Аладдин

Обеспечение безопасной дистанционной работы в соответствии с требованиями ФСТЭК, внедрение и использование решения Aladdin LiveOffice в ФНС России

05/2023

О документе

5 апреля 2023 г. в прямом эфире AM-Live прошёл открытый разговор с экспертами на тему "Обеспечение безопасной дистанционной работы, соответствие требованиям ФСТЭК, внедрение средства безопасной дистанционной работы Aladdin LiveOffice в ФНС России".

В данном документе мы постарались собрать все обсуждаемые вопросы по теме, а также вопросы, заданные в рамках прямого эфира и после него.
Эксперты, принимавшие участие в прямом эфире и подготовке ответов на вопросы:

- **Шевцов Дмитрий Николаевич, начальник Управления ФСТЭК России**
  — в части нормативной базы, гос. регулирования, требований к обеспечению безопасности дистанционной работы и к специализированным средствам обеспечения безопасной дистанционной работы
- **Груздев Сергей Львович, ген. директор компании "Аладдин"**
  — в части продуктов компании для организации безопасной дистанционной работы
- **Судаков Максим Сергеевич, Консультант Отдела правовой защиты информации и организации деятельности территориальных подразделений УИБ ФНС России ФНС России**
  — в части опыта внедрения и эксплуатации сертифицированного продукта Aladdin LiveOffice в ФНС России.

Запись прямого эфира

- Youtube: https://www.youtube.com/live/32vyuyxSOLY?feature=share
- VK: https://vk.com/video-21732035_456239772

Презентации

— Сертифицированное решение Aladdin LiveOffice для безопасной дистанционной работы — https://aladdin-rd.ru/upload/catalog/liveoffice/Aladdin_LiveOffice-Presentation-april-2023.pdf

Содержание:

Гос. регулирование, нормативная база, требования ФСТЭК России 4

Сертифицированное решение
для организации безопасной дистанционной работы – Aladdin LiveOffice 16

Другие рекомендуемые решения
для обеспечения безопасной дистанционной работы 18

Опыт ФНС России по внедрению и эксплуатации Aladdin LiveOffice 18

1. Гос. регулирование, нормативная база, требования ФСТЭК России

- **На кого распространяются Требования ФСТЭК России, обязательные для выполнения, а кто может пользоваться теми решениями, которые он сам выбрал и считает их эффективными?**

  Требования ФСТЭК России:

  a. ОБЯЗАТЕЛЬНЫЕ - для владельцев и операторов государственных и муниципальных информационных систем (ГИС).

  b. НАСТОЯТЕЛЬНО РЕКОМЕНДУЕМЫЕ – для субъектов КИИ, владельцев и операторов ИСПДн (решение о выборе тех или иных средств защиты информации – сертифицированных, либо прошедших оценку соответствия по требованиям безопасности информации, может приниматься ими самостоятельно в рамках проектирования системы защиты информации для их ИС с подтверждением результатов в рамках приёмочных испытаний).

- **Какой нормативной базой следует руководствоваться при организации безопасной дистанционной работы сотрудников и контрагентов в ГИС?**

  Понятие государственных информационных систем (ГИС) определено в Федеральном законе от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации".

  Согласно закону, государственными информационными системами являются федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов.

  За защиту информации в ГИС отвечает оператор такой системы.

  Помимо понятия ГИС, федеральным законом №149-ФЗ вводится понятие «муниципальная информационная система» (ИС, созданная на основании решения органа местного самоуправления). С точки зрения защиты информации, государственные и муниципальные информационные системы – идентичны.

  Нормативная база по защите информации в ГИС включает в себя:

  a. Федеральный закон "Об информации, информационных технологиях и о защите информации"

  b. "Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах" (утверждены приказом ФСТЭК России № 17 от 11 февраля 2013 года)

  c. "Меры защиты информации в государственных информационных системах" (утверждены ФСТЭК России от 11 февраля 2014 года) – достаточно объёмный и подробный документ - 176 страниц.

  Требования по обязательному применению сертифицированных средств для обеспечения безопасной дистанционной работы в ГИС регламентированы:

  d. Приказом ФСТЭК России от 11 февраля 2013 № 17 "Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах";

  e. Постановлением Правительства Российской Федерации от № 330;

  f. "Требованиями ФСТЭК России к средствам дистанционной работы" (ДСП) (утверждены Приказом ФСТЭК от 16 февраля 2021 года №32).

Кроме того, для защиты информации, содержащейся и обрабатываемой в ГИС, в т.ч. при дистанционной работе, также действуют "Требования о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств", утверждённые приказом ФСБ России от 24.10.2022 №524 в части:

— защиты каналов связи (передачи информации);

— защиты (шифрования) данных на носителях информации;

— обеспечения юридической значимости электронных документов и защиты от их подделки.

- **Почему возникла необходимость разработки новых Требований, почему (чем) не устраивали старые, точнее текущие, действующие требования, описанные в Мерах защиты к 17-му Приказу ФСТЭК России? В части дистанционной работы они уже не работают?**

Требования и рекомендации, приведенные в методическом документе "Меры защиты информации в государственных информационных системах", устанавливают лишь необходимость защиты информации "...при доступе пользователей ... к объектам доступа информационной системы через информационно-телекоммуникационные сети, в том числе сети связи общего пользования, с использованием стационарных и (или) мобильных технических средств", при этом никаких требований к средствам, используемым при этом, в документе не предъявляется, что и обусловило необходимость разработки новых Требований.

Во время пандемии в связи с экстренным переводом гос. служащих на дистанционный режим работы возникла необходимость организовывать безопасную дистанционную работу именно на личных компьютерах и ноутбуках сотрудников органов исполнительной власти.

На тот момент не было готового отработанного решения, которое можно бы было тиражировать на всю страну и рекомендовать его для использования при организации безопасной дистанционной работы для госслужащих. Не было бюджетов на покупку.

Поэтому к марту 2020 г. ФСТЭК России разработал комплект первоочередных мер по переводу госслужащих на дистанционный режим работы, дополнив рекомендации новым требованием по отслеживанию геолокации пользователя при его удалённом подключении к ИС. Эти рекомендации были доведены до всех гос. органов.

С началом пандемии первыми из продажи пропали ноутбуки.

Стало понятно, что оснастить всех служебными СВТ[1] не получится, нужно принимать экстренные меры и искать какое-то альтернативное решение, более простое и дешёвое.

