ГОСУДАРСТВЕННАЯ КОРПОРАЦИЯ ПО АТОМНОЙ ЭНЕРГИИ «РОСАТОМ»
(Госкорпорация «Росатом»)

ПРИКАЗ

28 ФЕВ 2023 № 1/326-П

Москва

Об утверждении Единых отраслевых методических указаний по оценке доверия и приведению в соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях

В целях выполнения требований по безопасности информации при эксплуатации защищенных с использованием криптографических средств информационных и телекоммуникационных систем

ПРИКАЗЫВАЮ:

1. Утвердить Единые отраслевые методические указания по оценке доверия и приведению в соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях (далее – Методические указания, приложение № 1).

2. Руководителям организаций Госкорпорации «Росатом», указанных в приложении № 2 к настоящему приказу, обеспечить принятие локальных нормативных актов возглавляемой организации, а также организаций в контуре ее управления, предусматривающих обязательность реализации положений Методических указаний, в соответствии с регламентом по взаимодействию организации и Госкорпорации «Росатом».

Срок – в течение трех недель с даты вступления в силу настоящего приказа.

3. Рекомендовать руководителям организаций Госкорпорации «Росатом», за исключением организаций Госкорпорации «Росатом», с которыми подписаны регламенты по взаимодействию организации и Госкорпорации «Росатом», и организаций, входящих в контур их управления, обеспечить принятие локальных нормативных актов организации, предусматривающих обязательность реализации положений Методических указаний.

Срок – в течение трех недель с даты вступления в силу настоящего приказа.

4. Руководителям организаций Госкорпорации «Росатом», указанных в пунктах 2 и 3 настоящего приказа, рекомендовать представить директору по информационным технологиям Абакумову Е.М. информацию о принятых локальных нормативных актах в организации и мерах по соблюдению требований Методических указаний.

Срок – в течение четырех недель с даты вступления в силу настоящего приказа.

5. Признать утратившими силу:

приказ Госкорпорации «Росатом» от 22.10.2015 № 1/1009-П «Об утверждении Единых отраслевых методических указаний по дистанционному банковскому обслуживанию в Госкорпорации «Росатом» и ее организациях»;

п. 1 приказа от 17.09.2013 № 1/984-П «Об утверждении Единых отраслевых методических указаний по организации поддержки систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях».

6. Установить, что настоящий приказ вступает в силу с 01.03.2023.

Генеральный директор А.Е. Лихачев

Бинкис Ян Андреевич
(499) 949-49-19, доб. 6705

Приложение № 1

УТВЕРЖДЕНЫ
приказом Госкорпорации «Росатом»
от 28 ФЕВ 2023 № 1/326-П

ЕДИНЫЕ ОТРАСЛЕВЫЕ МЕТОДИЧЕСКИЕ УКАЗАНИЯ
по оценке доверия и приведению в соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях

Оглавление

1. Назначение и область применения 3
2. Сокращения и аббревиатуры 3
3. Основные положения 5
3.1. Оценка доверия к Системам 5
3.2. Приведение Систем в соответствие требованиям по безопасности 6
4. Нормативные ссылки 7
Приложение № 1 к Методическим указаниям 10
Приложение № 2 к Методическим указаниям 16
Приложение № 3 к Методическим указаниям 20

1. Назначение и область применения

1.1. Настоящие Единые отраслевые методические указания по оценке доверия и приведению в соответствие требованиям по безопасности систем дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях (далее – Методические указания) разработаны для установления единых требований по оценке доверия и приведению в соответствие требованиям по безопасности с целью обеспечения безопасности информации при эксплуатации защищенных с использованием криптографических средств систем дистанционного банковского обслуживания (далее – Система).

1.2. Настоящие Методические указания разработаны в рамках группы процессов «Управление информационными технологиями».

1.3. Настоящие Методические указания не распространяются на системы, используемые в Госкорпорации «Росатом» и её организациях, предназначенные для обработки информации, составляющей государственную тайну, а также на Системы иностранных банков, не имеющих официальных представительств на территории Российской Федерации.

