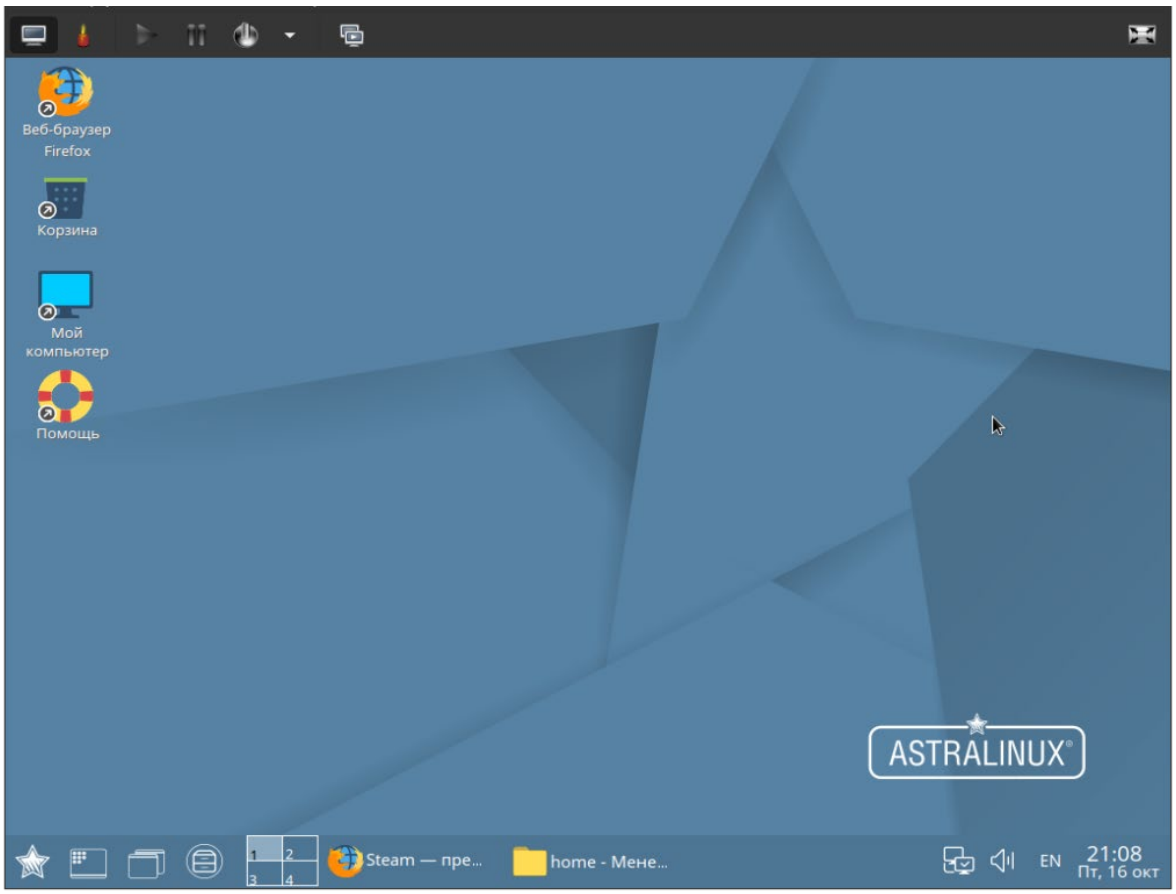

Рисунок 2. Графический рабочий стол Fly

§ 2. Основные характеристики и приемы работы с операционной системой Astra Linux

1. Начало и завершение работы. Графический вход в систему

Графический вход пользователя в систему осуществляется при помощи утилит *fly-dm* (запуск серверной части системы) и *fly-qdm* (поддержка графического интерфейса), переход к которым происходит после окончания работы загрузчика. Утилиты обеспечивают загрузку графической среды для работы пользователя в системе, соединение с удаленным *XDMCP*-сервером, а также завершение работы системы. После установки ОС значения параметров графического входа устанавливаются по умолчанию.

Изменение установленных значений осуществляется с помощью утилиты рабочего стола *fly-admin-dm* («Настройка графического входа») в

режиме администратора. Окно графического входа в систему показано на рисунке 3.

Для входа в систему необходимо в соответствующих полях ввести имя пользователя и пароль. Если для пользователя заданы мандатный уровень и категории, то после ввода пароля отобразится окно выбора соответствующих значений.

Описание утилит *fly-dm*, *fly-qdm* и *fly-admin-dm* можно найти в электронной справке. Вызов электронной справки осуществляется с помощью ярлыка «Помощь», размещенном на первом рабочем столе, или путем нажатия клавиши <F1> в активном окне графической программы.

