Разработка типовых АРМ для дистанционной работы

En **Development of Standard Automated Workstations for Remote Work**

L. S. Rathkeen,
PhD (Eng.), Scientific Secretary of Veteran's Council of Russian Academy of Sciences
rathkeen@bk.ru

February 2021 in the frame of forum «Safety Technologies» in Moscow was hold on the series of seminars and round tables for the discussing of the problems of safety in banking sphere, transport and other branches. Much attention of exponents and visitors of the forum was paid for the actual questions of information security, which were discussed on the so-named XI conference with the participation of academician institutions, industrial enterprises, vendors, exploitation organizations and designers of the systems of industrial safety.

Keywords: Russian Academy of Sciences, typical automated working place, information security, file storages, information systems, critical information infrastructure, enforced qualified electronic signature

В феврале 2021 года в рамках ежегодного форума «Технологии безопасности» в Москве была проведена серия семинаров и круглых столов по вопросам обеспечения безопасности в банковской сфере, транспортной и других отраслях. Особое внимание экспонентов и гостей форума было привлечено к актуальным вопросам защиты информации, которые были рассмотрены на одноименной XI конференции с участием представителей академических институтов, промышленных предприятий, вендоров, эксплуатантов и разработчиков систем индустриальной безопасности.

Ключевые слова: Российская академия наук (РАН), типовое автоматизированное рабочее место (ТАРМ), информационная безопасность, файловые хранилища, информационные системы, критическая информационная инфраструктура (КИИ), усиленная квалифицированная электронная подпись (УКЭП)

Леонид Сергеевич Раткин,
кандидат технических наук,
ученый секретарь Совета ветеранов Российской академии наук
rathkeen@bk.ru

Конференция открылась вступительным словом заместителя директора ФСТЭК России В. С. Лютикова, сообщившего о результатах работы ведомства в 2020 году и планируемых направлениях сотрудничества с государственными организациями и частными предприятиями в году текущем. В частности, отмечалась положительная динамика взаимодействия с институтами Российской академии наук (например, Институтом прикладной математики имени М. В. Келдыша РАН, Институтом системного программирования имени В. П. Иванникова РАН, Институтом программных систем имени А. К. Айламазяна РАН) и промышленными структурами [1–2] по вопросам разработки систем для противодействия киберугрозам и минимизации киберрисков.

Типовое автоматизированное рабочее место (ТАРМ) государственных служащих было представлено на конференции директором Департамента проектов по информатизации Министерства цифрового развития, связи и массовых коммуникаций (Минцифры) РФ К. А. Гурзовым. В качестве предпосылок к его разработке он отметил не только отсутствие подобных базовых российских сервисов (согласно результатам опросов Минцифры России по 64 федеральным органам исполнительной власти (ФОИВ), 28 % госслужащих не имеют корпоративной почты (многочисленные вневедомственные e-mail не учитываются) и цифровое неравенство (неравномерность финансирования и неравенство долей затрат на ИТ для федеральных и региональных (РОИВ) органов власти), но также необходимость обеспечить удобство применения и обслуживания рабочих сервисов (они не должны уступать в этом аспекте рыночным аналогам) и информационные утечки (по данным InfoWatch, 23 % утечек данных наблюдаются в госсекторе).

Соответственно, для создания ТАРМ необходимо обеспечить гос-

служащих доступным рабочим базовым инструментом с замещением 100 % бесплатных рабочих сервисов (e-mail, мессенджер, ВКС/АКС, файловое хранилище и репозитории), устранить неравенство в доступности технологий и сервисов между органами власти и предоставить возможность всем без исключения государственным и муниципальным служащим пользоваться платформой. Также для повышения показателей эффективности необходимо создать функционал внутриведомственных и межведомственных коммуникаций с сервисами и инструментами, не уступающими рыночным аналогам, и устранить причины несоблюдения мер информационной безопасности (ИБ) при сохранении комфортного использования сервиса.

