приходящих на корпоративные электронные адреса Учреждения сотрудникам или группам сотрудников, а также по мотивированным запросам прямых или непосредственных руководителей любых сотрудников, чью почту необходимо использовать в интересах Учреждения.

Использование сообщений корпоративной электронной почты в интересах Учреждения, в том числе ознакомление с содержанием сообщений, осуществляется в соответствии с правами доступа к информации, установленными внутренними Положениями о конфиденциальной информации и иными правовыми актами, регламентирующими порядок обращения с информацией ограниченного доступа.

Исходящие электронные сообщения сотрудников Учреждения должны содержать следующие поля:

- адрес получателя;
- тема электронного сообщения;
- текст электронного сообщения (вложенные файлы);
- подпись отправителя;
- предупреждение о служебном характере сообщения и его конфиденциальности.

6. Работа в сети

Доступ к сети Интернет предоставляется сотрудникам Учреждения в целях выполнения ими своих служебных обязанностей, требующих непосредственного подключения к внешним информационным ресурсам.

Для доступа сотрудников Учреждения к сети Интернет допускается применение ПО, входящего в Реестр разрешённого к использованию ПО.

При использовании сети Интернет необходимо:

- соблюдать требования настоящей Политики;
- использовать сеть Интернет исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований настоящей Политики.

При использовании сети Интернет запрещено:

- использовать предоставленный Учреждением доступ в сеть Интернет в личных целях;
- использовать несанкционированные аппаратные и программные средства, позволяющие получить несанкционированный доступ к сети Интернет;
- Совершать любые действия, направленные на нарушение нормального функционирования элементов ИС Учреждения;
- Публиковать, загружать и распространять материалы содержащие:
  - Конфиденциальную информацию, а также информацию, составляющую коммерческую тайну, за исключением случаев, когда это входит в должностные обязанности и способ передачи является безопасным, согласованным с отделом ИС СМТ;
  - угрожающую, клеветническую, непристойную информацию;
  - вредоносное ПО, предназначенное для нарушения, уничтожения либо ограничения функциональности любых аппаратных и программных средств, для осуществления несанкционированного доступа, а также ссылки на него;
  - фальсифицировать свой IP- адрес, а также прочую служебную информацию.

Учреждение оставляет за собой право блокировать или ограничивать доступ пользователей к Интернет-ресурсам, содержание которых не имеет отношения к исполнению служебных обязанностей, а также к ресурсам, содержание и направленность которых запрещены законодательством.

Блокирование и ограничение доступа пользователей к Интернет-ресурсам осуществляется на основе Регламента применения категорий Интернет-ресурсов.
Информация о посещаемых сотрудниками Учреждения Интернет-ресурсах протоколируется для последующего анализа и, при необходимости, может быть представлена Руководителям структурных подразделений, а также Руководству Учреждения для контроля.
Содержание Интернет-ресурсов, а также файлы, загружаемые из сети Интернет, подлежат обязательной проверке на отсутствие вредоносного ПО.

Шаблон 5

Политика использование мобильных устройств

Под использованием мобильных устройств (например, ноутбуков, планшетов и мобильных телефонов) и носителей информации в ИС Учреждения понимается их подключение к инфраструктуре ИС с целью обработки, приёма/передачи информации между ИС и мобильными устройствами, а также носителями информации.
На предоставленных Учреждением мобильных устройствах допускается использование ПО, входящего в Реестр разрешённого к использованию ПО.
К предоставленным Учреждением мобильным устройствам и носителям информации предъявляются те же требования ИБ, что и для стационарных АРМ. Целесообразность дополнительных мер обеспечения ИБ определяется отделом ИС СМТ.
При использовании предоставленных Учреждением мобильных устройств и носителей информации, сотрудник обязан:

- соблюдать требования настоящей Политики;
- использовать мобильные устройства и носители информации исключительно для выполнения своих служебных обязанностей;
- ставить в известность отдел ИС СМТ о любых фактах нарушения требований настоящей Политики;
- эксплуатировать и транспортировать мобильные устройства и носители информации в соответствии с требованиями производителей;
- обеспечивать физическую безопасность мобильных устройств и носителей информации всеми разумными способами;
- извещать отдел ИС СМТ о фактах утраты (кражи) мобильных устройств и носителей информации.

При использовании предоставленных сотрудника Учреждения мобильных устройств и носителей информации запрещено:

- использовать мобильные устройства и носители информации в личных целях;
- передавать мобильные устройства и носители информации другим лицам (за исключением администраторов ИС и ИБ);
- оставлять мобильные устройства и носители информации без присмотра, если не предприняты действия по обеспечению их физической безопасности.

Любое взаимодействие (обработка, приём\передача информации) инициированное сотрудником Учреждения между ИС и неучтёнными (личными) мобильным и устройствами, а также носителями информации, рассматривается как несанкционированное (за исключением случаев, оговорённых с администраторами ИС заранее). Учреждение оставляет за собой право блокировать или ограничивать использование таких устройств и носителей информации;
Информация об использовании сотрудниками Учреждения мобильных устройств и носителей информации в ИС протоколируется и, при необходимости, может быть представлена Руководителям структурных подразделений, а также руководству Учреждения.
Информация, хранящаяся на предоставляемых Учреждением мобильных устройствах и носителях информации, подлежит обязательной проверке на отсутствие вредоносного ПО.

В случае увольнения, предоставленные ему мобильные устройства и носители информации изымаются.
Перечень разрешенного программного обеспечения в мобильных устройствах определен в Приложении № 5 к настоящей Политике.

Шаблон 6

Политика защиты от вредоносного ПО

Отдел ИС СМТ регулярно проверяет сетевые ресурсы Учреждения антивирусным программным обеспечением и обеспечивает защиту входящей электронной почты от проникновения вирусов и другого вредоносного ПО.

При возникновении подозрения на наличие компьютерного вируса (нетипичная работа программ, появление графических и звуковых эффектов, искажений данных, пропадание файлов, частое появление о системных ошибках, увеличение исходящего/входящего трафика и т.п.) сотрудник Учреждения должен незамедлительно оповестить об этом отдел ИС СМТ. После чего администратор ИБ должен провести внеочередную полную проверку на вирусы рабочей станции пользователя, проверив, в первую очередь, работоспособность антивирусного ПО.

В случае обнаружения при проведении антивирусной проверки заражённых компьютерными вирусами файлов сотрудники подразделений обязаны:

- приостановить работу;
- немедленно поставить в известность о факте обнаружения заражения своего руководителя и отдел ИС СМТ, а также владельца файла и смежные подразделения, использующие эти файлы в работе.
- Совместно с владельцем зараженных вирусом файлов провести анализ необходимости дальнейшего их использования.

Правила предупреждения вирусного заражения в ГИС «Бухгалтерия и кадры» определены в Инструкции пользователя по обеспечению безопасности информации при её обработке в ИС.

Шаблон 7

Политика управления установкой (инсталяцией) компонентов программного обеспечения

В ГИС «Бухгалтерия и кадры» разрешено использование только того программного обеспечения, его компонентов, утилит и драйверов, которые необходимы для обеспечения функционирования информационной системы, а также необходимы для выполнения служебных (должностных) обязанностей пользователями.

Установка программного обеспечения, его компонент, утилит и драйверов осуществляется только системными администраторами или администратором безопасности в соответствии с Приложением № 7. Пользователям запрещена установка любого ПО в ГИС «Бухгалтерия и кадры».

Пользователь имеет право подать заявку в виде служебной записки на включение в список разрешенного в ГИС программного обеспечения, необходимых ему для выполнения служебных (должностных) обязанностей программ, утилит, драйверов. В такой служебной записке обязательно указывается обоснование необходимости включения в этот список нового программного обеспечения. Срок рассмотрения заявки должен составлять не более 3 рабочих дней.

Администратор ежемесячно с помощью инструмента XSpider 7.8.24 проводит проверку соответствия состава программного обеспечения в ГИС «Бухгалтерия и кадры» списку разрешенного ПО. В случае выявления постороннего программного обеспечения, созывается группа реагирования на инциденты информационной безопасности, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

На серверной части ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

На АРМ Пользователей ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

На АРМ Администратора ГИС «Бухгалтерия и кадры» при загрузке операционных систем серверов запускается следующее программное обеспечение:

- MS SQL Server;
- IIS;
- ...

Шаблон 8

Политика обеспечения доверенной загрузки средств вычислительно техники

В {Название Организации} в качестве средства доверенной загрузки технических средств применяется {Название МДЗ}. {Убрать, если применяются компенсирующие меры}

Для работы с ресурсами ГИС «Бухгалтерия и кадры» выбираются такие технические средства, базовая система ввода-вывода которых (BIOS/UEFI) позволяет отключить возможность выбора источника загрузки в обход настроек BIOS/UEFI (вызов вариантов источников загрузки одной из функциональных клавиш).

Администратор контролирует работоспособность {Название МДЗ} в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяются компенсирующие меры}

В случае некорректной работы средства доверенной загрузки на техническом средстве, такое техническое средство изымается из ГИС на время проведения ремонта/замены средства доверенной загрузки. В случае необходимости продолжения работы на техническом средстве, применяются следующие компенсирующие меры {Убрать, если применяются компенсирующие меры}:

- опечатываются USB-порты, входы для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводы и сами технические средства;
- устанавливается пароль администратора на вход в BIOS/UEFI и отключается возможность вызова источника загрузки нажатием функциональной клавиши (F1-F12) при загрузке;
- устанавливается усиленный визуальный контроль за техническим средством.

В проектной документации на систему защиты информации в ГИС «Бухгалтерия и кадры» обосновано применение компенсирующих мер, нейтрализующих угрозы безопасности информации, связанные с недоверенной загрузкой технических средств ГИС. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется опечатывание USB-портов, входов для SD/Micro-SD и других карт памяти, CD/DVD/Blu-Ray-приводов и самих технических средств. Данная мера обеспечивает контроль доступа злоумышленника к интерфейсам ввода-вывода, позволяющим осуществить недоверенную загрузку. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется установка пароля администратора на вход в BIOS/UEFI и отключение возможности вызова источника загрузки во время загрузки технического средства. Данная мера позволяет блокировать на программном уровне изменение источника загрузки при срыве пломбы с интерфейса ввода-вывода. {Убрать, если применяется МДЗ}

В качестве компенсирующей меры в ГИС «Бухгалтерия и кадры» применяется усиленный визуальный контроль за техническими средствами ГИС. Данная мера позволяет своевременно детектировать факты нарушения пломб технического средства, выявлять факты несанкционированного доступа и принимать меры реагирования. {Убрать, если применяется МДЗ}

Администратор контролирует выполнение компенсирующих мер в соответствии с планом периодических мероприятий по контролю защищенности информации. По результатам проверки делается запись в журнал периодического тестирования средств защиты информации. {Убрать, если применяется МДЗ}

Шаблон 9

Политика использования криптографического контроля

Все, поступающие в Учреждение, СКЗИ должны быть учтены в соответствующем журнале поэкземплярного учёта СКЗИ.

В Учреждении должно осуществляться управление ключами для эффективного применения криптографических методов. Компрометация или потеря криптографических ключей может привести к нарушению конфиденциальности, подлинности и/или целостности информации.

Все ключи должны быть защищены от изменения, утери и уничтожения. Кроме того, секретные и закрытые ключи должны быть защищены от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Соглашения с внешними поставщиками криптографических услуг (например, удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Криптографические системы и методы следует использовать для защиты конфиденциальной информации, когда другие средства контроля не обеспечивают адекватной защиты.

Для критической информации должно использоваться шифрование при их хранении в базах данных или передаче по коммерческим или открытым сетям, таким как Интернет.

Шифрование любой другой информации в ИС Учреждения должно осуществляться только после получения письменного разрешения на это.

1. Требований по обеспечению ИБ при использовании шифрования

Шифрование – это криптографический метод, который может использоваться для обеспечения защиты конфиденциальной, важной или критичной информации.

СКЗИ должны поставляться разработчиками с полным комплектом эксплуатационной документации, включающей описание ключевой системы, правила работы с ней и обоснование необходимого организационно-штатного обеспечения.

Порядок применения СКЗИ определяется руководством Учреждения и должен включать:

- порядок ввода в действие, включая процедуры встраивания СКЗИ в ИС;
- порядок эксплуатации;
- порядок восстановления работоспособности в аварийных случаях;
- порядок внесения изменений;
- порядок снятия с эксплуатации;
- порядок управления ключевой информацией;
- порядок обращения с ключевой информацией, включая действия при смене и компрометации ключей.

Для шифрования конфиденциальной информации минимально допустимой длинной ключа является 128 бит.

При использовании шифрования в ИС Учреждения должны применяться только утверждённые стандартные алгоритмы и сертифицированные ФСБ России продукты, их реализующие.

2. Электронные цифровые подписи

ЭЦП обеспечивают защиту аутентификации и целостности электронных документов.

ЭЦП могут применяться для любой формы документа, обрабатываемого электронным способом. ЭЦП должны быть реализованы при использовании криптографического метода, основывающегося на однозначно связанной паре ключей, где один ключ используется для создания подписи (секретный/личный ключ), а другой – для проверки подписи (открытый ключ).

Необходимо с особой тщательностью обеспечивать конфиденциальность личного ключа, который следует хранить в секрете, так как любой, имеющий к нему доступ, может подписывать документы (платежи, контракты), тем самым фальсифицируя подпись владельца ключа. Защиты целостности открытого ключа должна обеспечиваться при использовании сертификата открытого ключа.

Криптографические ключи, используемые для цифровых подписей, должны отличаться от тех, которые используются для шифрования.

При использовании ЭЦП, необходимо учитывать требования действующего законодательства Российской Федерации, определяющего условия, при которых цифровая подпись имеет юридическую силу.

3. Управление ключами

Управление криптографическими ключами важно для эффективного использования криптографических средств.

Любая компрометация или потеря криптографических ключей может привести к компрометации конфиденциальности, подлинности и/или целостности информации. Следует применять систему защиты для обеспечения использования в ИС Учреждения криптографических методов в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и личный ключ (который должен храниться в секрете). Методы с открытыми ключами должны использоваться для шифрования и для генерации цифровых подписей.

Ключи необходимо защищать от изменения и разрушения, а секретным и личным ключам необходима защита от неавторизованного раскрытия. Криптографические методы могут также использоваться для этой цели. Физическую защиту следует применять для защиты оборудования, используемого для изготовления, хранения и архивирования ключей.

Сервер сертифицированного центра КУЦ должен хранить текущие открытые ключи для всех авторизованных на это сотрудников. Для безопасного взаимодействия с внешними пользователями ИС Учреждения необходимо использовать электронные сертификаты только из утверждённого списка сертифицированных центров.

Секретные ключи пользователей должны храниться так же, как и пароли. О любом подозрении на компрометацию секретного ключа пользователь должен немедленно доложить в отдел ИС СМТ.

Необходимо, чтобы система обеспечения безопасности использования ключей основывалась на согласовании способов, процедур и безопасных методов для:

- генерации ключей при использовании различных криптографических систем и приложений;
- генерации и получения сертификатов открытых ключей;
- рассылки ключей, предназначенных пользователям, включая инструкции по их активации при получении;
- хранения ключей (при этом необходимо наличие инструкции авторизованным пользователям для получения доступа к ключам);
- смены или обновления ключей, включая правила порядка и сроков смены ключей;
- порядка действий в отношении скомпрометированных ключей;
- аннулирования ключей, в том числе способы аннулирования или дезактивации ключей, если ключи были скомпрометированы или пользователь уволился из организации (в этом случае ключи необходимо архивировать);
- восстановление ключей, которые были утеряны или испорчены, для рассекречивания зашифрованной информации;
- архивирования и резервного копирования ключей;
- разрушения ключей;
- регистрация ключей и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации, для ключей необходимо определить даты начала и конца действия, чтобы их можно было использовать лишь в течении ограниченного периода времени, который зависит от обстоятельств использования криптографических средств, контроля и от степени риска раскрытия информации.

Может потребоваться наличие процедур обработки юридических запросов, касающихся доступа к криптографическим ключам, например, чтобы зашифрованная информация стала доступной в незашифрованном виде для доказательств в суде.

Необходимо обеспечивать защиту открытых ключей от угроз подделывания цифровой подписи и замены открытого ключа пользователя своим. Эта проблема решается с помощью сертификата открытых ключей. Сертификаты необходимо изготавливать таким способом, который однозначно связывал бы информацию, относящуюся к владельцу пары

открытого/секретного ключей, с открытым ключом. Поэтом важно, чтобы процессу управления, в рамках которого формируются эти сертификаты, можно было доверять.

Соглашения с внешними поставщиками криптографических услуг (например, с удостоверяющими центрами) об уровне предоставляемого сервиса должны охватывать вопросы ответственности, надёжности сервиса и времени реакции при предоставлении сервиса.

Шаблон 10

Политика резервного копирования

Резервирование информационных ресурсов (программного обеспечения, баз данных, средств защиты информации) ГИС «Бухгалтерия и кадры» осуществляется в соответствии с инструкцией администратора безопасности информации и в соответствии с Приложением № 10 к настоящей Политике.

Администратор осуществляет с периодичностью, установленной в плане мероприятий по обеспечению режима защиты информации проверку работоспособности средств резервного копирования, средств хранения резервных копий и средств восстановления информации из резервных копий. По результатам проверки делается запись в журнале учета мероприятий по контролю за соблюдением режима защиты информации. В случае выявления проблем с системой резервирования, принимаются меры по восстановлению ее работоспособности. После восстановления работоспособности системы резервирования осуществляется внеплановое резервное копирование всех информационных ресурсов ГИС «Бухгалтерия и кадры».

Резервирование технических средств осуществляется в соответствии с проектной документацией (эскизным проектом) на систему защиты информации ГИС «Бухгалтерия и кадры».

Восстановление из резервных копий является основным методом восстановления работоспособности информационной системы после ликвидации нештатных ситуаций.

Нештатными ситуациями являются:

- разглашение информации ограниченного доступа сотрудниками {Название Организации}, имеющими к ней право доступа, в том числе:
  - разглашение информации лицам, не имеющим права доступа к защищаемой информации;
  - передача информации по незащищенным каналам связи;
  - обработка информации на незащищенных технических средствах обработки информации;
  - опубликование информации в открытой печати и других средствах массовой информации;
  - передача носителя информации лицу, не имеющему права доступа к ней;
  - утрата носителя с информацией.
- неправомерные действия со стороны лиц, имеющих право доступа к защищаемой информации:
  - несанкционированное изменение информации;
  - несанкционированное копирование информации;
- несанкционированный доступ к защищаемой информации:
  - несанкционированное подключение технических средств к средствам и системам ГИС «Бухгалтерия и кадры»;
  - использование закладочных устройств;

- использование злоумышленником легальных учетных записей пользователей для доступа к информационным ресурсам ГИС «Бухгалтерия и кадры»;
- использование злоумышленником уязвимостей программного обеспечения ГИС;
- использование злоумышленником программных закладок;
- заражение ГИС злоумышленником программными вирусами;
- хищение носителей информации;
- нарушение функционирования технических средств обработки информации;
- блокирование доступа к защищаемой информации путем перегрузки технических средств обработки информации ложными заявками на ее обработку;
- дефекты, сбои, отказы, аварии технических средств и систем ГИС;
- дефекты, сбои, отказы программного обеспечения ГИС;
- сбои, отказы и аварии систем обеспечения ГИС;
- природные явления, стихийные бедствия:
  - термические, климатические факторы (аномально низкие или аномально высокие температуры воздуха, пожары, наводнения, снегопады и т. д.);
  - механические факторы (повреждения зданий, землетрясения и т. д.);
  - электромагнитные факторы (отключение электропитания, скачки напряжения, удары молний и т. д.).

В случае возникновения нештатной ситуации, порядок действий при которой не регламентирован настоящей Политикой, Администратором, Ответственным и ГРИИБ вырабатывается конкретный план действий с учетом текущей ситуации.

Порядок оповещения должностных лиц и сроки выполнения мероприятий при нештатных ситуациях определены в Приложении № 11 настоящей Политики.

С целью усовершенствования координации действий должностных лиц по реагированию на нештатные ситуации должны проводиться регулярные тренировки по различным видам нештатных ситуаций. В случае выявления по результатам тренировок изъянов в положениях настоящей Политики, касающихся реагирования на нештатные ситуации, в нее могут вноситься изменения.

Инциденты безопасности информации также являются нештатной ситуацией. При выявлении нештатных ситуаций, повлекших нарушение целостности, доступности или конфиденциальности защищаемой информации по вине внутреннего или внешнего нарушителя, созывается ГРИИБ, которая действует в соответствии с инструкцией по реагированию на инциденты информационной безопасности.

В случае сбоев, отказов и аварий систем электроснабжения, вентиляции, других обеспечивающих инженерных систем предпринимаются следующие действия:

- корректное отключение технических средств ГИС до истощения ресурса источников бесперебойного питания, перегрева технических средств и до наступления других негативных последствий;
- предпринимаются меры по устранению причин, вызвавших сбои, отказы и аварии средств и систем ГИС а также меры по замене/ремонту вышедших из строя средств и систем;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации, Администратор восстанавливает их из резервных копий.

В случае нештатных ситуаций, связанных со стихийными бедствиями и деструктивными природными явлениями выполняются следующие действия:

- Пользователи корректно отключают и обесточивают свои рабочие места;
- системные администраторы корректно отключают и обесточивают серверы и сетевое оборудование;
- Администратор предпринимает меры к эвакуации носителей информации и носителей резервных копий;
- в случае нарушения корректной работы технических средств в ГИС в результате стихийных бедствий или природных явлений принимаются меры по ремонту/замене вышедшего из строя оборудования;
- в случае потери/утраты защищаемых данных или нарушения целостности программного обеспечения, баз данных, средств защиты информации в результате стихийных бедствий или природных явлений, Администратор восстанавливает их из резервных копий;
- в случае стихийных действий/природных явлений, опасных для жизни человека в первую очередь организуется эвакуация сотрудников и только по возможности организуется эвакуация технических средств, носителей информации и носителей с резервными копиями.