В качестве базовой технологии для такого решения была выбрана технология LiveUSB, разработаны рекомендации, что и как должно быть сделано (самостоятельно, ибо готового решения на тот момент ещё не было), какое ПО и СЗИ должны быть установлены на съёмном носителе.

Однако, в числе рекомендаций по их применению указывалось, что данные подходы и средства должны применяться только при условии:

— крайней необходимости;

— чёткого определения тех ресурсов, к которым может быть предоставлен удалённый доступ, без расширенного или полного доступа ко всей ГИС;

— надёжной идентификации и мониторинга осуществления удалённого доступа – кто осуществляет, сколько сотрудников имеет удалённый доступ, к каким именно ресурсам ИС, с каких СВТ (в т.ч. личных) и т.д.

[1] Средство вычислительной техники

Это были экстренные и временные меры, необходимые во время пандемии 2020-2021 гг.

ФСТЭК России был вынужден взять ответственность на себя и временно разрешить использование подобных решений, содержащих набор установленных сертифицированных СЗИ, но без комплексной проверки безопасности, соответствия такого решения требованиям, и, соответственно, без сертификации такого решения.

Позже, на основе полученного опыта, были разработаны новые требования непосредственно к СРЕДСТВАМ безопасной дистанционной работы. К работе над новыми требованиями были привлечены ведущие разработчики СЗИ, производители USB-токенов, СКЗИ, VPN, российских ОС.

В феврале 2021 г. на ТБ-Форуме ФСТЭК России впервые анонсировал и подробно рассказал о новых требованиях, а компания "Аладдин Р. Д." подготовила, апробировала и сертифицировала первое комплексное решение, готовое для применения – Aladdin LiveOffice.

Регистрация новых Требований в Минюсте России и оценка регулирующего воздействия заняли немного больше времени, чем разработка и сертификация самого решения.

Таким образом, сегодня на рынке есть и специализированные средства обеспечения безопасной дистанционной работы при использовании личных средств вычислительной техники (Aladdin LiveOffice), и сертифицированные программно-аппаратные комплексы (ПАКи) с использованием служебных СВТ с набором предустановленных СЗИ и набора необходимого ПО для дистанционной работы.

- **Кто выступил инициатором разработки новых Требований и специализированных средств обеспечения безопасной дистанционной работы и почему?**

  Новые Требования и само средство для обеспечения безопасной дистанционной работы были разработаны в целях принятия мер по распространению коронавирусной инфекции и переводу работников на дистанционный режим исполнения должностных обязанностей, обеспечивающий бесперебойное функционирование федеральных органов исполнительной власти и подведомственных организаций по поручению:

  — Председателя Правительства РФ №ММ-П9-1861 от 16.03.2020;
  — Зам. Председателя Правительства РФ №ДГ-П17-1987 от 18.03.2020;
  — Рабочей группы Минцифры, ФСТЭК и ФСБ России по организации удалённого рабочего места государственного служащего в рамках федерального проекта "Цифровое государственное управление" национальной программы "Цифровая экономика";
  — Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности (№3 от 26.10.2020), во исполнение ФЗ-407.

  Инициатором и разработчиком новых требований выступил ФСТЭК России.

  По инициативе Минцифры для работы над новыми требованиями и подготовки решения для организации безопасной дистанционной работы была создана рабочая группа, в которую вошли представители ФСТЭК России, ФСБ России, Минцифры, ведущих разработчиков российских ОС, СЗИ.

- **Есть ли принципиальная разница между использованием служебного ноутбука с набором предустановленного ПО и СЗИ и специализированным средством для обеспечения безопасной дистанционной работы на базе технологии LiveUSB? Какое из этих решений более безопасно?**

  При использовании служебного ноутбука с набором предустановленного ПО и СЗИ обрабатываемая информация, как правило, хранится и обрабатывается на нём.

Это сложнейший програмно-аппаратный комплекс, с огромным количеством подсистем, интерфейсов, каналов обмена, уязвимостей, наводок и т.п., а следовательно, и потенциальных каналов утечки обрабатываемой на нём информации.

В случае применения специализированного средства, использующего технологию LiveUSB и терминального доступа, вся информация хранится и обрабатывается на рабочем или виртуальном (VDI) компьютере, находящемся в закрытом контуре ИС организации, на пользовательский (личный, недоверенный) компьютер обрабатываемая информация не копируется и там не хранится. Вместо этого на экран монитора "прилетают" лишь отрисованные "картинки"/элементы экрана, а обратно передаются лишь скан-коды нажимаемых клавиш и координаты указателя мыши.

Весь обмен производится по защищённому VPN каналу. При этом все локальные ресурсы личного компьютера – жёсткие диски, NAS, флешки, принтеры и пр. – которые могут быть использованы в качестве канала утечки служебной информации, либо для организации атаки на ресурсы компании – в терминальном режиме работы заблокированы и недоступны.

В качестве специализированного защищённого флеш-накопителя в Aladdin LiveOffice используется аппаратная платформа JaCarta SF/ГОСТ, разработанная и сертифицированная в МО РФ для работы с гостайной.

Следовательно, специализированное решение (Aladdin LiveOffice) имеет существенно меньшую поверхность для атаки и более безопасно при организации дистанционной работы.

— *Примечание: набор сертифицированных СЗИ, ОС и др. ПО, установленных на сертифицированный флеш-накопитель, не является основанием говорить о сертифицированном средстве для безопасной дистанционной работы. Сертифицированным является только комплексный продукт, выполняющий соответствующие требования, и имеющий собственный сертификат соответствия.*

Различия и ответственность использования служебного ноутбука и специализированного сертифицированного решения:

— *Применение служебного ноутбука с набором предустановленных СЗИ для обеспечения удалённого доступа к ГИС, ИС или АС организаций КИИ, ИСПДн – как правило, это всегда проектные решения, "затачиваемые"под ИС организации. Это всегда самостоятельный выбор оператора ИС, и его ОТВЕТСТВЕННОСТЬ за возможные утечки и другие инциденты.*

— *В случае же специализированного сертифицированного средства риски утечки и возникновения инцидентов существенно меньше, поскольку такое средство было всесторонне изучено, проверено и сертифицировано именно для противодействия подобным атакам и утечкам. Следовательно, и ОТВЕТСТВЕННОСТЬ в случае инцидентов при его применении будет другой, существенно меньшей.*

- **Классический вариант для обеспечения дистанционной работы сотрудников – это "служебный ноутбук" с набором установленного ПО. Где, в каких документах регламентировано, какое ПО и средства защиты должны быть установлены? Какие дополнительные меры и ограничения следует применять?**

Возможность удалённого подключения и дистанционной работы в ГИС, КИИ, ИСПДн были предусмотрены во всех регламентирующих документах, Требованиях, Мерах защиты, о которых говорилось выше[2].