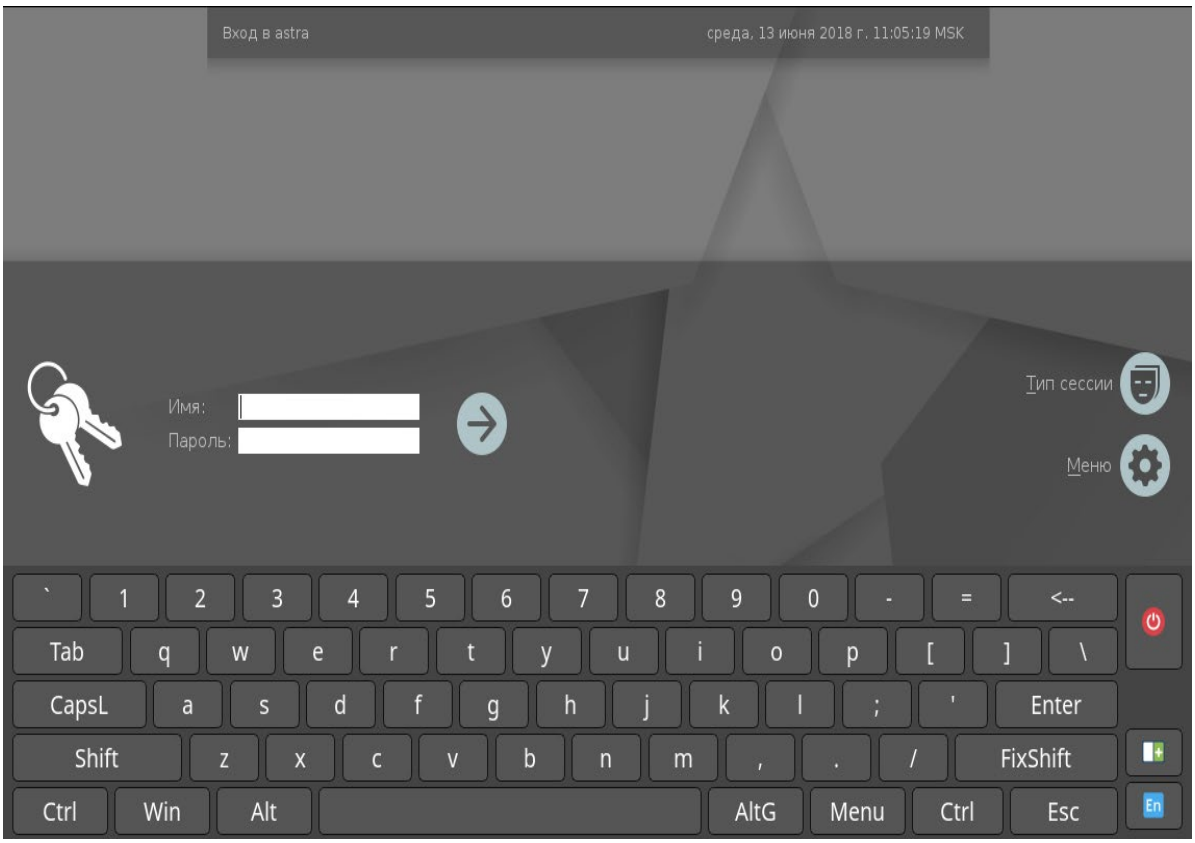

Рисунок 3. Окно входа в систему

2. Завершение работы в графическом режиме

Если рабочий стол Fly запущен, то для завершения работы пользователю следует нажать кнопку меню «Пуск» на панели задач и затем на открывшейся панели меню нажать на кнопку [Завершение работы] (в случае классического меню «Пуск» – выбрать пункт «Завершение работы») либо выполнить в терминале команду: *fly-shutdown-dialog*.

Откроется окно «Выход или выключение» для установки режима завершения работы и выключения, приведенное на рисунке 4.

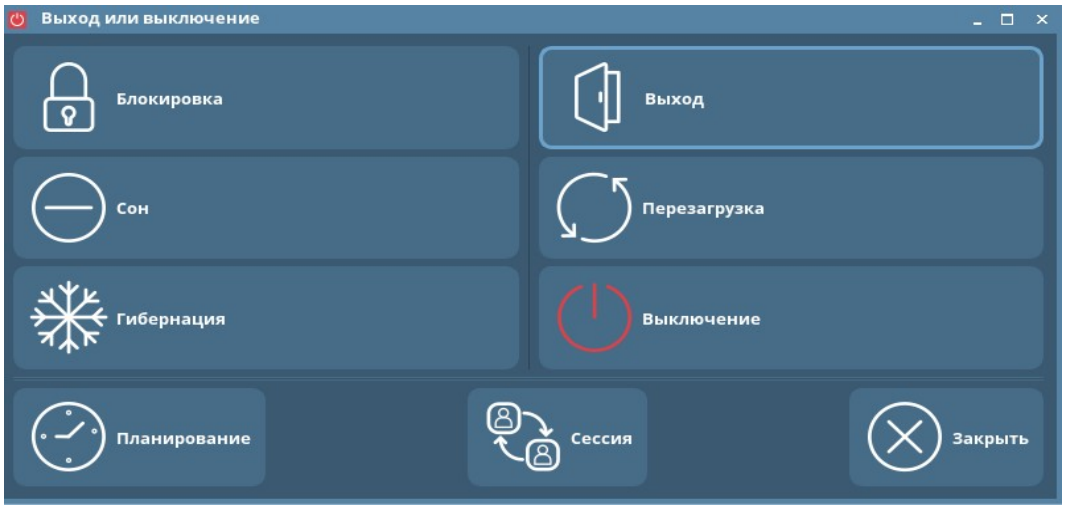

Рисунок 4. Окно для выбора режима завершения работы

Для завершения работы в графическом режиме выбрать один из вариантов:

– [Выход] – завершается пользовательская сессия и выполняется переход в окно графического входа в систему;

– [Перезагрузка] – выполняется перезапуск ОС;

– [Выключение] – выполняется программа выключения компьютера.

Описание установки всех режимов завершения работы и выключения приведено в электронной справке к программе «Менеджер окон» (утилита *fly-wm*).

3. Консольный вход в систему

Переход в консольный (текстовый) режим работы может быть осуществлен из окна графического входа в систему или из графического режима работы.

Для перехода в консольный режим из графического окна входа в систему следует нажать кнопку [Меню] графического окна и в открывшемся меню выбрать пункт «Консольный вход». Появится модальное окно с сообщением о том, что переключение в консольный режим приведет к показу только консольного входа, а графический вход будет показан снова через 10 с после окончания последнего успешного консольного входа или через 40 с, если ни один консольный вход не будет выполнен. Управляющие кнопки окна:

– [Да] – закрыть окно и выполнить переход к виртуальной консоли;

– [Отмена] – закрыть окно и вернуться в окно графического входа в систему.

После перехода к виртуальной консоли на экране монитора появится приглашение командной строки. Для входа в систему следует ввести имя учетной записи пользователя и пароль, а также подтвердить мандатный уровень и категорию пользователя, если они заданы.

Для завершения работы в консольном режиме следует выполнить команду *exit.*

На экране монитора снова отобразится приглашение командной строки. Если после этого не выполнять других операций, то через 10 с будет выполнен переход к графическому окну входа в систему.

Для перехода в консольный режим из графического режима следует нажать на клавиатуре сочетание клавиш <Ctrl+левый Alt+F1> либо <Ctrl+левый Alt+F2> и т. д. до <Ctrl+левый Alt+F6>. Будет выполнен переход к одной из шести виртуальных консолей. Для возврата из консольного режима к графическому нажать <Ctrl+левый Alt+F7>.

4. Рабочий стол Astra Linux: назначение и основные возможности

Защищенная графическая подсистема в составе ОС функционирует с использованием графического сервера Xorg.

В нее также входит рабочий стол Fly, который состоит из программы «Менеджер окон» (утилита fly-wm) и набора пользовательских и административных графических утилит и программ.

Для загрузки рабочего стола ОС необходимо при графическом входе в ОС установить тип сессии «Десктоп».

Рабочий стол также запускается в режимах, оптимизированных для работы на устройствах с сенсорными экранами: в планшетном режиме (тип сессии «Планшетный») и в режиме для мобильных устройств (тип сессии «Мобильный»).

По умолчанию для входа в систему установлен тип сессии, с которым осуществлялся вход последний раз.

В графическую подсистему встроена мандатная защита. В области уведомлений (системном трее) панели задач располагается индикатор мандатного уровня и мандатной категории, на котором в числовой форме и в виде цвета фона сообщается о величине уровня:

1. «Уровень 0» – голубой;
2. «Уровень 1» – желтый;
3. «Уровень 2» – оранжевый;
4. «Уровень 3» – темно-розовый;
5. «Уровень 4» – красный;
6. «Уровень 5» – коричневый;
7. «Уровень 6» – пурпурный;
8. «Уровень 7» – темно-фиолетовый.

Любое окно вновь запущенного приложения будет снабжено цветной рамкой, цвет которой будет совпадать с цветом индикатора.

При работе на разных мандатных уровнях и категориях пользователю следует учитывать, что ОС формально рассматривает одного и того же пользователя, но с различными мандатными уровнями как разных пользо-

вателей и создает для них отдельные домашние каталоги, одновременный прямой доступ пользователя к которым не допускается.