Шаблон 11

Политика контроля состава технических средств, программного обеспечения и средств защиты информации

Состав технических средств (далее – ТС), программного обеспечения (далее – ПО) и средств защиты информации (далее – СрЗИ) ГИС «Бухгалтерия и кадры» фиксируется в техническом паспорте на информационную систему. Технический паспорт является эталоном состава ТС, ПО и СрЗИ, по которому осуществляется периодический контроль.

В случае добавления новых ТС, ПО и СрЗИ в состав ГИС «Бухгалтерия и кадры» или удаления существующих компонентов, на основании акта ввода в эксплуатацию (или акта вывода из эксплуатации) максимально оперативно вносятся изменения в Технический паспорт.

Администратор осуществляет контроль состава ТС, ПО и СрЗИ не реже одного раза в месяц.

Выявление несоответствия состава ТС, ПО и СрЗИ техническому паспорту ГИС «Бухгалтерия и кадры» является инцидентом безопасности. В случае выявления фактов несоответствия Администратор устанавливает причины самостоятельно или созывает ГРИИБ.

В случае выявления несоответствия состава ТС, ПО и СрЗИ, Администратор принимает меры по оперативному исключению (восстановлению) из состава (в составе) информационной системы несанкционированно установленных (удаленных) технических средств, программного обеспечения и средств защиты информации.

Администратор осуществляет контроль выполнения условий и сроков действия сертификатов соответствия на средства защиты информации и принимает меры, направленные на устранение выявленных недостатков. В случае, если сертификат соответствия истек, но был продлен производителем СрЗИ, Администратор запрашивает актуальную заверенную копию сертификата. В случае, если сертификат соответствия истек, но не был продлен производителем СрЗИ, то Администратор сообщает об этом руководителю {Название Организации}, который принимает решение об организации самостоятельной сертификации используещегося СрЗИ, либо об обновлении используещегося СрЗИ до актуальной версии, либо о замене используещегося СрЗИ на другое аналогичное сертифицированное СрЗИ.

Шаблон 12

Политика дистанционной работы

1. Ответственность

Ответственность за установку, настройку и администрирование средств обработки информации на рабочем месте пользователя возлагается на службу информационных технологий или иную службу {Название Организации}.

Ответственность за соблюдение правил или политики организации рабочего места возлагается на всех работников фирмы и третьих лиц, использующих средства обработки информации.

Контроль выполнения политики организации рабочего места возлагается на службу информационной безопасности {Название Организации}.

Провести анализ

2. Назначение и область действия

Настоящая политика устанавливается для эффективной организации дистанционной работы пользователей в целях:

- Защиты сетевых сервисов;
- Предотвращения неавторизованного доступа к операционным системам;
- Обеспечение информационной безопасности при работе в дистанционном режиме.

Правила распространяются на всех работников фирмы и третьих лиц, участвующих в организации работы и работающих в дистанционном режиме, и являются обязательными для исполнения.

Все исключения из настоящих правил должны быть согласованы со службой информационной безопасности {Название Организации}..

3. Основные требования

Предоставление пользователю дистанционного доступа должно быть согласовано с руководителем подразделения данного сотрудника и владельцем информационных ресурсов, к которым предоставляется доступ. Управление дистанционным доступом осуществляется в соответствии с установленными процедурами.

Для контроля доступа пользователя в дистанционном режиме должны использоваться надежные методы аутентификации, включая:

- обратный вызов;
- аутентификацию узла по физическому адресу;
- решения для VPN;
- выделенные физические линии и т.д.

При использовании обратного вызова должна быть блокирована возможность переадресации

Доступ в дистанционном режиме обязательно организуется с использованием установленных средств шифрования траффика.

Дистанционный доступ к используемым диагностическим и конфигурационным портам оборудования должен регистрироваться. Возможность дистанционного доступа к неиспользуемым диагностическим или конфигурационным портам оборудования должна быть исключена.

Для сеансов дистанционного доступа должно быть установлено время бездействия, во время которого оборудование отключается, и сеанс работы прекращается.

Для критических приложений должно использоваться ограничение времени соединения дистанционного доступа.

Обязательными условиями предоставления дистанционного доступа к информационным ресурсам фирмы являются:

- Установка и своевременное обновление на компьютере пользователя средств антивирусной защиты.
- Установка и надлежащая настройка на компьютере пользователя применяемых в фирме или организации средств предотвращения атак.

Настройка локальных параметров безопасности на компьютере пользователя в соответствии с применяемыми в компании групповыми политиками безопасности.

4. Ответственность

Ответственность за организацию работы в дистанционном режиме возлагается на службу информационных технологий {Название Организации}.

Ответственность за соблюдение правил возлагается на всех сотрудников фирмы и третьих лиц, работающих в дистанционном режиме. Контроль выполнения и пересмотр политики возлагается на службу безопасности информации. Провести анализ

Шаблон 13

Политика использования сетевых служб

Политика сетевой безопасности в {Название Организации} представляет совокупность положений, правил и лабораторных приемов, устанавливающих подход организации к использованию ее сетевых ресурсов и определяющих, как следует обеспечивать защиту ее сетевой инфраструктуры и сервисов.

Политика сетевой безопасности {Название Организации} включает:

- политику доступа к сетевым сервисам;
- политику реализации межсетевых экранов.

Политика доступа к сетевым сервисам определяет список сервисов Интернет, к которым пользователи должны иметь ограниченный доступ. Под сервисами Интернет будем понимать сервисы, предоставляемые в сети Интернет пользователям, программам, системам, уровням, функциональным блокам. Наиболее распространенными сервисами являются хранение данных, передача сообщений и блоков данных, электронная и речевая почта, предоставление соединений, видеосервис.

Необходимо ограничение методов доступа, чтобы пользователи не могли обращаться к «запрещенным» сервисам Интернет обходными путями. Набор обходных путей зависит от политики безопасности для данного межсетевого экрана.

Политика реализации межсетевых экранов определяет правила доступа к ресурсам внутренней сети. Правила доступа к внутренним ресурсам должны базироваться на одном из следующих принципов:

- запрещать все, что не разрешено в явной форме;
- разрешать все, что не запрещено в явной форме.

Реализация межсетевого экрана на основе обоих принципов.

Шаблон 14

Политика по работе с инцидентами информационной безопасности

Политика разработана в целях выявления, предотвращения и устранения последствий нарушений законодательства Российской Федерации в области обработки конфиденциальной информации.

1. Инциденты в области информационной безопасности возникают при нарушении правил и требований информационной безопасности.

В ходе инцидента реализуются (или создается возможность для реализации) угрозы информационной безопасности, что, как правило, приводит к нанесению вреда активам {название организации}.

Работа с инцидентами в области информационной безопасности помогает определить наиболее актуальные угрозы информационной безопасности и создает обратную связь в системе обеспечения информационной безопасности, что способствует повышению общего уровня защиты информационных ресурсов информационных систем персональных данных.

Работа с инцидентами включает в себя 3 направления:

- выявление инцидентов в области информационной безопасности;
- реакция на инциденты в области информационной безопасности;
- предупреждение инцидентов в области информационной безопасности.

2. Выявление инцидентов в области информационной безопасности

Работа по выявлению инцидентов в области информационной безопасности включает в себя мероприятия, направленные на:

- выявление инцидентов в области информационной безопасности с помощью технических средств;
- выявление инцидентов в области информационной безопасности в ходе мероприятий по контролю за обработкой персональных данных;
- выявление инцидентов с помощью персонала {название организации}.

3. Реакция на инциденты в области информационной безопасности

Реакция на инциденты в области информационной безопасности включает в себя:

- фиксацию инцидента в области информационной безопасности;
- определение границ инцидента и ущерба (в том числе потенциального) от реализации угроз информационной безопасности в ходе инцидента;
- ликвидация последствий инцидента и полное либо частичное возмещение ущерба;
- наказание виновных в инциденте информационной безопасности.

4. Предупреждение инцидентов в области информационной безопасности

Предупреждение инцидентов строится на:

- планомерной деятельности по повышению уровня осознания информационной безопасности руководством и сотрудниками {название организации};
- проведения мероприятий по обучению сотрудников {название организации} правилам и способам работы со средствами защиты информационных систем персональных данных;
- доведении до сотрудников норм законодательства в области защиты персональных данных и внутренних документов {название организации}, устанавливающих ответственность за нарушение требований информационной безопасности;
- разъяснительной работе с увольняющимися сотрудниками и сотрудниками, принимающимися на работу;
- своевременной модернизации системы обеспечения информационной безопасности информационных систем персональных данных с учетом возникновения новых угроз информационной безопасности;
- своевременном обновлении программного обеспечения, в т. ч. баз сигнатур антивирусных средств.

5. Причины инцидентов в области информационной безопасности

Причинами инцидентов в области информационной безопасности являются:

- действие враждебных интересам {название организации} организаций и отдельных лиц;
- отсутствие персональной ответственности за обеспечение информационной безопасности персональных данных сотрудников {название организации} их руководителей;
- недостаточная работа с персоналом по обеспечению необходимого режима соблюдения конфиденциальности персональных данных;
- отсутствие моральной и материальной стимуляции за соблюдение правил и требований информационной безопасности;

- недостаточная техническая оснащённость подразделений, ответственных за обеспечение информационной безопасности;
- совмещение функций по разработке и сопровождению или сопровождению и контролю за информационными системами;
- наличие привилегированных бесконтрольных пользователей в информационной системе;
- пренебрежение правилами и требованиями информационной безопасности сотрудниками {название организации};
- и другие причины.

6. Расследование инцидентов в области информационной безопасности

Расследование инцидентов в области информационной безопасности должно включать в себя:

- формирование комиссии по расследованию инцидента в области информационной безопасности;
- определение границ инцидента – информационных ресурсов, технических средств и персонала, затронутых инцидентом;
- определение причин инцидента, факторов, влияющих на возникновение инцидента;
- определение участников инцидента;
- определение последствий инцидента;
- составление заключения по результатам расследования;
- выработка рекомендаций по предотвращению возникновения подобных инцидентов в будущем.

7. Работа с персоналом по предупреждению инцидентов

Как правило, самым слабым звеном в любой системе безопасности является человек. Наличие современных доступных способов воздействия на персонал {название организации}, таких как социальная инженерия, фишинг, подмена электронных идентификаторов, номеров телефонов и т. д., делает пользователя информационной системы персональных данных частым объектом внимания злоумышленника. Поэтому направление работы с персоналом является основным направлением работы подразделений информационной безопасности.

В работе с персоналом основной упор должен делаться не на наказание сотрудника за нарушения в области информационной безопасности, а на поощрение за надлежащие выполнение требований информационной безопасности, проявление личной инициативы в укреплении системы информационной безопасности.

Персонал {название организации} является так же важным источником сведений об инцидентах информационной безопасности. Поэтому необходимо донести до сотрудников информацию о том, что оперативно предоставленные сведения об инциденте информационной безопасности являются поводом для смягчения либо отмены наказания за нарушение требований информационной безопасности.

Частой причиной инцидентов информационной безопасности является личная обида подчиненных на своих руководителей, либо коллег. Поэтому благоприятный микроклимат в коллективе является необходимым фактором обеспечения информационной безопасности в организации.

Шаблон 15

Политика обеспечения непрерывности ИТ-сервисов

Настоящая политика устанавливает принципы менеджмента непрерывности ИТ-сервисов в {название организации}. Процесс Управления Непрерывностью ИТ-сервисов входит в общий Процесс Менеджмента Непрерывностью Бизнеса (МНБ).

Политика МНБ определяет следующие процессы:

- организационную деятельность по установлению способности к непрерывности бизнеса;
- непрерывный менеджмент и поддержку способности к обеспечению непрерывности бизнеса.

1. Организационная деятельность включает в себя установление требований и полного цикла непрерывности бизнеса от проектирования, построения, внедрения до первоначального применения проверки способности организации к непрерывности бизнеса.

2. Непрерывная поддержка и менеджмент включают в себя: внедрение непрерывности бизнеса в организации; проведение регулярных учений по применению планов обеспечения непрерывности бизнеса; актуализацию и обмен информацией в соответствии с этим планом, особенно, если происходят существенные изменения в производственных площадях, персонале, организационной структуре, производственных и технологических процессах или рыночных условиях.

3. Цели применения

Политика в области МНБ должна соответствовать природе, масштабу, сложности, географии и критичности видов деятельности организации, отражать ее культуру, взаимосвязанные области и деловую среду. Политика в области МНБ определяет требования к процессу обеспечения непрерывности бизнеса и должна обеспечивать соответствие действий в области непрерывности бизнеса потребностям организации в случае возникновения инцидента, а также развитие способности организации к непрерывности бизнеса. Способность к МНБ должна быть интегрирована в деятельность организации по управлению изменениями таким образом, чтобы способность к непрерывности бизнеса способствовала росту номенклатуры продукции и объема услуг.

4. Основные положения политики непрерывности бизнеса

Политика в области непрерывности бизнеса должна обеспечивать организации документированные принципы и цели, к которым должна стремиться организация и, на соответствие которым, необходимо проводить измерение способности к непрерывности бизнеса. Политика в области МНБ утверждается руководителем организации {название организации}, например, генеральным директором или председателем совета директоров.

В области МНБ организацией {название организации} определены:

- области применения МНБ в организации;
- необходимые ресурсы для МНБ;
- принципы, руководящие указания и минимальное количество стандартов организации в области МНБ;

- ссылки на соответствующие стандарты, инструкции или другие нормативные акты организации, которые должны быть включены в документы или могут быть использованы как точки отсчета.

Организация {название организации} должна поддерживать в рабочем состоянии политику, стратегии, планы и решения в области МНБ и проводить их анализ через запланированные интервалы времени в соответствии с потребностями организации.

5. Распределение ответственности и полномочий

Высшее руководство организации {название организации} должно назначить:

- лицо из числа высшего руководства, наделенное соответствующими полномочиями, ответственное за политику в области МНБ и ее внедрение;
- одного или несколько лиц, ответственных за выполнение и поддержку программы МНБ.

Обязанности, подотчетность, ответственность и полномочия персонала должны быть установлены в рабочих и должностных инструкциях.
Анализ этих обязанностей необходимо проводить в процессе аудита организации.

Надлежащее выполнение обязанностей в области обеспечения непрерывности бизнеса может быть усилено путем их включения в политику организации в области аттестации, компетентности и поощрения персонала.

6. Осуществление непрерывности бизнеса в организации

Деятельность по выполнению программы непрерывности бизнеса должна включать в себя проектирование, разработку и внедрение программы.
Организация должна осуществлять следующие действия:
- обмен информацией о программе с причастными сторонами;
- организацию и/или обеспечение соответствующего обучения персонала;
- проведение учений по обеспечению непрерывности бизнеса (см. раздел 9).

5.3.2 Организация может адаптировать признанные методы менеджмента для обеспечения эффективного управления программой непрерывности бизнеса.

13. Порядок действий сотрудников (персонала) банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций

Порядок действий сотрудников (персонала) головного офиса банка и перечень мероприятий, которые должны быть выполнены в момент и после возникновения нестандартных и чрезвычайных ситуаций, определён приложениями к настоящей политике с учётом особенности и причин возникновения нестандартных и чрезвычайных ситуаций.

Шаблон 16

Политика обеспечения восстановления

В Учреждении должны быть разработаны и реализованы планы, которые позволят продолжить или восстановить операции и обеспечить требуемый уровень доступности информации в установленные сроки после прерывания или сбоя критически важных бизнес-процессов.

В каждом плане поддержки непрерывности бизнеса должны быть чётко указаны условия начала его исполнения и сотрудники, ответственные за выполнение каждого фрагмента плана. При появлении новых требований необходимо внести поправки в принятые планы действия в нештатных ситуациях.
Для каждого плана должен быть назначен определённый владелец. Правила действия в нештатных ситуациях, планы ручного аварийного восстановления и планы возобновления деятельности должны находиться в ведении владельцев соответствующих ресурсов или процессов, к которым они имеют отношение.

План восстановления определён приложением к настоящей политике.

Шаблон 17

Предоставление услуг сторонним организациям

1. Соглашения о предоставлении услуг.
В соглашения о предоставлении услуг {Название Организации} сторонним организациям должны быть включены требования безопасности, описание, объёмы и характеристики качества предоставляемых услуг.

2. Анализ предоставления услуг
Услуги, отчёты и записи, предоставляемые {Название Организации} сторонним организациям, должны постоянно проверяться и анализироваться. В отношениях со сторонней организацией должны присутствовать следующие процессы:

- контроль объёма и качества услуг, оговоренных в соглашениях;
- предоставление сторонней организации информации об инцидентах ИБ, связанных с предоставляемыми услугами, и совместное изучение этой информации;
- анализ предоставленных сторонними организациями отчётов о предоставленных услугах;
- управление любыми обнаруженными проблемами.

3. Приёмка систем
В {Название Организации} должен быть разработан и утверждён порядок приёмки новых ИС, обновления и новых версий ПО.

ПРИЛОЖЕНИЕ Е

Оформлене акта классификации информационных систем.

Утверждаю
Руководитель предприятия
"_____"_____"_____"г.

АКТ

классификации информационной системы обработки информации

_____ХХХХХХХХХХХХХХХХ_____

(наименование информационной системы)

Комиссия, в соответствии с приказом от "_____"_____"_____"г.	N____	в составе:
председатель: Хххххххххххх Х.Х.		
члены комиссии: Хххххххххххх Х.Х. Хххххххххххх Х.Х. Хххххххххххх Х.Х.		

провела классификацию информационной системы

_____ХХХХХХХХХХХХХХХХ_____,

(наименование информационной системы)

рассмотрев исходные данные на автоматизированную систему обработки информации (АС) наименование автоматизированной системы условия ее эксплуатации (многопользовательский, однопользовательский; с равными или разными правами доступа к информации {выбрать нужное}), с учетом характера обрабатываемой информации (служебная тайна, коммерческая тайна, персональные данные и т.д. {выбрать нужное}) и в соответствии с руководящими документами Гостехкомиссии России "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации,

РЕШИЛА:

Установить АС *наименование автоматизированной системы*

класс _ХХ_.

Председатель _____ Хххххххххххх Х.Х.

Члены комиссии _____ Хххххххххххх Х.Х.

_____ Хххххххххххх Х.Х.

_____ Хххххххххххх Х.Х.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E

Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023

ПРИЛОЖЕНИЕ Ж

Условные обозначения к планировкам выделенных помещений

Обозначение	Наименование
	Граница контролируемой зоны

Таблица. Характеристики конструкций

№ варианта	Стены	Дверь	Окно
1	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 1,5 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 3,0 мм
2	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: с уплотняющими прокладками	Одинарное остекление без уплотнительных прокладок, толщина 4,0 мм
3	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2,5 кирпича	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 6,0 мм
4	Стена из кирпичной кладки без штукатурки (из красного кирпича): в 2 кирпича	-	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 3,0/3,0
5	Стена из пустотелого кирпича, толщина 380,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом, толщина 3,0/3,0
6	Стена из пустотелого кирпича, толщина 510,0 мм	Глухая щитовая дверь, толщиной 40 мм, облицованная с двух сторон фанерой, толщиной 4 мм: С уплотняющими прокладками	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 3,0/3,0
7	Стена из железобетона, толщина 160,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным	-

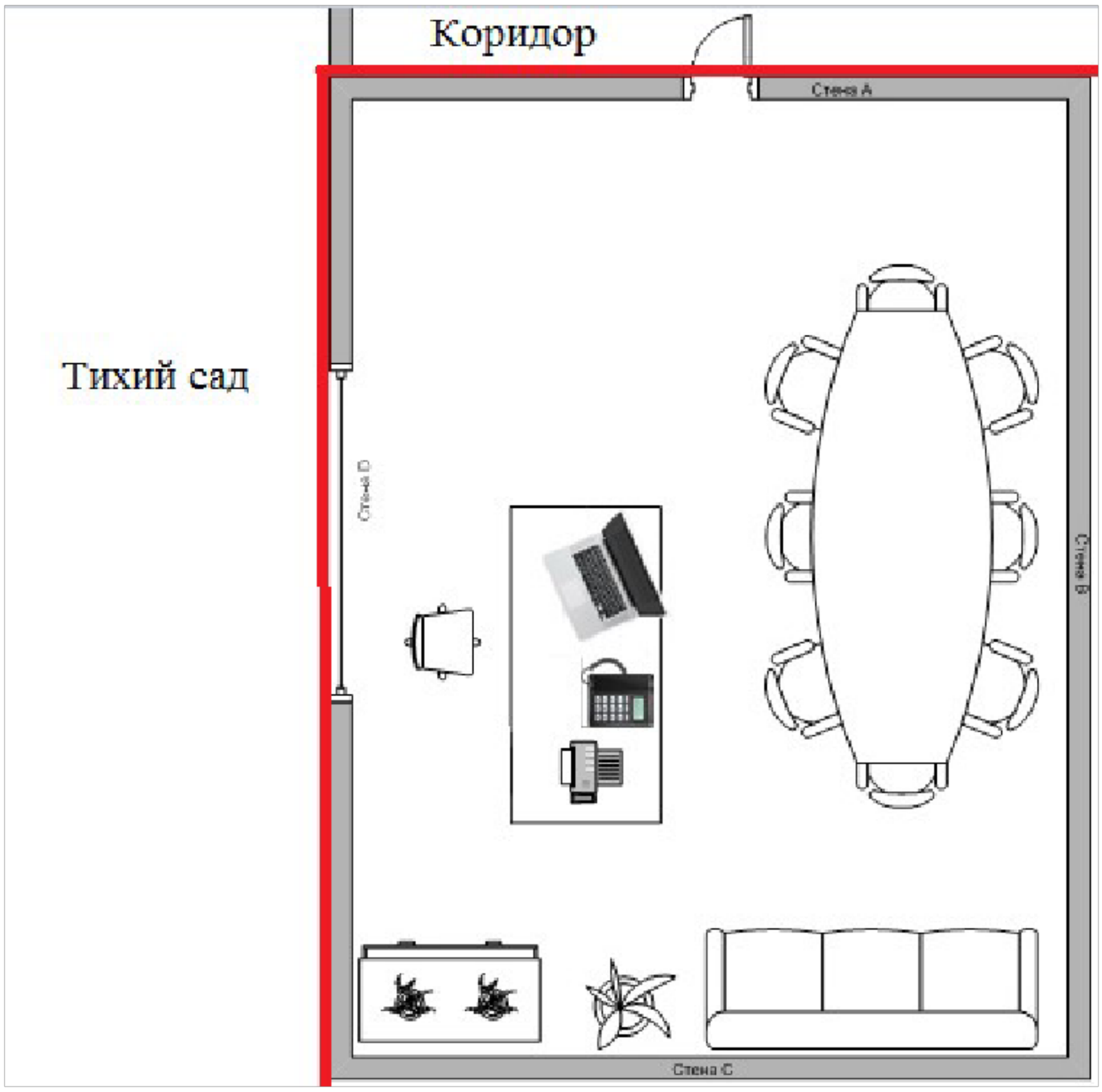
		стекловатой: Без уплотняющих прокладок	