[2] См. вопрос: Какой нормативной базой следует руководствоваться при организации безопасной дистанционной работы сотрудников и контрагентов в ГИС?

Все БАЗОВЫЕ меры защиты там есть, включая идентификацию и двухфакторную аутентификацию пользователей, антивирусную защиту, применение межсетевого экранирования, регистрацию событий безопасности, защиту канала передачи информации, шифрование данных на дисках и пр.

Все эти Требования и Меры защиты информации предполагали использование служебного ноутбука.

Это всегда проектное решение, при котором выбор тех или иных средств защиты и организация безопасной дистанционной работы в ГИС (а также КИИ, ИСПДн) – это всегда ответственность оператора данного информационного ресурса. И его ОТВЕТСТВЕННОСТЬ в случае утечки и инцидентов.

Поэтому, с учётом новых реалий, возросшей роли внутреннего нарушителя, усилившихся атак зарубежных спецслужб на наши ГИС, КИИ, ИСПДн рекомендуется применять специализированные средства, имеющие меньшую поверхность атаки и более безопасные при организации дистанционной работы.

- **Если есть требования, то, наверное, нужно проверять их выполнение, иначе никто не будет их выполнять? Как обстоят дела с выполнением этих требований? ФСТЭК проводит проверки?**

  ФСТЭК России регулярно проверяет ГИСы по всей полноте имеющихся требований. Если дистанционная работа организована неправильно, с нарушениями, то выписывается предписание, требующее устранить выявленные нарушения.

- **Требуется ли аттестация рабочего места для дистанционной работы?**

  Аттестация в обязательном порядке предусмотрена только для ГИС.

  При аттестации учитывается технология обработки информации. Если при обработке информации на АРМе обрабатывается защищаемая информации, то он аттестуется в составе ИС. На АРМе на базе Aladdin LiveOffice защищаемая информация не обрабатывается, следовательно в аттестации нет необходимости.

  В случае применения служебных СВТ они являются объектами воздействия и должны включаться в контур ИС организации. Соответственно, при проведении аттестации ГИС такие СВТ, используемые для дистанционной работы, также должны быть учтены, включены в список инвентаризации и должны проходить соответствующие процедуры аттестационных испытаний.

  В случае применения специализированных средств обеспечения безопасной дистанционной работы с использованием личных СВТ в список инвентаризации ресурсов должны включаться именно они, а не домашние СВТ, используемые лишь в качестве терминала. Личные СВТ, аттестационные испытания не проходят.

  Крайне важно, чтобы средство обеспечения безопасной дистанционной работы было сертифицированным. И важно выполнять требования эксплуатационной документации на такое средство, в частности, чтобы оно было "привязано" (авторизовано администратором) к ограниченному количеству используемых пользователем СВТ.

  Набор установленных на флешку сертифицированных СЗИ и др. компонентов не является сертифицированным средством, как пытаются утверждать некоторые недобросовестные производители таких решений.

  В остальных случаях аттестация, как форма оценки соответствия, носит добровольный характер - субъекты КИИ, операторы ИСПДн, ИС/АС вправе сами принимать решение, требуется ли им оценивать, насколько их ИС соответствует требованиям по ИБ.

- **Как обеспечить контролируемую зону в домашних условиях? 152-ю инструкцию никто не отменял…**

  Контролируемая зона должна обеспечиваться самим пользователем. На него возложена обязанность по сохранению сведений и данных при исполнении им своих функций и должностных обязанностей, в том числе и при дистанционной работе.

  Правила обеспечения контролируемой зоны должны устанавливаться самой организацией в своих организационно-распорядительных документах по защите информации, в т.ч. при дистанционной работе.

  Дистанционная работа должна рассматриваться как привилегия, как возможность поработать дома, не тратить время на дорогу, не ехать в офис, если плохо себя чувствуешь, если нужно срочно что-то сделать по работе и при этом не срываться на работу из дома. Это право сотрудника – работать дистанционно.

  Но с возникновением прав появляются и обязательства, и ответственность. Вместе с правом работать дистанционно появляется обязанность и ответственность обеспечить вокруг себя контролируемую зону.

  При дистанционной работе сотрудник должен обеспечить такой режим работы, чтобы никто из посторонних не мог видеть информацию на экране компьютера, не мог следить и считывать набираемый на клавиатуре текст и т.д.

  Не можешь обеспечить такие условия при дистанционной работе – не подключайся.

  Рекомендуется сделать памятку для пользователей по обеспечению безопасности при дистанционной работе (как, например, сделали в ФНС России).

- **Каким образом орган по аттестации будет проверять контролируемую зону, обеспеченную пользователем?**

  Орган по аттестации проверяет контролируемую зону для ГИС.

  Личный компьютер пользователя, используемый вместе с сертифицированным средством безопасной дистанционной работы, не содержит, не обрабатывает защищаемую информацию и не входит в информационную систему организации, но должен быть учтён как СВТ, с которого допускается дистанционная работа при использовании сертифицированного средства.

  Контролируемая зона должна обеспечиваться самим пользователем согласно разработанным организационно-распорядительным документам по защите информации.

  Орган по аттестации контролируемую зону в таком случае не проверяет.

- **Работодатель выдал сотруднику ноутбук, работник использует его дома автономно, без удалённого подключение к ГИС – является ли такой случай дистанционной работой со всеми вытекающими из этого требованиями?**

  В данном случае речь идёт об использовании автономного автоматизированного рабочего места (АРМ АС) вне периметра организации, на другой неконтролируемой территории, а не о дистанционной работе.