Рабочий стол Fly предоставляет пользователю:

– графический вход, позволяющий входить в локальную или удаленную систему и запускать графические приложения на заданных мандатных уровнях;

– рабочий стол для размещения элементов графического интерфейса;

– значки на рабочем столе, представляющие как файлы и/или каталоги, так и ярлыки для программ, устройств, ссылок на файлы, каталоги и/или адреса в сети;

– панель задач, содержащую: кнопку меню «Пуск», панель быстрого запуска с кнопками управления окнами приложений, переключатель рабочих столов, панель переключения задач и область уведомлений со значками программ, использующих системные разделы;

– меню приложений (в виде меню – панели или классическое меню), доступное через кнопку меню «Пуск» на панели задач;

– интегрированный менеджер рабочих столов, позволяющий размещать окна приложений в пространстве, превышающем размер видимой области экрана, оперативно управлять окнами приложений и навигацией рабочих столов, а также настраивать конфигурацию рабочих столов;

– механизм прямого переноса данных из меню «Пуск» на рабочий стол и на панель быстрого запуска, а также с рабочего стола на панель быстрого запуска;

– индикатор мандатного уровня (секретности) и мандатной категории;

– стандартное оформление окон приложений, дополненное цветовой индикацией мандатных уровней, и стандартные способы манипулирования окнами;

– высокую гибкость в настройке как внешнего вида, так и процесса функционирования рабочего стола, значков и окон приложений, панелей и их реквизитов;

– «горячие» клавиши, назначаемые и редактируемые с помощью специальной графической утилиты;

– средства для редактирования меню, доступного через кнопку меню «Пуск», и панели быстрого запуска, а также для создания ярлыков и коллекций ярлыков;

– набор утилит для администрирования как системы в целом, так и самого рабочего стола, в том числе для поддержки механизма мандатного управления доступом;

– набор приложений для повседневного использования (менеджер файлов, текстовый редактор и т. п.);

– переключение в планшетный режим.

Описание всех графических утилит и программ рабочего стола Fly, а также полное описание его режимов работы и предоставляемых возможностей также приведено в электронной справке.

5. Панель управления

Программа «Панель управления» (утилита fly-admin-center) позволяет централизовано использовать некоторые административные и пользовательские утилиты рабочего стола Fly, которые для удобства разделены на несколько категорий (рисунок 5).

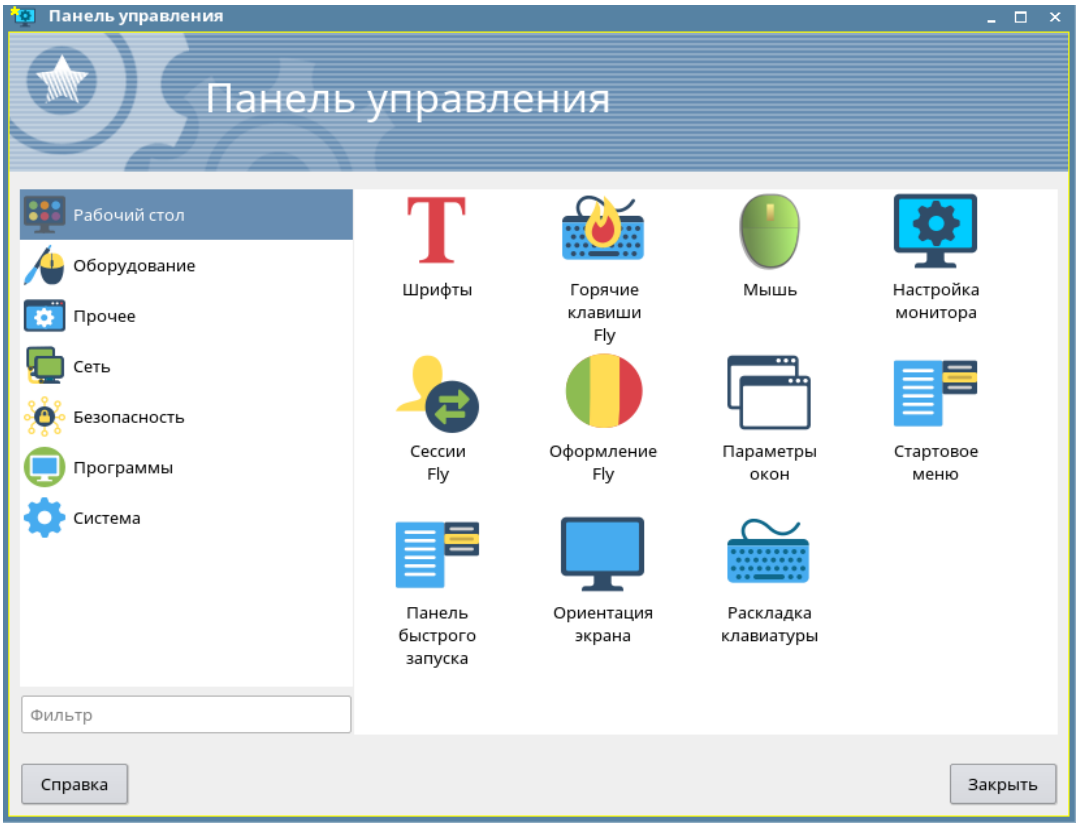

Рисунок 5. Панель управления

6. Настройка рабочего стола пользователя

Каждый пользователь в системе имеет возможность выполнить индивидуальные настройки своего рабочего стола (внешний вид, расположение элементов, особенности работы с клавиатурой и мышью). Однако часть настроек жестко задана администратором и недоступна обычному пользователю. Некоторые из возможностей настройки могут быть реализованы при использовании утилит настройки из меню «Пуск – Настройки – Панель управления» или непосредственно из меню «Пуск – Настройки».

Категория «Рабочий стол» программы «Панель управления» объединяет графические утилиты, которые могут быть применены для индивидуальной настройки рабочего стола. Перечень утилит, доступных пользова-

телю, приведен в таблице 1, описание утилит приведено в электронной справке.

Таблица 1. Утилиты для настройки рабочего стола

Утилита	Описание
fly-admin-fonts «Шрифты»	Просмотр и импорт системных шрифтов
fly-admin-hotkeys «Горячие клавиши Fly»	Запуск редактора горячих клавиш для настройки соответствия между сочетаниями клавиш и действиями
fly-admin-mouse «Мышь»	Настройка кнопок мыши и скорости перемещения курсора
fly-admin-screen «Настройка монитора»	Настройка размера изображения, разрешения, частоты обновления и других параметров монитора
fly-admin-session «Сессии Fly»	Настройки для сессий рабочего стола
fly-admin-theme «Оформление Fly»	Настройка обоев, тем, шрифтов, экрана блокировки и других элементов рабочего стола
fly-admin-winprops «Параметры окон»	Настройка поведения и внешнего вида окон рабочего стола
fly-menuedit «Стартовое меню»	Настройка структуры меню «Пуск»
fly-menuedit «Панель быстрого запуска»	Добавление и удаление программ из панели запуска

Доступ к графическим программа и утилитам осуществляется из меню «Пуск». Программы сгруппированы по категориям в соответствии с их назначением.