8	Стена из железобетона, толщина 180,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой: С уплотняющими прокладками	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 4,0/4,0
9	Стена из железобетона, толщина 160,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, со звукопоглощающим материалом, толщина 4,0/4,0
10	Стена из железобетона, толщина 200,0 мм	-	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 4,0/4,0
11	Стена из железобетона, толщина 300,0 мм	-	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 6,0/3,0
12	Стена из железобетона, толщина 800,0 мм	-	Двойное остекление, расстояние между стеклами 90 мм, без звукопоглощающего материала, толщина 6,0/3,0
13	Газобетонная плита, толщина 240,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: без уплотняющих прокладок	-
14	Газобетонная плита, толщина 240,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 4,5 см: с уплотняющими прокладками	Двойное остекление, расстояние между стеклами 190 мм, без звукопоглощающего материала, толщина 6,0/6,0

15	Керамзитобетонная плита, толщина 100,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок	-
16	Керамзитобетонная плита, толщина 120,0 мм	Дверь обычного типа с филенкой из 2,5 см досок (с двумя панелями) с обвязкой толщиной 2,5 см из 3 мм фанеры без уплотняющих прокладок, оклеенная фанерой размером 90х200 см без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 3,0 мм
17	Шлакоблоки, отштукатуренные с двух сторон, толщина 220,0 мм	Глухая щитовая дверь, толщиной 40 мм, облицованная с двух сторон фанерой, толщиной 4 мм: Без уплотняющих прокладок	Одинарное остекление без уплотнительных прокладок, толщина 4,0 мм
18	Стена из пемзобетона, толщина 140,0 мм	-	Одинарное остекление без уплотнительных прокладок, толщина 6,0 мм
19	Стена из пемзобетона, толщина 140,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой: Без уплотняющих прокладок	Двойное остекление, расстояние между стеклами 57 мм, без звукопоглощающего материала, толщина 3,0/3,0
20	Стена из пемзобетона, толщина 140,0 мм	Щитовая дверь из твердых древесноволокнистых плит толщиной 4-6 мм с воздушным зазором 50 мм, заполненным стекловатой: С уплотняющими прокладками	Одинарное остекление без уплотнительных прокладок, толщина 3,0 мм

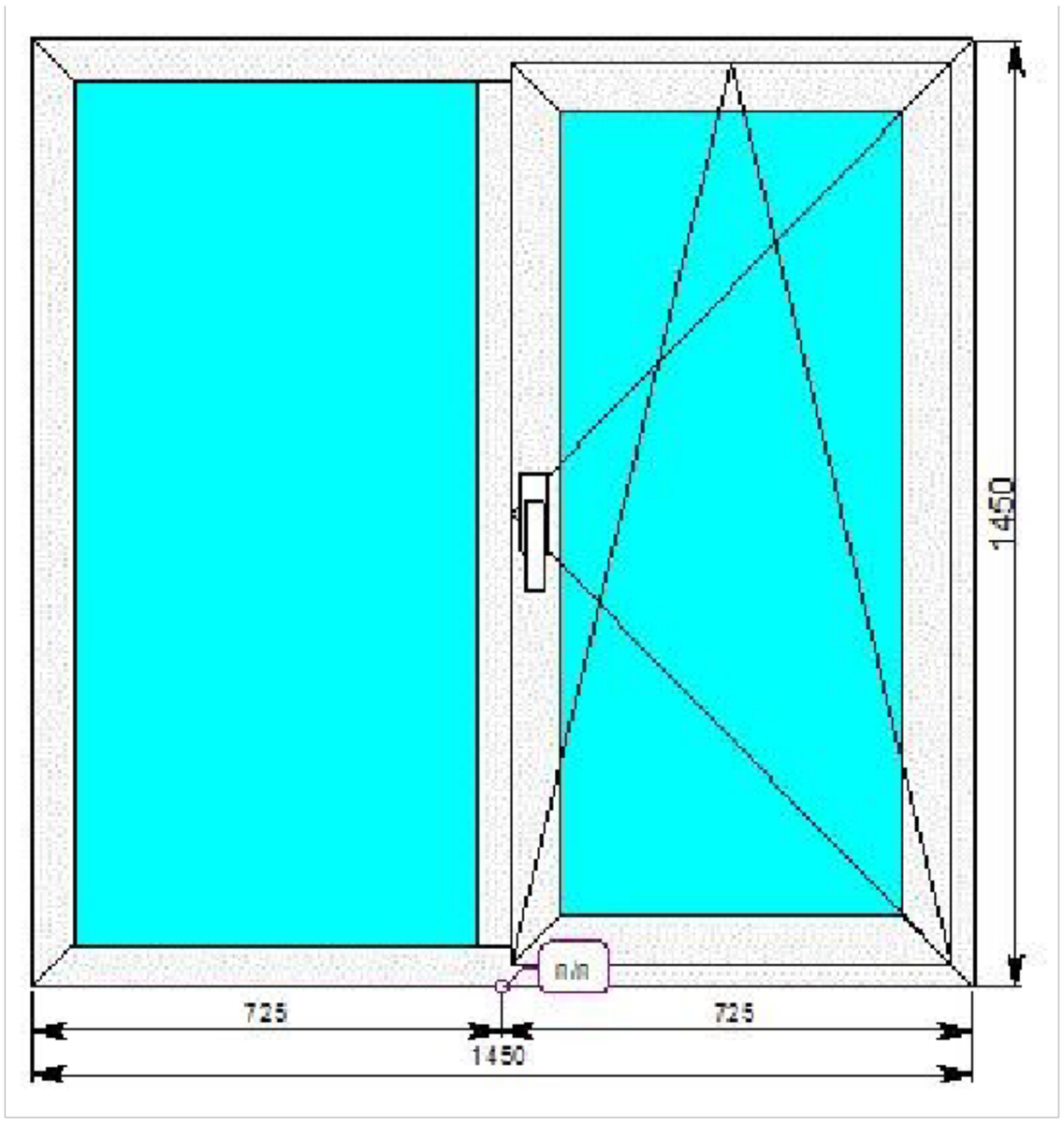
Варианты планировок выделенных помещений

1. Помещение для переговоров №1



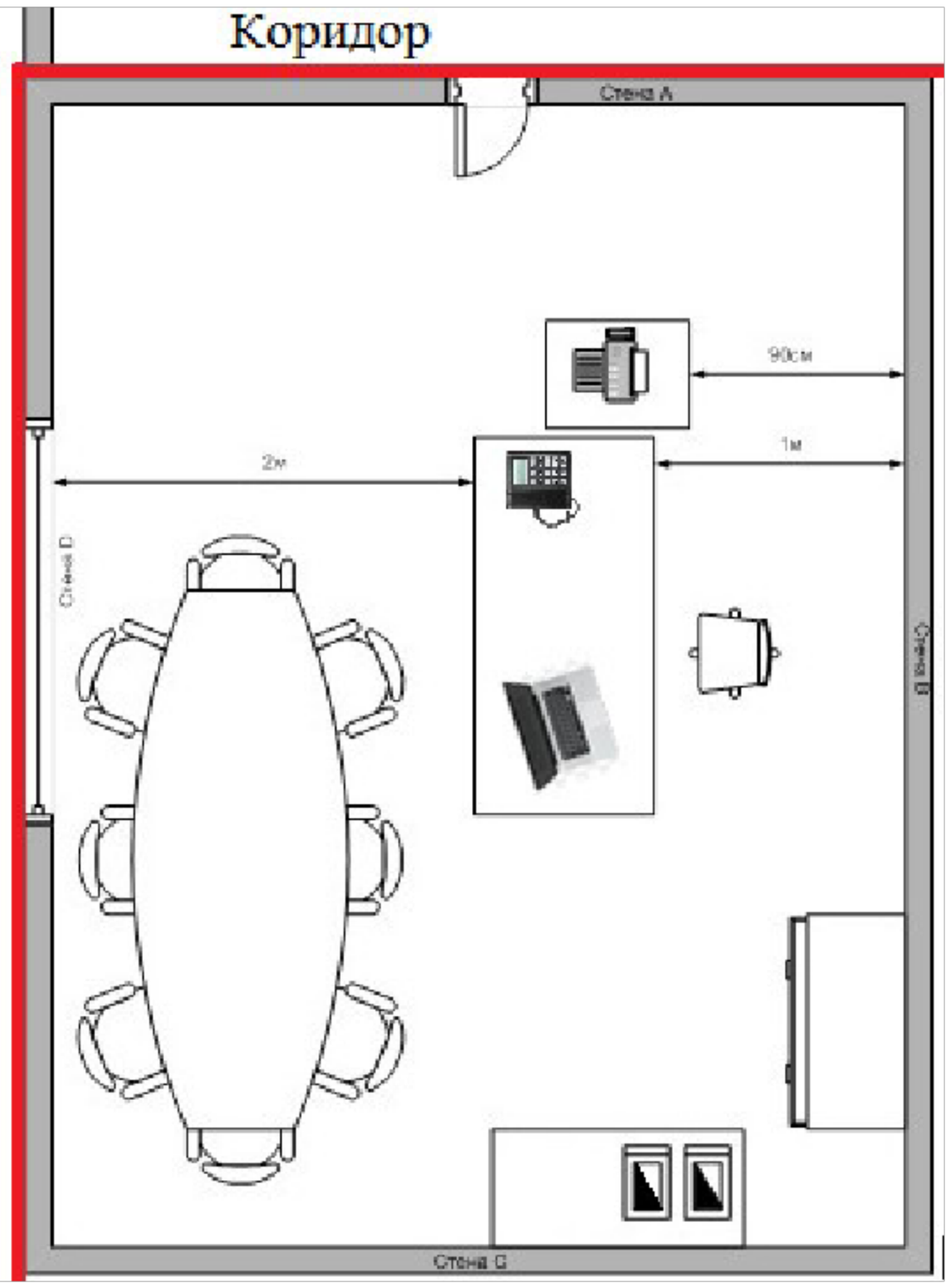
Размеры помещ.: 4х6м, h=3м.

Размер двери: 2х0,9м.



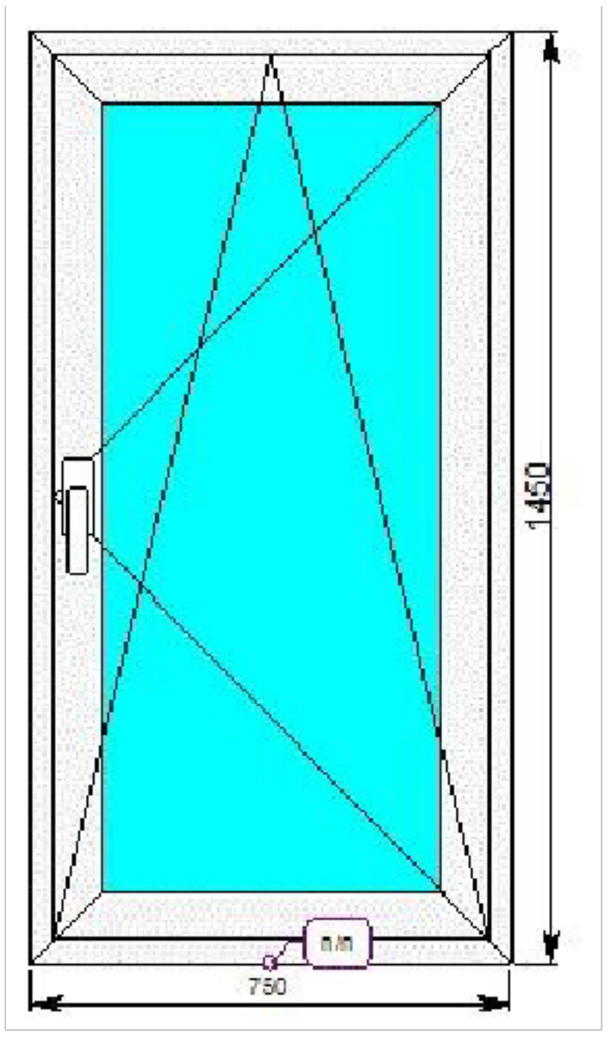
2. Помещение для переговоров №2

Тихая улица



Размеры: 4,5х6м, h=3,5м.

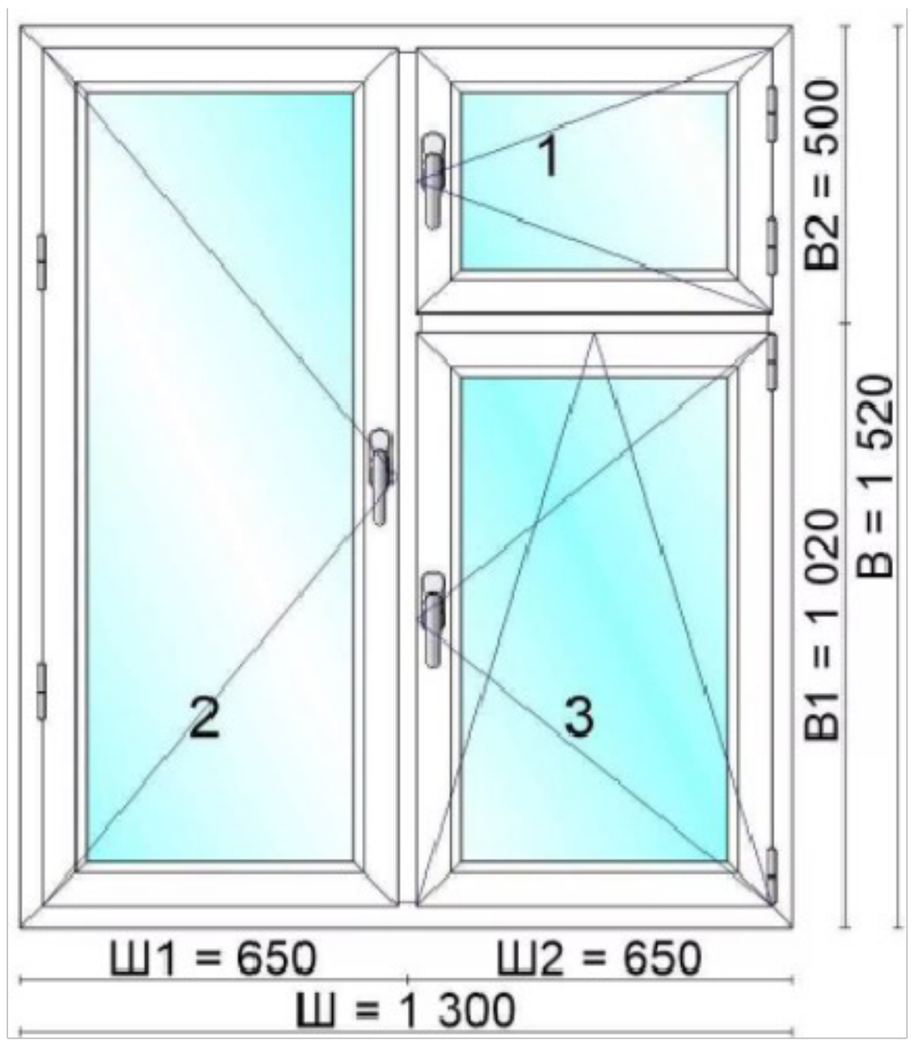
Размер двери: 2х0,9м.



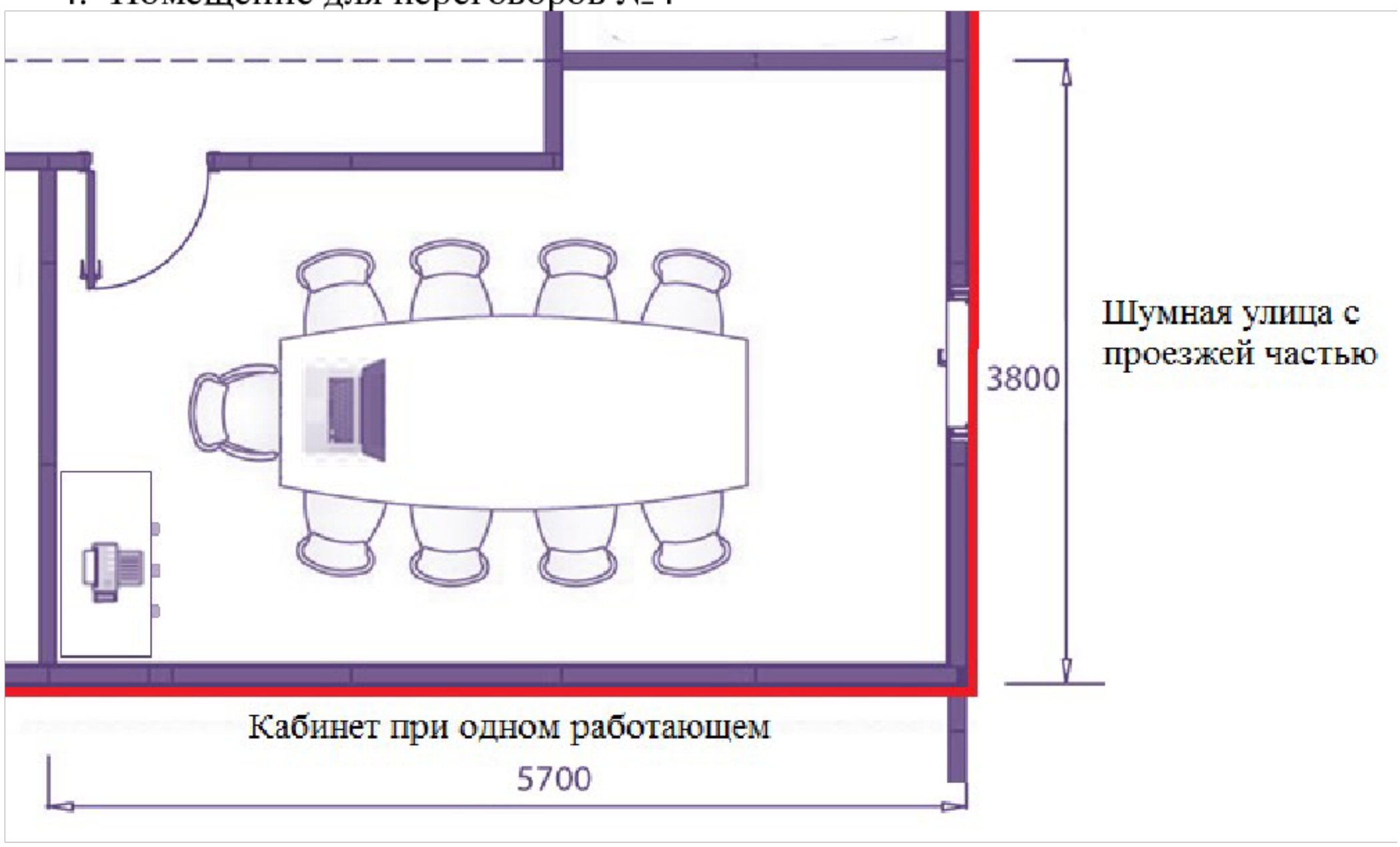
3. Помещение для переговоров №3

Размеры: 4,5х6м, h=3м.

Размер двери: 2х0,9м.