  А это уже немного другая история…

- **Сотрудник на удалёнке – является ВНУТРЕННИМ НАРУШИТЕЛЕМ? Если ДА, то почему? Он же наш сотрудник – лояльный, честно делающий свою работу, только не на работе, а дома? Такое отношение к удаленному сотруднику (что его записали как внутреннего нарушителя) не обижает сотрудников?**

  Сотрудник, работающий дистанционно, считается потенциальным внутренним нарушителем наравне с любым другим сотрудником организации

  Поэтому к обеспечению безопасной дистанционной работы и к средствам обеспечения безопасной дистанционной работы предъявляются повышенные требования, призванные снизить потенциальные риски и возможности кражи информации, утечки чувствительных служебных данных (аккаунты, пароли, настройки СЗИ и пр.) атаки на ИС организацию.

  Повышенные меры безопасности, особенно в текущих условиях, не должны никого обижать.

- **Обязательно ли обеспечивать шифрование дисков ноутбуков для удалённых пользователей?**

  При использовании специализированного средства обеспечения безопасной дистанционной работы (Aladdin LiveOffice) жёсткий диск компьютера для хранения обрабатываемой информации не используется, поэтому шифровать данные на нём не имеет смысла.
  Все разделы съёмного флеш-накопителя самого специализированного средства зашифрованы аппаратно, поэтому при утере, краже такого средства получить доступ к настройкам на нём практически невозможно, а защищаемых данных он не содержит по используемой технологии обработки информации.

  При использовании служебного ноутбука, содержащего обрабатываемую информацию, риск потерять служебные данные (параметры подключения, настройки СЗИ и пр.) существенно возрастает. Когда ноутбук выносят за пределы периметра организации, риски его кражи, утери, попадания в чужие руки (в том числе, и к специалистам технической разведки) существенно возрастают, поэтому содержимое его жёстких дисков должно быть зашифровано

  Для госструктур данной требование является обязательным.

  Субъекты КИИ и операторы ИСПДн вправе принимать решение самостоятельно, однако при проведении оценки соответствия и аттестации ИС без системы прозрачного шифрования данных на дисках, аттестовать такую ИС будет затруднительно.

  Для прозрачного шифрования дисков необходимо использовать сертифицированные средства, например, Secret Disk. Выпущены версии Secret Disk и для ОС Windows, и для российских ОС на базе Linux.

- **Накладывает ли удалённая работа из-за границы какие-либо дополнительные требования ИБ со стороны Регуляторов? Или это недопустимо?**

  В общедоступных документах ФСТЭК России каких-либо ограничений или запретов на дистанционную работу из-за границы нет.

  Ограничения могут вводится самими организациями из-за специфики и особенностей их деятельности, необходимости и обоснованности такой работы из-за границы, например, во время загранкомандировки или отпуска, при наличии служебной необходимости.
  Если надо, то специализированной сертифицированное средство позволяет это сделать.

  Ограничения на дистанционную работу могут и должны быть наложены внутренними нормативными документами организации. В качестве примера – в ФНС России дистанционная работа из-за границы запрещена внутренними организационно-распорядительными документами.

- **Почему многие Требования и другие регламентирующие документы ФСТЭК России имеют гриф ДСП и не публикуются в открытом доступе?**

  Это обусловлено спецификой взаимодействия гос. органов со своими контрагентами. Многие документы, в частности, Требования к средствам безопасной дистанционной работы предназначены исключительно для разработчиков подобных средств, а все они являются лицензиатами ФСТЭК России и могут получать подобные документы по запросу.

- **Есть в открытом доступе новые требования к средствам безопасной дистанционной работы и Приказ ФСТЭК России №32? Если нет, то почему?**

  Документы, выпускаемые ФСТЭК России, зачастую имеют ограничительную пометку для служебного пользования и не предполагают публикацию.
  Приказы относятся к документам для служебного пользования (ДСП). Требований к средствам обеспечения безопасной дистанционной работы в открытом доступе нет, получить их могут разработчики подобных средств по запросу.

- **Какие ещё средства сертифицированы ФСТЭК России на соответствие Требованиям по безопасности информации к средствам обеспечения безопасной дистанционной работы?**

  На данный момент пока единственным сертифицированным решением является Aladdin LiveOffice от компании "Аладдин Р. Д.".

- **На какие требования нужно ориентироваться коммерческим организациям, чтобы сделать дистанционную работу своих сотрудников действительно безопасной? Им обязательно использовать сертифицированные СЗИ, обязательно выполнять сложные требования регуляторов, разработанные для гос. органов?**

  Новые требования ФСТЭК России по организации безопасной дистанционной работы вобрали в себя все лучшие практики и, как и многие другие Правила, буквально "написаны кровью". К сожалению, лучше пока никто ничего не придумал.

  В новых Требованиях ФСТЭК России к средствам безопасной дистанционной работы все эти риски были просчитаны и учтены, а также прописаны способы и меры по их устранению.

  Несмотря на то, что Требования делались для гос. организаций, ФСТЭК накопил огромный опыт в этой области, прекрасно понимает цену информации во многих коммерческих структурах, понимает риски и последствия атак на ИС, утечек данных из коммерческих ИС (например, в торговых сетях, ритейле), связанные с этим риски и для государства, для граждан. Поэтому ФСТЭК готов консультировать, помогать и рекомендовать оптимальные для бизнеса решения.

  Вместе с сертифицированной версией Aladdin LiveOffice компания выпускает и кастомизируемую версию (Common Edition) для коммерческих организаций, она может быть адаптирована под существующую инфраструктуру.

  На "борт" этой версии могут ставиться несертифицированные компоненты, например, OpenVPN, Cisco AnyConnect, клиенты для работы с Citrix Workspace App, VMware Horizon и др. Коммерческая версия Aladdin LiveOffice CE существенно дешевле сертифицированной (за счёт использования несертифицированных ОС и др. компонент).

- **Если мы не ГИС и не субъект КИИ, то требования ФСТЭК на нас не распространяются, и мы можем использовать упрощённые и более дешёвые варианты решений для дистанционной работы? Например, несертифицированный VPN без ГОСТа, несертифицированные сборки Linux?**

  Да, можно.

  Выбор средств защиты своих ИС, в т.ч. и средств обеспечения дистанционного доступа, осуществляется владельцем таких ИС самостоятельно. Ответственность за возможные утечки информации и инциденты он несёт сам.

- **Много лет нам продвигалась тема BYOD (принеси и используй для работы свой девайс), многие активно это используют. ФСТЭК поддерживает эту тему или относится к ней негативно и запрещает?**

  С началом пандемии, где-то с 2020 г. ФСТЭК России как раз и допустил использование личных компьютеров для целей дистанционной работы сотрудников гос. организаций.