Интересны результаты опроса 64 ФОИВ Минцифрой РФ: 83 % применяют сервисы Microsoft для организации почты, 59 % не используют технологий интеграции с коммуникационными системами, 19 % не обладают комплементарными базовыми сервисами (например, по организации встреч, ведению календарей учета рабочего времени). Кроме того, до сих пор не разработан единый стандарт обеспечения защиты и сохранности служебной информации!

Также необходимо обеспечить доступность удобных рабочих базовых инструментов и сервисов (на основе отечественных разработок и технологий) для корпоративной почты (включая рабочий календарь и адресную книгу), мессенджеров, АКС и ВКС (согласно экспертным оценкам, современный сотрудник в среднем использует три бесплатных облачных мессенджера в своей работе для переписки с коллегами и через незащищенные каналы отправляет 3 Мбайта служебной информации ежедневно), оптимизировать работу файловых хранилищ (ФХ) и репозиторных систем (при применении корпоративного ФХ время на поиск и отправку файлов сокращается втрое), создать разветвленную систему кадрового сервиса и управления развитием (включая модули профессиональной адаптации и ориентации, управления знаниями и планирования совещаний, а также систему подготовки и обработки результатов опросов).

Интересны данные по оценке цифрового неравенства, приведенные в отчете компании McKinsey «Digital Russia Report», в котором утверждается, что передовой опыт в создании цифровых продуктов реализован в наиболее продвинутых регионах в формате, предполагающем общий подход для цифровизации государственных органов. По мнению экспертов, базовый бюджет на ИКТ сконцентрирован в регионах – «лидерах по цифровизации», что обусловливает необходимость передачи ИКТ и опыта работы с ними отстающим регионам (так, в Москве сконцентрировано порядка 40 % расходов на ИКТ!)

При разработке защищенной среды ТАРМ одной из ключевых является подсистема ИБ ТАРМ. Среди проблем ИБ следует особо отметить:

- утечку конфиденциальных документов или их временных копий при краткосрочной передаче собственных устройств третьим лицам, их продаже, сдаче в ремонт, взломе или утере, а также при удаленной работе вне закрытого контура;
- утечку из-за преднамеренного копирования конфиденциальной информации из ведомственных информационных систем (ИС);
- угрозу взлома несертифицированных TSL устаревших версий 1.1. и 1.2 (среднее время реализации атаки – 38 часов);
- утечку конфиденциальной информации через онлайн-сервисы или мессенджеры при обмене и общении в рабочих группах с неконтролируемым составом участников;
- отсутствие антивирусов.

Мерами пресечения кибератак и минимизации киберугроз, в частности, являются:

- применение доверенного программного обеспечения и среды исполнения (загрузка с защищенного токена);
- аутентификация с применением УКЭП с «гостированной» защитой системы обмена данными (VPN);
- запрет копирования загружаемых данных на незащищенные носители;
- антивирусная защита с контролем целостности и мониторингом уровня защищенности;
- сетевая сегментация [3] с выявлением и предотвращением вторжений, а также постоянный контроль действий и коммуникаций пользователя с фиксацией ИБ-событий.

Типовой внутренний ИБ-нарушитель (63 % всех утечек, по данным InfoWatch) – это рядовой сотрудник, имеющий доступ к информации ограниченного доступа в связи с должностными обязанностями. Как правило, он не соблюдает регламент работы с ДСП (не считает его важным, будучи ознакомлен с ним формально), применяет собственный телефон и/или планшет (для работы с e-mail и другими ресурсами по документообороту), недоволен отношением к нему со стороны руководства (уровень зарплаты и премий, отсутствие карьерного роста и другие «демотивирующие» факторы), часто использует открытые мессенджеры и онлайн-сервисы и готов сотрудничать с внешними нарушителями за вознаграждение (вследствие финансовых затруднений).