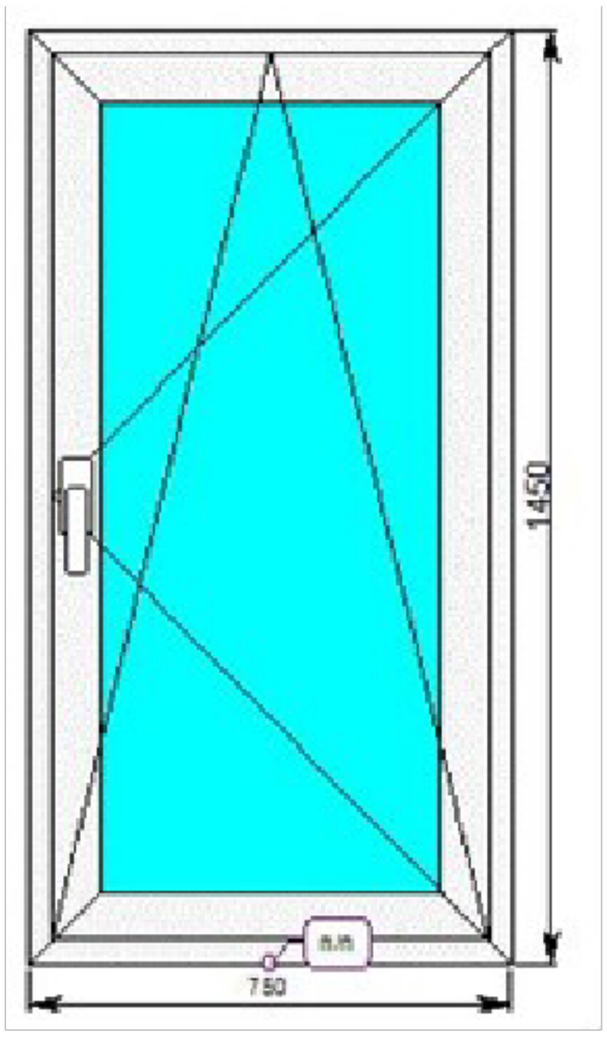


4. Помещение для переговоров №4

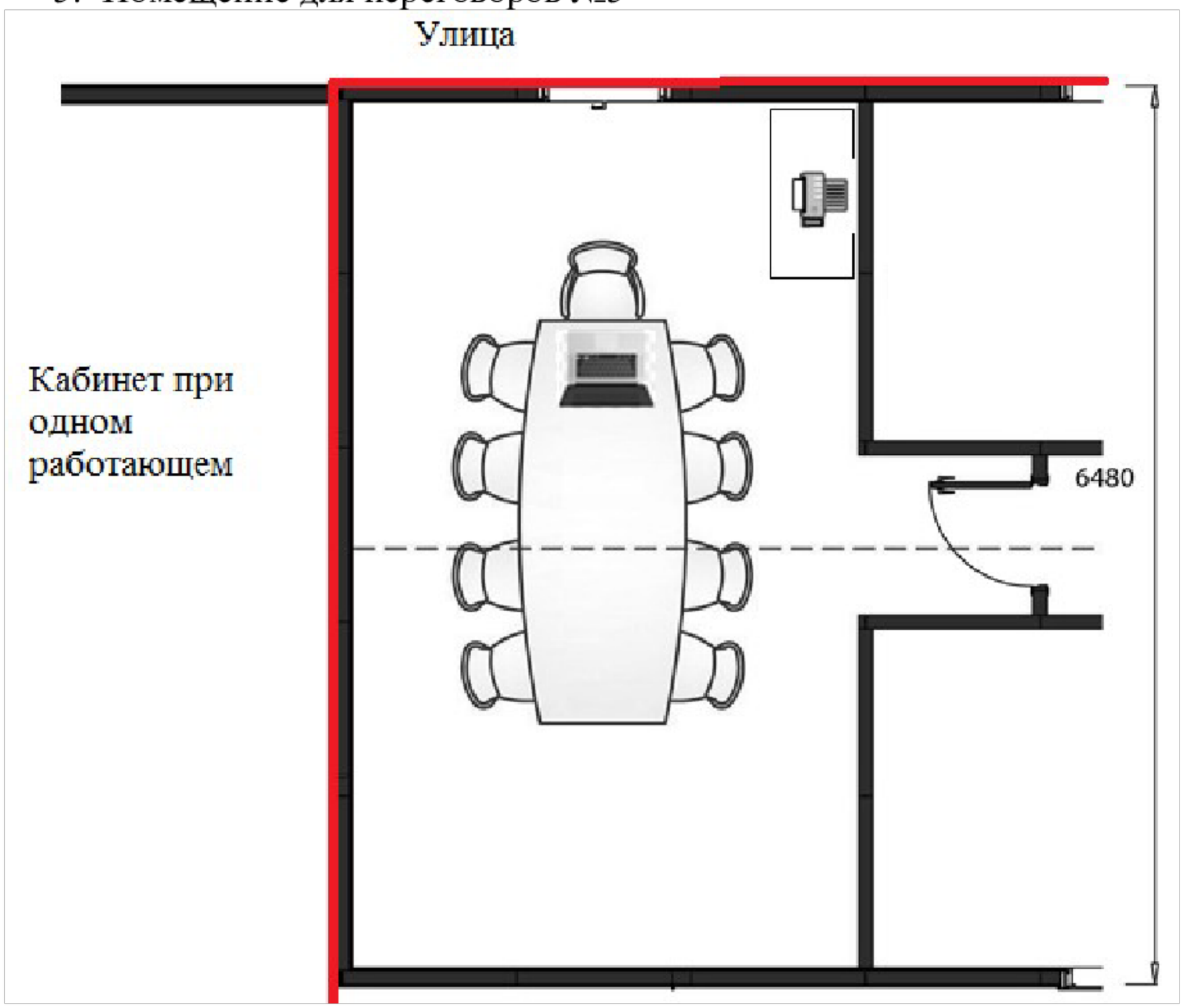


h=3м

Размер окна:

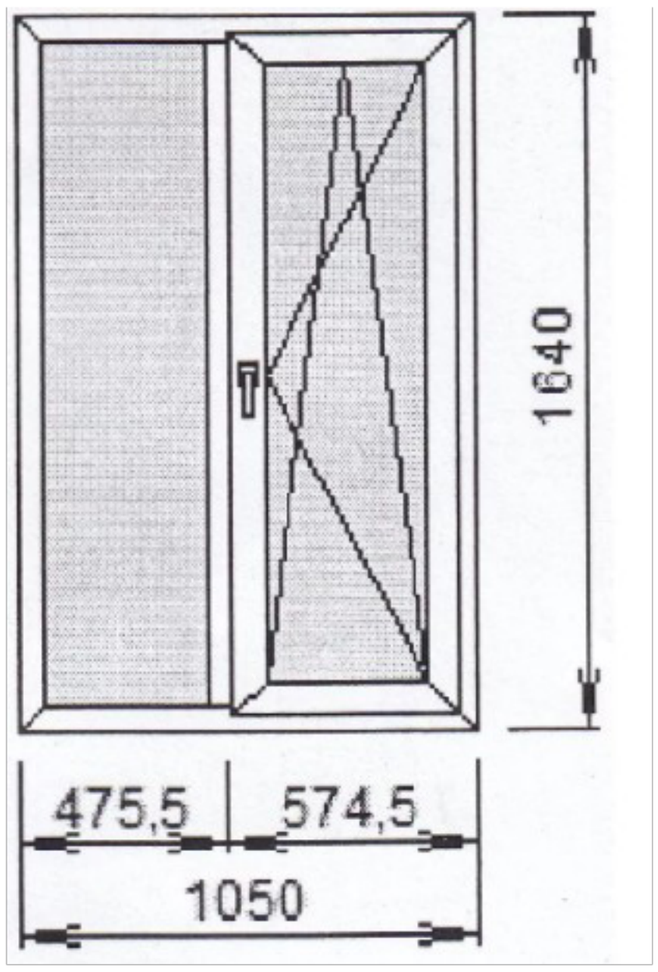


5. Помещение для переговоров №5

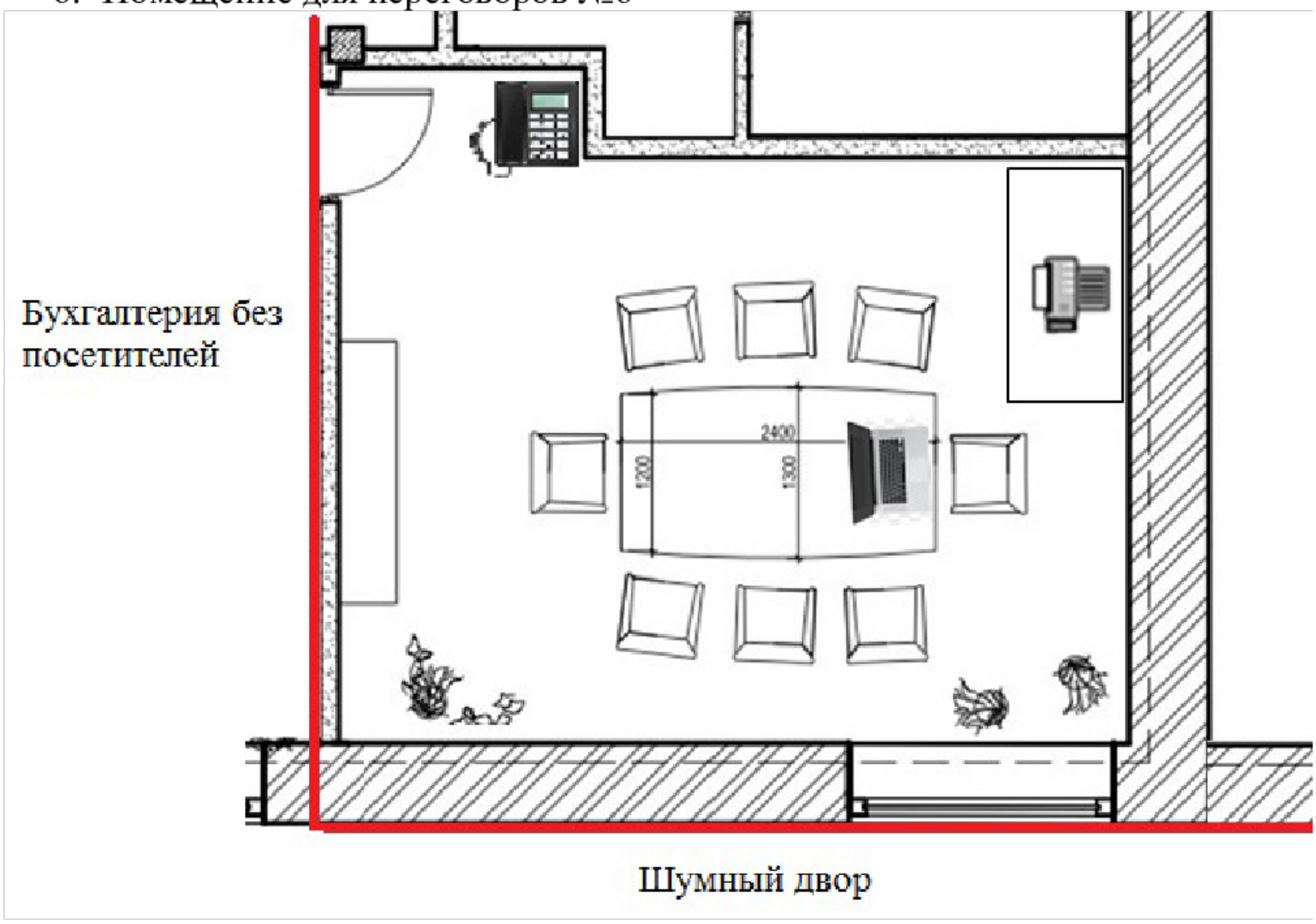


Ширина: 3820 мм, h=3000 мм

Размер окна:

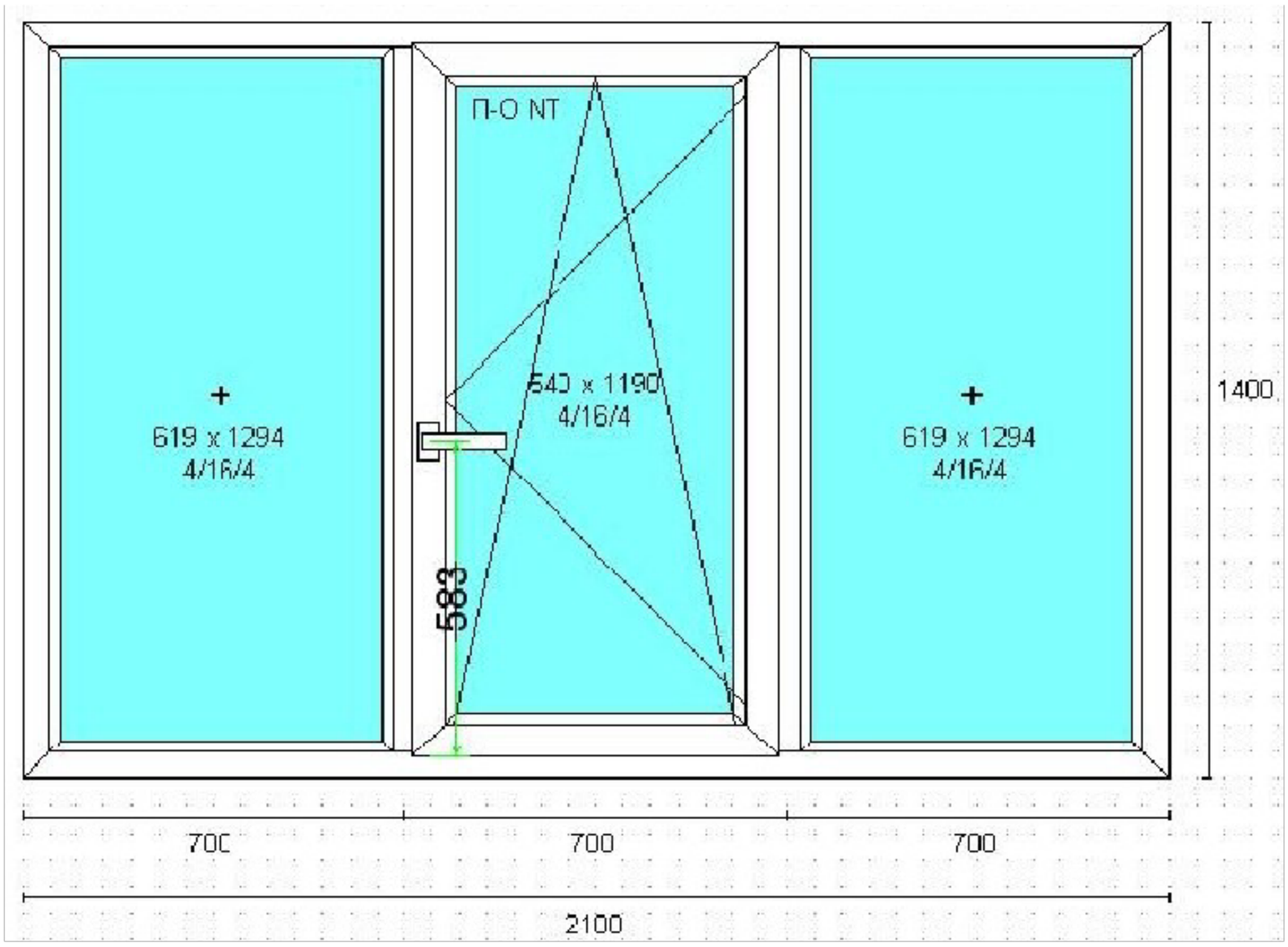


6. Помещение для переговоров №6



Размеры: 4,5х6м, h=3,5м

Размер двери: 2х0,9м.



7. Помещение для переговоров №7

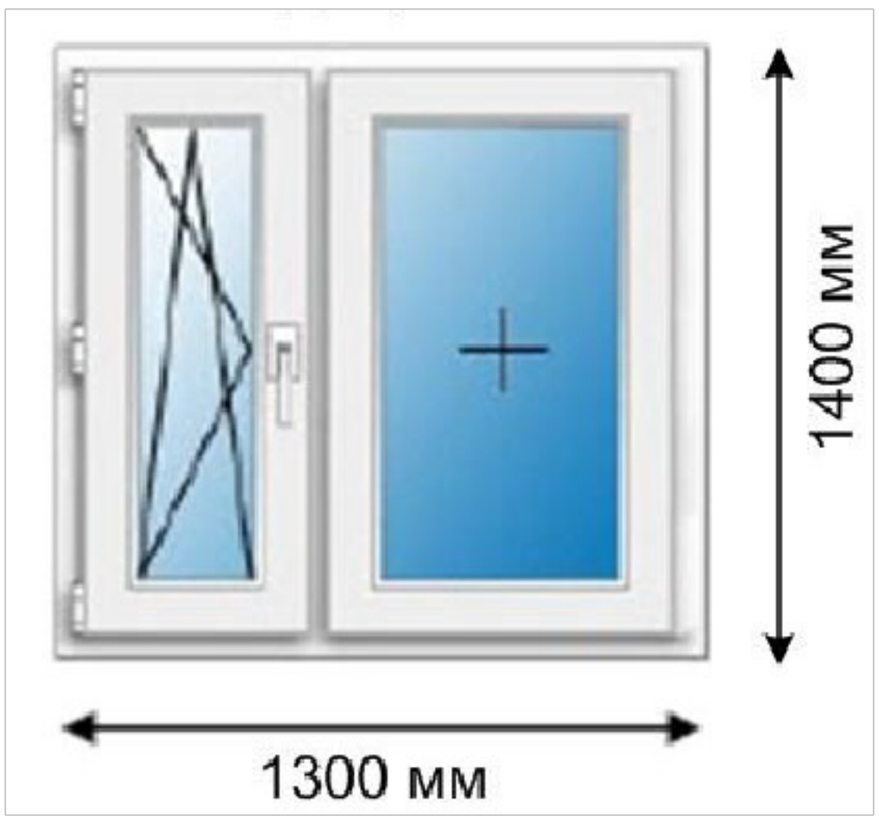
h=3,5m

Размер двери: 2х0,9м.

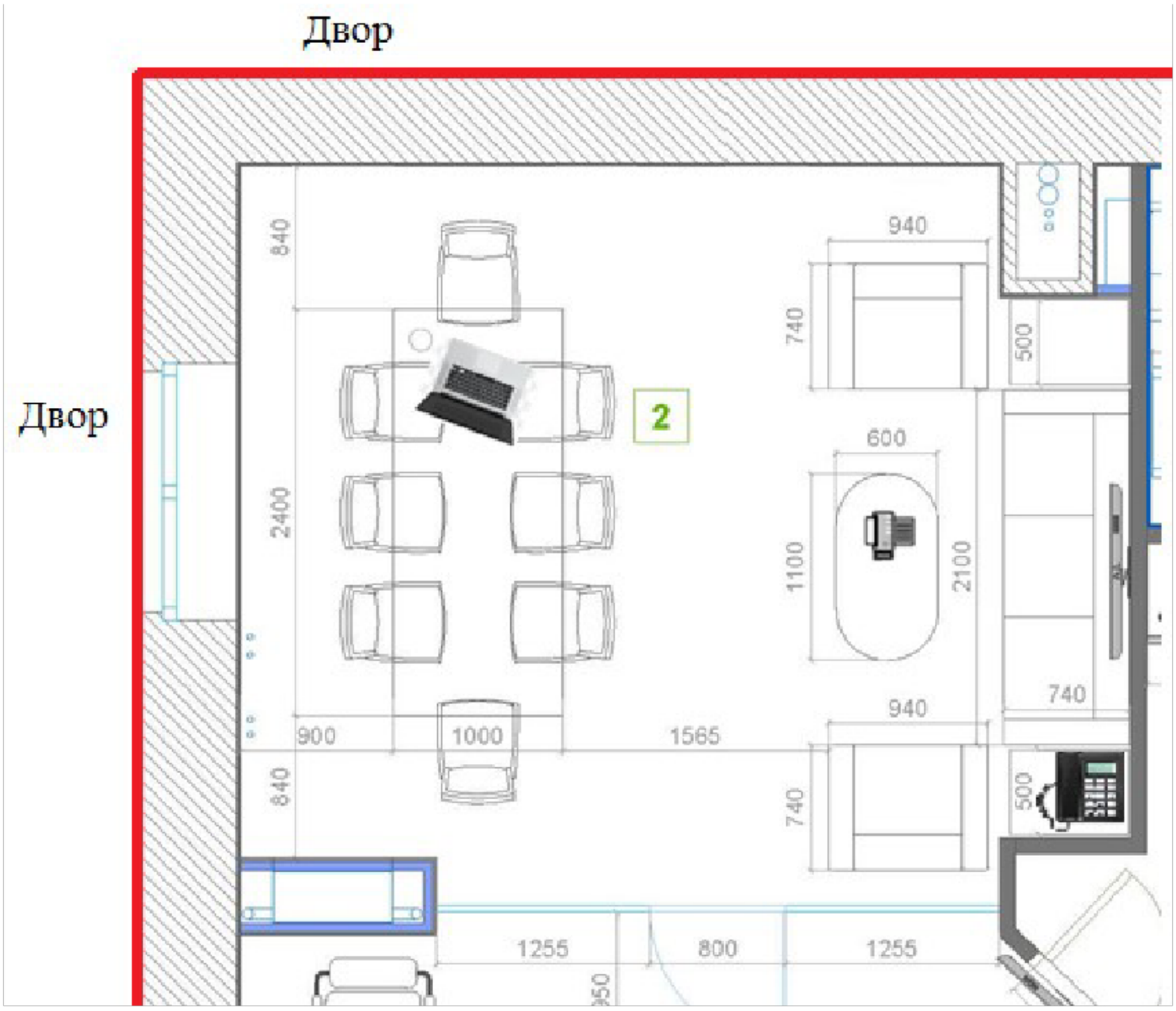
8. Помещение для переговоров №8

h=3м

Размер двери: 2х0,9м.