  Это была вынужденная мера, вызванная необходимостью продолжения работы в условиях карантина, пандемии.

  Сейчас же, после появления специализированных сертифицированных средств обеспечения безопасной работы, использование личных СВТ совершенно легально и допустимо.

- **Допустимо ли в настоящий момент рассмотрение таких решений для защиты удалённого доступа, как Check Point Harmony? Можно ли провести оценку соответствия такого продукта? Или не имеет смысл рассматривать такие решения?**

  Для ГИС использование подобных зарубежных продуктов недопустимо.

  Для коммерческих ИС ограничений нет, но ответственность ложится на компанию. Она сама должна проводить оценку соответствия решения требованиям по безопасности информации и сама нести ответственность за возможные последствия утечки информации, атаки на её ИС.

- **Можно ли использовать отечественные VPN-шлюзы, но без использования ГОСТового шифрования?**

  Если необходимость защиты информации определена законодательно (ГИС, ИСПДн, КИИ и др.), то применяемые СКЗИ (VPN) должны быть сертифицированы. В сертифицированных СКЗИ может использоваться только шифрование по ГОСТу.

- **Есть ли варианты решения для безопасной дистанционной работы для смартфонов или планшетов на базе Android, одобренные ФСТЭК России?**

  Сертифицированных или одобренных решений для мобильных платформ нет.

- **Почему при работе на недоверенном железе (домашнем компьютере) ФСТЭК считает, что можно обеспечить безопасность обработки персональных данных и служебной тайны?**

  Общая идея решения, которая обеспечила возможность безопасной дистанционной работы с подключением к государственным информационным системам и др. и работу со всеми видами служебной тайны и ДСП-информации, выглядит так: на недоверенном (личном) компьютере с внешнего защищённого носителя загружается преднастроенная замкнутая доверенная программная среда, из которой производится подключение и работа на служебном компьютере пользователя (или на виртуальном, если в организации развёрнута VDI).

При этом, все задачи и все конфиденциальные документы обрабатываются внутри организации, не покидая его периметра, а на личный компьютер по защищённому каналу "прилетают" лишь отрисованные картинки экрана, а обратно "улетают" лишь скан-коды нажимаемых клавиш и координаты указателя мыши.

Пользователь удалённо работает на своём рабочем компьютере, но в терминальном режиме, в привычной для него среде (Windows, Linux). Все документы на своих привычных местах, доступ в ГИС, АСУ ТП, ИБС, ИСПДн и др., выход в Интернет (если разрешён), переучиваться не надо.

При этом локальные ресурсы его личного компьютера – жёсткие диски, NAS, флешки, принтеры и пр., которые могут быть использованы в качестве канала утечки служебной информации, либо для атаки на ресурсы организации, в этом режиме заблокированы и недоступны. Использовать Aladdin LiveOffice можно ТОЛЬКО на авторизованных компьютерах ("привязанных" к устройству), так что если устройство попало к злоумышленнику, и он знает от него пароль, то на «незнакомом» компьютере устройство не заработает, и подключиться к ИС организации злоумышленник не сможет.

Более того, пользователь не знает, а следовательно и не сможет дискредитировать свой логин и пароль для удалённого подключения, адрес шлюза, настройки VPN и др. Пользователь также не сможет ни модифицировать преднастроенную программную среду, ни изменить её настройки, ни установить какое-то своё приложение, ни сохранить у себя, ни распечатать на локальный принтер служебный документ.

Вся работа производится на удалённом рабочем компьютере, в ИС организации. Такой режим работы достаточно безопасен.

- **Сертификат №4355 на Aladdin LiveOffice был выдан 10.02.2021, ещё до утверждения новых требований к средствам дистанционной работы, утверждённых Приказом №32 ФСТЭК России. Означает ли это, что данным сертифицированным средством можно полноценно пользоваться при дистанционной работе сотрудников с подключением к ГИС до 1-го класса защищённости, к ИСПДн до 1-го уровня защищённости? Есть какие-то условия и ограничения, требующие, например, пересертификации данного средства?**

  Дифференциация требования к средствам безопасной дистанционной работы в зависимости от класса ГИС не предусмотрена.

  Угрозы для ГИС 1-го класса или 3-го класса при дистанционной работе будут идентичны, поэтому ФСТЭК посчитал избыточным их дифференцировать. Что касается требований доверия, то это 4-й класс (УД-4).

  Это означает, что сертифицированное средство обеспечения безопасной дистанционной работы можно использовать:

  — В государственных информационных системах до 1-го класса защищённости включительно;
  — В информационных системах персональных данных до 1-го уровня защищённости персональных данных включительно;
  — В ИС значимых объектов критической информационной инфраструктуры до 1-ой категории включительно;
  — В АСУ ТП на критически важных объектах до 1-го класса защищённости включительно;
  — В информационных системах общего пользования II класса.

- **Какие виды тайн и служебных сведений можно обрабатывать с использованием сертифицированного средства дистанционной работы?**

Виды тайн и служебных сведений, с которыми можно работать дистанционно, прописаны в Формуляре сертифицированного средства, в частности:

- налоговая тайна;
- банковская тайна;
- врачебная тайна;
- нотариальная тайна;
- адвокатская тайна;
- аудиторская тайна;
- тайна страхования;
- тайна связи;
- тайна следствия и др.;
- информация о новых решениях и технических знаниях (результаты интеллектуальной деятельности);
- информация о проектных решениях и иная конфиденциальная информация, которая стала известна органу исполнительной власти или организации, проводившим экспертизу проектной документации и (или) результатов инженерных изысканий в связи с проведением экспертизы;
- информация, предоставляемая организациям (гражданам), осуществляющим производство и выпуск средств массовой информации;
- инсайдерская информация;
- информация, входящая в состав кредитной истории;
- секрет производства (ноу-хау);
- сведения о должнике, просроченной задолженности и любые другие персональные данные должника;
- информация о получателе социальных услуг;
- информация, содержащаяся в профилях и индикаторах рисков, применяемых таможенными органами;
- отдельные сведения при осуществлении закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд;
- сведения, содержащиеся в индивидуальных лицевых счетах в системе обязательного пенсионного страхования;
- информация о пенсионных счетах и др.

- **Может ли пользователь сфотографировать информацию с экрана, а затем слить её в Интернет?**

С экрана можно сделать фото. Но сфотографировать экран со служебным документом или персональными данными можно и на работе. В чем принципиальная разница – дома или на работе?