1.4. Соблюдение настоящих Методических указаний является обязательным для работников Госкорпорации «Росатом» и ее организаций, осуществляющих эксплуатацию и обслуживание Систем.

1.5. Ответственным за актуализацию настоящих Методических указаний и контроль их исполнения в соответствии с требованиями Положения о системе регламентирующих документов Госкорпорации «Росатом», утвержденного приказом Госкорпорации «Росатом» от 04.12.2015 № 1/1176-П [27], является директор по информационным технологиям.

2. Сокращения и аббревиатуры

2.1. Сокращения, используемые в целях данного документа, и расшифровки:

Сокращение	Расшифровка
Дистанционное банковское обслуживание	Технологии предоставления банковских услуг на основании распоряжений, передаваемых клиентом удаленным образом (то есть без его визита в банк)
Доверие	Выполнение соответствующих действий или процедур для обеспечения уверенности в том, что оцениваемая Система соответствует своим целям безопасности
Жизненный цикл Системы	Развитие Системы от создания до вывода из эксплуатации
Лицензиат ФСБ России	Организация Госкорпорации «Росатом», эксплуатирующая или планирующая эксплуатировать Систему, или организация, организующая и обеспечивающая безопасность информации в Госкорпорации «Росатом» или в

	организации Госкорпорации «Росатом» на договорной основе[1], имеющие лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) в соответствии с законодательством Российской Федерации с разрешенными соответствующими видами выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств
Оценка доверия	Исследование Системы в соответствии с перечнем показателей по уровням доверия, указанных в Методических указаниях, для получения уверенности в том, что Система отвечает целям безопасности
Система	Защищенная с использованием криптографических средств система дистанционного банковского обслуживания (за исключением систем Центрального банка Российской Федерации) или Информационная система «Расчетный центр Корпорации»[2].

[1] В такие договоры включается положение о том, что осуществление работ по оценке доверия организациями, организующими и обеспечивающими безопасность информации в Госкорпорации «Росатом» или в организациях Госкорпорации «Росатом», должно производиться согласно требованиям Методических указаний.

[2] Введена в промышленную эксплуатацию приказом ОАО «Атомэнергопром» от 25.01.2013 №5/3-П «О запуске в промышленную эксплуатацию информационной системы «Расчетный центр Корпорации».

2.2. Аббревиатуры, используемые в целях данного документа, и расшифровки:

Аббревиатура	Расшифровка
АРМ	Автоматизированное рабочее место
КИИ	Критическая информационная инфраструктура
ОКИИ	Объект критической информационной инфраструктуры
СКЗИ	Средство криптографической защиты информации

3. Основные положения

3.1. Оценка доверия к Системам

До принятия решения о заключении Госкорпорацией «Росатом» или организацией Госкорпорации «Росатом» договора, предусматривающего эксплуатацию Системы, с банком, Лицензиатом ФСБ России должны быть проведены:

3.1.1. Оценка доверия к Системе в соответствии с требованиями по безопасности

Должно быть оценено:

доверие к ключевой системе;

доверие к СКЗИ, входящим в состав Системы;

доверие к среде функционирования СКЗИ;

доверие к Системе, как к ОКИИ;

доверие к участникам процессов обработки данных.

Уровни доверия (высокий, средний и низкий) к Системам устанавливаются в соответствии с перечнем показателей по уровням доверия (приложение № 1 к настоящим Методическим указаниям).

Целесообразно иметь утвержденные планы приведения Систем с низким и средним уровнями доверия к высокому уровню доверия с указанием конкретных мероприятий, сроков исполнения и ответственных лиц.

В Госкорпорации «Росатом» и организациях Госкорпорации «Росатом» проведение первой оценки доверия и выполнение требований по безопасности систем дистанционного банковского обслуживания согласно Методическим указаниям следует осуществить не позднее 30.06.2023.

3.1.2. Анализ заключаемого договора на эксплуатацию Системы (в случае наличия такого договора)

При анализе договора Лицензиатом ФСБ России должны быть оценены:

противоречия положениям нормативных правовых актов Российской Федерации по защите информации и эксплуатации СКЗИ;

требования к условиям эксплуатации Системы и правила ее использования, а также взаимоотношения сторон по договору в соответствии с жизненным циклом Системы.