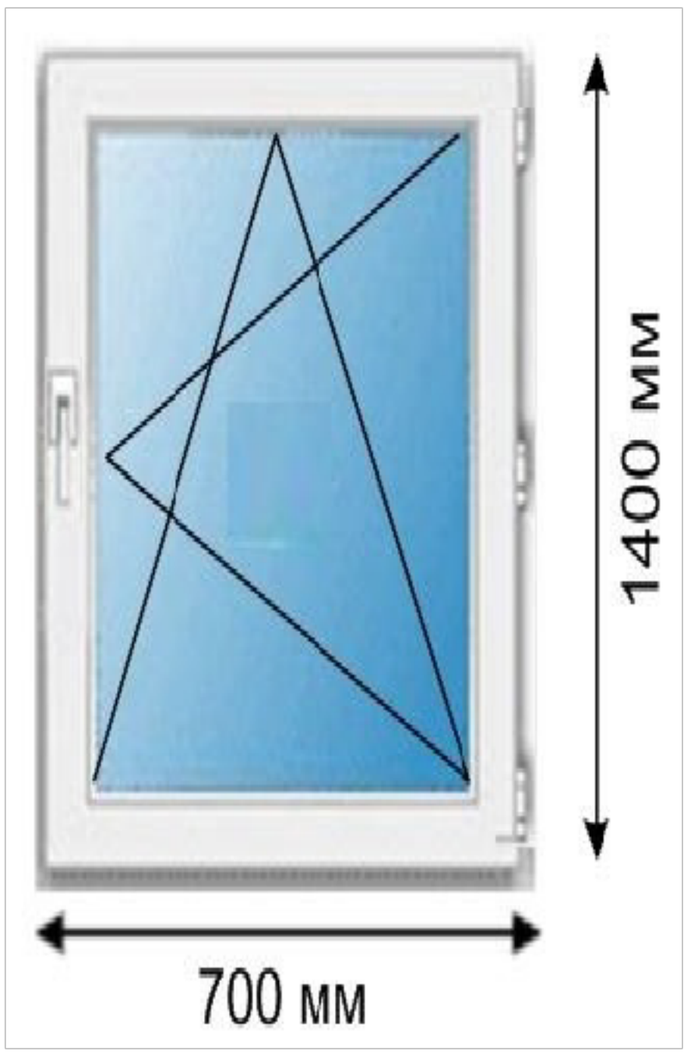


9. Помещение для переговоров №9

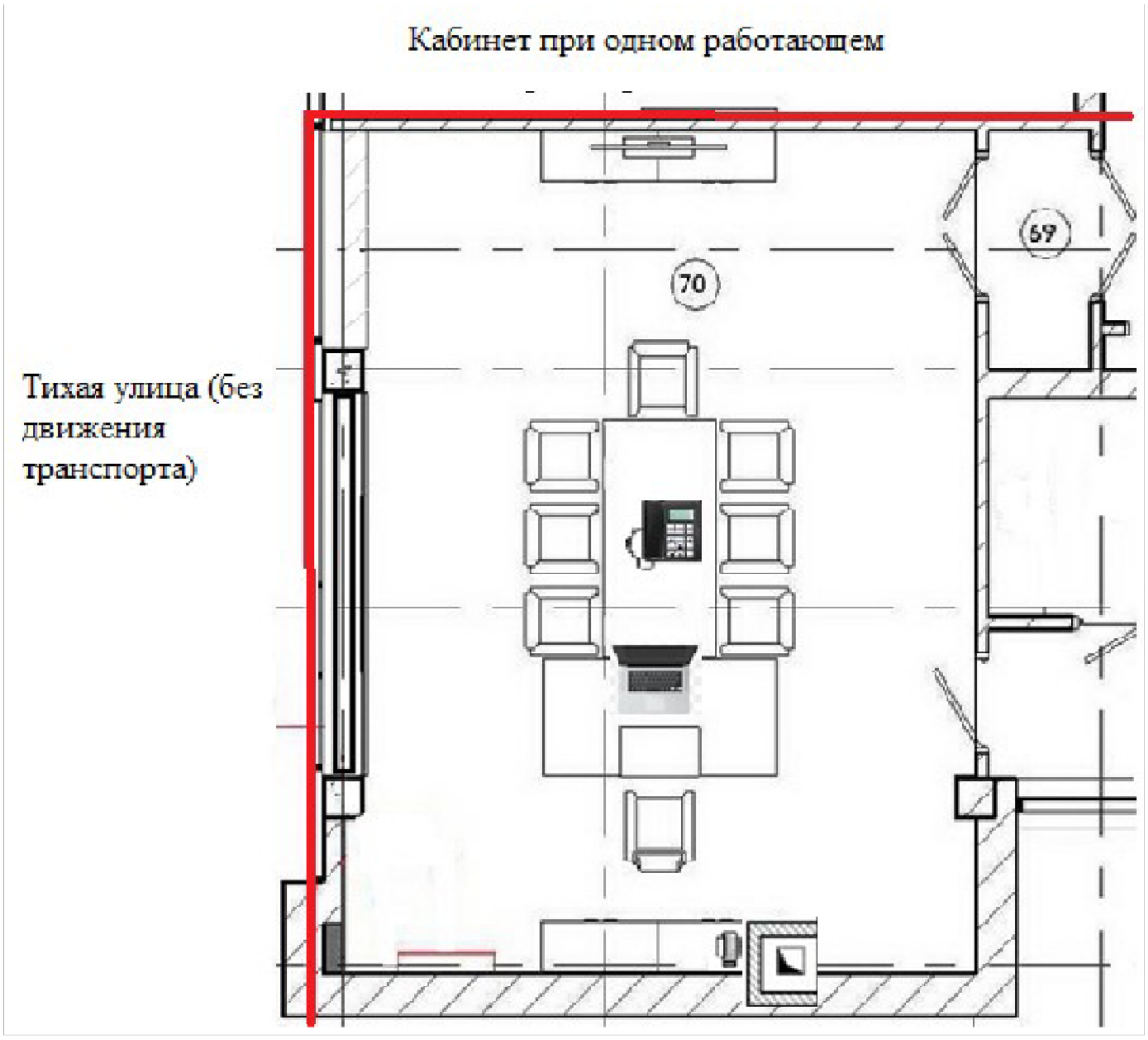


Размеры: 4,5х4,5м, h=3м.

Размер окна:

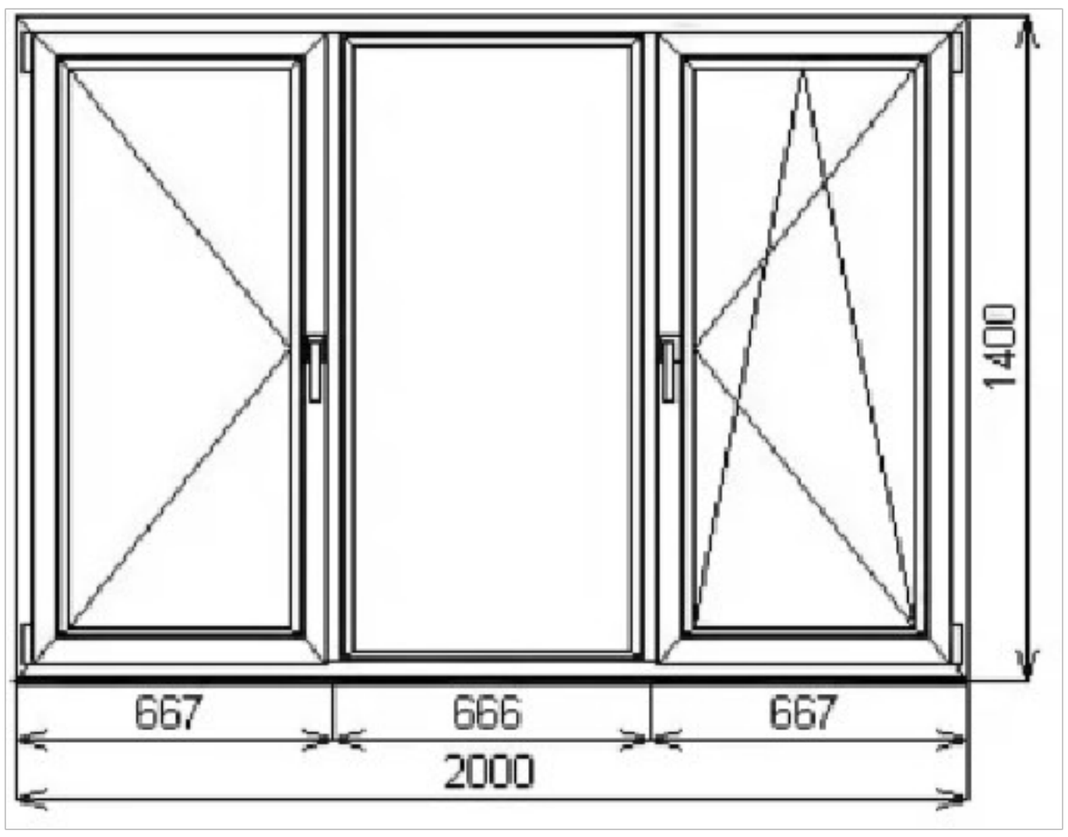


10.Помещение для переговоров №10



Размеры: 4,5х6,5м, h=3,5м.

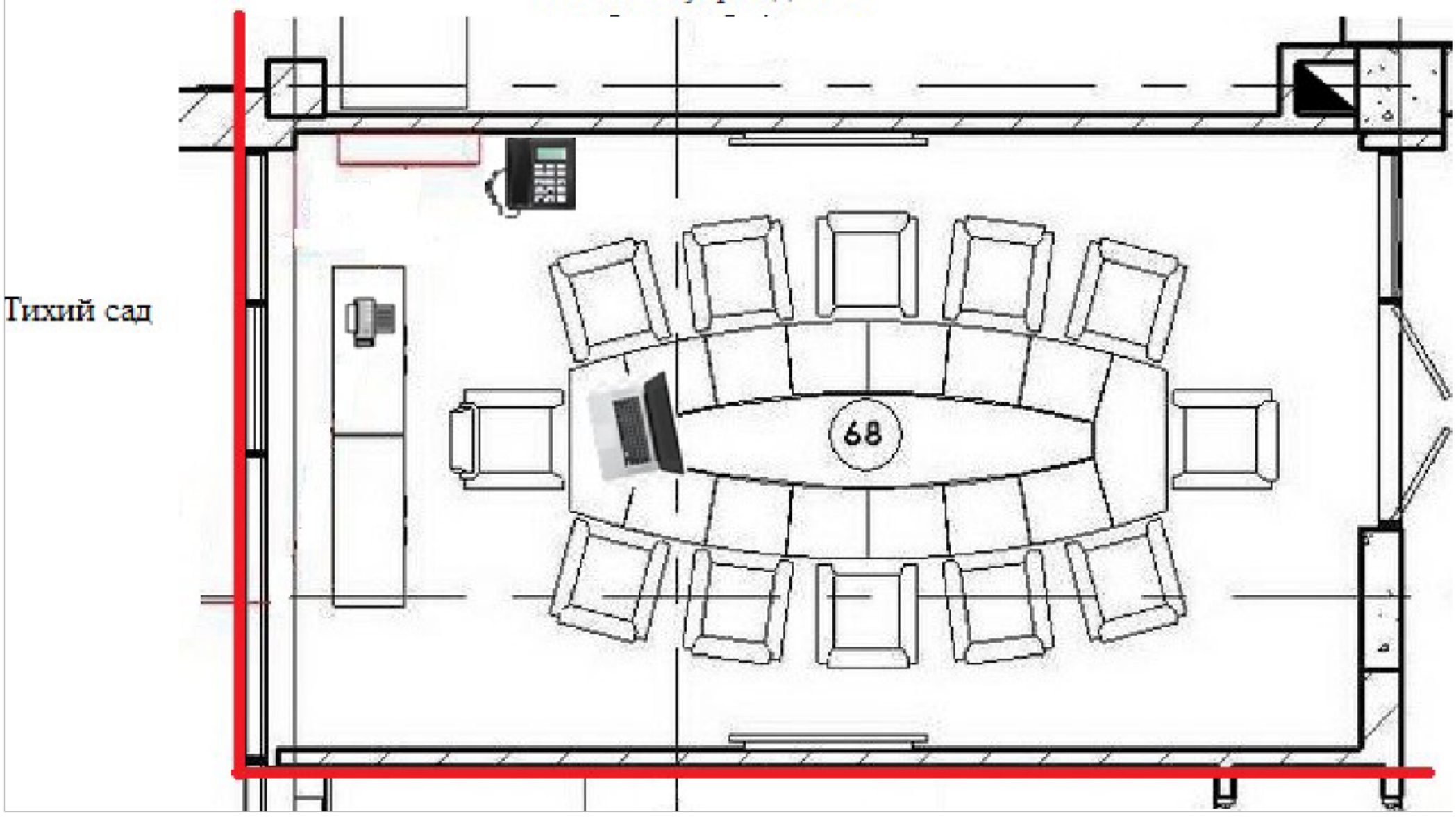
Размер окна:



11.Помещение для переговоров №11

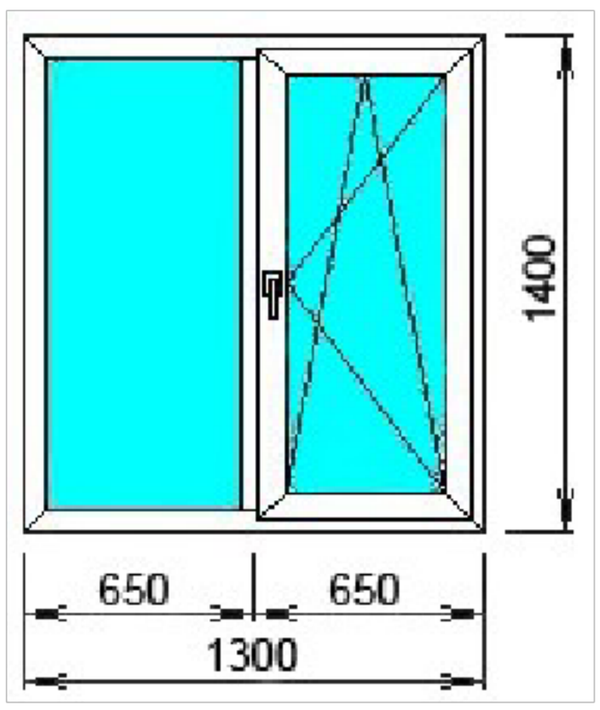
Обычное учреждение

Тихий сад

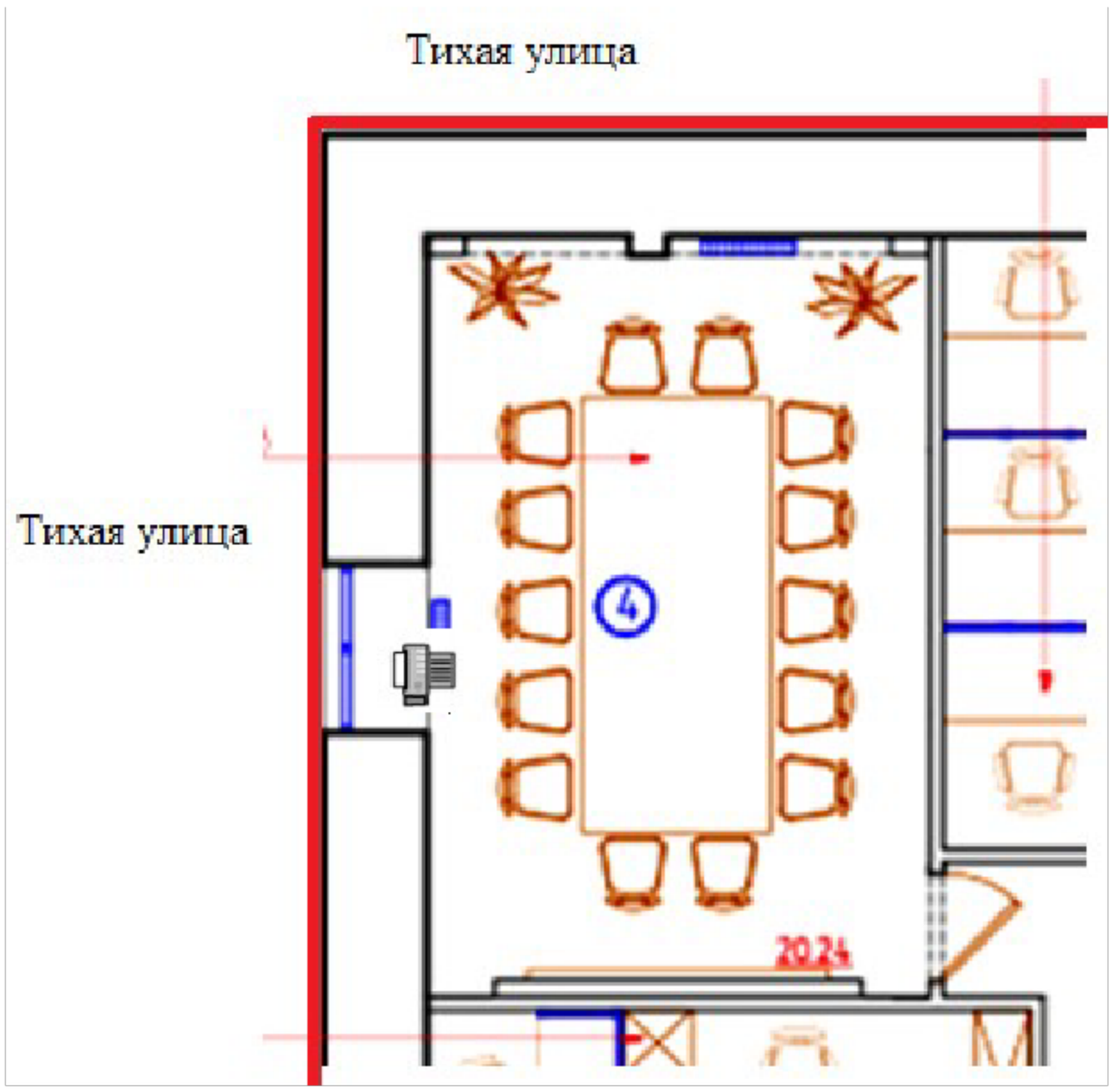


Размеры: 4,5х6,5м, h=3,5м.

Размер окна:

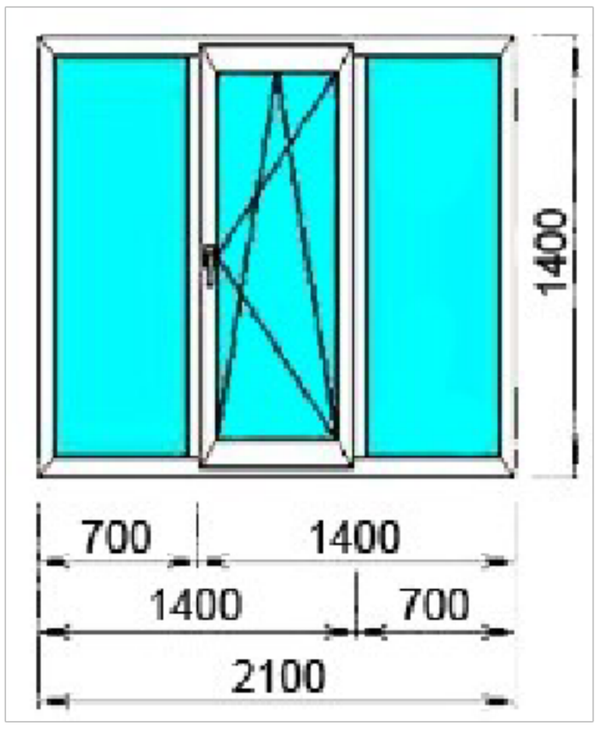


12.Помещение для переговоров №12

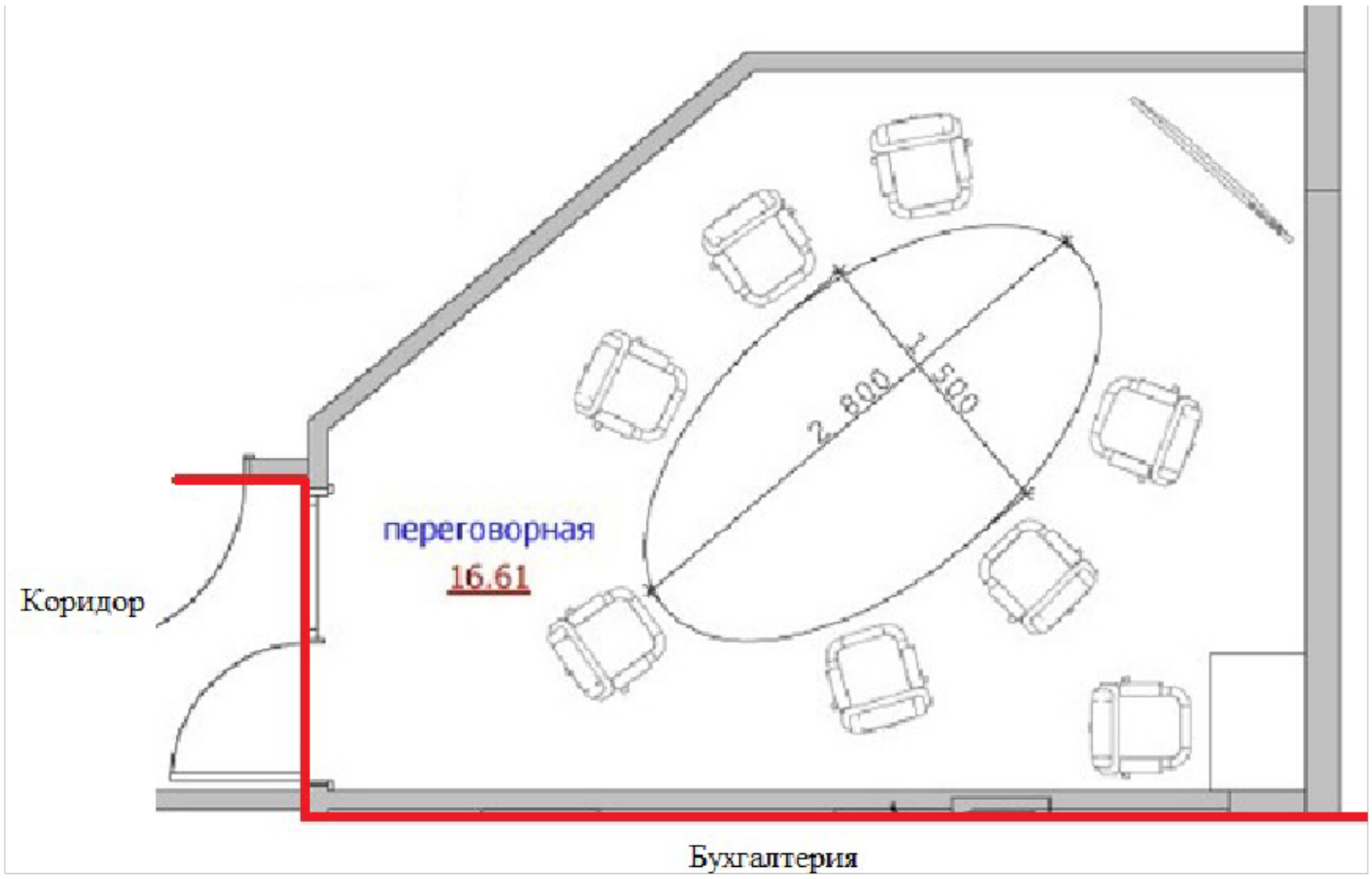


Размеры: 4,5х6,5м, h=3,5м.

