**Приложение №\_\_. Типовые схемы подключения**

1. Обеспечение конфиденциальности[[1]](#footnote-1), доступности[[2]](#footnote-2) и целостности[[3]](#footnote-3) информации
	1. **Средства криптографической защиты информации (вариант №1)**

Физическая схема подключения автоматизированного рабочего места пользователя предприятия/организации Госкорпорации «Росатом» (далее - АРМ Пользователя) к серверу системы дистанционного банковского обслуживания (далее – Система):



АРМ Пользователя:

Для шифрования канала связи между АРМ Пользователя и сервером Банка на АРМ Пользователя устанавливаются сертифицированные ФСБ России средства криптографической защиты информации (далее – СКЗИ) «С-Терра CSP VPN Client» и СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

Сервер Банка:

На стороне Банка устанавливается сертифицированный ФСБ России ПАК «С-Терра VPN Gate» и СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

* 1. **Средства криптографической защиты информации (вариант №2)**

Физическая схема подключения АРМ Пользователя к серверу Системы:



АРМ Пользователя:

Для шифрования канала связи между АРМ Пользователя и сервером Банка на АРМ Пользователя устанавливается сертифицированное ФСБ России СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

Сервер Банка:

На стороне Банка устанавливается сертифицированное ФСБ России СКЗИ «КриптоПро CSP» с классом защищенности не ниже КС2.

1. Защита информации от несанкционированного доступа

Для обеспечения защиты информации от несанкционированного доступа на стороне Банка и на стороне предприятия/организации Госкорпорации «Росатом» должны выполняться требования следующих документов:

* инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утв. Приказом ФАПСИ от 13 июня 2001г. №152;
* единых отраслевых методических указаниях по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях, утв. Приказом Госкорпорации «Росатом» от 22.10.2015 №1/1009-П;

На стороне предприятия/организации Госкорпорации «Росатом» также должны выполняться:

* отраслевые требования по информационной безопасности Госкорпорации «Росатом» от  13.07.2012;
* отраслевые требованиями по информационной безопасности, утв. Приказом от 23.09.2014 №1/910-П-дсп.

 Программно-технические средства защиты, которые должны быть установлены на АРМ Пользователей и на сервере Системы:

* Сертифицированное ФСТЭК России антивирусное программное обеспечение.

Эксплуатация АРМ Пользователей без установленного антивирусного программного обеспечения или его отключение не допускается. Антивирусная проверка поступающей на АРМ Пользователей информации осуществляется в автоматическом режиме;

* Сертифицированное ФСТЭК России средство защиты информации от несанкционированного доступа.

В качестве средств защиты от несанкционированного доступа необходимо использовать средства, указанные в эксплуатационной и технической документации на СКЗИ «КриптоПро CSP», С-Терра CSP VPN Client или ПАК «С-Терра VPN Gate» (Аппаратно-программный модуль доверенной загрузки универсальный М-526Б «КРИПТОН-ЗАМОК/У» или ПАК защиты от НСД «Соболь» RU.40308570.501410.001)

1. **Выполнение требований по безопасности информации**

АРМ Пользователей и сервер Системы должны соответствовать требованиям по безопасности информации и иметь соответствующие аттестаты соответствия.

Органом криптографической защиты должна быть проведена проверка выполнения требований Инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, утв. Приказом ФАПСИ от 13 июня 2001г. №152 на АРМ Пользователя Системы и на сервере Банка, где установлены СКЗИ. Подтверждением возможности эксплуатации СКЗИ в Системе является Заключение Органа криптографической защиты о возможности эксплуатации СКЗИ.

1. Конфиденциальность информации - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранение в тайне информации от субъектов, не имеющих полномочий на ознакомление с ней. [↑](#footnote-ref-1)
2. Доступность информации - состояние информации, характеризуемое способностью автоматизированной системы обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия. [↑](#footnote-ref-2)
3. Целостность информации - состояние защищенности информации, характеризуемое способностью автоматизированной системы обеспечивать сохранность и неизменность конфиденциальной информации при попытках несанкционированных или случайных воздействий на нее в процессе обработки или хранения. [↑](#footnote-ref-3)