7. Программа «Менеджер файлов»

Программа «Менеджер файлов» (утилита fly-fm) предназначена для просмотра папок рабочего стола и элементов файловой системы (далее – ФС) и выполнения основных функций управления файлами. Позволяет подключать и отключать ФС носителей доступных устройств хранения данных, таких как локальные жесткие диски и их разделы, компакт- и DVD-диски, USB-накопители. Также позволяет обращаться к сетевым Samba-ресурсам, работать с архивами и выполнять кодирующее/раскодирующее преобразование. Главное окно программы приведено на рисунке 6.

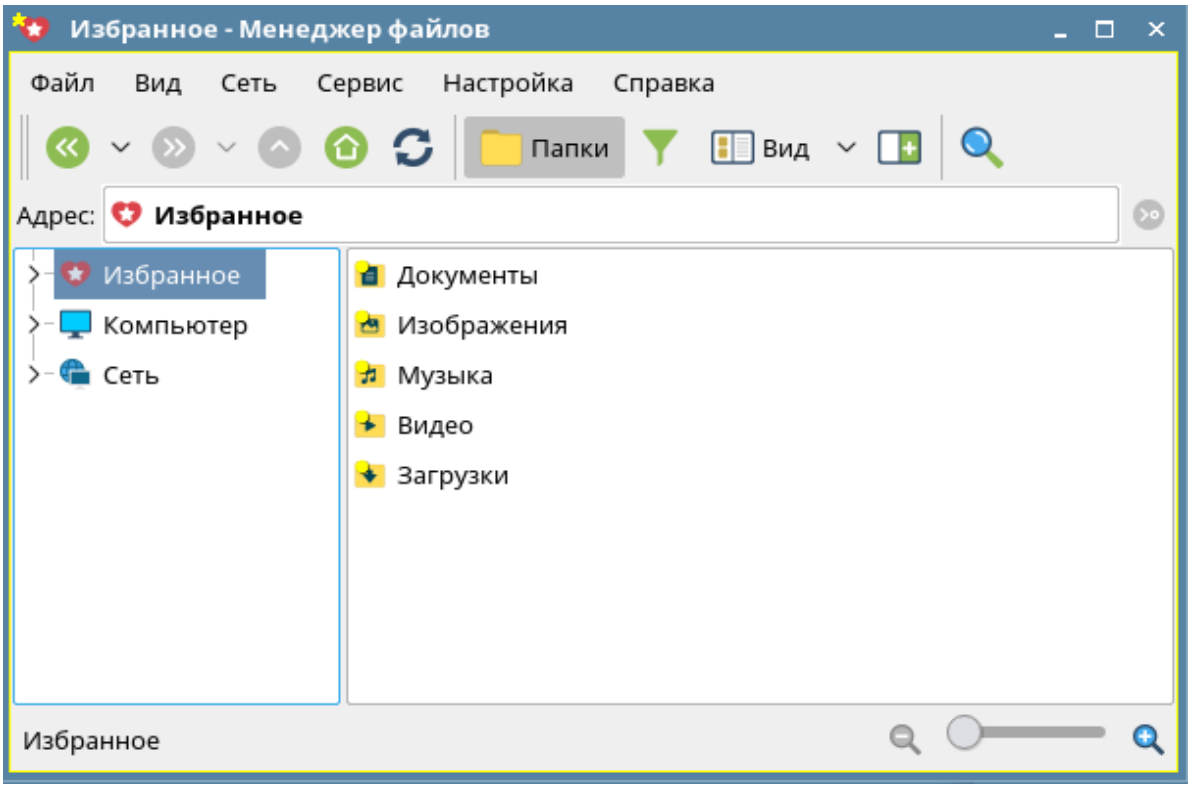

Рисунок 6. Менеджер файлов

В планшетном режиме программа по умолчанию запускается с установленными настройками, оптимизированными для работы на устройствах с сенсорными экранами. В частности, на панели просмотра слева от имени элемента отображаются значки для переключения флага выполнения групповых операций, при котором отображение графических элементов видоизменяется.

8. Раздел «Настройки»

Перечень утилит раздела «Настройки», доступных пользователю, приведен в таблице 2.

Таблица 2

Утилита	Описание
fly-admin-autostart «Автостарт»	Установки приложений, запускаемых автоматически при загрузке рабочего стола
fly-admin-hotkeys «Горячие клавиши Fly»	Запуск редактора горячих клавиш для настройки соответствия между сочетаниями клавиш и действиями
fly-admin-date «Дата и время»	Просмотр установленного времени, даты, часового пояса, календаря, изменение формата отображения времени на системных часах, даты и времени на всплывающем сообщении при наведении курсора мыши на системные часы в области уведомлений на панели задач

systemdgenie «Инициализация системы»	Графическая утилита управления службой Systemd
fly-admin-mouse «Мышь»	Настройка кнопок мыши и скорости перемещения курсора
«Настройка межсетевого экрана»	Графическая утилита Gufw настройки межсетевого экрана UFW (Uncomplicated Firewall). Подробная информация о программе доступна непосредственно из графической утилиты
fly-admin-screen «Настройка монитора»	Настройка размера изображения, разрешения, частоты обновления и других параметров монитора
fly-brightness «Настройка яркости Fly»	Программа для настройки яркости в планшетном режиме
fly-admin-reflex «Обработка «горячего» подключе-	Настройка реакций при подключении устройств в процессе работы
fly-orientation «Ориентация экра-	Настройка ориентации экрана
fly-admin-theme «Оформление Fly»	Настройка обоев, тем, шрифтов, экрана блокировки и других элементов рабочего стола
fly-menuedit «Панель быстрого запуска»	Добавление и удаление программ из панели быстрого запуска
fly-admin-center «Панель управле-	Централизованный доступ к графическим утилитам настройки и администрирования системы
fly-admin-winprops «Параметры окон»	Настройка поведения и внешнего вида окон рабочего стола
fly-admin-env «Переменные окружения»	Добавление, изменение и удаление переменных окружения
fly-mimeapps «Приложения для типов файлов»	Просмотр доступных приложений и установка приложения по умолчанию для типов файлов, установка команды для запуска обозревателя и для создания вложений почтового клиента. П р и м е ч а н и е . Утилита запускается только с аргументом -d

9. Раздел «Системные»

Системные утилиты, доступные пользователю, приведены в таблице 3.

Таблица 3

Утилита	Описание
fly-shutdown-dialog «Завершение работы»	Завершение работы пользователя в графическом режиме
fly-run «Запуск приложения»	Запуск программы или осуществление доступа к ресурсу из командной строки
kinfocenter «Информация о системе»	Централизованный просмотр сведений о системе и об устройствах
fly-admin-device-manager «Менеджер устройств»	Получение информации об устройствах, доступных в системе, а также для настройки некоторых из них
fly-fm «Менеджер файлов»	Просмотр папок рабочего стола и элементов ФС, выполнение основных функций управления файлами, подключение и отключение ФС-носителей доступных устройств хранения данных, обращение к сетевым Samba-ресурсам, работа с архивами, выполнение кодирующего/раскодирующего преобразования
Qbat «Монитор батарей QBat»	Программа QBat для мониторинга батарей электропитания
fly-print-monitor «Монитор печати»	Обзор и управление системой печати из области уведомлений на панели задач
fly-find «Поиск файлов»	Поиск файлов и каталогов
fly-admin-marker «Редактор	Настройка маркировки печати сопроводительной надписи документов
ksysguard «Системный монитор»	Отслеживание системных параметров

Также пользователю доступна графическая утилита «HPLIP Toolbox» для запуска программы управления системой печати принтеров HP.