ТАРМ является полностью (на 100 %) доверенным ПО и инструментом безопасной удаленной работы с информацией ограниченного доступа (ДСП), предполагающим строгую аутентификацию и «гостированную» защиту обмена данными с применением УКЭП, мониторингом действий и коммуникаций пользователя и передаваемых данных, при этом DLP позволяет выявлять и блокировать передачу чувствительной информации. При переходе всех ведомств на ТАРМ:

- повысится межведомственная эффективность и уровень взаимодействия ФОИВ, РОИВ и органов местного самоуправления (ОМСУ) с населением;
- станет возможна безопасная удаленная работа с любого места без угрозы утечки информации и равноправным доступом всех органов государственной власти к общей витрине приложений;
- гибкая модель ценообразования (базовый набор сервисов SaaS – единый для всех, остальные опции

подключаются дополнительно, в том числе оборудование и ПО);
- унификация технических решений с едиными SLA (информатизация ФОИВ, РОИВ и ОМСУ в едином темпе в рамках общей «Дорожной карты»);
- применимость технологических решений ТАРМ для предоставления населению и бизнесу всего спектра услуг.

Возможна следующая классификация ФОИВов, РОИВов и ОМСУ: ведомства с базовым уровнем развития (ВБУР) ИТ, «консервативные» ведомства (КВ) и «продвинутые» ведомства (ПВ): соответственно, для них разработаны различные стратегии.

Как правило, ВБУР недоукомплектованы современными средствами ИТ и имеют сложности с финансами: для них обеспечена доступность сервисов ТАРМ всем сотрудникам ведомства в условиях ограниченного бюджета, предусмотрена возможность работы с любого типа устройств, включая домашние ПК, увеличен срок использования существующего парка оборудования на 30 % за счет технологии VDI, а также обеспечены передовые механизмы ИБ.

КВ, не имеющие проблем с бюджетом, традиционно следуют «исторически» сложившимся на «классическом» офисном ПО стандартам ИТ. Переход на ТАРМ обеспечит им сокращение затрат и повышение автоматизации рабочих мест, оптимизирует кадровую политику, сократит санкционные риски и будет способствовать импортозамещению коммерческих сервисов, повысит уровень ИБ в условиях коллективной работы с другими ведомствами благодаря применению единых политик, стандартов и методик.

Наконец, для ПВ, активно инвестирующих в развитие внутренних и внешних ИТ-сервисов и применяющих в повседневной жизни современные технологии, благодаря ТАРМ повышается эффективность работы госслужащих за счет предоставления универсальных и объединенных сервисов коммуникации и коллективной работы с другими ведомствами с возможностью создания и опубликования новых сервисов ФОИВ и культуры client experience (клиентский опыт, получаемый при упрощении процедур подключения и применения сервиса ТАРМ с единым стандартизированным и интуитивно понятным интерфейсом).

Архитектура платформы ТАРМ следующая: технические и функциональные компоненты объединяют инструментарий для работы с управляемыми страницами, системой поиска, системой управления правами пользователей, уведомлениями и событиями, моделями бизнес-процессов и компонентами отчетности, профилями сотрудников и групп и «интеграционным слоем». В ТАРМ предусмотрены:
- платформа социализации госслужащих (каждый из компонентов может быть заменен в течение пяти суток), интегрирующая новостные ленты, ведомственные порталы, рабочие календари и адресные книги;
- проектные группы, почтовые сервисы, мессенджеры, кадровые профили, системы рейтингования и оценки рабочих достижений, ВКС и АСК, блоки управления задачами и поручениями, файловые хранилища и репозитории (включая криптографические и стеганографические репозитории);
- инструменты подготовки отчетных форм и опросных листов, управления знаниями и пр.

В Security Operations Center представлены DLP, средства антивирусной защиты, межсетевые экраны, доверенное программное обеспечение среды исполнения, средства строгой аутентификации (VPN) и средства сбора и анализа событий ИБ.