Если сотрудник пошёл на это – то это вопрос к службе внутренней безопасности, или к другому Ведомству…

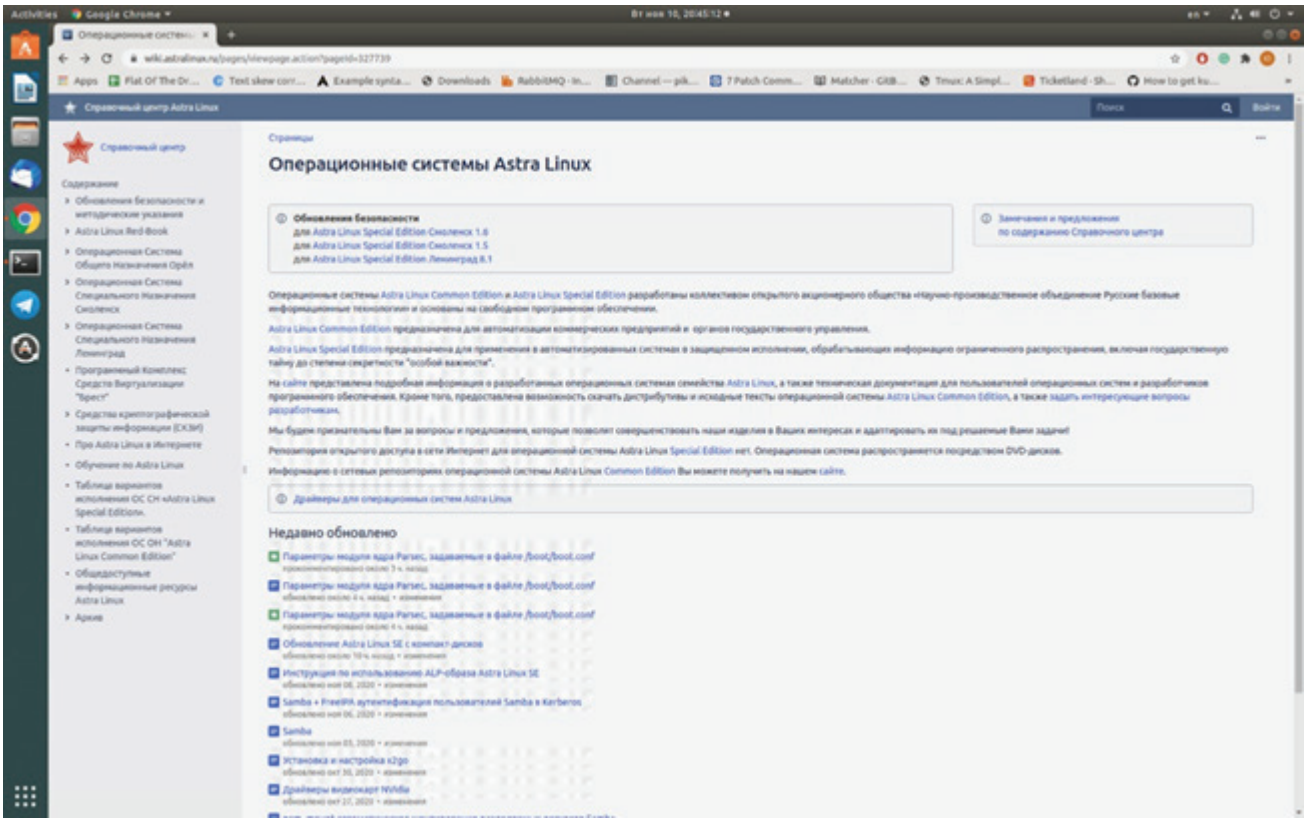
Защититься от фотографирования экрана технически сложно. Чаще, спрашивая про защиту от фотографирования экрана, имеют в виду возможность идентифицировать того, кто сфотографировал служебный документ и слил его в Интернет или в соцсети.

Для этого у компании "Аладдин Р. Д." есть дополнительное решение (опция) – водяные знаки, которые выводятся на экран, глазу они практически не заметны, но позволяют по сделанной

фотографии точно определить серийный номер устройства, на котором производилась работа, а по нему и пользователя, который это сделал.

Знание того, что наказание неотвратимо – для подобных нарушителей очень серьёзный сдерживающий фактор. Это даёт хороший положительный эффект.

Как выглядит такой экран с водяными знаками – см. ниже.



- **Требования к аппаратной части устройства достаточно сложные – наличие скрытых дисков, прозрачное шифрование данных, доверенная загрузка… Почему нельзя использовать обычную (не специализированную) флешку?**

  Средство для обеспечения безопасной дистанционной работы — это технологически сложное изделие, основу которого составляет специализированная аппаратная платформа.

  Большинство функций безопасности в ней должно быть реализовано аппаратно и защищено от внешних воздействий и атак, инвазивных и неинвазивных - иначе финальное устройство не будет безопасным – ключи шифрования и коды доступа можно будет перехватить, а сами средства бесконтрольно клонировать.

  Сделать надёжное решение с защитой от внутреннего нарушителя на базе обычной USB-флешки нельзя.

- **На сайтах нескольких российских разработчиков аналогичных решений (также применяющих технологию LiveUSB) указано, что они тоже обеспечивают безопасную дистанционную работу и используют практически такие же сертифицированные элементы – USB-токены с флешкой, ОС, VPN. Можно ли использовать их при работе с ГИС, ведь они по своим функциям очень похожи на продукт Аладдина и, более того, используют такие же сертифицированные компоненты?**

Для дистанционной работы с ГИС должны использоваться только сертифицированные решения, т.е. средства, имеющие сертификат на единое изделие, как комплекс, а не на его составные части.

Набор сертифицированных компонент, использованных для создания схожего по функциональности с LiveOffice средства, не обеспечивает необходимый уровень безопасности – это лишь голословное утверждение разработчиков. Безопасность такого средства никем не проверена и ничем не подтверждена. Такое средство не является сертифицированным средством обеспечения безопасной дистанционной работы и не должно применяться для работы с ГИС, субъектами КИИ, владельцами и операторами ИСПДн.

2. Сертифицированное решение для организации безопасной дистанционной работы – Aladdin LiveOffice

- **Есть ли ограничения на используемый ПК?**

  — Большинство ПК соответствуют требуемым характеристикам СВТ. Некоторые ограничения распространяется лишь на продукцию фирмы Apple.