3.1.3. Формирование заключения Лицензиата ФСБ России по результатам оценки доверия

По результатам оценки доверия к Системе и анализа заключаемого договора (в случае наличия такого договора) составляется заключение Лицензиата ФСБ России по результатам оценки доверия к Системе (шаблон – приложение № 2 к настоящим Методическим указаниям).

3.2. Приведение Систем в соответствие требованиям по безопасности

На основании заключения Лицензиата ФСБ России по результатам оценки доверия к Системе:

Госкорпорацией «Росатом» или организацией Госкорпорации «Росатом», планирующими заключить или заключившими договор с банком на услугу по дистанционному банковскому обслуживанию и банком составляются планы приведения Системы в соответствие требованиям безопасности с указанием конкретных мероприятий, сроков исполнения и ответственных лиц и предлагаются типовые решения;

Лицензиатом ФСБ России контролируется процесс приведения Системы в соответствие требованиям безопасности и при изменении уровня доверия выдается новое заключение Лицензиата ФСБ России;

Госкорпорацией «Росатом» или организацией Госкорпорации «Росатом», планирующими заключить или заключившими договор с банком на услугу по дистанционному банковскому обслуживанию и банком согласовываются и вносятся корректировки в текст договора на эксплуатацию Системы (в случае наличия такого договора);

Лицензиатом ФСБ России осуществляется постоянный мониторинг актуальности сведений по защите информации, на основе которой была произведена оценка доверия к Системе.

Методами приведения Систем в соответствие требованиям по безопасности являются:

выполнение требований нормативных и правовых актов Российской Федерации;

инфраструктурные решения, соответствующие требованиям нормативных и правовых актов Российской Федерации, локальным нормативным актам Госкорпорации «Росатом» и требованиям Лицензиата ФСБ России.

Защита информации в Системах Госкорпорации «Росатом» и ее организаций должна удовлетворять требованиям, приведенным в приложении № 3 к настоящим Методическим указаниям.

Организации, привлекаемые на договорной основе для оценки доверия и приведения в соответствие требованиям по безопасности Систем в соответствии с Инструкцией № 152 [21] должны иметь лицензию ФСБ России на осуществление разработки, производства, распространения шифровальных (криптографических) средств, информационных и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнение работ, оказание услуг в области шифрования информации, технического обслуживания шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием

шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя) в соответствии с законодательством Российской Федерации с разрешенными соответствующими видами выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств.

4. Нормативные ссылки

1. Федеральный закон от 29.07.2004 № 98-ФЗ «О коммерческой тайне».
2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных».
3. Федеральный закон от 06.04.2011 № 63-ФЗ «Об электронной подписи».
4. Федеральный закон от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности».
5. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
6. Постановление Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности».
7. Постановление Правительства Российской Федерации от 15.05.2010 № 330 «Об утверждении Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов её проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения».
8. Постановление Правительства Российской Федерации от 03.02.2012 № 79 «О лицензировании деятельности по технической защите конфиденциальной информации».
9. Постановление Правительства Российской Федерации от 16.04.2012 № 313 «Об утверждении Положения о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию; шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных

с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)».

10. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

11. Постановление Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

12. Национальный стандарт Российской Федерации ограниченного распространения ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения», утвержденный приказом Федерального агентства по техническому регулированию и метрологии от 17.04.2012 № 2-ст РО.

13. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К), утверждённые приказом Гостехкомиссии России от 30.08.2002 № 282.

14. Методические рекомендации по технической защите информации, составляющей коммерческую тайну, утверждённые заместителем директора ФСТЭК России 25.12.2006.

15. Пособие по организации технической защиты информации, составляющей коммерческую тайну, утверждённое заместителем директора ФСТЭК России 25.12.2006.

16. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

17. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

18. Приказ ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий».

19. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

20. Порядок организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утв. приказом ФСТЭК России от 29.04.2021 № 77.