По поручению Правительства РФ разработаны «Требования к устройствам обеспечения безопасной удаленной работы» (далее – Требования), предусматривающие возможность сотрудникам ФОИВ, РОИВ и государственных организаций удаленно работать с ГИС с использованием неаттестованных средств вычислительной техники (включая личные). Согласно Требованиям, защищенное устройство должно обеспечивать:
- хранение, формирование и проверку усиленной квалифицированной электронной подписи (УКЭП) с неизвлекаемым закрытым ключом;
- удаленный запуск и дистанционную работу с установленными на служебном компьютере приложениями;
- автоматическую настройку и подключение к шлюзу организации с применением сертифицированного VPN-клиента;
- загрузку компьютера с внешнего USB-носителя с записанной сертифицированной операционной системой;
- автономную работу со служебными документами и возможностью их сохранения на защищенный раздел USB-устройства;
- удаленное подключение к рабочему столу служебного компьютера (Remote Desktop) или работу с виртуальным рабочим столом (VDI);
- двухфакторную аутентификацию пользователя.

В соответствии с Требованиями, защищенное устройство должно быть сертифицировано для работы в ИС общего пользования (II класса), в ИС значимых объектов критической информационной инфраструктуры по первую категорию включительно, в ГИС – по первый класс защищенности включительно, в медицинских, банковских и других отраслевых ИС – по первый класс защищенности включительно, в ИС персональных данных – по первый уровень защищенности включительно.

Наличие защищенного устройства в удаленном ТАРМ позволяет осуществлять централизованное удаленное администрирование устройства (например, обновлять пользовательские настройки, профили, цифровые сертификаты, ключи доступа), отказаться от применения запоминаемых паролей (вводимых пользователями вручную при удаленном подключении к ИС организации), использовать личный компьютер для автономной или дистанционной работы с возможностью обработки документов ограниченного распространения, применять надежную двухфакторную аутентификацию пользователей и задейство-

вать привычный USB-токен при работе со служебным компьютером (в частности, в качестве защищенной «флешки» для хранения конфиденциальной информации, для УКЭП в СЭД и различных электронных сервисах и web-порталах).

Разработанное устройство предотвращает:

- доступ к сохраненным в своей памяти служебным или пользовательским данным в случае утери или кражи устройства, загрузку на компьютер любого файла (возможно, зараженного) с внешнего носителя или из сети Интернет с передачей его в ИС организации;
- копирование или сохранение обрабатываемой служебной информации на накопители (локальные и съемные диски, флеш-карты и т. д.);
- выход в Интернет при дистанционной работе напрямую со своего личного компьютера (минуя средства защиты организации);
- печать обрабатываемой служебной информации на локальный или сетевой принтер, использование LiveUSB на неавторизованном (неизвестном) компьютере.

Необходимый уровень безопасности достигается комбинированным применением сертифицированных ОС, сертифицированных VPN и средств VDI с выполнением всех задач на служебном ПК или на виртуальной машине (на неаттестованный ПК передаются лишь выводимые на экран изображения).

Требования по защите информации при осуществлении дистанционной работы были представлены в докладе начальника управления ФСТЭК России Д. Н. Шевцова. Выступающий напомнил о переходе на дистанционную работу государственных органов весной 2020 года, инициированном Поручением Председателя Правительства РФ от 16 марта 2020 года № ММ-П9-1861 и Поручением Заместителя Председателя Правительства РФ от 18 марта 2020 года № ДГ-П17-1987, согласно которым «в рамках принятия мер по противодействию (распространения) короновирусной инфекции предусмотрен перевод работников на дистанционный режим исполнения должностных обязанностей, обеспечивающий бесперебойное функционирование федеральных органов исполнительной власти и подведомственных организаций».

В результате была создана группа по организации удаленного рабочего места государственного служащего в рамках федерального проекта «Цифровое государственное управление» национальной программы «Цифровая экономика». В сотрудничестве с ведущими отраслевыми предприятиями и рядом академических институтов разработаны рекомендации по обеспечению безопасной дистанционной работы в ГИС. В частности, рекомендации ФСТЭК России относительно мер защиты информации, принимаемых в информационных системах ФОИВ и подведомственных организаций в целях минимизации рисков возникновения дополнительных угроз безопасности информации при осуществлении удаленного доступа их работников направлены в федеральные органы исполнительной власти в установленном порядке (исх. от 20 марта 2020 г. № 240/22/1204дсп).