Размер окна:



13.Помещение для переговоров №13



Размеры: 4,5х6,5м, h=3м.

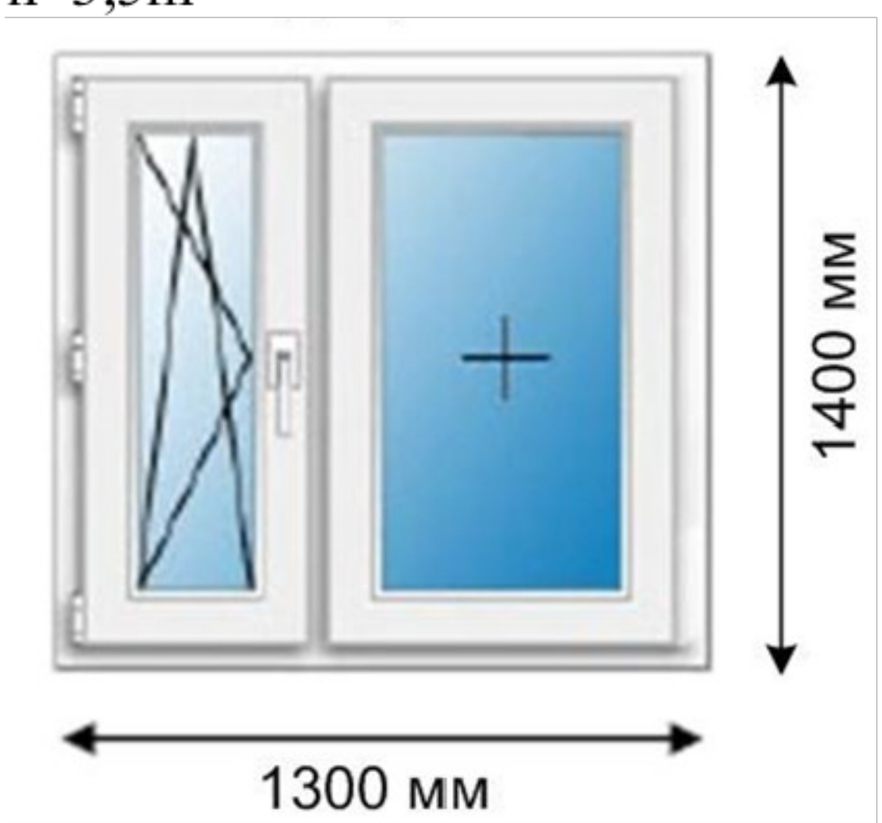
Размер двери: 2х0,9м.

14.Помещение для переговоров №14

Размеры: 4,5х6,5м, h=3,5м.

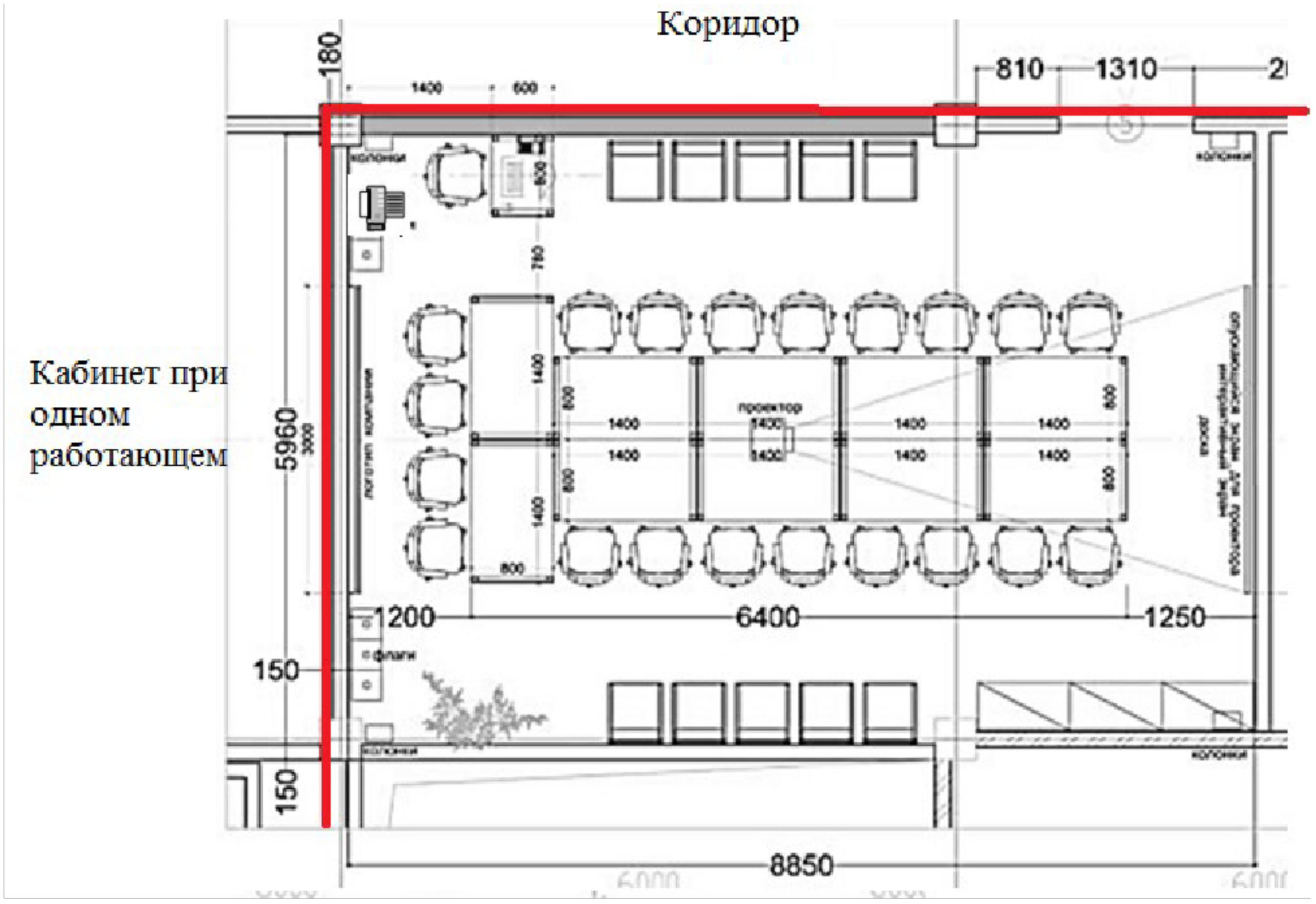
Размер двери: 2х0,9м.

h=3,5m



15.Помещение для переговоров №15

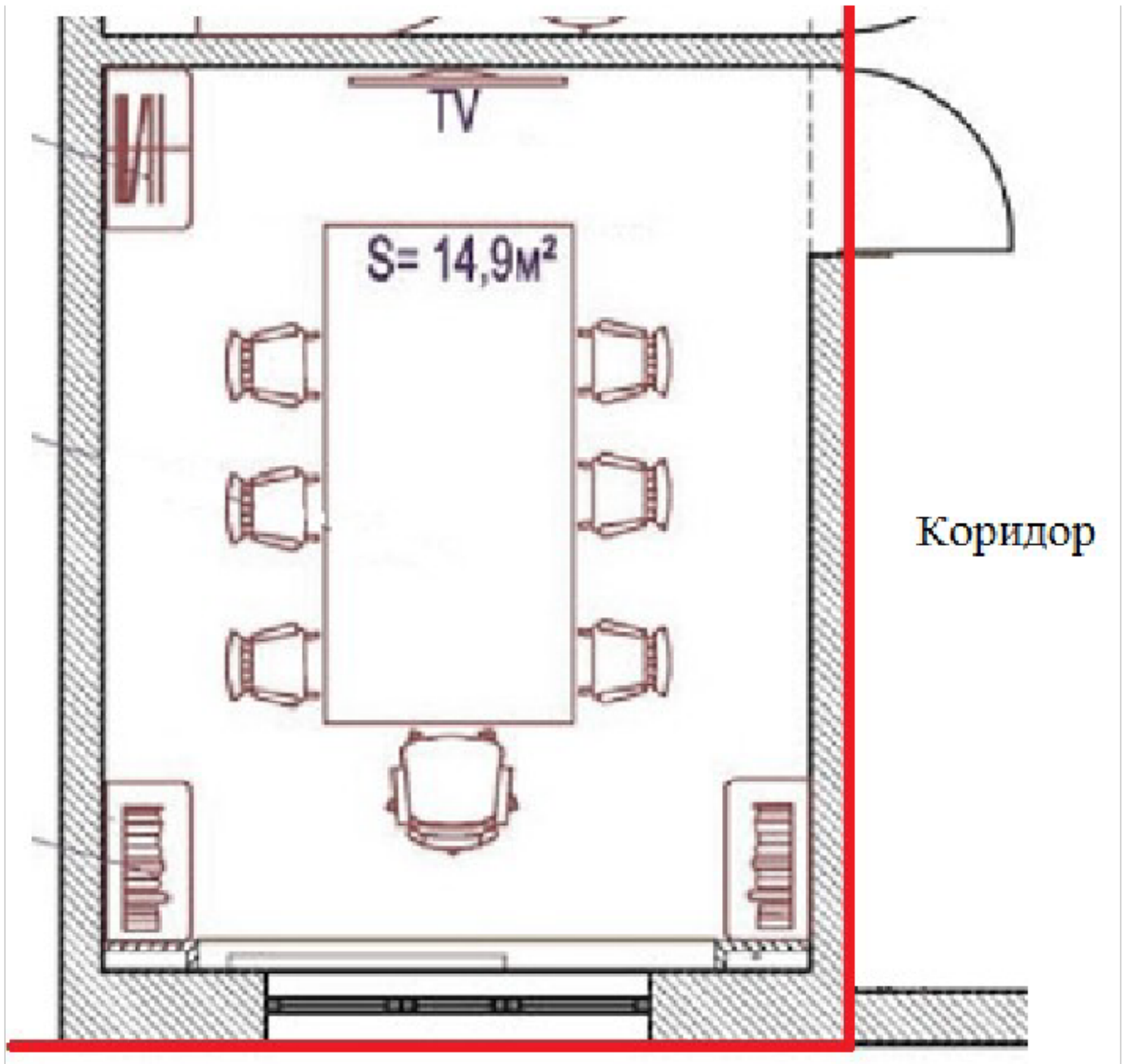
Кабинет при одном работающем



h=3,5м.

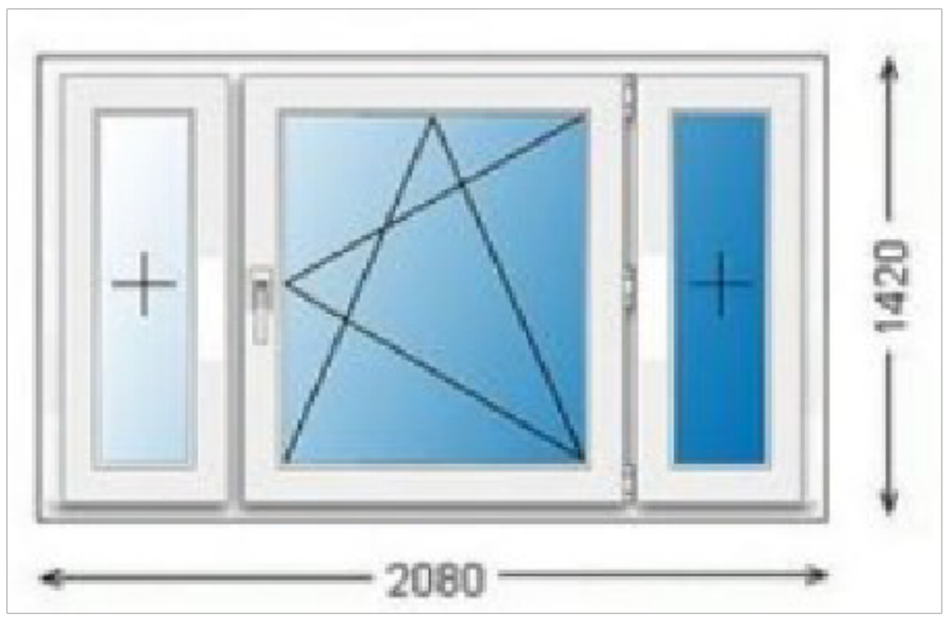
Размер двери: 2х0,9м.

16.Помещение для переговоров №16

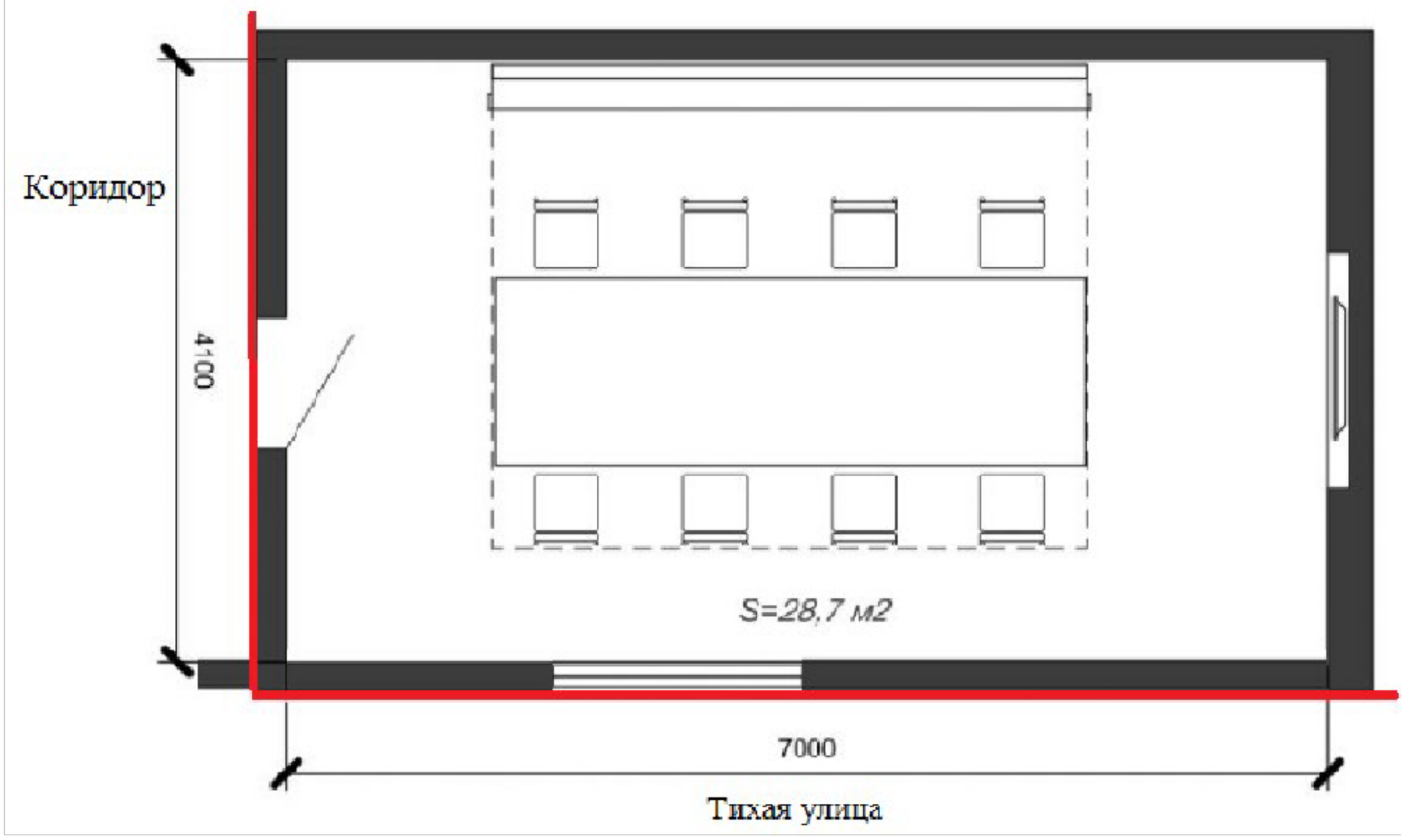


Размеры: 3х5м, h=3mм.

Размер двери: 2х0,9м.

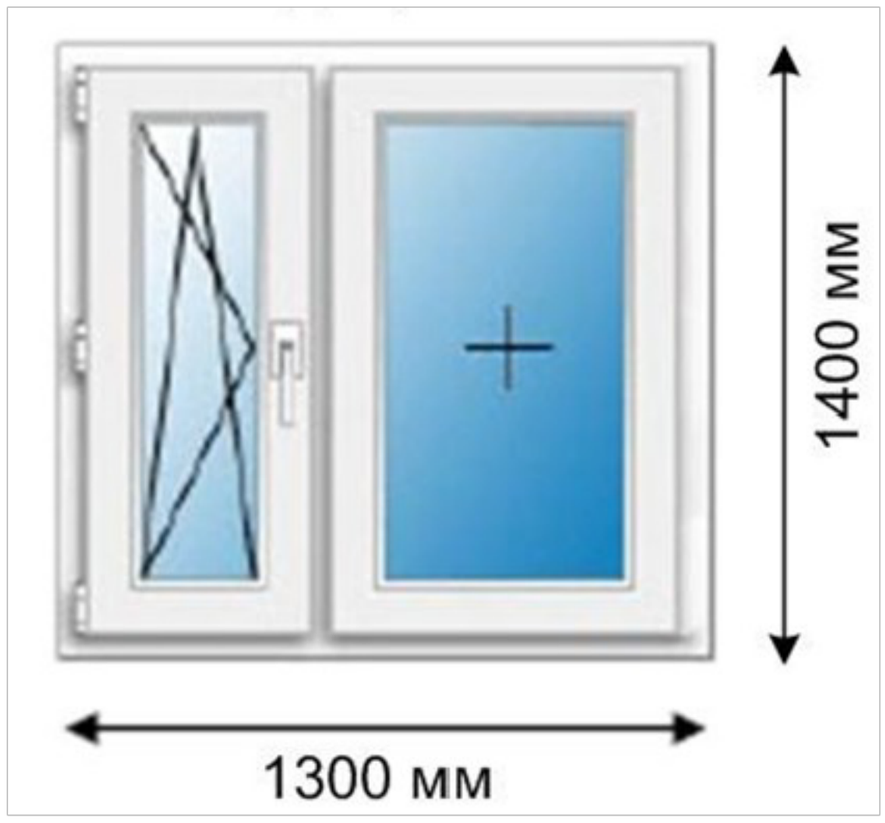


17. Помещение для переговоров №17

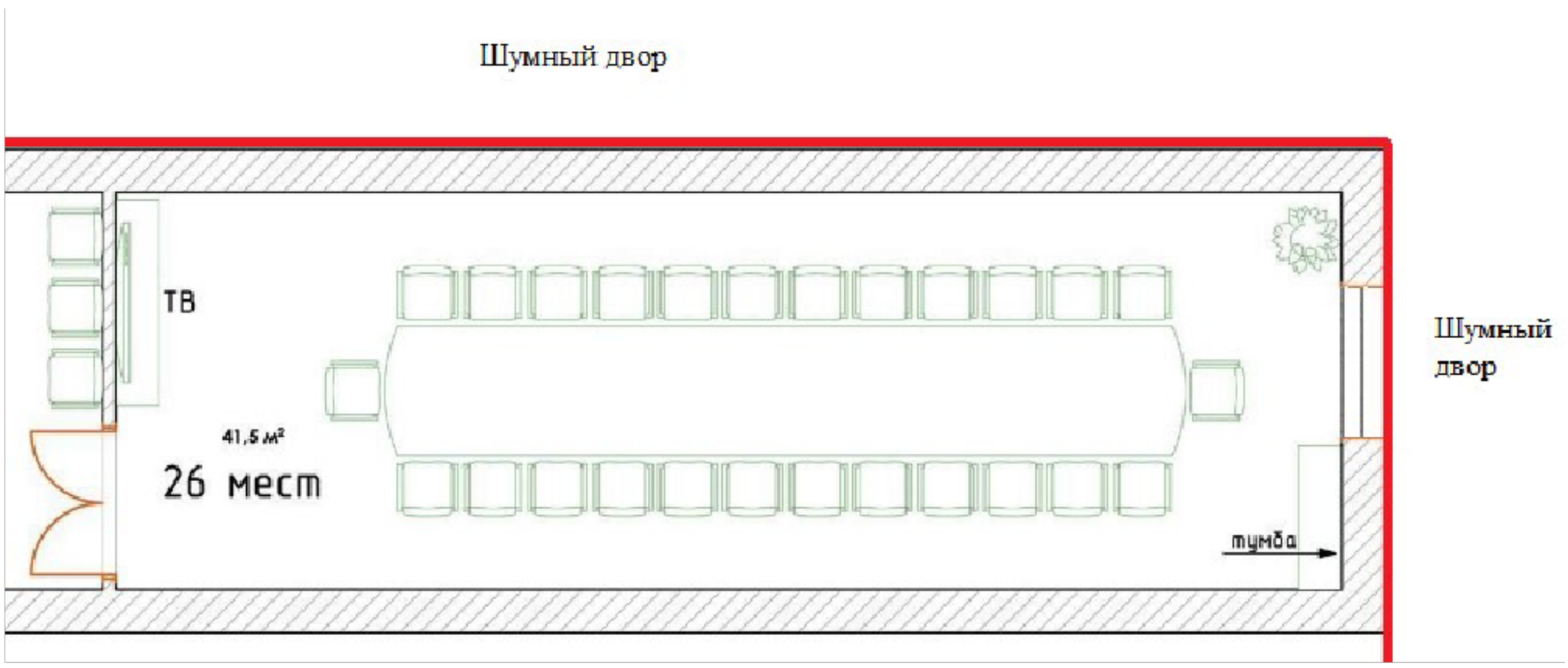


h=3,5м

Размер двери: 2х0,9м.