21. Приказ ФАПСИ от 13.06.2001 № 152 «Об утверждении 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».

22. Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)».

23. Приказ ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

24. Приказ ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра».

25. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

26. Приказ Госкорпорации «Росатом» от 20.06.2012 № 1/540-П-дсп «Об оценке видов информации ограниченного доступа при создании, модернизации и эксплуатации автоматизированных систем в защищённом исполнении и прикладных информационных систем».

27. Приказ Госкорпорации «Росатом» от 04.12.2015 № 1/1176-П «Об утверждении Положения о системе регламентирующих документов Госкорпорации «Росатом».

28. Приказ Госкорпорации «Росатом» от 19.07.2016 № 1/656-П «Об утверждении Единых отраслевых методических указаний по установлению режима коммерческой тайны в Госкорпорации «Росатом» и ее организациях».

29. Приказ Госкорпорации «Росатом» от 14.07.2020 № 1/729-П «Об утверждении Единых отраслевых методических указаний по категорированию объектов критической информационной инфраструктуры».

30. Приказ Госкорпорации «Росатом» от 10.02.2021 № 1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях.

Приложение № 1
к Методическим указаниям

Перечень показателей по уровням доверия

Приведенные в таблице № 1 наборы требований к показателям каждого уровня являются минимально необходимыми.

Высокий уровень доверия к Системе устанавливается в случае соответствия всех показателей высокому уровню доверия.

Средний уровень доверия к Системе устанавливается в случае соответствия как минимум одного показателя среднему уровню доверия и отсутствии показателей низкого уровня доверия.

Низкий уровень доверия к Системе устанавливается в случае соответствия как минимум одного показателя низкому уровню доверия.

« – » - нет требований к данному уровню;
« + » - требования к данному уровню предъявляются.

Таблица № 1

Наименование показателя Системы	Документ	Уровень доверия		
		Низкий	Средний	Высокий
1. Оценка доверия к ключевой системе				
Законное основание для владения и использования средств, реализующих инфраструктуру ключевой системы	Копии договора, лицензии, заполненного формуляра или др.	-	+	+
Использование средства, реализующего инфраструктуру ключевой системы, сертифицированного в соответствии с системой сертификации РОСС RU.0001.030001 по классу КС2 и выше	Копии заполненного формуляра, сертификата соответствия ФСБ России или др.	-	+	+
Регламентация жизненного цикла ключей	Копия регламента ключевой системы или др.	-	+	+
Использование усиленной электронной подписи	Копии свидетельства об аккредитации удостоверяющего центра, договора/проекта договора с указанием используемой электронной подписи или др.	-	+	+
Использование дополнительных служб удостоверяющего центра (службы онлайновой проверки статусов сертификатов и службы штампов времени)	Копия регламента ключевой системы или др.	-	-	+

Наименование показателя Системы	Документ	Уровень доверия		
		Низкий	Средний	Высокий
2. Оценка доверия к СКЗИ, входящим в состав Системы				
Законное основание для владения, использования и передачи СКЗИ	Копии договора, лицензии на СКЗИ или др.	-	+	+
Использование СКЗИ для обеспечения конфиденциальности информации при ее передаче в сети Интернет сертифицированных ФСБ России по классу КС1	Копии сертификата соответствия ФСБ России на СКЗИ с актуальным сроком действия, формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника) или др.	-	+	-
Использование СКЗИ для обеспечения конфиденциальности информации при ее передаче в сети Интернет сертифицированных ФСБ России по классу КС2 и выше	Копии сертификата соответствия ФСБ России на СКЗИ с актуальным сроком действия, формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника) или др.	-	-	+
Использование СКЗИ для обеспечения целостности информации при ее передаче в сети Интернет сертифицированных ФСБ России по классу КС1	Копии сертификата соответствия ФСБ России на СКЗИ с актуальным сроком действия, формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из доверенного источника) или др.	-	+	-
Использование СКЗИ для обеспечения целостности информации при ее передаче в сети Интернет сертифицированных ФСБ России по классу КС2 и выше	Копии сертификата соответствия ФСБ России на СКЗИ с актуальным сроком действия, формуляра на СКЗИ с отметкой об учётном номере дистрибутива СКЗИ (полученного из	-	-	+