Также в письме ФСТЭК России от 30 марта 2020 года № 240/22/389 представлены рекомендации по обеспечению безопасности объектов критической информационной инфраструктуры при реализации дистанционного режима исполнения должностных обязанностей работниками субъектов критической информационной инфраструктуры.

Среди наиболее важных документов о защите информации при осуществлении дистанционной работы отметим «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» (утверждены приказом ФСТЭК России от 11 февраля 2013 года № 17), «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах» (утверждены приказом ФСТЭК России от 18 февраля 2013 года № 21) и «Меры защиты информации в государственных информационных системах» (утверждены ФСТЭК России 11 февраля 2014 года). В них, в частности, рассмотрены методы многофакторной (двухфакторной) аутентификации для удаленного доступа в систему, установления (в том числе документального) видов доступа (разрешенных при удаленных действиях), обеспечения доверенного канала связи при удаленном доступе к системе, регистрации попыток удаленного доступа, контроля удаленного доступа пользователей (процессов, запускаемых от имени пользователей), управления удаленным запуском компонентов ПО, мониторинга и контроля удаленного доступа, очистки информации в мобильном техническом устройстве после завершения сеанса удаленного доступа.

В соответствии с протоколом заседания Межведомственной комиссии Совета Безопасности РФ по ИБ от 26 октября 2020 года № 3, ФСТЭК России поручено разработать и утвердить «Требования по безопасности информации к средствам обеспечения безопасной дистанционной работы в информационных (автоматизированных) системах». Проект проходит экспертное обсуждение с анализом возможных оценок регулирующего воздействия, подготовлен к утверждению в Минюст РФ на государственную регистрацию.

Также подготовлены «Изменения в Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденные приказом ФСТЭК России от 11.02.2013 № 17» и «Изменения в Меры защиты информации в государственных информационных системах».

При применении личных СВТ по технологии LiveUSB для обеспечения дистанционной работы возможно появление дополнительных угроз, в частности, перехвата информации по каналами передачи данных (передаваемых между LiveUSB и ИС), подмены доверенного пользователя LiveUSB, внедрения на LiveUSB вредоносного кода через личное СВТ, запуска LiveUSB с неавторизованного СВТ, несанкционированного копирования защищаемой информации с LiveUSB на носители личного СВТ,

утечек защищаемой информации за счет включения сторонних периферийных устройств к личному СВТ. В качестве мер защиты, помимо сертифицированных средств доверенной загрузки, ОС и двухфакторной аутентификации, предлагаются сертифицированные СКЗИ для защиты канала передачи данных и шифрования защищаемой информации на LiveUSB с дистанционным доступом к системе через технологии RDP и VDI, с централизованным управлением LiveUSB и удаленным администрированием.

Требования к средствам дистанционной работы применяются к программно-техническим системам защиты информации, обеспечивающим безопасную дистанционную работу в информационной (автоматизированной) системе с использованием СВТ, не входящих в ее состав. Средства дистанционной работы применяются в ГИС по 1 класс защищенности включительно, в значимых объектах КИИ – по 1 категорию включительно, в АСУ ТП – по 1 класс защищенности включительно, в ИСПДн – по 1 уровень защищенности включительно, в информационных системах общего пользования 2 класса.

Требования по безопасности информации относятся к составу средства дистанционной работы, конструкции защищенного носителя, среде функционирования средства дистанционной работы, уровню доверия средства дистанционной работы – не ниже 4 уровня доверия, средству доверенной загрузки средства дистанционной работы – не ниже 4 класса защиты, ОС средства дистанционной работы – тип «А» не ниже 4 класса защиты, идентификации и аутентификации пользователей, идентификации и авторизации СВТ, управлению доступом в средстве дистанционной работы, администрированию и централизованному управлению средством дистанционной работы, контролю целостности средства дистанционной работы, регистрации и учету событий безопасности в средстве дистанционной работы.

