Памятка
По обеспечению требований КБ при использовании сервиса Zoom

1. Общие положения

1.1. Настоящий документ определяет требования по обеспечению кибербезопасности (далее – КБ) при использовании сервиса Zoom (далее – Сервис) работниками подразделений ПАО «Сбербанк» (далее – Банк).

1.2. Сервис Zoom – сторонний сервис, не принадлежащий Банку, используемый для проведения онлайн сеансов телефонной и видеоконференцсвязи (далее – ТКС и ВКС соответственно).

1.3. Сервис рекомендуется использовать в целях обеспечения непрерывности деятельности, в случаях недоступности штатного сервиса ВКС/ТКС Банка, а также при взаимодействии с работниками внешних организаций.

1.4. Настоящий документ распространяется на всех работников Банка.

1.5. Ключевые требования при использовании Сервиса:

Обсуждение конфиденциальной информации	**К3-К4**
Передача файлов	**запрещено**
Демонстрация рабочего стола	**разрешено**
Запись конференции	**запрещено**

2. Требования по обеспечению КБ

2.1. Работникам, участвующим в проведении ВКС/ТКС, назначаются следующие роли:

- организатор – лицо, инициировавшее проведение ВКС/ТКС;
- участник – лицо, участвующее в проведении ВКС/ТКС.

2.2. Требования к организации ВКС/ТКС.

При создании ВКС/ТКС организатор должен обеспечить следующие требования:

2.2.1. При первичной регистрации в Сервисе, работникам Банка рекомендуется использовать вход с доменной учетной записи (Sigma). При регистрации требуется установленный сертификат безопасности[1], выпущенный УЦ Банка.

2.2.2. Участникам, не имеющим учетные записи в домене Sigma (работники ДЗО, Компаний партнеров, Компаний Экосистемы Сбербанк и пр.), пересылается идентификатор конференции (далее – ИК) на личный/рабочий адрес электронной почты.

[1] Ссылка на сайт Центра сертификации – https://pki.sberbank.ru/

2.2.3. Организатор должен запретить подключение к ВКС/ТКС пользователям недоверенных доменов (рис. 1).

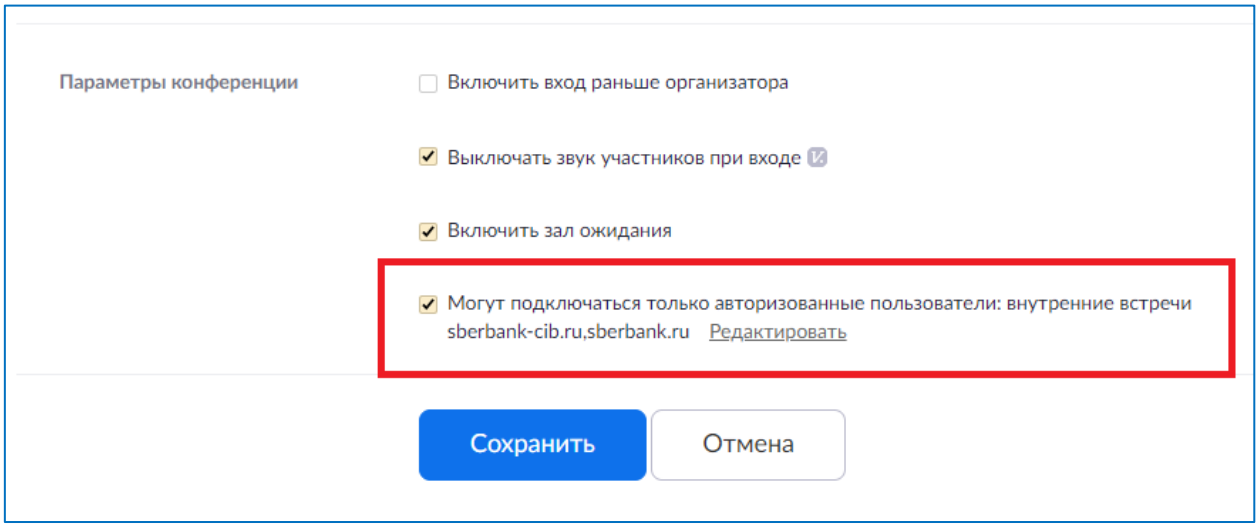

рис. 1 – подключение авторизованных пользователей

2.2.4. ИК должен рассылаться адресно по электронной почте участникам, приглашенным к участию в мероприятии. Публикация ИК в открытых источниках запрещена.

2.2.5. При создании ВКС/ТКС организатор должен использовать случайный ИК (рис. 2).