Перед установкой новой версии HPLIP необходимо удалить предыдущую версию, выполнив следующую команду:
sudo apt purge hplip hplip-gui –y и *sudo apt autoremove –f.*

10. Раздел «Утилиты»

Утилиты рабочего стола, доступные пользователю, приведены в таблице 4.

Таблица 4

Утилита	Описание
Fly-vkbd «Виртуальная клавиатура»	Ввод символов и знаков в приложение так же, как с помощью обычной клавиатуры – щелчками кнопки мыши на клавишах клавиатуры, отображаемой на рабочем столе
ark «Работа с архивами Ark»	Программа для работы с архивами файлов
kgpg «KGpg»	Программа управления ключами GPG

Также пользователю доступны графические утилиты:

«Recoll» – программа полнотекстового контекстного поиска по словам или логическим критериям;

«XCA» – графический инструмент управления сертификатами XCA.

11. Раздел «Научные»

Из научных утилит пользователю доступен «Калькулятор Speedcrunch» – калькулятор для выполнения сложных математических операций над числами с сохранением и использованием результата операций.

12. Раздел «Мультимедиа»

Мультимедийные утилиты, доступные пользователю, приведены в таблице 5.

Таблица 5

Утилита	Описание
fly-videocamera «Видеокамера»	Подключение и настройка видеокамеры, запись снимка и видеоизображения в файл, настройка просмотра показаний датчика движения
k3b «Запись дисков	Программа для записи образов и данных на CD- и DVD-диски
fly-camera «Камера»	Программа для работы с фотокамерой
Pavucontrol «Регулятор громко-	Регулирование уровня громкости
kmix «KMix»	Программа управления громкостью звуковых устройств

13. Раздел «Офис»

Большая часть работы, осуществляемая в ОВД, производится в офисных пакетах. Достойной заменой проприетарному пакету MS Office является кроссплатформенный, свободно распространяемый офисный пакет с открытым исходным кодом – офисный пакет Libreoffice.

Libreoffice содержит инструменты для решения офисных задач, например, таких как написание текстов, работа с электронными таблицами, создание графических объектов и презентаций.

Libreoffice предназначен для обработки следующих видов документов:

1) тексты с профессиональной разметкой, включающей встроенные объекты, формы, развитую систему ссылок, сносок, правок и т. п.;

2) электронные таблицы, в том числе сопряженные с БД и автоматизацией на языках Basic, Java, Pytho№, C/C++;

3) презентации с возможностью экспорта в форматы PDF, SWF, HTML;

4) деловая графика с возможностью импорта и экспорта графики во все популярные векторные (SVG, WMF, EMF и т. д.) и растровые (BMP, P№G, TIFF, GIF, JPEG и т. д.) форматы хранения изображений;

5) математические формулы с языком описания, диаграммы и БД.

Libreoffice состоит из шести компонентов:

5.1) текст Libreoffice – текстовый редактор и редактор web-страниц Writer;

5.2) таблица Libreoffice – редактор электронных таблиц Calc;

5.3) презентация Libreoffice – средство создания и демонстрации презентации Impress;

5.4) рисунок Libreoffice – векторный редактор Draw;

5.5) база данных Libreoffice – система управления базами данных Base;

5.6) математика Libreoffice – редактор Math для создания и редактирования математических формул.

Таким образом, все наиболее применяемые программы из состава пакета MS Office имеют аналогичные по функционалу программы в Libreoffice.

Первое и самое главное отличие MS Office и Libreoffice в архитектуре программ. Если MS – набор отдельных программ, то Libreoffice – единый организм с несколькими интерфейсами управления. При этом установленный Libreoffice занимает в 2-3 раза меньше места на жестком диске.

Существенное повышение эффективности работы в Libreoffice позволяет использование горячих клавиш:

– Ctrl+Q – выход;
– Ctrl+W – закрыть текущий документ;
– Ctrl+E – выровнять текст по центру;
– Ctrl+Shift+E – запись изменений в документе;
– Ctrl+R – выровнять текст по правому краю;
– Ctrl+Shift+R – показать/скрыть линейку;
– Ctrl+Y – вернуть отмененное действие;
– Ctrl+Shift-Y – повторить последнее действие (или продублировать введенное слово);
– Ctrl+U – подчеркивание;
– Ctrl+I – курсив;
– Ctrl+O – открыть файл;
– Ctrl+Shift+O – просмотр печати;
– Ctrl+P – печать документа;
– Ctrl+Shift+P – верхний индекс;
– Ctrl+A – выделить весь текст;
– Ctrl+S – сохранить;
– Ctrl+D – двойное подчеркивание;
– Ctrl+Shift+S – сохранить как;
– Ctrl+F – поиск;
– Ctrl+H – замена;
– Ctrl+J – выравнивание по ширине;
– Ctrl+Shift+J – полноэкранный режим;
– Ctrl+K – вставка гиперссылки;
– Ctrl+L – выравнивание по левому краю;
– Ctrl+Z – отменить действие;
– Ctrl+X – вырезать;
– Ctrl+C – копировать;
– Ctrl+Shift+C – вставить как;
– Ctrl+Alt+C – вставить примечание/комментарий;
– Ctrl+V – вставить;
– Ctrl+Shift+V – вставить как;
– Ctrl+Shift+Alt+V – вставить неформатированный текст;
– Ctrl+B – полужирный шрифт;
– Ctrl+Shift+B – нижний индекс;
– Ctrl+№ – новый документ;
– Ctrl+M – отмена форматирования;
– Ctrl+[0–5] – стили текста;
– Alt+Shift+F8 – режим блочного/обычного выделения;
– Ctrl+F3 – редактор автотекста;
– Shift+F3 – переключение регистра текста (заглавные/прописные);
– F4 – источники данных;
– F5 – навигатор документа;
– F7 – правописание;
– F11 – выбор стилей;
– F12 – нумерованный список;
– Ctrl+F12 – вставить таблицу.

Для вычисления непосредственно в документе и в таблицах достаточно нажать клавишу F2 и ввести выражение для вычисления, и после нажатия «Enter» результат будет отображен. Двойной клик на результате применяется для изменения формулы.

В таблице – в ячейке после набора «=» таблица будет работать в режиме считающей ячейки, и появится возможность набора формул. Редактирование осуществляется также по нажатию клавиши F2.

Сохранение осуществляется в форматах Jpeg/PNG/PDF/MediaWiki через меню «Экспорт» (бывает полезно при склейке сканов).