Таким образом, научная кооперация отраслевых регуляторов с академическими институтами при разработке типовых автоматизированных рабочих мест и требований по защите информации при осуществлении дистанционной работы позволила не только оптимизировать работу по ключевым направлениям ИБ с поиском капиталовложений для реализации приоритетных отраслевых инвестиционных проектов, но способствовала гармонизации законодательной базы [4]. В частности, был выявлен и устранен ряд правовых пробелов, идентифицированы и ликвидированы внутренние и внешние противоречия в текстах некоторых нормативно-правовых документов.

Для достижения поставленных целей при создании ТАРМ предстоит решить ряд ключевых задач, в том числе по созданию централизованных базовых сервисов для всех органов власти с едиными стандартами и протоколами, внедрению вовлекающих механизмов и инструментов, обеспечению сквозной интеграции коммуникативных инструментов в госсекторе, формированию единого уровня доступности цифровых инструментов для всех ФОИВ, РОИВ, ОМСУ и бюджетных учреждений, централизации инфраструктуры для ИТ-решений, внедрению соответствующих российских инструментов, применению ИТ с открытым исходным кодом, ориентации на передовых технологических партнеров с созданием функционала внутриведомственных и межведомственных коммуникаций, переводом госслужащих в защищенный контур, повышением контроля за передачей информации и созданием инструментария для работы с документами, имеющими различные грифы секретности. ■

ЛИТЕРАТУРА

1. Горелик А. Л., Тимушев А. Г., Шабаров В. В. Организация внутреннего консалтинга промышленных корпораций // Тяжелое машиностроение. – 2001. – № 6. – С. 16–20.

2. Горелик А. Л., Шабаров В. В. Ситуационный анализ промышленных корпораций // Вопросы оборонной техники. – 2001. – № 1 (302). – С. 8.

3. Горелик А. Л., Раткин Л. С. Об устойчивости корпоративных информационных сетей // Вопросы оборонной техники. – 2003. – № 2 (315). – С. 43–45.

4. Раткин Л. С. К столетию со дня рождения Президента АН СССР М. В. Келдыша: у истоков программы пилотируемых космических полетов (пленарный доклад) // Материалы Второй международной научно-технической конференции «Нестационарные, энерго- и ресурсосберегающие процессы и оборудование в химической, нано- и биотехнологии – НЭРПО-2011» / Под общей редакцией Г. И. Ефремова. – М.: Изд-во МГОУ. – 2011. – С. 13–16.

Безопасная дистанция

На конференции ФСТЭК России «Актуальные вопросы защиты информации» было представлено решение Aladdin LiveOffice для безопасной дистанционной работы.

Традиционная конференция ФСТЭК России «Актуальные вопросы защиты информации», ежегодно проходящая в рамках форума «Технологии безопасности» (09–11.02.2021), в этом году состоялась 10 февраля. Целью мероприятия стало обсуждение актуальных проблем обеспечения необходимого уровня защиты информации для удаленных сотрудников. В своих докладах представители ФСТЭК России рассказали о требованиях по защите информации при обеспечении дистанционной работы, а также о новых требованиях, которые будут предъявляться к программно-техническим средствам защиты информации, обеспечивающим безопасную дистанционную работу в информационной (автоматизированной) системе с использованием средств вычислительной техники, не входящих в состав указанной информационной (автоматизированной) системы.

«Аладдин Р. Д.» и «ГК Astra Linux» представили на совместном стенде сертифицированное средство обеспечения безопасной дистанционной работы Aladdin LiveOffice[1], представляющее собой специализированное защищенное USB-устройство, обеспечивающее загрузку компьютера с внешнего USB-носителя, на котором находится сертифицированная операционная система Astra Linux Special Edition версии 1.6 SE «Смоленск» с набором предустановленного ПО для подключения к сети Интернет (Ethernet или Wi-Fi). Устройство осуществляет автоматическую настройку и подключение к шлюзу организации с использованием сертифицированного на соответствие требованиям ФСБ России к средствам криптографической защиты информации класса КС1 VPN-клиента ViPNet Client 4U for Linux[2] производства компании «ИнфоТеКС».

