|  |
| --- |
| **Банк** |
| Наименование Банка |  |
| **Контактное лицо** |
| ФИО |  |
| Должность |  |
| Телефон |  |
| e-mail |  |

| **№** | **Вопрос** | **Ответ** |
| --- | --- | --- |
| 1. **Необходимые работы**
 |
| 1.1 | Оценка степени соответствия требованиям 716-П только в части ОР в информационных системах и рисков информационной безопасности | *Да\нет* |
| 1.2 | Оценка степени соответствия требованиям 716-П в только части общебанковских ОР | *Да\нет* |
| 1. **Информация о банке**
 |
| 2.1 | Тип лицензии на банковскую деятельность |  |
| 2.2 | Территория деятельности | *Отдельный регион \ несколько регионов \ вся территория РФ* |
| *2.2.1* | *Укажите основные регионы деятельности* |  |
| 2.3 | Используется ли собственный процессинговый центр  | *Собственный процессинг с интеграцией с МПС и НСПК\* *Собственный процессинг с интеграцией с банком-партнером или UCS \**Собственный процессинг отсутствует* |
| 2.4 | Подключенные платежные системы |  |
| *2.4.1* | *Наименование платежной системы* | *Роль Банка* |
|  |  |
|  |  |
|  |  |
| 2.5 | Обладает ли Банк лицензией ФСТЭК России на осуществление деятельности по технической защите конфиденциальной информации? |  |
| 2.6 | Обладает ли Банк лицензией ФСБ России на осуществление технического обслуживания шифровальных (криптографических) средств? |  |
| 2.7 | Опишите основные направления бизнеса: |
| *2.7.1* | *прием вкладов от населения* | *Да\нет* |
| *2.7.2* | *предоставление кредитов населению* | *Да\нет* |
| *2.7.3* | *ипотечное кредитование* | *Да\нет* |
| *2.7.4* | *предоставление депозитных ячеек* | *Да\нет* |
| *2.7.5* | *выпуск и обслуживание платежных карт* | *Да\нет* |
| *2.7.6* | *поддержание собственного карточного процессинга* | *Да\нет* |
| *2.7.7* | *предоставление услуг процессинга* | *Да\нет* |
| *2.7.8* | *обслуживание собственной сети банкоматов* | *Да\нет* |
| *2.7.9* | *обслуживание собственной сети pos-терминалов* | *Да\нет* |
| *2.7.10* | *зарплатные проекты* | *Да\нет* |
| *2.7.11* | *кредитование бизнеса* | *Да\нет* |
| *2.7.12* | *Лизинг* | *Да\нет* |
| *2.7.13* | *Факторинг* | *Да\нет* |
| *2.7.14* | *инвестиционное управление* | *Да\нет* |
| *2.7.15* | *услуги инкассации* | *Да\нет* |
| *2.7.16* | *предоставление прочих финансовых сервисов для бизнеса* | *Перечислите основные* |
| *2.7.17* | *прочие услуги* | *Перечислите основные* |
| 1. **Информация об управлении рисками**
 |
| 3.1 | Используется ли сейчас в банке альтернативная методика оценки операционных рисков (отличная от 652-П)? | *Да\нет* |
| *3.1.1* | *Если да, соответствует ли эта методика требованиям указания ЦБ 3624-У* | *Да\нет* |
| 3.2 | Разработаны ли в банке KRI (КИР), относящиеся к ИТ- и ИБ-рискам? | *Да\нет* |
| *3.2.1* | *Какое количество KRI (КИР), относящиеся к ИТ- и ИБ-рискам, описано?* |  |
| 3.3 | Организованы ли эти KRI (КИР) в дерево с описанными зависимостями и источниками? | *Да\нет* |
| 3.4 | Проводилась ли раньше качественная оценка степени влияния ОР в ИТ и в ИБ на деятельность банка? | *Да\нет* |
| 3.5 | Проводилась ли раньше количественная оценка степени влияния ОР в ИТ и в ИБ на деятельность банка? | *Да\нет* |
| 1. **Персонал**
 |
| 4.1 | Примерная численность персонала кредитной организации | *10 - 100 человек \* *100 - 300 человек \* *300 - 500 человек \* *500 – 1000 человек \* *1000 – 5000 человек \* *Более 5000 человек* |
| 4.2 | Существует ли выделенное подразделение, занимающееся оценкой и управлением операционным риском? | *Да\нет* |
| *4.2.1* | *Сколько сотрудников задействовано в данном подразделении?* |  |
| 4.3 | Существует ли отдельное подразделение, занимающееся ИТ безопасностью? | *Да\нет* |
| *4.3.1* | *В чьем подчинении находится это подразделение?* | *Департамент безопасности \ департамент ИТ \ другое* |
| *4.3.2* | *Сколько сотрудников задействовано в данном подразделении?* |  |
| *4.3.3* | *из них – администраторов средств защиты информации* |  |
| 4.4 | Общее кол-во сотрудников ИТ-подразделения |  |
| *4.4.1* | *из них – администраторов сетевого оборудования* |  |
| *4.4.2* | *из них – администраторов операционных систем* |  |
| *4.4.3* | *из них – администраторов баз данных* |  |
| *4.4.4* | *из них – администраторов ПО систем денежных переводов и обработки персональных данных* |  |
| *4.4.5* | *из них – программистов, участвующих в разработке ПО денежных переводов и обработки персональных данных* |  |
| 1. **Инфраструктура**
 |
| 5.1 | Реализован ли в банке проект по оценке соответствия требованиям ГОСТ57580.1? | *Да\нет* |
| *5.1.1* | *внедрены ли в банке средства и процессы защиты в соответствии с ГОСТ57580.1?* | *Да\нет* |
| 5.2 | Проходил ли Банк оценку соответствия требованиям СТО БР-ИББС-1.0? |  |
| 5.3 | Внедрена ли CMDB? | *Да\нет* |
| 5.4 | Каково примерное количество ИТ-систем\сервисов в каталоге систем\сервисов |  |
| 5.5 | Какое количество из них относится к критичным приложениям? |  |
| 5.6 | Используется ли DWH? какой? |  |
| 5.7 | Какое количество основных ЦОД используется? |  |
| 5.8 | Проводились ли когда-либо учения по отказоустойчивости? | *Да\нет* |
| 5.9 | Внедрена ли система контроля уязвимостей и версий? | *Да\нет* |
| 5.10 | Внедрен ли SIEM или SOC? | *Да\нет* |
| 5.11 | Используются ли для предоставления критичных сервисов сторонние провайдеры услуг? | *Да\нет* |
| 1. **Документирование**
 |
| 6.1 | Документирована ли схема сети Банка? |  |
| 6.2 | Документирован ли реестр используемых в Банке информационных систем? |  |
| 6.3 | Документирована ли Политика ИБ? |  |
| 6.4 | Документирована ли Политика непрерывности? |  |
| 6.5 | Сколько времени (в среднем) занимает согласование и утверждение нормативных документов в Банке? |  |