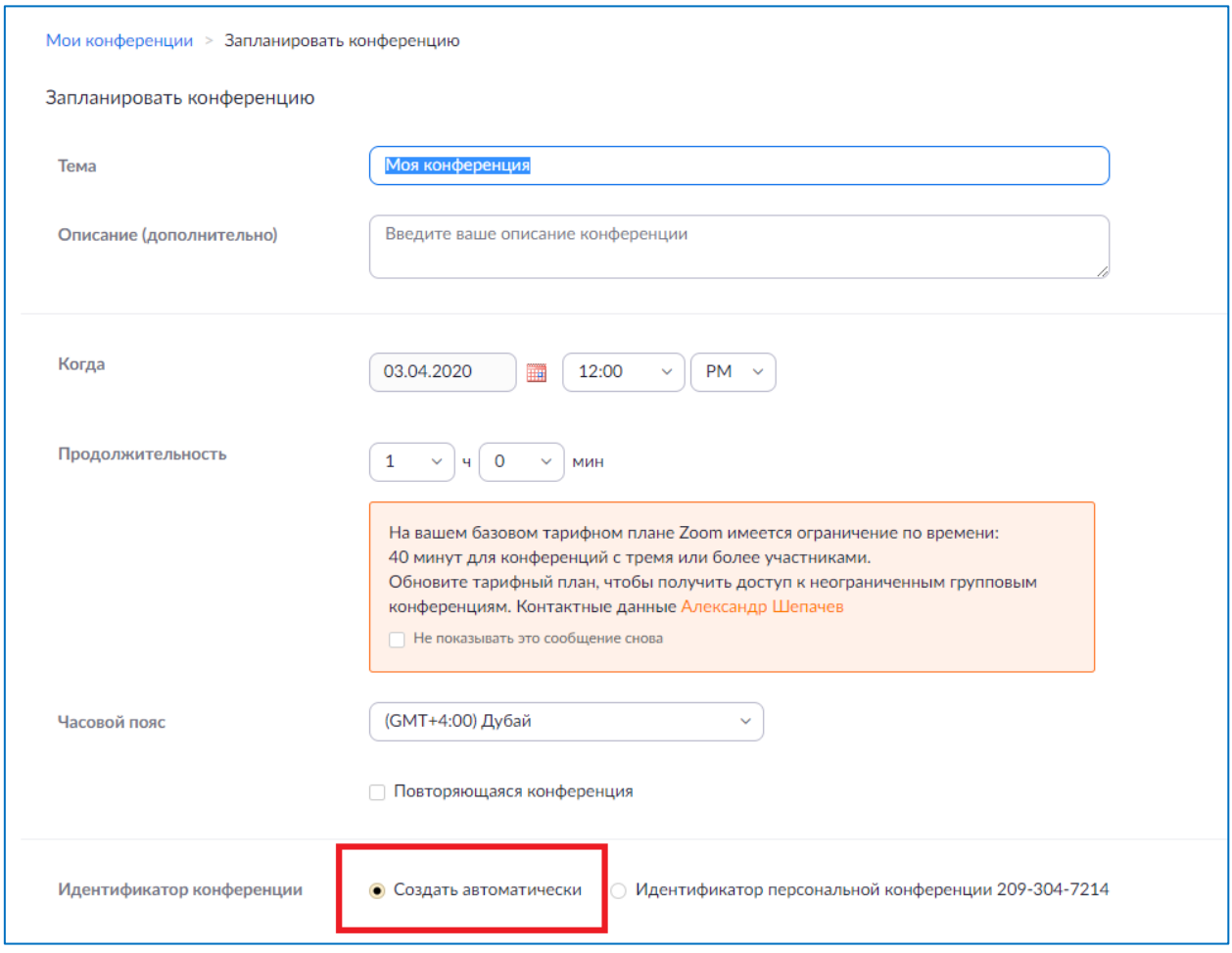

рис. 2 – создание автоматического ИК

2.2.6. Рассылка сгенерированной прямой ссылки на подключение к конференции запрещена.

2.2.7. При создании ВКС/ТКС организатор должен установить сложный уникальный пароль (рис. 3) для подключения к конференции (пароль должен содержать не менее восьми символов, прописные и строчные латинские буквы, цифры, знаки пунктуации).