- **Почему введено ограничение на количество ПК, используемых для дистанционной работы?**

  — Должен вестись строгий учёт пользовательских СВТ, на которых может проводиться именно безопасная дистанционная работа. Ограничение количества вызвано желанием упростить учёт и контроль за авторизованными домашними ПК, а также требованиями ФСТЭК.

- **Почему в составе решения отсутствует антивирус и файрволл?**

  — В сценариях применения решения данные классы программ не требуются. Создаётся замкнутая среда работы с созданием vpn тоннеля, не разрешающего никаких подключений, кроме шифрованных подключений к конкретному шлюзу, и подключением к корпоративному рабочему месту по протоколу RDP, т.е. средство работает в режиме "монитор, клавиатура, мышь".

- **Если сотрудник потеряет свою флешку Aladdin LiveOffice и её попробует использовать злоумышленник? Что будет, какие угрозы и риски для всех ИС организации?**

  — Рисков нет. Злоумышленник не сможет получить доступ к функционалу носителя, а защищаемая информация на нем отсутствует. В том числе за счёт использования жёсткой привязки админом компьютеров пользователя к устройству.

- **Много лет нам продвигалась тема BYOD (принеси и используй для работы свой девайс), многие активно это используют. Решение, которое сделал и сертифицировал Аладдин (Aladdin LiveOffice), использует технологию LiveUSB – загрузка замкнутой преднастроенной доверенной программной среды с недоверенного (домашнего – ЛИЧНОГО) компьютера сотрудника. Это, в каком-то смысле, тоже развитие технологии BYOD… Так в чём же принципиальные различия? Почему смартфон нельзя, а личный домашний ПК, на котором играют дети, могут сидеть трояны, вирусы – можно?**

  — Смартфон использовать нельзя, потому что он не подходит в качестве средства вычислительной техники, используемого для подключения защищенного носителя.

- **Дистанционная работа сейчас практически невозможна без онлайн обсуждений и совещаний по ВКС. Если Aladdin LiveOffice позволяет дистанционно работать с документами ограниченного доступа, обеспечивает замкнутую доверенную среду, то, очевидно, можно организовать и безопасные ВКС? Есть ли на этот счет какие-то специальные ограничения или требования?**

  — Для обеспечения безопасной ВКС необходимо, чтобы сервер располагался в защищённом периметре организации.

- **Снимаются ли риски эксплуатации уязвимостей домашнего роутера, недоверенных точек доступа Wi-Fi при использовании сертифицированного решения LiveOffice?**

  — Риски снимаются, трафик шифруется СКЗИ.

- **Проводилась ли оценка рисков "взлома" WiFI домашнего роутера из-за уязвимой прошивки или короткого пароля? А если у соседского парнишки Kali Linux и много энтузиазма?**

  — Конфиденциальность и целостность передаваемой информации осуществляется с использованием сертифицированного СКЗИ.

- **Насколько велик риск использования недоверенных точек WiFi в гостиницах?**

  — Риски снимаются, трафик шифруется СКЗИ.

- **Можно ли дистанционно работать с документами ограниченного доступа (ДСП), обрабатывать служебную информацию (какую)?**

  — Возможность такой работы определяется в первую очередь возможностями автоматизированной (информационной) системы, к которой подключаются с использованием данного средства. Информация обрабатывается на служебном компьютере.

- **Если сотрудник работает дистанционно (дома, или релоцировался в другую страну – ведь многие ИТишники уехали с началом СВО), сложно понять, это работает действительно он, или от его имени кто-то? Планируется ли что-то сделать для этого? Ведь угрозы постоянно меняются/возрастают?**

  — Для защиты от подобных угроз сейчас идёт разработка функционала аутентификации пользователя с помощью биометрии (третьего, дополнительного, фактора аутентификации, наряду с фактором владения носителем и знанием пароля) – датчика отпечатка пальца, встроенного в решение.

- **Обеспечивает ли набор сертифицированных средств (компонентов) решения требуемый уровень безопасности и может ли такое решение считаться сертифицированным? Если нет, то почему?**

  — Решение должно быть сертифицировано комплексно, как единый ПАК. Особенности внутренних взаимодействий между отдельными компонентами не позволяют автоматически признать всё решение сертифицированным.

- **Есть ли потребность обновлять ПО на изделии?**

  — Есть возможность обновления отдельных компонентов решения.

- **Есть ли вариант без УКЭП (может он дешевле)?**

  — Устройство может содержать сертификат УКЭП, это ключи и сертификаты в устройстве. Стоимость изделия не зависит от наличия/отсутствия УКЭП.

- **На данный момент невозможно создавать Юридическую подпись на сотрудников только на Руководителя. А многие информационные системы требуют именно такую подпись. Руководитель не может передавать ЭЦП, но и физически подписать в день более 500 документов невозможно. Как быть с ЭЦП, если передача в 3 руки невозможна?**

  — Используйте машиночитаемые доверенности (МЧД).

- **Удалённый рабочий стол подключается по какому протокол? Какая операционная система должна быть на удалённом сервере?**

  — На удалённой стороне необходим RDP сервер. В Windows он есть по умолчанию, для отечественных ОС – необходимо развернуть.

- **Какие сертифицированные ОС успешно прошли тестирование на данном устройстве? Готовое устройство будет иметь в комплекте ОС + софт или набор будет определён пользователем (в том числе разновидности ОС)?**

  — Сертифицированная ОС и все необходимое ПО включено в состав. На данный момент есть несколько базовых исполнений. Для наших заказчиков можем подготовить разные исполнения с кастомным функционалом и набором ПО.

- **А если пользователю лень будет вводить пароли для WI-FI и он не будет прерывать сессию? Против этого есть таблетка в решении?**

  — Изделие запоминает введённый однажды пароль от Wi-Fi и в следующий раз его вводить не требуется. При отключении устройства, компьютер выключается, сессия разрывается.

3. Другие рекомендуемые решения для обеспечения безопасной дистанционной работы

- **В каких рабочих сценариях "удаленки" шифрование информации на дисках рабочих станций является необходимой мерой защиты?**

  — Для предотвращения информационных утечек при дистанционной работе и гибридном графике работы необходимо использовать шифрование данных на дисках компьютеров. Продукт, который обеспечит надежную защиту информации и при этом будет "прозрачным" для авторизованных пользователей, максимально снизит риски утечки.