Специализированное защищенное USB-устройство Aladdin LiveOffice разработано во исполнение поручений Правительства РФ № ММ-П9-1861, № ДГ-П17-1987 от 16 и 18 марта 2020 года для противодействия распространению коронавирусной инфекции и обеспечения работы сотрудников органов исполнительной власти и государственных организаций в удаленном режиме с использованием личных средств вычислительной техники с предоставлением им удаленного доступа к ГИС.

Сертифицированное средство обеспечения безопасной дистанционной работы Aladdin LiveOffice:

- обеспечивает возможность удаленного подключения с домашнего компьютера к служебному компьютеру или виртуальному рабочему столу (VDI), которое может использоваться для дистанционной работы в ГИС до 1 класса защищенности включительно, в значимых объектах КИИ до 1 категории включительно, в АСУ ТП до 1 класса защищенности включительно, в ИСПДн до 1 уровня защищенности включительно, в медицинских (МИС), банковских (ИБС) и других ИСОП до II класса, как это и определено соответствующими требованиями ФСТЭК России;
- допускает обработку банковской, налоговой, врачебной, нотариальной, аудиторской и других видов тайн и служебных сведений;
- позволяет использовать в служебных целях личные компьютеры сотрудников;
- позволяет использовать электронную подпись.

При этом Aladdin LiveOffice ***не позволяет:***

- использовать устройство на чужом (неавторизованном) компьютере: все его функции, а также служебные и пользовательские данные будут недоступны, даже при вводе правильного пароля доступа;
- скопировать или сохранить обрабатываемую служебную информацию на локальные, съемные диски, флеш-накопители и на другие устройства с функцией хранения информации;
- распечатать обрабатываемую служебную информацию на локальном или сетевом принтере;

- загрузить на свой компьютер какой-либо файл (возможно, зараженный) с внешнего носителя или из сети Интернет и передать его в ИС организации;
- выйти в сеть Интернет при дистанционной работе напрямую со своего личного компьютера (сеть будет доступна только через служебный компьютер, а работа в сети защищена используемыми в организации средствами защиты);
- получить доступ к сохраненным в памяти устройства служебным или пользовательским данным, а также использовать его для удаленного доступа в ИС организации в случае утери или кражи устройства.

Aladdin LiveOffice может администрироваться дистанционно с использованием системы централизованного управления JMS[3], которая автоматизирует большинство рутинных операций и позволяет обновлять пользовательские настройки, профили, цифровые сертификаты, ключи.

Анонсированное решение вызвало большой интерес аудитории, что неудивительно, поскольку Aladdin LiveOffice на ОС AstraLinux – единственное на сегодняшний день решение на основе технологии LiveUSB, соответствующее требованиям защиты информации ФСТЭК России по 4-му уровню доверия. Данное устройство может существенно снизить расходы и сроки по организации безопасности удаленных рабочих мест, что очень актуально в текущих условиях, когда большинство компаний переходит на гибридный и удаленный режимы работы. Это простое и удобное средство с установленными на нем отечественной ОС и набором необходимых средств защиты, которое может стать для заказчиков полноценной, но гораздо более дешевой альтернативой служебному ноутбуку.

В рамках конференции был также представлен доклад на тему «Техническое решение по обеспечению дистанционной работы в информационной системе с личных средств вычислительной техники пользователей»[4], в котором подробно рассказывалось про Aladdin LiveOffice. ■

[1] *https://www.liveoffice.ru.*
[2] *https://infotecs.ru/product/vipnet-client-4u.html#soft*
[3] *https://www.aladdin-rd.ru/catalog/jms/.*
[4] *https://www.aladdin-rd.ru/support/downloads/90453341-564e-44c5-8d0f-7800ea955558/get/.*