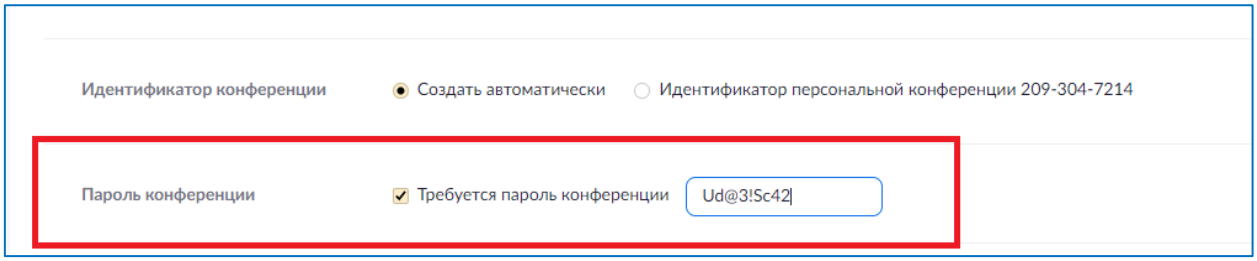

рис. 3 – создание пароля ВКС/ТКС

2.2.8. При создании ВКС организатор должен включить функцию зала ожидания (рис. 4), заблаговременно подключиться к конференции для разрешения доступа участникам к ВКС и, в ходе проведения совещания, контролировать список участников на предмет присутствия посторонних лиц с последующей их блокировкой (при наличии).

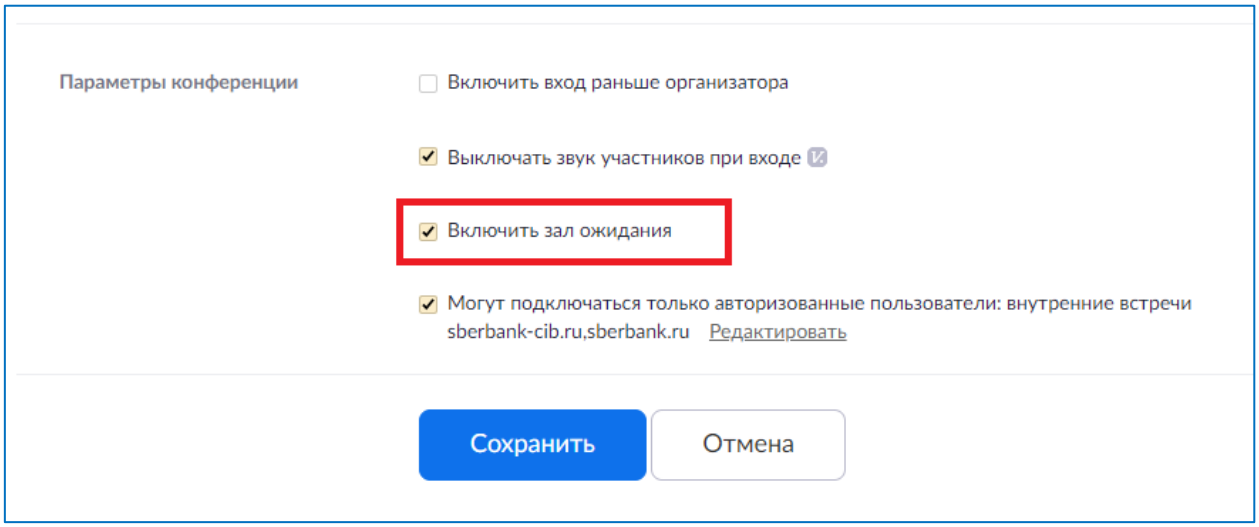

рис. 4 – создание зала ожидания

2.2.9. В случае, если на ВКС/ТКС участвует полный состав участников, организатор должен заблокировать конференцию, в целях недопущения сторонних подключений.

2.3. Требования к проведению ВКС/ТКС

В ходе проведения ВКС/ТКС организатор и участники обязаны выполнять следующие требования и рекомендации:

2.3.1. Передача ИК сторонним лицам строго запрещена.

2.3.2. Адресная рассылка ВКС/ТКС по электронной почте производится без указания в теме и описании детального предмета встречи, раскрывающего суть обсуждаемых конфиденциальных вопросов, а также информации, которая может прямо или косвенно повлиять на бренд Банка.

2.3.3. До подключения к ВКС/ТКС рекомендуется закрыть сторонние программы.

2.3.4. Запрещается обсуждать конфиденциальные вопросы в присутствии посторонних лиц или в публичных местах.

2.3.5. Запрещается переходить по ссылкам, полученным от недоверенных лиц.

2.3.6. В ходе проведения ВКС/ТКС запрещена передача файлов.

2.3.7. Демонстрация документов, содержащих конфиденциальную информацию категорий К-1 и К-2[2], строго запрещена.

2.3.8. В ходе проведения ВКС/ТКС запрещено организовывать и проводить аудио- и видеозапись совещания как инструментами Сервиса, так и сторонними способами.