Открытие файла можно производить независимо от формата. Через меню «Открыть» можно открывать любой поддерживаемый файл, т. е. из Writer(Word) можно открыть файл Calc(Excel), и он нормально откроется в Calc.

Возможно открытие и редактирование файлов формата PDF (схема работы такая же, как и с обычным текстовым файлом).

В Libreoffice содержится «Меню оперативного редактирования таблиц». Окно с оперативными функциями по работе с таблицами (вставка/удаление/выделение ячеек/строк/столбцов) отображается, пока курсор находится в таблице.

Возможна массовая вставка строк и столбцов в таблицу через меню правой кнопки мыши (строка/столбец – вставить).

Допускается смена регистра через меню правой кнопки мыши и при комбинации клавиш Shift+F3.

Кнопка I№sert переключает режимы редактирования текста «Добавление»/«Замена». Эта функция также содержится в MS Office.

Замену абзацев местами можно произвести комбинацией клавиш Ctrl+Alt+Вверх.

Таким образом, можно сделать вывод, что пакет Libreoffice, свободно распространяемый с открытым исходным кодом, представляет собой практически полноценную замену проприетарному MS Office. Трудности перехода на данное ПО могут вызвать небольшие различия в интерфейсе программ и различная реализация одних и тех же функций.

§ 3. Взаимодействие пользователя со средствами защиты информации

1. Возможности, предоставляемые пользователю

В соответствии с моделью управления доступом обычный пользователь может выполнять следующие действия, связанные с работой со средствами защиты информации (СЗИ) ОС:

– устанавливать мандатные атрибуты (уровень и категории) при создании новой сессии;

– получать информацию об установленных для текущей сессии мандатных атрибутах;

– изменять свой пароль для входа в систему с помощью команды passwd;

– изменять группу собственного файла или каталога с помощью утилиты *fly-fm*;

– изменять дискреционные права доступа к собственному файлу или каталогу (утилита *fly-fm*);

– задавать дискреционные права доступа при создании файла или каталога (утилита *fly-fm*).

2. Мандатное управление доступом

После того как пользователь, для которого установлены возможные мандатные уровни и категории, отличные от нуля, войдет в систему, ему будет предложено установить конкретный мандатный уровень и конкретную категорию для данной сессии в пределах разрешенных диапазонов. Выбранные значения этих параметров можно будет проверить с помощью цветного индикатора с числом внутри, расположенного в области уведомлений (правый нижний угол экрана). Для получения информационного сообщения следует навести курсор на индикатор (рисунок 7).

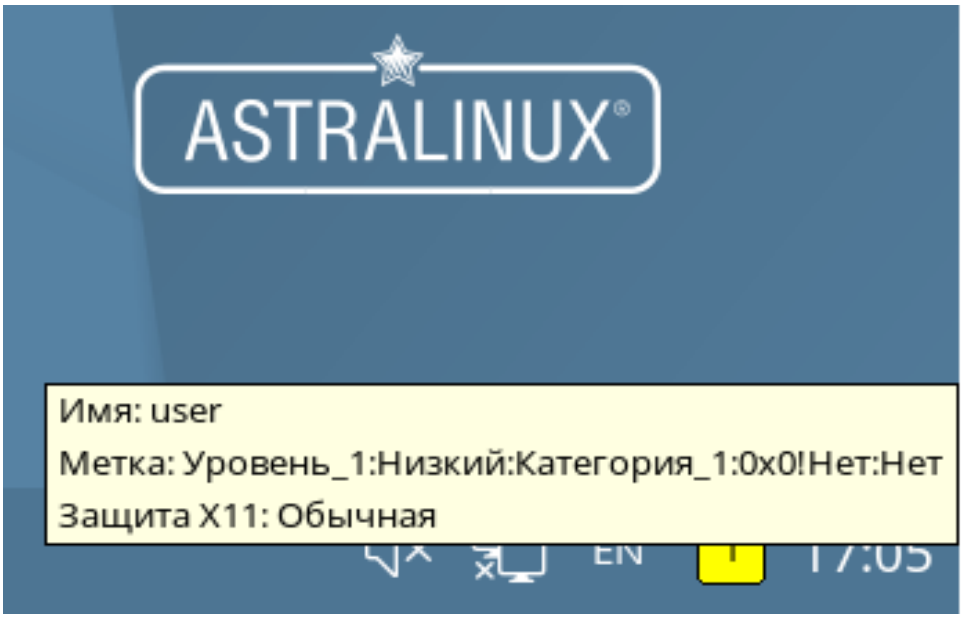

Рисунок 7. Информация об уровне мандатного доступа

Также для просмотра своих мандатных атрибутов пользователь может воспользоваться консольной утилитой *pdp-id*.

Создаваемые пользователем в контексте текущей сессии объекты (например, файлы и каталоги) будут наследовать мандатные атрибуты текущей сессии. Непривилегированному пользователю не предоставляются права на изменение мандатных атрибутов объектов доступа.

3. Команда who

Команда who идентифицирует обратившегося к ней пользователя.

Задавая различные опции, с помощью команды who можно получить информацию о времени начала и конца сеансов и перезагрузок, корректировках системных часов, а также о других процессах, порожденных процессом init.

Команду who можно использовать без каких-либо опций или аргументов. В таком случае отобразится набор данных по умолчанию об учетных записях подключенных пользователей – имя пользователя, название пользовательского терминала, время подключения.

Также можно прописывать команду в виде who am i – тогда она будет идентифицировать конкретно того пользователя, который работает сейчас в терминале (аналогично опции -m).

Используя различные опции, можно получать именно ту информацию, которая нужна здесь и сейчас:

1) -a (--all) – включает в себя все основные опции;
2) - b (--boot) – показывает время загрузки операционной системы;
3) -d (--dead) – выводит перечень зомби-процессов;
4) - H (--heading) – никак не влияет на получаемую информацию, зато добавляет колонкам заголовки и помогает понять, что где находится;
5) -m – показывает пользователя, который сейчас работает в терминале;
6) -r – выводит текущий уровень запуска (runinit);
7) -t – показывает последнее изменение системных часов;
8) -s – выводит только имя, терминальную сессию и время.
9) -q – выводит количество авторизованных пользователей;
10) -T – сообщает данные о терминальной сессии;
11) -u – показывает активных пользователей;
12) --ips – вместо названия хостов показывает ips;
13) --lookup – используется в сочетании с --ips, выводит данные, которые основываются на сохраненном IP, если он доступен, а не на названии хоста.

§ 4. Защищенная система управления базами данных (СУБД)

Входящий в состав системы управления базами данных (далее – СУБД) PostgreSQL набор программных средств можно разделить на следующие классы:

– управление базами данных (далее – БД);
– выполнение запросов пользователя;
– оптимизация производительности;
– обеспечение средств копирования и восстановления.

Работа с СУБД требует установки соединения с сервером БД, что при использовании клиентских утилит командной строки обеспечивается заданием свойств соединения с помощью аргументов (опций) командной строки, приведенных в таблице 6.

Корректная работа с СУБД предполагает использование механизма единого пространства пользователей (далее – ЕПП), что подразумевает использование в качестве пользователей СУБД пользователей домена ЕПП.