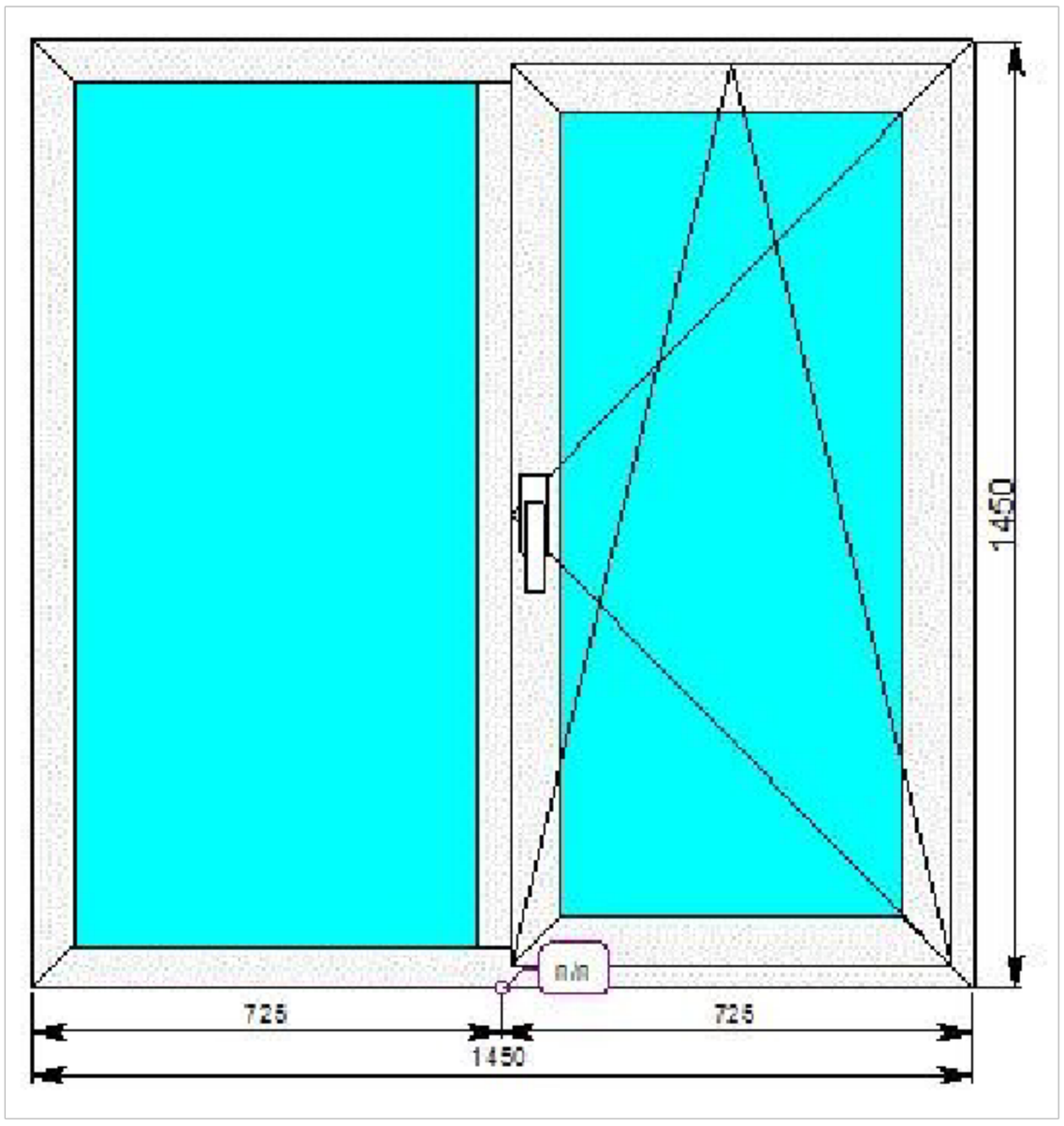


18.Помещение для переговоров №18



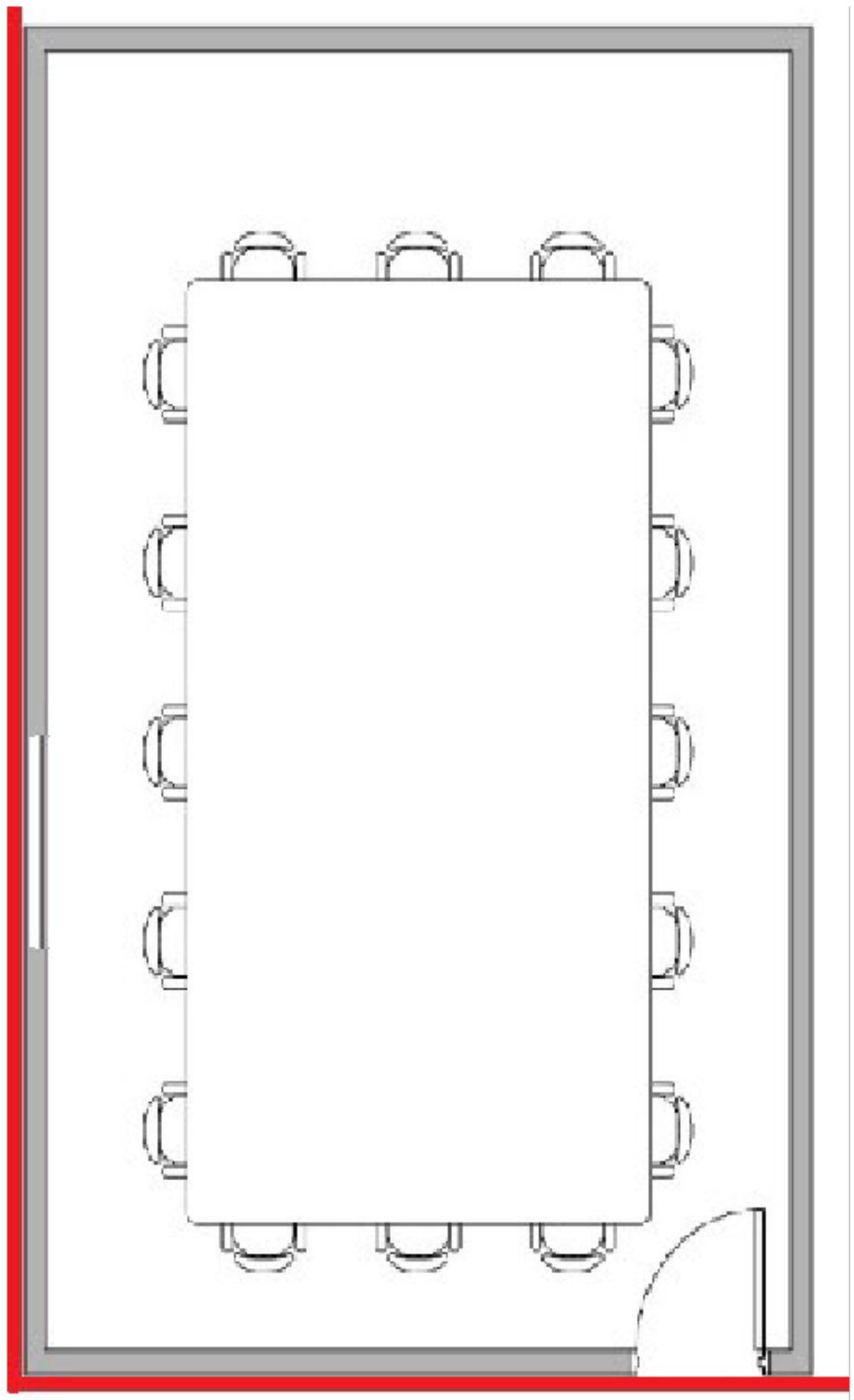
Размеры: 3х10м, h=3м.

Размер окна:



19.Помещение для переговоров №19

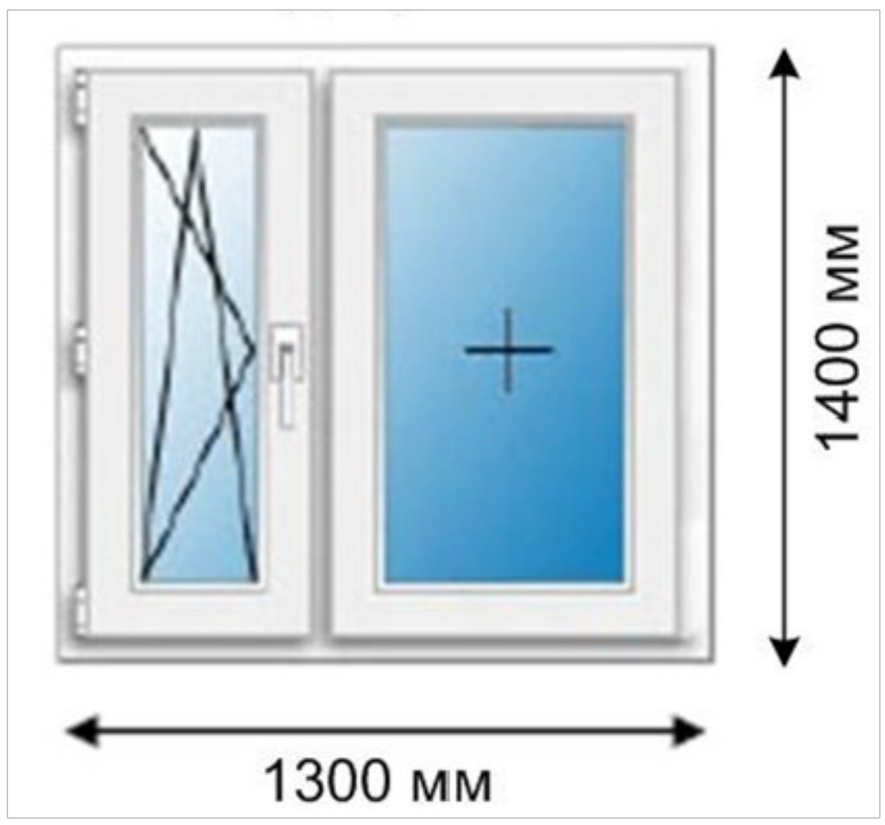
Тихая улица



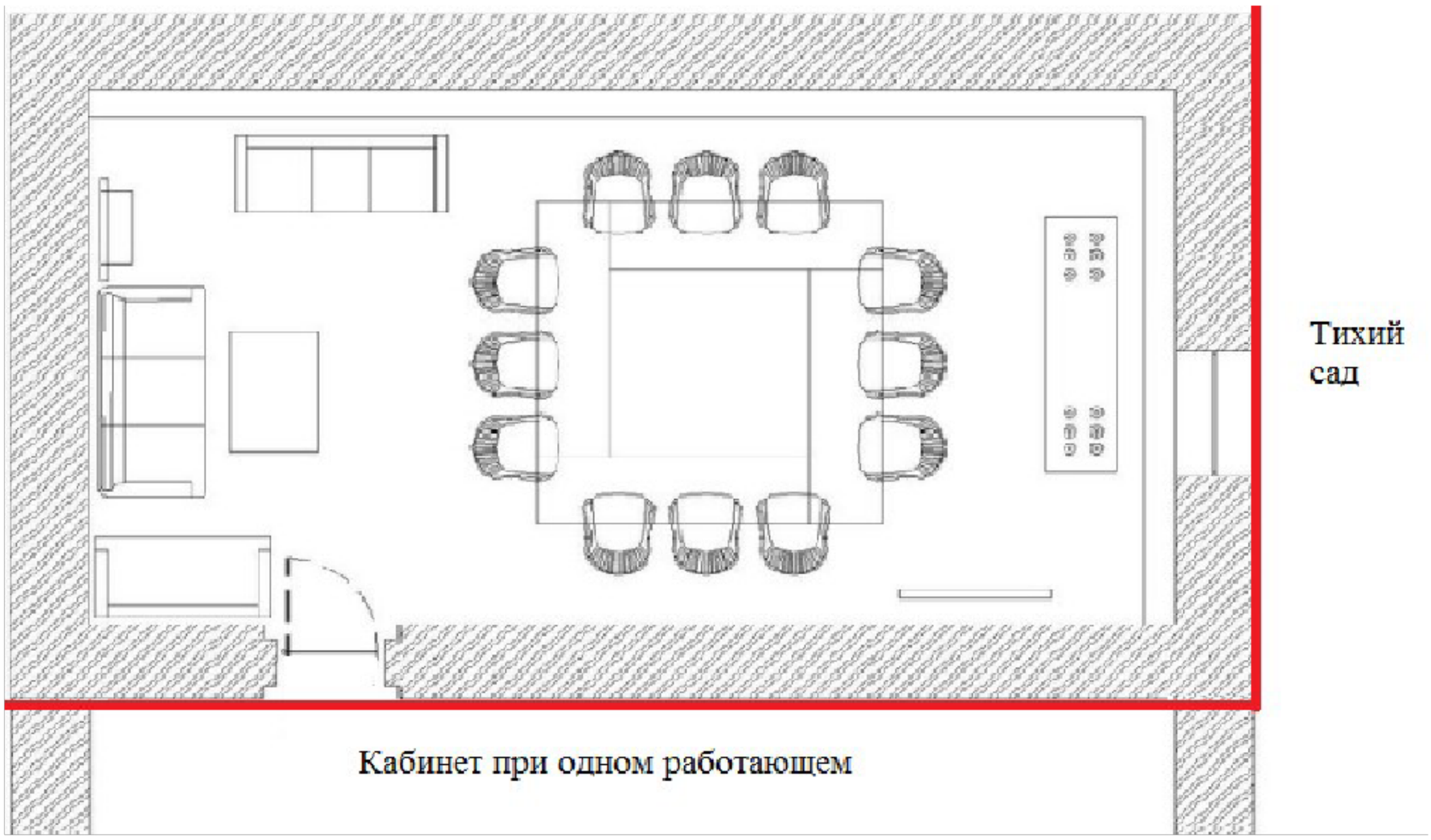
Комната тихая

Размеры помещения: а=8м, в=4м, h=3,5м

Размер двери: 2х0,9м.



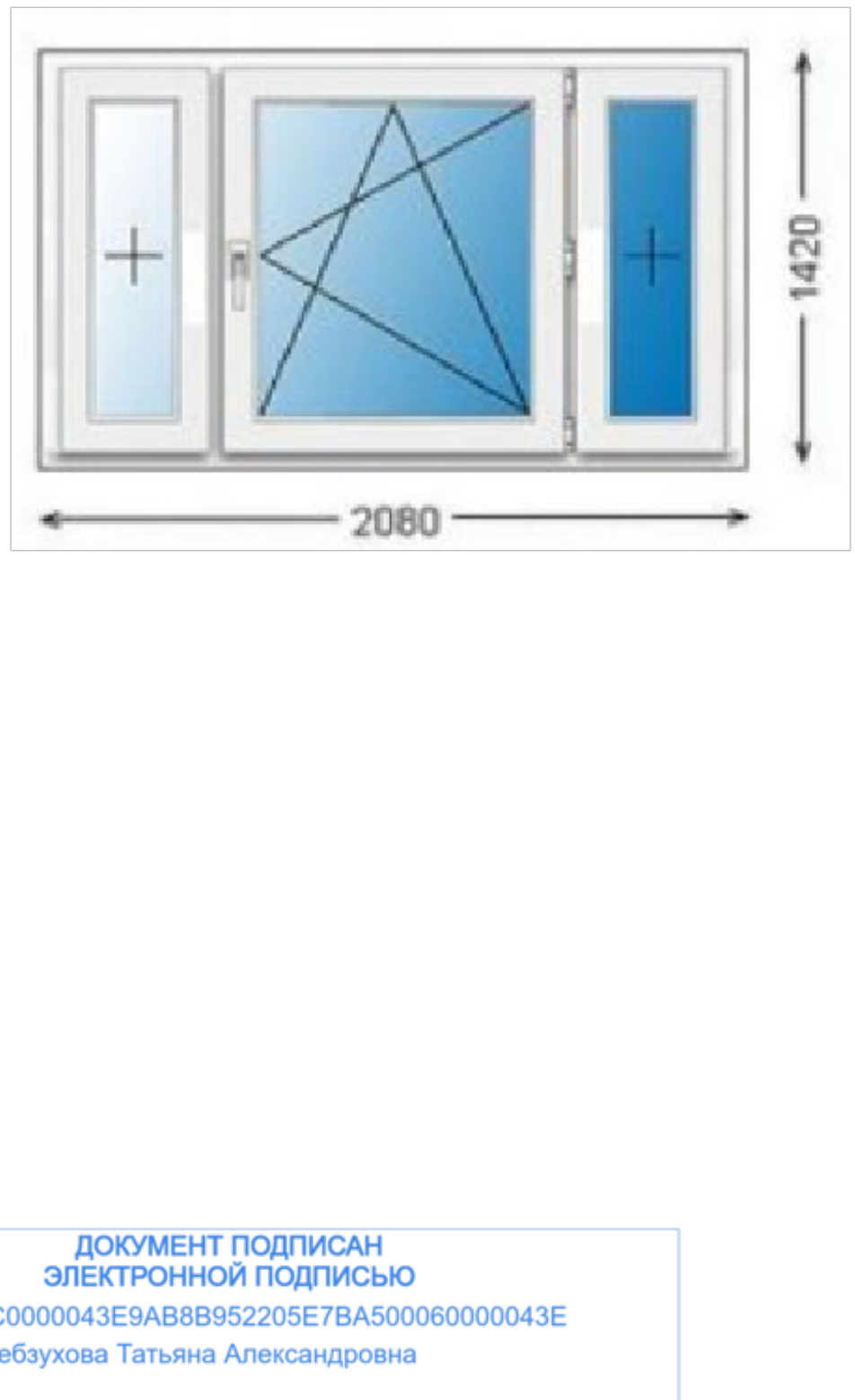
20.Помещение для переговоров №20



Кабинет при одном работающем

Размеры: 4х7м, h=3м

Размер двери: 2х0,9м.



МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»
Пятигорский институт (филиал) СКФУ

Методические указания

для обучающихся по организации и проведению самостоятельной работы
по дисциплине «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ»
для студентов направления подготовки **09.03.02 Информационные системы и технологии**
направленность (профиль) **Информационные системы и технологии обработки цифрового контента**

Пятигорск, 2022

СОДЕРЖАНИЕ

1. Общие положения

Самостоятельная работа - планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное (аудиторное) время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия (при частичном непосредственном участии преподавателя, оставляющем ведущую роль за работой студентов).

Самостоятельная работа студентов (СРС) в ВУЗе является важным видом учебной и научной деятельности студента. Самостоятельная работа студентов играет значительную роль в рейтинговой технологии обучения.

К основным видам самостоятельной работы студентов относятся:

– формирование и усвоение содержания конспекта лекций на базе рекомендованной лектором учебной литературы, включая информационные образовательные ресурсы (электронные учебники, электронные библиотеки и др.);

– написание докладов;

– подготовка к семинарам, практическим и лабораторным работам, их оформление;

– составление аннотированного списка статей из соответствующих журналов по отраслям знаний (педагогических, психологических, методических и др.);

– выполнение учебно-исследовательских работ, проектная деятельность;

– подготовка лабораторных разработок и рекомендаций по решению проблемной ситуации;

– выполнение домашних заданий в виде решения отдельных задач, проведения типовых расчетов, расчетно-компьютерных и индивидуальных работ по отдельным разделам содержания дисциплин и т.д.;

– компьютерный текущий самоконтроль и контроль успеваемости на базе электронных обучающих и аттестующих тестов;

– выполнение курсовых работ (проектов) в рамках дисциплин;

– выполнение выпускной квалификационной работы и др.

Методика организации самостоятельной работы студентов зависит от структуры, характера и особенностей изучаемой дисциплины, объема часов на ее изучение, вида заданий для самостоятельной работы студентов, индивидуальных качеств студентов и условий учебной деятельности.

Процесс организации самостоятельной работы студентов включает в себя следующие этапы:

- подготовительный (определение целей, составление программы, подготовка методического обеспечения, подготовка оборудования);
- основной (реализация программы, использование приемов поиска информации, усвоения, переработки, применения, передачи знаний, фиксирование результатов, самоорганизация процесса работы);
- заключительный (оценка значимости и анализ результатов, их систематизация, оценка эффективности программы и приемов работы, выводы о направлениях оптимизации труда).

Самостоятельная работа по дисциплине «Информационная безопасность» направлена на формирование следующих **компетенций**:

Код	Формулировка:
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

2. Цель и задачи самостоятельной работы

Ведущая цель организации и осуществления СРС совпадает с целью обучения студента – формирование набора общенаучных, профессиональных и специальных компетенций будущего бакалавра по соответствующему направлению подготовки

При организации СРС важным и необходимым условием становятся формирование умения самостоятельной работы для приобретения знаний, навыков и возможности организации учебной и научной деятельности. Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Задачами СРС являются:

- систематизация и закрепление полученных теоретических знаний и лабораторных умений студентов;
- углубление и расширение теоретических знаний;
- формирование умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развитие исследовательских умений;
- использование материала, собранного и полученного в ходе самостоятельных занятий на семинарах, на лабораторных и лабораторных занятиях, при написании курсовых и выпускной квалификационной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

3. Технологическая карта самостоятельной работы студента

Коды реализуемых компетенций	Вид деятельности студентов	Средства и технологии оценки	Объем часов, в том числе (астр.)		
			СРС	Контактная работа с преподавателем	Всего
ОПК-3 (ИД-$1_{ОПК-3}$ИД-$2_{ОПК-3}$ ИД-$3_{ОПК-3}$)	Самостоятельное изучение литературы и источников	Собеседование	38,52	4,28	42,8
ОПК-3 (ИД-$1_{ОПК-3}$ИД-$2_{ОПК-3}$ ИД-$3_{ОПК-3}$)	Подготовка к лабораторным занятиям	Защита ПР	6,48	0,72	7,2
ОПК-3 (ИД-$1_{ОПК-3}$ИД-$2_{ОПК-3}$ ИД-$3_{ОПК-3}$)	Написание реферата/доклада	Защита доклада	9	1	10
		Итого	54	6	60

4. Порядок выполнения самостоятельной работы студентом

4.1. Методические рекомендации по работе с учебной литературой

При работе с книгой необходимо подобрать литературу, научиться правильно ее читать, вести записи. Для подбора литературы в библиотеке используются алфавитный и систематический каталоги.