2.3.9. В ходе проведения ВКС, до подключения режима демонстрации экрана, участнику совещания необходимо убедиться в соблюдении «политики чистого экрана» – участник обязан не допустить демонстрацию информации, не относящейся к теме ВКС.

2.3.10. Запрещено использование облачного хранилища Сервиса.

2.3.11. Документированный результат ВКС/ТКС (протокол, перечень поручений и пр.) должен направляться участникам адресно на электронную почту.

2.4. Требования к оборудованию для подключения к ВКС/ТКС

Организатор и участники ВКС/ТКС должны убедиться в соблюдении следующих требований к личным устройствам, с которых планируется подключение к Сервису:

2.4.1. На устройстве должна быть установлена одна из следующих операционных систем[3]: iOS (за исключением устройств с процедурой jailbreak), Android (за исключением устройств с root правами), Windows, masOS.

2.4.2. На устройстве должны быть установлены актуальные обновления операционной системы, а также установлено и функционировать антивирусное программное обеспечение с последними обновлениями антивирусных баз (актуальность базы не более 3-х дней).

2.4.3. Инструкция по установке Сервиса на корпоративные и личные устройства представлена на сайте SberStore[4] в разделе «инструкции для удаленной работы».

2.4.4. Запрещено использовать Сервис без установленных актуальных обновлений приложения Сервиса. Участники ВКС/ТКС обязаны проверять выпуск новых версий

[2] Категории конфиденциальной информации изложены в стандарте от 27.11.2019 № 4727 часть 4.
[3] Версии используемых операционных систем должны поддерживаться производителем
[4] Ссылка на ресурс – https://apps.sberbank.ru/pki-gateway

приложения (на официальном сайте Сервиса, Apple Store или Google Play,) не реже одного раза в неделю и своевременно устанавливать обновления, при их наличии. Пользователи ОС Windows и macOS должны ежедневно перед подключением к ВКС/ТКС проверять наличие обновлений (рис. 5).

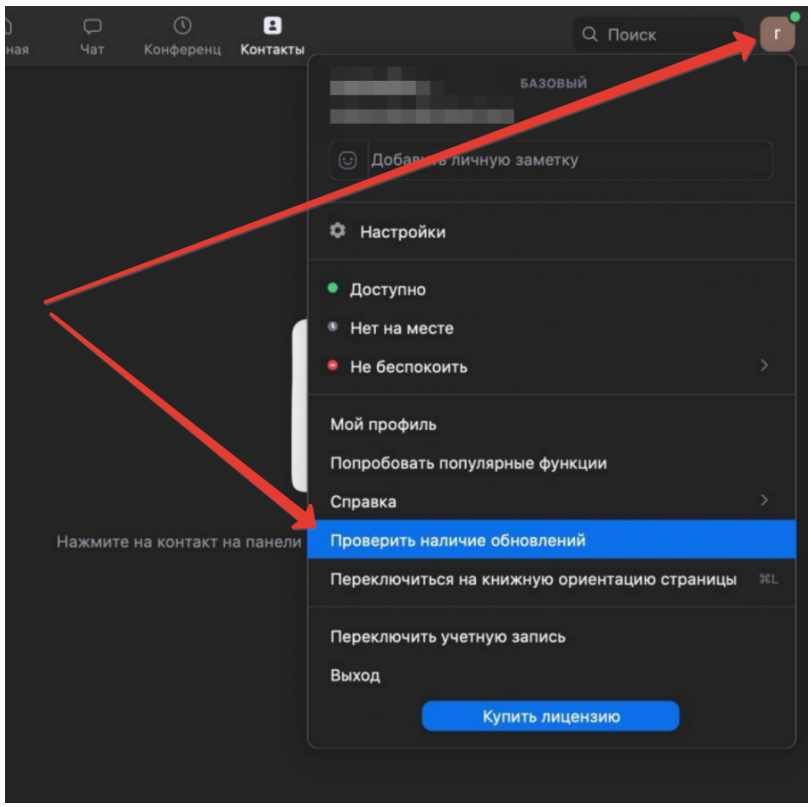

рис. 5 – проверка обновлений

3. Заключительные положения

3.1. Ответственность за соблюдение требований КБ при использовании Сервиса возлагается на всех участников ВКС/ТКС.

3.2. Нарушения требований настоящего документа является инцидентом КБ и расследуется в соответствии с требованиями Стандарта от 04.03.2020 № 4510 ч. 4 «Стандарт проведения экспертиз и расследований инцидентов кибербезопасности ПАО Сбербанк».