Наименование показателя Системы	Документ	Уровень доверия		
		Низкий	Средний	Высокий
	доверенного источника) или др.			
Использование сертифицированных ключевых носителей для хранения ключевой информации, в том числе сертифицированных облачных хранилищ	Копия сертификата соответствия ФСБ России/ФСТЭК России или др.	-	+	+
Использование несертифицированных ключевых носителей типа токен или смарт-карты	Копия договора/проекта договора с указанием об использовании типа ключевых носителей или др.	-	+	-
3. Оценка доверия к среде функционирования СКЗИ				
Выполнение 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, утвержденной приказом ФАПСИ от 13.06.2001 № 152	Копия заключения органа криптографической защиты о возможности эксплуатации СКЗИ	-	+	+
Выполнение Стандарта Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации» / проведение сторонней организацией, имеющей лицензию ФСТЭК России, оценки соответствия защиты информации, требуемой положением от 04.06.2020 № 719-П «О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению зашиты информации при осуществлении переводов денежных средств»	Копия отчета о проведении оценки соответствия уровням защиты информации	-	+	+
Использование сертифицированного ФСТЭК России прикладного программного обеспечения Системы и приложений	Копия сертификата ФСТЭК России на Систему	-	-	+
Использование идентификации в Системе, при которой не подтверждаются заявленные идентификационные данные	Копия регламента процесса идентификации пользователей в Системе или иной документ	+	-	-
Использование идентификации в Системе, при которой подтверждаются заявленные идентификационные данные	Копия регламента процесса идентификации пользователей в	-	+	-

Наименование показателя Системы	Документ	Уровень доверия		
		Низкий	Средний	Высокий
	Системе или иной документ			
Использование идентификации в Системе, при которой официально подтверждаются заявленные идентификационные данные	Копия регламента процесса идентификации пользователей в Системе или иной документ	-	-	+
Использование в Системе однофакторной односторонней аутентификации с применением протоколов аутентификации, в том числе криптографических (простая аутентификация)	Копия технического задания/ пояснительной записки на Систему или иной документ	+	-	-
Использование в Системе многофакторной односторонней или взаимной аутентификации с применением протоколов аутентификации, в том числе криптографических (усиленная аутентификация)	Копия технического задания/ пояснительной записки на Систему или иной документ	-	+	-
Использование в Системе многофакторной взаимной аутентификации с применением криптографических протоколов (строгая аутентификация)	Копия технического задания/ пояснительной записки на Систему или иной документ	-	-	+
Выполнение требований эксплуатационной и технической документации по встраиванию СКЗИ в Систему	Копия заключения о корректности встраивания СКЗИ в Систему	-	-	+
Выполнение требований по безопасности информации в Системе	Копия аттестата соответствия требованиям по безопасности информации или др.	-	+	+
Наличие документации на Систему	Копия эксплуатационной документации на Систему	-	+	+
Использование лицензионных сертифицированных ФСТЭК России антивирусных средств на серверах/АРМ где функционируют средства, реализующие инфраструктуру ключевой системы/ СКЗИ пользователей Системы	Копии сертификата соответствия ФСТЭК России, лицензии на использование, акта установки или др.	-	+	+
Использование лицензионных сертифицированных ФСТЭК России средств защиты информации от несанкционированного доступа на серверах/АРМ где функционируют средства, реализующие	Копии сертификата соответствия ФСТЭК России, лицензии на использование, акта установки или др.	-	+	+