- **А есть ли отечественные конкуренты у решения для дистанционки Aladdin?**

  — Сертифицированных конкурентов нет.

4. Опыт ФНС России по внедрению и эксплуатации Aladdin LiveOffice

- **Сложно себе представить, что до пандемии такое крупное ведомство, как ФНС, решится на дистанционную работу своих сотрудников. Что произошло или что послужило поводом для принятия такого смелого решения?**

  — Решение назревало давно, так как была необходимость работать в любое время, включая праздники. Принимать управленческие решения необходимо быстро и в выходные, праздничные дни.

- **Решение о переходе на дистанционную работу возникло спонтанно или к нему достаточно долго и хорошо готовились? Как долго?**

  — Работа с удалённым рабочим столом нужна была всегда. В 2020 году поняли, что необходимо переводить сотрудников на дистанционную работу. Решение было принято, учитывая требования к сертификации средства для организации безопасной дистанционной работы.

- **Какие решения и технологии рассматривали и почему?**

  — Использование полностью защищенного ноутбука (с соболем и т.п.). Но они дорогие и могут быть сломаны, утеряны. Никто на себя такую ответственность брать не хочет.

- **Известно, что вы рассматривали и тестировали альтернативное решение. Почему всё-таки выбрали решение от компании "Аладдин Р. Д."?**

  — Решение Aladdin LiveOffice СЕРТИФИЦИРОВАНО, совмещает в себе простоту исполнения и использования со всем требуемым функционалом для задач ФНС по организации безопасной дистанционной работы.

- **В каждом деле всегда есть скептики, наверняка, они были и у вас. Какие у них были опасения и аргументы против перевода сотрудников на дистанционную работу?**

  — Опасения, что будут из дома копировать информацию из ГИС ФНС, но это не удалось.

- **Подтвердились ли опасения пользователей?**

  — И да, и нет. Запуск УД стал немного сложнее, поскольку Aladdin LiveOffice выдает изолированную среду, Aladdin LiveOffice не работает со стационарными ПК, не видит на них Wi-Fi, однако Ethernet видит. Провода RG45 нет ни у кого и тянуть его по квартире не хочется. Не получается скопировать информацию из ГИС.

- **Ваши аргументы в пользу выбранного решения от компании "Аладдин Р. Д."? Что стало главным фактором в принятии решения – административный ресурс или техническое решение и результаты предварительного тестирования?**

  — Самодостаточность технического решения наряду с коммерческой составляющей относительно покупки парка ноутбуков стало главным фактором выбора.

- **Как ставилась задача или формулировался ваш бизнес-кейс? Каких результатов или показателей вы должны были достичь? Что являлось критерием успеха?**

  — Была задача организовать безопасную дистанционную работу с информацией, которая содержит налоговую тайну. С применением решения Aladdin LiveOffice она была успешно решена. Количество удалённых пользователей, поддерживаемых одним сотрудником подразделения по информатизации – порядка 500 пользователей на удаленном доступе (из 1050 сотрудников).

- **Насколько сложно внедрять LiveOffice?**

  — Внедрение потребовало издания внутренних документов и регламентов, проведения обучения сотрудников. Сказать, что это было драматически сложным, нельзя.

- **Насколько возрастёт нагрузка на администраторов и не потребуется после внедрения LiveOffice ещё набирать кого-то в штат?**

  — Нагрузка будет штатной и плановой, в рамках первоначальной задачи она не потребует набирать дополнительный штат – это верно.

  — На 480 пользователей работает 1 сотрудник в Центральном Аппарате на поддержке (занимает 1-3 часа в день), не считая ЦОДа.

- **Известно, что технология LiveUSB работает далеко не на всех компьютерах (на многих нет поддержки загрузки с внешнего носителя или она сделана очень криво). Какой процент несовместимости был выявлен в рамках вашего проекта? Насколько это соотносится с обещаниями (декларациями) производителя – а то обещают одно, а на практике - совсем другое.**

  — Процент не превысил 15%, это допустимо в рамках наших потребностей.

- **Как вы поступаете, если выявляются случаи несовместимости LiveOffice и они не стартуют на чьём-то личном компьютере?**

  — В таких случаях выделяется служебный ноутбук или сотрудник выходит в офис.

- **Известно, что сертифицированные российские ОС на одно-два поколения отстают от темпов выпуска современных процессоров, и одно время они не работали на INTELовских процессорах 10-го и 11-го поколений. Какой процент подобных несовместимостей был выявлен у вас? Что-то меняется с этим в лучшую сторону?**

  — На подавляющем большинстве личных компьютеров сотрудников удалось организовать дистанционную работу. В случаях несовместимости выдавался рабочий ПК.

- **Многие пользуются личными Mac'ами, как вы поступаете в подобных случаях? Пробовали использовать LiveOffice на Mac'ах?**

  — Современные модели Mac обладают загрузчиком UEFI. Пользователь может загрузить УД не более 3- х раз. При каждой загрузке ОС для токена это новое устройство.

- **Что можно было бы доработать, что не было учтено в продукте?**

  — Текущего функционала RDP подключения достаточно для полноценной дистанционной работы. Хотелось бы видеть функционал ВКС в следующих версиях решения.

- **Рекомендовали бы решение другим заказчикам?**

  — Да, на личном опыте проверили и убедились в работоспособности решения.

- **На что надо обратить внимание при внедрении?**

  — Необходимо создать информационную и обучающую базу для пользователей;

  — Определить какие устройства (АРМ) будут исполльзоваться для УД (лучше всего подходят ноутбуки HP);

  — Определиться со скоростью интернет канала связи (нужна стабильная скорость от 10Мбит);

  — Интернет провайдер должен обеспечить работу IKE v.2 и RDP соединение.

- **Мне понравилось данное решение, но моё руководство не пойдёт на внедрение, пока не убедится собственными глазами, что оно работает, и не выяснит для себя все подводные камни. Сможете ли организовать референс-визит к вам и помочь снять внутренние недоверие? (правда, тяжело поверить, что маленькая флешка способна заменить целый ноутбук)**

  — Вопрос обсуждается индивидуально.

Аладдин

+7 (495) 223 00 01
www.aladdin.ru
aladdin@aladdin.ru
129226, Москва, ул. Докукина, 16с1