Создание кластера выполняется администратором на сервере с помощью утилиты *initdb*.

Таблица 6

Аргумент	Описание
-h, --host=HOSTNAME	Указывает имя сервера БД или каталог сокетов UNIX, если начинается с символа «/»
-p, --port=PORT	Указывает порт сервера БД или расширение имени сокета UNIX, по которым сервер принимает соединения
-U, --username=USERNAME	Указывает имя пользователя для установки соединения
-w, --no-password	Подавление запроса пароля пользователя. В случае, когда установка соединения с сервером требует ввода пароля, а пароль недоступен, например из файла .pgpass, попытка установки соединения завершается ошибкой. Опция полезна при выполнении пакетов заданий или скриптов, в процессе обработки которых отсутствует пользователь, который может вводить пароль
-W,--password	Принудительный запрос пароля при установке соединения. Опция не является существенной, так как утилита по умолчанию всегда запрашивает пароль в случае, когда сервер требует ввода пароля при установке соединения. В то же время для определения необходимости ввода пароля утилита делает дополнительный запрос к серверу, которого можно избежать, указав эту опцию

При отсутствии перечисленных аргументов используются переменные окружения (PGDATABASE, PGHOST, PGPORT, PGUSER), определяющие параметры соединения по умолчанию. Информацию о версии и способе вызова утилит и допустимых аргументов можно получить с помощью аргументов: --help – показать справку по вызову команды; --version – показать версию.

1. Управление базами данных

Под управлением БД подразумевается непосредственно создание и удаление БД, управление пользователями и процедурными языками. Как правило, указанные действия должны выполняться администратором.

Создание кластера БД состоит из создания каталогов для хранения данных БД, создания разделяемых таблиц системного каталога (таблиц, относящихся ко всему кластеру БД, а не к конкретной БД) и создания БД template1 и postgres. При создании в дальнейшем новых БД в них копируется содержимое БД template1. Таким образом, все, что установлено в БД template1, автоматически будет скопировано в каждую создаваемую в дальнейшем БД. БД postgres является БД по умолчанию для использования пользователями, утилитами и сторонними приложениями.

Создание кластера выполняется администратором на сервере с помощью утилиты *initdb*.

2. Создание и удаление баз данных

Для создания новой БД используется утилита *createdb*, а для удаления – утилита *dropdb*.

По умолчанию владельцем новой БД становится пользователь, выполняющий команду. В то же время в качестве владельца новой БД может быть указан другой пользователь с помощью опции *-O*, если выполняющий команду пользователь обладает соответствующими привилегиями. При этом удаление может выполнить только суперпользователь или владелец БД.

Обобщенный способ вызова заключается в передаче опций и имени БД. При этом используются правила установки соединения, рассмотренные выше.

Синтаксис: *createdb* [ОПЦИИ]... [БАЗА_ДАННЫХ] [ОПИСАНИЕ] *dropdb* [ОПЦИИ]... [БАЗА_ДАННЫХ].

3. Управление пользователями

В СУБД PostgreSQL для управления правами на доступ к БД используется концепция ролей. Под ролью в зависимости от её параметров понимается пользователь или группа пользователей БД. Роли могут являться владельцами объектов БД (например, таблиц) и могут назначать привилегии на управление объектами для других ролей, имеющих доступ к данным объектам. Кроме того, существует возможность предоставления членства в роли для другой роли, что позволяет членам роли использовать привилегии, назначенные роли, членами которой они являются. Таким образом, концепция ролей объединяет концепции «пользователи» и «группы».

Корректная работа с СУБД предполагает использование механизма ЕПП, что подразумевает использование в качестве пользователей СУБД пользователей домена ЕПП.

Для создания нового пользователя или роли используется утилита *createuser*, для удаления – *dropuser*. Только суперпользователи и пользователи с привилегией *CREATEROLE* могут создавать и удалять пользователей и роли. Удалять суперпользователей может только суперпользователь.

Синтаксис: *createuser* [ОПЦИИ]... [РОЛЬ] *dropuser* [ОПЦИИ]... [РОЛЬ]. При вызове используются правила установки соединения (см. таблицу 6).

4. Использование процедурных языков

СУБД PostgreSQL предоставляет пользователям возможность создавать хранимые процедуры (функции) и триггеры для обработки данных, хранящихся в БД. Для этого могут использоваться следующие процедурные языки: PL/Perl, PL/pgSQL, PL/Python и PL/Tcl.

Для возможности использования конкретного процедурного языка его необходимо установить в конкретную БД. Для установки поддержки процедурного языка в БД используется утилита *createla№g*, для удаления поддержки языка из БД – *droplang*.

Синтаксис: createlang [ОПЦИИ]... ЯЗЫК [БАЗА_ДАННЫХ] droplang [ОПЦИИ]... ЯЗЫК [БАЗА_ДАННЫХ].

Несмотря на то, что поддержка процедурного языка может быть выполнена непосредственно некоторыми SQL-командами (например, DROP LANGUAGE), рекомендуется использовать данные утилиты, поскольку они осуществляют необходимые проверки.

5. Выполнение запросов

Взаимодействие пользователя с СУБД в основном осуществляется с помощью прикладного ПО, созданного для решения конкретных прикладных задач.

В то же время в состав СУБД входят средства интерактивного взаимодействия с пользователем. Для этого предлагается консольная утилита psql (интерактивный терминал) и утилита администрирования с визуальным пользовательским интерфейсом pgadmin3.

Интерактивный терминал. Утилита psql является интерактивным клиентом PostgreSQL и позволяет интерактивно набирать запросы, отправлять их серверу и получать результаты. Так же ввод может осуществляться из файла. В дополнение утилита поддерживает метакоманды и некоторые возможности командной оболочки для облегчения создания скриптов и автоматизации широкого круга задач.

Синтаксис: psql [ОПЦИИ]... [БАЗА_ДАННЫХ [ПОЛЬЗОВАТЕЛЬ]].

Утилита psql является клиентским приложением PostgreSQL. Для установки соединения требуется указание БД, имени и номера порта сервера и имени пользователя, под которым устанавливается соединение. Существует возможность указать эти параметры с помощью аргументов командной строки -d, -h, -p и -U соответственно (см. таблицу 7). Если аргумент не соответствует ни одной из опций, он воспринимается как имя БД (или имя пользователя, если имя БД уже было получено).

Если значения по умолчанию неверны, существует возможность их переопределения установкой переменных окружения PGDATABASE, PGHOST, PGPORT и/или PGUSER в соответствующие значения. Также

удобно использовать файл ~/.pgpass для устранения необходимости регулярного ввода пароля.

Альтернативным путем задания параметров соединения является строка соединения, используемая вместо имени БД. Этот механизм предоставляет широкие возможности по управлению установкой соединения. Например: *$ psql "service=myservice sslmode=require".*

При невозможности установки соединения в силу тех или иных причин (например, недостаток прав доступа, сервер не запущен и т. п.) утилита psql возвращает ошибку и завершает работу.