Наименование показателя Системы	Документ	Уровень доверия		
		Низкий	Средний	Высокий
инфраструктуру ключевой системы/ СКЗИ пользователей Системы				
4. Оценка доверия к Системе, как к ОКИИ				
4.1. Для незначимых и значимых ОКИИ (Систем)				
Создание комиссии по категорированию и принятие решения о присвоении категории значимости ОКИИ (Системы)	Копия подписанного руководителем организации акта категорирования Системы и приказа о создании комиссии по категорированию	-	-	+
Направление сведений в ФСТЭК России о присвоении категории значимости ОКИИ (Системы), либо об отсутствии присвоения категории, и получение согласования ФСТЭК России	Копия ответного письма ФСТЭК России о согласовании присвоенной категории значимости (для значимого ОКИИ прилагается номер реестра значимого ОКИИ)	-	-	+
4.2. Только для значимых ОКИИ (Систем)				
Для значимого ОКИИ (Системы) необходимо составление плана мероприятий по обеспечению безопасности значимого ОКИИ (Системы) и плана реагирования на инциденты	Копии приказа, утверждающего план, или плана реагирования на инциденты, приказа, утверждающего план, или плана мероприятий по обеспечению безопасности значимого ОКИИ (Системы)	-	-	+
5. Оценка доверия к участникам процессов обработки данных				
Право осуществлять лицензируемые виды деятельности	Копия лицензии ФСБ России на виды деятельности в области криптографической защиты	-	+	+
Обеспечение повышения осведомленности работников в области обеспечения защиты информации по порядку применения организационных мер защиты информации и использования технических средств защиты информации	Копии порядка периодического обучения, сертификатов об обучении или др.	-	+	+

Наименование показателя Системы	Документ	Уровень доверия		
		Низкий	Средний	Высокий
Определение прав, обязанностей и ответственности работников в Системе	Копия приказа о допуске пользователей работников к работе в Системе с указанием полномочий и ответственности, матрица доступа или др.	-	+	+
Контроль выполнения условий использования СКЗИ согласно 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, утвержденной приказом ФАПСИ от 13.06.2001 № 152	Копия порядка проведения контроля или др.	-	-	+

Рег. № _____
от _____

Приложение № 2
к Методическим указаниям

УТВЕРЖДАЮ

<указывается должность>

_____/_____
(подпись) (Ф.И.О)

«___»_____ 20__ г.

ЗАКЛЮЧЕНИЕ
по результатам оценки доверия

<указывается наименование Системы>

г. Москва

1. Термины, определения и сокращения

2. Вводная часть

2.1. Основание для выдачи заключения

Указываются реквизиты договора, на основании которого проводятся работы.

2.2. Наименование защищенной с использованием шифровальных (криптографических) средств информационной системы

Указывается наименование Системы.

2.3. Вопросы для исследования

доверие к ключевой системе;
доверие к СКЗИ, входящим в состав Системы;
доверие к среде функционирования СКЗИ;
доверие к Системе, как к ОКИИ;
доверие к участникам процессов обработки данных.

3. Исследовательская часть

Оценка доверия к Системе проводится в соответствии с Методическими указаниями.

Методы исследования:
анализ представленной в орган криптографической защиты <указывается наименование лицензиата ФСБ России> документации на Систему;
анализ договора на эксплуатацию Системы.

4. В процессе исследования установлено

4.1. Описание Системы

В данном разделе указывается описание Системы.

4.2. Инфраструктура ключевой системы

Указывается используемая ключевая система, программно-аппаратный комплекс удостоверяющего центра, дополнительные службы удостоверяющего центра, аккредитация удостоверяющего центра и другая информация в соответствии с Методическими указаниями.

4.3. Жизненный цикл ключевых документов

Указывается жизненный цикл ключей пользователей Системы (процессы создания, передачи/получения, эксплуатации, хранения, замены и уничтожения), типы ключевых носителей и другая информация в соответствии с Методическими указаниями.

4.4. Жизненный цикл СКЗИ

Указывается жизненный цикл СКЗИ, использующихся в Системе (процессы передачи/получения, эксплуатации, хранения, замены и уничтожения), и другая информация в соответствии с Методическими указаниями.

4.5. Механизм обеспечения конфиденциальности и целостности информации в Системе

Указывается механизм обеспечения конфиденциальности и целостности информации в Системе (используемые СКЗИ, протоколы) и другая информация в соответствии с Методическими указаниями.