Важно помнить, что рациональные навыки работы с книгой - это всегда большая экономия времени и сил.

Правильный подбор учебников рекомендуется преподавателем, читающим лекционный курс. Необходимая литература может быть также указана в методических разработках по данному курсу.

Изучая материал по учебнику, следует переходить к следующему вопросу только после правильного уяснения предыдущего, описывая на бумаге все выкладки и вычисления (в том числе те, которые в учебнике опущены или на лекции даны для самостоятельного вывода).

При изучении любой дисциплины большую и важную роль играет самостоятельная индивидуальная работа.

Особое внимание следует обратить на определение основных понятий курса. Студент должен подробно разбирать примеры, которые поясняют такие определения, и уметь строить аналогичные примеры самостоятельно. Нужно добиваться точного представления о том, что изучаешь. Полезно составлять опорные конспекты. При изучении материала по учебнику полезно в тетради (на специально отведенных полях) дополнять конспект лекций. Там же следует отмечать вопросы, выделенные студентом для консультации с преподавателем.

Выводы, полученные в результате изучения, рекомендуется в конспекте выделять, чтобы они при перечитывании записей лучше запоминались.

Опыт показывает, что многим студентам помогает составление листа опорных сигналов, содержащего важнейшие и наиболее часто употребляемые формулы и понятия. Такой лист помогает запомнить формулы, основные положения лекции, а также может служить постоянным справочником для студента.

Чтение научного текста является частью познавательной деятельности. Ее цель – извлечение из текста необходимой информации. От того на сколько осознанна читающим собственная внутренняя установка при обращении к печатному слову (найти нужные сведения, усвоить информацию полностью или частично, критически проанализировать материал и т.п.) во многом зависит эффективность осуществляемого действия.

Выделяют ***четыре основные установки в чтении научного текста***:

информационно-поисковый (задача – найти, выделить искомую информацию)

усваивающая (усилия читателя направлены на то, чтобы как можно полнее осознать и запомнить как сами сведения излагаемые автором, так и всю логику его рассуждений)

аналитико-критическая (читатель стремится критически осмыслить материал, проанализировав его, определив свое отношение к нему)

творческая (создает у читателя готовность в том или ином виде – как отправной пункт для своих рассуждений, как образ для действия по аналогии и т.п. – использовать суждения автора, ход его мыслей, результат наблюдения, разработанную методику, дополнить их, подвергнуть новой проверке).

Основные виды систематизированной записи прочитанного:

Аннотирование – предельно краткое связное описание просмотренной или прочитанной книги (статьи), ее содержания, источников, характера и назначения;

Планирование – краткая логическая организация текста, раскрывающая содержание и структуру изучаемого материала;

Тезирование – лаконичное воспроизведение основных утверждений автора без привлечения фактического материала;

Цитирование – дословное выписывание из текста выдержек, извлечений, наиболее существенно отражающих ту или иную мысль автора;

Конспектирование – краткое и последовательное изложение содержания прочитанного.

Конспект – сложный способ изложения содержания книги или статьи в логической последовательности. Конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.

Методические рекомендации по составлению конспекта:

1. Внимательно прочитайте текст. Уточните в справочной литературе непонятные слова. При записи не забудьте вынести справочные данные на поля конспекта;
2. Выделите главное, составьте план;
3. Кратко сформулируйте основные положения текста, отметьте аргументацию автора;
4. Законспектируйте материал, четко следуя пунктам плана. При конспектировании старайтесь выразить мысль своими словами. Записи следует вести четко, ясно.
5. Грамотно записывайте цитаты. Цитируя, учитывайте лаконичность, значимость мысли.

В тексте конспекта желательно приводить не только тезисные положения, но и их доказательства. При оформлении конспекта необходимо стремиться к емкости каждого предложения. Мысли автора книги следует излагать кратко, заботясь о стиле и выразительности написанного. Число дополнительных элементов конспекта должно быть логически обоснованным, записи должны распределяться в определенной последовательности, отвечающей логической структуре произведения. Для уточнения и дополнения необходимо оставлять поля.

Овладение навыками конспектирования требует от студента целеустремленности, повседневной самостоятельной работы.

4.2. Методические рекомендации по подготовке к практическим и лабораторным занятиям

Для того чтобы практические и лабораторные занятия приносили максимальную пользу, необходимо помнить, что упражнение и решение задач проводятся по вычитанному на лекциях материалу и связаны, как правило, с детальным разбором отдельных вопросов лекционного курса. Следует подчеркнуть, что только после усвоения лекционного материала с определенной точки зрения (а именно с той, с которой он излагается на лекциях) он будет закрепляться на лабораторных занятиях как в результате обсуждения и анализа лекционного материала, так и с помощью решения проблемных ситуаций, задач. При этих условиях студент не только хорошо усвоит материал, но и научится применять его на практике, а также получит дополнительный стимул (и это очень важно) для активной проработки лекции.

При самостоятельном решении задач нужно обосновывать каждый этап решения, исходя из теоретических положений курса. Если студент видит несколько путей решения проблемы (задачи), то нужно сравнить их и выбрать самый рациональный. Полезно до начала вычислений составить краткий план решения проблемы (задачи). Решение проблемных задач или примеров следует излагать подробно, вычисления располагать в строгом порядке, отделяя вспомогательные вычисления от основных. Решения при необходимости нужно сопровождать комментариями, схемами, чертежами и рисунками.

Следует помнить, что решение каждой учебной задачи должно доводиться до окончательного логического ответа, которого требует условие, и по возможности с выводом. Полученный ответ следует проверить способами, вытекающими из существа данной задачи. Полезно также (если возможно) решать несколькими способами и сравнить полученные результаты. Решение задач данного типа нужно продолжать до приобретения твердых навыков в их решении.

4.3. Методические рекомендации по самопроверке знаний

После изучения определенной темы по записям в конспекте и учебнику, а также решения достаточного количества соответствующих задач на лабораторных занятиях и самостоятельно студенту рекомендуется, провести самопроверку усвоенных знаний, ответив на контрольные вопросы по изученной теме.

В случае необходимости нужно еще раз внимательно разобраться в материале.

Иногда недостаточность усвоения того или иного вопроса выясняется только при изучении дальнейшего материала. В этом случае надо вернуться назад и повторить плохо усвоенный материал. Важный критерий усвоения теоретического материала - умение решать задачи или пройти тестирование по пройденному материалу. Однако следует помнить, что правильное решение задачи может получиться в результате применения механически заученных формул без понимания сущности теоретических положений.

4.4. Методические рекомендации по написанию научных текстов (докладов, докладовов, эссе, научных статей и т.д.)

Перед тем, как приступить к написанию научного текста, важно разобраться, какова истинная цель вашего научного текста - это поможет вам разумно распределить свои силы и время.

Во-первых, сначала нужно определиться с идеей научного текста, а для этого необходимо научиться либо относиться к разным явлениям и фактам несколько критически (своя идея – как иная точка зрения), либо научиться увлекаться какими-то известными идеями, которые нуждаются в доработке (идея – как оптимистическая позиция и направленность на дальнейшее совершенствование уже известного). Во-вторых, научиться организовывать свое время, ведь, как известно, свободное (от всяких глупостей) время – важнейшее условие настоящего творчества, для него наконец-то появляется время. Иногда именно на организацию такого времени уходит немалая часть сил и талантов.

Писать следует ясно и понятно, стараясь основные положения формулировать четко и недвусмысленно (чтобы и самому понятно было), а также стремясь структурировать свой текст. Каждый раз надо представлять, что ваш текст будет кто-то читать и ему захочется сориентироваться в нем, быстро находить ответы на интересующие вопросы (заодно представьте себя на месте такого человека). Понятно, что работа, написанная «сплошным текстом» (без заголовков, без выделения крупным шрифтом наиболее важным мест и т, п.), у культурного читателя должна вызывать брезгливость и даже жалость к автору (исключения составляют некоторые древние тексты, когда и жанр был иной и к текстам относились иначе, да и самих текстов было гораздо меньше – не то, что в эпоху «информационного взрыва» и соответствующего «информационного мусора»).

Объем текста и различные оформительские требования во многом зависят от принятых в конкретном учебном заведении порядков.

Доклад - это самостоятельное исследование студентом определенной проблемы, комплекса взаимосвязанных вопросов.

Доклад не должна составляться из фрагментов статей, монографий, пособий. Кроме простого изложения фактов и цитат, в доклад е должно проявляться авторское видение проблемы и ее решения.

Рассмотрим основные этапы подготовки

а студентом.

Выполнение доклада начинается с выбора темы.

Затем студент приходит на первую консультацию к руководителю, которая предусматривает:

- обсуждение цели и задач работы, основных моментов избранной темы;
- консультирование по вопросам подбора литературы;
- составление предварительного плана.

Следующим этапом является работа с литературой. Необходимая литература подбирается студентом самостоятельно.

После подбора литературы целесообразно сделать рабочий вариант плана работы. В нем нужно выделить основные вопросы темы и параграфы, раскрывающие их содержание.

Составленный список литературы и предварительный вариант плана уточняются, согласуются на очередной консультации с руководителем.

Затем начинается следующий этап работы - изучение литературы. Только внимательно читая и конспектируя литературу, можно разобраться в основных вопросах темы и подготовиться к самостоятельному (авторскому) изложению содержания доклада. Конспектируя первоисточники, необходимо отразить основную идею автора и его позицию по исследуемому вопросу, выявить проблемы и наметить задачи для дальнейшего изучения данных проблем.

Систематизация и анализ изученной литературы по проблеме исследования позволяют студенту написать работу.

Рабочий вариант текста доклада предоставляется руководителю на проверку. На основе рабочего варианта текста руководитель вместе со студентом обсуждает возможности доработки текста, его оформление. После доработки доклад сдается на кафедру для его оценивания руководителем.

Требования к написанию доклада

Написание 1 доклада является обязательным условием выполнения плана СРС по любой дисциплине профессионального цикла.

Тема доклада может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Доклад должен быть написан научным языком.

Объем доклада должен составлять 20-25 стр.

Структура доклада:

● Введение (не более 3-4 страниц). Во введении необходимо обосновать выбор темы, ее актуальность, очертить область исследования, объект исследования, основные цели и задачи исследования.

● Основная часть состоит из 2-3 разделов. В них раскрывается суть исследуемой проблемы, проводится обзор мировой литературы и источников Интернет по предмету исследования, в котором дается характеристика степени разработанности проблемы и авторская аналитическая оценка основных теоретических подходов к ее решению. Изложение материала не должно ограничиваться лишь описательным подходом к раскрытию выбранной темы. Оно также должно содержать собственное видение рассматриваемой проблемы и изложение собственной точки зрения на возможные пути ее решения.

● Заключение (1-2 страницы). В заключении кратко излагаются достигнутые при изучении проблемы цели, перспективы развития исследуемого вопроса

● Список использованной литературы (не меньше 10 источников), в алфавитном порядке, оформленный в соответствии с принятыми правилами. В список использованной литературы рекомендуется включать работы отечественных и зарубежных авторов, в том числе статьи, опубликованные в научных журналах в течение последних 3-х лет и ссылки на ресурсы сети Интернет.

● Приложение (при необходимости).

Требования к оформлению:

● текст с одной стороны листа;
● шрифт Times New Roman;
● кегль шрифта 14;
● межстрочное расстояние 1,5;
● поля: сверху 2,5 см, снизу – 2,5 см, слева - 3 см, справа 1,5 см;
● доклад должен быть представлен в сброшюрованном виде.

Порядок защиты доклада:

Защита доклада проводится на лабораторных занятиях, после окончания работы студента над ним и исправления всех недочетов, выявленных преподавателем в ходе консультаций. На защиту доклада отводится 5-7 минут времени, в ходе которого студент должен показать свободное владение материалом по заявленной теме. При защите доклада приветствуется использование мультимедиа-презентации.

Оценка доклада

Доклад оценивается по следующим критериям:

• соблюдение требований к его оформлению;

• необходимость и достаточность для раскрытия темы приведенной в тексте доклада информации;

• умение студента свободно излагать основные идеи, отраженные в докладе;

• способность студента понять суть задаваемых преподавателем и сокурсниками вопросов и сформулировать точные ответы на них.

Критерии оценки:

Оценка «отлично» выставляется студенту, если в докладе студент исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует для написания доклада современные научные материалы; анализирует полученную информацию; проявляет самостоятельность при написании доклада.

Оценка «хорошо» выставляется студенту, если качество выполнения доклада достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопросы по теме доклада.

Оценка «удовлетворительно» выставляется студенту, если материал доклада излагается частично, но пробелы не носят существенного характера, студент допускает неточности и ошибки при защите доклада, дает недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении материала.

Оценка «неудовлетворительно» выставляется студенту, если он не подготовил доклад или допустил существенные ошибки. Студент неуверенно излагает материал доклада, не отвечает на вопросы преподавателя.

Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным 55. Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.5. Методические рекомендации по выполнению исследовательских проектов

Исследовательская проектная работа – это групповая работа, для выполнения которой необходим выбор и приложение научной методики к поставленной задаче, получение собственного теоретического или экспериментального материала, на основании которого необходимо провести анализ и сделать выводы об исследуемом явлении. Выполнение проекта – это всегда коллективная, творческая лабораторная работа, предназначенная для получения определенного продукта или научно-технического результата. Такая работа подразумевает четкое, однозначное формирование поставленной задачи, определение сроков выполнения намеченного, определение требований к разрабатываемому объекту.

Выполнение 1 группового проекта является обязательным условием выполнения самостоятельной работы по любой дисциплине профессионального цикла. Тема проектного задания может быть выбрана студентом из предложенных в рабочей программе или фонде оценочных средств дисциплины, либо определена самостоятельно, исходя из интересов студента (в рамках изучаемой дисциплины). Выбранную тему необходимо согласоваться с преподавателем.

Требования по выполнению и оформлению проекта

При выполнении проекта приветствуется работа в группе (2-3 человека). Проект – это исследовательская работа, в ходе которой студенты должны продемонстрировать владение навыками научного исследования, умения проводить анализ, обобщать информацию, делать выводы, предлагать свои решения проблемы, рассматриваемой в проекте.

При подготовке материалов проекта студенты должны продемонстрировать владение современными методами компьютерной обработки данных.

Критерии оценки работы участника проекта.

Для каждого из участников проекта оцениваются:

• профессиональные теоретические знания в соответствующей области;

• умение работать со справочной и научной литературой, осуществлять поиск необходимой информации в Интернет;

• умение работать с техническими средствами;

• умение пользоваться соответствующими выполняемому проекту информационными технологиями;

• умение готовить материалы проекта для презентации: составлять и редактировать тексты, формировать презентацию проекта;

• умение работать в команде;

• умение публично представлять результаты собственной деятельности;

• коммуникабельность, инициативность, творческие способности.

Критерии выставления оценки участникам проекта

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
«Отлично»	Работа выполнена на высоком профессиональном уровне. Представленный материал в основном фактически верен, допускаются негрубые фактические неточности. Студент свободно отвечает на вопросы, связанные с проектом.	Технические средства и информационные технологии освоены и использованы для реализации проекта полностью	Студент проявил инициативу, творческий подход, способность к выполнению сложных заданий, навыки работы в коллективе, организационные способности.	Проект представлен полностью и в срок.
«Хорошо»	Работа выполнена на достаточно высоком профессиональном уровне. Допущено до 4–5 фактических ошибок. Студент отвечает на вопросы, связанные с проектом, но недостаточно полно.	Обнаруживаются некоторые ошибки в использовании соответствующих технических средств и информационных технологий	Студент достаточно полно, но без инициативы и творческих находок выполнил возложенные на него задачи.	Проект представлен достаточно полно и в срок, но с некоторыми недоработками.
«Удовлетворительно»	Уровень недостаточно высок. Допущено до 8 фактических ошибок. Студент может ответить лишь на некоторые из заданных вопросов, связанных с проектом.	Обнаруживает недостаточное владение навыками работы с техническими средствами и соответствующими информационными технологиями	Студент выполнил большую часть возложенной на него работы.	Проект сдан со значительным опозданием (более недели) и не полностью
«Неудовлетворительно»	Работа не выполнена или выполнена на низком уровне. Допущено более 8 фактических ошибок. Ответы на	Навыков работы с техническими средствами нет, информационные технологии не освоены	Студент практически не работал, не выполнил свои задачи или выполнил лишь	Проект не сдан.

Оценка	Профессиональные компетенции	Компетенции, связанные с использованием соответствующих выполняемому проекту технических средств и информационных технологий	Иные универсальные компетенции (коммуникабельность, инициативность, умение работать в «команде», управленческие навыки и т.д.)	Отчетность
	связанные с проектом вопросы обнаруживают непонимание предмета и отсутствие ориентации в материале проекта.		отдельные не существенные поручения в групповом проекте.	

Студенты должны: защитить проект в режиме презентации, предъявить файлы выполненного проекта, уметь рассказать о технологиях, использованных ими при выполнении проекта, дать оценку работы каждого члена группы (*если проект групповой*).

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	100
Хороший	80
Удовлетворительный	60
Неудовлетворительный	0

4.6. Методические рекомендации по подготовке к экзаменам и зачетам

Изучение многих общепрофессиональных и специальных дисциплин завершается экзаменом. Подготовка к экзамену способствует закреплению, углублению и обобщению знаний, получаемых, в процессе обучения, а также применению их к решению лабораторных задач. Готовясь к экзамену, студент ликвидирует имеющиеся пробелы в знаниях, углубляет, систематизирует и упорядочивает свои знания. На экзамене студент демонстрирует то, что он приобрел в процессе обучения по конкретной учебной дисциплине.

Экзаменационная сессия - это серия экзаменов, установленных учебным планом. Между экзаменами интервал 3-4 дня. Не следует думать, что 3-4 дня достаточно для успешной подготовки к экзаменам.

В эти 3-4 дня нужно систематизировать уже имеющиеся знания. На консультации перед экзаменом студентов познакомят с основными требованиями, ответят на возникшие у них вопросы. Поэтому посещение консультаций обязательно.

Требования к организации подготовки к экзаменам те же, что и при занятиях в течение семестра, но соблюдаться они должны более строго. Во-первых, очень важно соблюдение режима дня; сон не менее 8 часов в сутки, занятия заканчиваются не позднее, чем за 2-3 часа до сна. Оптимальное время занятий - утренние и дневные часы. В перерывах между занятиями рекомендуются прогулки на свежем воздухе, неутомительные занятия спортом. Во-вторых, наличие хороших собственных конспектов лекций. Даже в том случае, если была пропущена какая-либо лекция, необходимо во время ее восстановить (переписать ее на кафедре), обдумать, снять возникшие вопросы для того, чтобы запоминание материала было осознанным. В-третьих, при подготовке к экзаменам у студента должен быть хороший учебник или конспект литературы, прочитанной по указанию преподавателя в течение семестра. Здесь можно эффективно использовать листы опорных сигналов.

Вначале следует просмотреть весь материал по сдаваемой дисциплине, отметить для себя трудные вопросы. Обязательно в них разобраться. В заключение еще раз целесообразно повторить основные положения, используя при этом листы опорных сигналов.

Систематическая подготовка к занятиям в течение семестра позволит использовать время экзаменационной сессии для систематизации знаний.

Контроль самостоятельной работы студентов

Контроль самостоятельной работы проводится преподавателем в аудитории.

Предусмотрены следующие виды контроля: собеседование, оценка доклада, оценка презентации, оценка участия в круглом столе, оценка выполнения проекта.

Подробные критерии оценивания компетенций приведены в Фонде оценочных средств для проведения текущей и промежуточной аттестации.

Список литературы для выполнения СРС

Основная литература:

1. Галатенко В.А. Информационная безопасность [Электронный ресурс]/ Галатенко В.А.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 266 c. - Книга находится в базовой версии ЭБС IPRbooks., экземпляров неограниченно

2. Нестеров С.А. Информационная безопасность [Электронный ресурс]: учебное пособие/ Нестеров С.А.— Электрон. текстовые данные.— СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2014.— 322 c.- Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-87623-969-3, экземпляров неограниченно

Дополнительная литература:

1. Фаронов А.Е. Информационная безопасность при работе на компьютере [Электронный ресурс]/ Фаронов А.Е.— Электрон. текстовые данные.— М.: Интернет-Университет Информационных Технологий (ИНТУИТ), 2016.— 154 c. - Книга находится в премиум-версии ЭБС IPR BOOKS. - ISBN 978-5-9500999-7-7, экземпляров неограниченно

2. Защита информации в операционных системах: учеб.пособие.- Ставрополь: Изд-во СГУ, 2015.- 318 с - Книга находится в базовой версии ЭБС IPRbooks. - ISBN 978-5-91359-219-4, экземпляров неограниченно

Методическая литература:

1. Методические рекомендации по выполнению лабораторных работ по дисциплине "Информационная безопасность"

2. Методические рекомендации по организации самостоятельной работы студентов по дисциплине "Информационная безопасность"

Интернет-ресурсы:

1. http://el.ncfu.ru/ – система управления обучением ФГАОУ ВО СКФУ. Дистанционная поддержка дисциплины «Цифровая грамотность и обработка больших данных»
2. http://www.un.org - Сайт ООН Информационно-коммуникационные технологии
3. http://www.intuit.ru – Интернет-Университет Компьютерных технологий.

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 2C0000043E9AB8B952205E7BA500060000043E
Владелец: Шебзухова Татьяна Александровна

Действителен: с 19.08.2022 по 19.08.2023