При нормальном функционировании psql выводит приглашение с именем БД, с которой в настоящее время установлено соединение, за которым следует =>. Например*: $ psql testdb psql (x.x.0)* testdb=>.

После приглашения пользователь имеет возможность ввода SQL-команд. Обычно введенный запрос отсылается серверу после ввода завершающего символа «;». Перевод строки не завершает команду. Таким образом, команда может быть записана в несколько строк для лучшего восприятия. Если команда была отослана серверу и выполнена без ошибок, на экран выводится результат ее выполнения.

В случае ввода строки, начинающейся с не заключенного в кавычки символа «\», она воспринимается как метакоманда и обрабатывается непосредственно утилитой psql. Подобные команды делают утилиту более удобной для администрирования и создания скриптов.

ЗАКЛЮЧЕНИЕ

Процесс замещения импортного программного обеспечения является вынужденной и необходимой мерой, от которой зависит суверенитет и безопасность государства. Несмотря на запоздалые меры, была выработана эффективная программа поддержки отечественных производителей ПО и меры, обязывающие государственные и муниципальные структуры использовать российское ПО. Начиная со времени начала реализации программы импортозамещения проделана огромная работа, сформирован реестр российских программ, насчитывающий на начало 2021 года почти 10 000 программ. Также ведется активная работа по созданию отечественных процессоров, например, серии «Эльбрус», «Байкал», «КОМДИВ-64» и других. Современные отечественные операционные системы, (например, «Astra Linux» или «Альт Линукс») уже поддерживают работу отечественных процессоров и микроконтроллеров, что является безусловно успехом отечественной промышленности и индустрии программного обеспечения.

В первой главе пособия был произведен анализ реализации программы импортозамещения иностранного программного обеспечения, обозначены основные проблемы и динамика процесса. Обеспечение информационной безопасности системообразующих организаций, в особенности объектов КИИ – сложный процесс, который требует системного подхода с учетом необходимости одновременного перехода на отечественное ПО и поддержания в работоспособном состоянии всех процессов информационных систем. Отдельно обозначены цели и задачи обновления информационных систем правоохранительных органов.

Во второй главе пособия представлены описание операционной системы Astra Linux, некоторые особенности, методы настройки и приемы работы с утилитами в базовой версии: работа с офисным пакетом Libreoffice и системой управления базами данных PostgreSQL.

Анализ реестра российского программного обеспечения показывает, что практически все операционные системы, большая часть офисных программ и системы управления базами данных берут за основу свободное ПО с открытым исходным кодом. Данный подход представляется разумным, однако даже эта категория ПО не всегда является независимой от зарубежных компаний, которые осуществляют финансовую и техническую поддержку.

Учебное пособие предназначено для профессорско-преподавательского состава и обучающихся высших учебных заведений, а также всех тех, кто в своей профессиональной деятельности использует отечественное программное обеспечение.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. **Российская Федерация. Законы.** Об информации, информационных технологиях и о защите информации : Федеральный закон от 27 июля 2006 г. № 149-ФЗ // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 11.01.2022). – Текст : электронный.

2. **Российская Федерация. Законы.** О безопасности : Федеральный закон от 28 декабря 2010 г. № 390-ФЗ // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 11.01.2022). – Текст : электронный.

3. **Российская Федерация. Законы.** Об электронной подписи : Федеральный закон от 6 апреля 2011 г. № 63-ФЗ // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 12.01.2022). – Текст : электронный.

4. Об утверждении Доктрины информационной безопасности Российской Федерации : указ Президента Российской Федерации от 5 декабря 2016 г. № 646 // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 12.01.2022). – Текст : электронный.

5. О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы : указ Президента Российской Федерации от 9 мая 2017 г. № 203 // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 12.01.2022). – Текст : электронный.

6. О национальных целях и стратегических задачах развития Российской Федерации на период до 2024 г. : указ Президента Российской Федерации от 7 мая 2018 г. № 204 // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 13.01.2022). – Текст : электронный.

7. Об утверждении плана перехода в 2016–2018 годах федеральных органов исполнительной власти и государственных внебюджетных фондов на использование отечественного офисного программного обеспечения : распоряжение Правительства Российской Федерации от 26 июля 2016 г. № 1588-р // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 13.01.2022). – Текст : электронный.

8. Об утверждении плана-графика перехода Министерства внутренних дел Российской Федерации на использование отечественного офисного программного обеспечения на 2018 год и на плановый период до 2020 года : приказ МВД России от 10 мая 2018 г. № 284 // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 13.01.2022). – Текст : электронный.

9. Об утверждении Инструкции по организации защиты персональных данных, содержащихся в информационных системах ОВД Российской Федерации : приказ МВД России от 6 июля 2012 г. № 678 // Официальный интернет-портал правовой информации. – URL: http:// www.pravo.gov.ru (дата обращения: 17.01.2022). – Текст : электронный.

10. Единый реестр российских программ для электронных вычислительных машин и баз данных // Официальный сайт единого реестра российских программ для электронных вычислительных машин и баз данных. – URL: https://reestr.digital.gov.ru/reestr/ (дата обращения: 17.01.2022). – Текст : электронный.

11. **Фролов, А.** Минкомсвязи включило первые приложения в реестр российского ПО. – URL: https://vc.ru/flood/13308-minsvyaz-first-reestr (дата обращения: 17.01.2022). – Текст : электронный.

12. **Морозов, И.** Импортозамещение в ИТ-отрасли. Взгляд из 2020. – URL: https://www.it-world.ru/cionews/business/153205.html (дата обращения: 16.01.2022). – Текст : электронный.

13. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ. Решение председателя Гостехкомиссии России от 30 марта 1992 г. ФСТЭК России. Федеральная служба по техническому и экспортному контролю. – URL: https://fstec.ru/index?id=384:rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g (дата обращения: 17.01.2022). – Текст : электронный.

14. Методический документ ФСТЭК России от 5 февраля 2021 г. «Методика оценки угроз безопасности информации». – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/2170-metodicheskij-dokument-utverzhden-fstek-rossii-5-fevralya-2021-g (дата обращения: 16.01.2022). – Текст : электронный.

15. Операционная система специального назначения «Astra Linux Special Edition». Руководство пользователя. – URL: https://astraLinux.ru (дата обращения: 17.01.2022). – Текст : электронный.

Учебное издание

Антонов Вячеслав Викторович
(доктор технических наук, профессор)
Харисова Зарина Ирековна
(кандидат технических наук, б/з)
Гурьянова Венера Рафисовна
(кандидат физико-математических наук, б/з)
и др.

ОСОБЕННОСТИ ИНФОРМАЦИОННОГО ОБЕСПЕЧЕНИЯ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ

Учебное пособие

Редактор Р. Р. Гафарова

Подписано в печать 15.03.2022	Выход в свет 28.03.2022
Гарнитура Times	Формат 60x84 1/16
Уч.-изд. л. 2,8	Усл. печ. л. 3
Тираж 75 экз.	Заказ № 1

Редакционно-издательский отдел
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2

Отпечатано в группе полиграфической и оперативной печати
Уфимского юридического института МВД России
450103, г. Уфа, ул. Муксинова, 2