4.6. Выполнение требований по безопасности информации

Указываются реквизиты документов, подтверждающих выполнение требований по безопасности информации на стороне банка и на стороне Госкорпорации «Росатом» или организации Госкорпорации «Росатом», планирующими заключить или заключившими договор с банком на услугу по дистанционному банковскому обслуживанию.

5. Оценка соответствия

5.1. Результаты исследования доверия к ключевой системе

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.2. Результаты исследования доверия к СКЗИ, входящим в состав Системы

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.3. Результаты исследования доверия к среде функционирования СКЗИ

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.4. Результаты исследования доверия к Системе, как к ОКИИ

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

5.5. Результаты исследования доверия к участникам процессов обработки данных

Критерии оценки	Наличие подтверждающего документа	Дата начала действия	Дата окончания действия	Номер документа	Уровень доверия

6. Выводы и рекомендации

6.1. Выводы

На момент составления настоящего заключения уровень доверия к Системе <указывается выявленный уровень доверия>.

6.2. Рекомендации

Для приведения Системы к среднему уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается наименование банка> провести следующие работы в краткосрочной перспективе:

<указывается перечень мероприятий по приведению Системы к среднему уровню доверия>.

Для приведения Системы к высокому уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается наименование банка> провести следующие работы в среднесрочной перспективе:

<указывается перечень мероприятий по приведению Системы к высокому уровню доверия>.

Для приведения Системы к среднему уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается Госкорпорация «Росатом» или организация Госкорпорации «Росатом», планирующие заключить или заключившие договор с банком на услугу по дистанционному банковскому обслуживанию> провести следующие работы в краткосрочной перспективе:

<указывается перечень мероприятий по приведению Системы к среднему уровню доверия>.

Для приведения Системы к высокому уровню доверия орган криптографической защиты <указывается наименование лицензиата ФСБ России> рекомендует <указывается Госкорпорация «Росатом» или организация Госкорпорации «Росатом», планирующие заключить или заключившие договор с банком на услугу по дистанционному банковскому обслуживанию> провести следующие работы в среднесрочной перспективе:

<указывается перечень мероприятий по приведению Системы к высокому уровню доверия>.

Заключение составил:

<указывается должность> _____/_____
(подпись) (Ф.И.О)

Приложение № 3
к Методическим указаниям

Требования, предъявляемые к системам дистанционного банковского обслуживания в Госкорпорации «Росатом» и ее организациях

Защита информации в Системах Госкорпорации «Росатом» и ее организаций должна удовлетворять требованиям, приведенным ниже.

Для обеспечения контроля правильности определения вида информации ограниченного доступа, обрабатываемой в Системах, необходимо руководствоваться требованиями приказа Госкорпорации «Росатом» от 20.06.2012 № 1/540-П-дсп «Об оценке видов информации ограниченного доступа при создании, модернизации и эксплуатации автоматизированных систем в защищённом исполнении и прикладных информационных систем» [26].

Для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных необходимо руководствоваться требованиями Федерального закона от 27.07.2006 № 152-ФЗ «О персональных данных» [2], постановления Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [10], приказа ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [16].

Требования по безопасности информации, составляющей коммерческую тайну, должны выполняться в соответствии с Федеральным законом от 29.07.2004 № 98-ФЗ «О коммерческой тайне» [1], Методическими рекомендациями по технической защите информации, составляющей коммерческую тайну, утверждёнными заместителем директора ФСТЭК России 25.12.2006 [14], Пособием по организации технической защиты информации, составляющей коммерческую тайну, утверждённым заместителем директора ФСТЭК России 25.12.2006 [15], приказом Госкорпорации «Росатом» от 19.07.2016 № 1/656-П «Об утверждении Единых отраслевых методических указаний по установлению режима коммерческой тайны в Госкорпорации «Росатом» и ее организациях» [28].

При организации защиты служебной информации ограниченного распространения следует руководствоваться постановлением Правительства Российской Федерации от 03.11.1994 № 1233 «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти и уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» [6], Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К), утверждёнными приказом Гостехкомиссии России от 30.08.2002 № 282 [13], приказом Госкорпорации

«Росатом» от 10.02.2021 № 1/140-П-дсп «Об утверждении Единых отраслевых методических указаний по информационной безопасности и использованию средств защиты информации в Госкорпорации «Росатом» и ее организациях [30].

В соответствии с законодательством Российской Федерации до ввода в эксплуатацию Системы (как объекта информатизации) должна проводиться ее аттестация в соответствии с постановлением Правительства Российской Федерации от 15.05.2010 № 330 «Об утверждении Положения об особенностях оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, относимых к охраняемой в соответствии с законодательством Российской Федерации информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну, а также процессов её проектирования (включая изыскания), производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации, утилизации и захоронения» [7]. Целью аттестации объекта информатизации является подтверждение соответствия его системы защиты информации требованиям безопасности информации в реальных условиях эксплуатации.

Порядок проведения аттестации объектов информатизации определён Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей государственную тайну, утвержденным приказом ФСТЭК России от 29.04.2021 № 77 [20], а также национальным стандартом Российской Федерации ограниченного распространения ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения», утвержденным приказом Федерального агентства по техническому регулированию и метрологии от 17.04.2012 № 2-ст РО [12].

Деятельность организации, выполняющей работы по аттестации объектов информатизации, предназначенных для обработки информации конфиденциального характера, лицензируется уполномоченным федеральным органом исполнительной власти (ФСТЭК России) в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 03.02.2012 № 79 [8].

Деятельность организации, обеспечивающей безопасность хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты конфиденциальной информации лицензируется ФСБ России в соответствии с Положением о лицензировании деятельности по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических)

средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя), утвержденным постановлением Правительства Российской Федерации от 16.04.2012 № 313 [9].

Единый порядок организации и обеспечения безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну, определен Инструкцией 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, утвержденной приказом ФАПСИ от 13.06.2001 № 152 (далее – Инструкция № 152) [21].

Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности, определен приказом ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [25].

Системы Госкорпорации «Росатом» и ее организаций должны быть защищены сертифицированными ФСБ России СКЗИ, к которым предъявляются требования Федерального закона от 06.04.2011 № 63-ФЗ «Об электронной подписи» [3], Федерального закона от 04.05.2011 № 99-ФЗ «О лицензировании отдельных видов деятельности» [4], Инструкции № 152 [21], приказа ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005) [22], приказа ФСБ России от 27.12.2011 № 795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи» [23], приказа ФСБ России от 27.12.2011 № 796 «Об утверждении Требований к средствам электронной подписи и Требований к средствам удостоверяющего центра» [24], приказа ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» [25].

Для систем выставляются требования безопасности для критической информационной инфраструктуры. Реализация мер по обеспечению безопасности ОКИИ необходима на всех стадиях жизненного цикла Систем, в соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [5], постановлением Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений» [11], приказом ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования» [17], приказом ФСТЭК России от 22.12.2017 № 236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий» [18], приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [19], приказом Госкорпорации «Росатом» от 14.07.2020 № 1/729-П «Об утверждении Единых отраслевых методических указаний по категорированию объектов критической информационной инфраструктуры» [29].

Приложение № 2
к приказу Госкорпорации «Росатом»
от 28 ФЕВ 2023 № 1/326-П

Перечень
организаций Госкорпорации «Росатом», с которыми подписаны регламенты по взаимодействию между хозяйственным обществом/федеральным государственным унитарным предприятием и Госкорпорацией «Росатом»

1. АО «Атомэнергомаш».
2. АО «РИР».
3. АО «РЭИН».
4. АО «Техснабэкспорт».
5. АО «ЦентрАтом».
6. АО «АТА».
7. АО «Наука и инновации».
8. АО «Атомкомплект».
9. ФГУП «РФЯЦ-ВНИИЭФ».
10. АО «Концерн Росэнергоатом».
11. АО «РХК».
12. АО «ЮМАТЕКС».
13. АО «Русатом Сервис».
14. АО РАОС.
15. АО «НИКИЭТ».
16. АО «РАСУ».
17. АО «НоваВинд».
18. АО «Русатом Гринвэй».