УТВЕРЖДЕНО
решением Правления
АО «РОСКОСМОСБАНК»
протокол от 18 июня 2020 г.
№ 40/2020-П

ПОЛИТИКА

ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

АО «РОСКОСМОСБАНК»

Москва
2020

СОДЕРЖАНИЕ

1. Общие положения 3
2. Термины и определения 3
3. Цели, задачи и принципы обеспечения информационной безопасности 4
4. Описание объектов защиты 6
5. Меры обеспечения информационной безопасности 6
6. Определение общих ролей и обязанностей, связанных с обеспечением информационной безопасности 7
7. Актуальные угрозы безопасности информации 8
8. Модель нарушителя информационной безопасности 9
9. Механизм реализации политики информационной безопасности 9
10. Ответственность за соблюдение положений настоящей Политики 10
11. Санкции и последствия нарушений настоящей Политики 10
12. Контроль за соблюдением положений настоящей Политики 10
13. Заключительные положения 10
Приложение 1 12
Приложение 2 14

1. Общие положения

1.1. Настоящая Политика информационной безопасности АО «РОСКОСМОСБАНК» (далее — Политика) определяет цели, задачи и условия обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется АО «РОСКОСМОСБАНК» (далее – Банк) в своей деятельности.

1.2. Положения и требования настоящей Политики распространяются на всех работников Банка и пользователей Автоматизированной системы Банка.

1.3. Настоящая Политика разработана в соответствии с требованиями действующего законодательства Российской Федерации, государственных стандартов, стандартов и нормативных актов Банка России в области обеспечения информационной безопасности и Политики информационной безопасности Госкорпорации «Роскосмос». Ссылки на нормативные правовые акты и стандарты приведены в приложении 1 к Политике.

1.4. Настоящая Политика является документом, доступным всем работникам Банка и пользователям Автоматизированной системы Банка, представляет собой официально принятую коллегиальным исполнительным органом Банка – Правлением систему взглядов по вопросам обеспечения информационной безопасности и устанавливает принципы построения системы управления (менеджмента) информационной безопасностью.

1.5. Правление Банка осознает важность и необходимость применения мер и средств обеспечения информационной безопасности в контексте развития законодательства Российской Федерации, государственных стандартов, стандартов и нормативных актов Банка России, а также внедрения новых информационных технологий.

1.6. Соблюдение требований информационной безопасности создает конкурентные преимущества Банка, обеспечивает его финансовую стабильность, рентабельность, соответствие правовым и договорным требованиям и способствует улучшению имиджа Банка.

1.7. Требования информационной безопасности, предъявляемые Банком, соответствуют целям его деятельности и предназначены для обеспечения требуемого уровня защищенности информации, а также снижения уровня рисков информационной безопасности до приемлемого уровня.

2. Термины и определения

Автоматизированная система (АС) — система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Пользователь автоматизированной системы (пользователь) — лицо, участвующее в функционировании автоматизированной системы или использующее результаты ее функционирования.

Информация — сведения (сообщения, данные) независимо от формы их предоставления.

Информационные ресурсы (ИР) — информация и информационные массивы, используемые в автоматизированных системах.

Владелец информационного ресурса — работник, назначенный приказом, уполномоченный разрешать или ограничивать доступ к информации, обрабатываемой в АС, и контролировать её достоверность и целостность.

Информационная безопасность (ИБ) — свойство информации сохранять конфиденциальность, целостность и доступность.

Субъект доступа — лицо, действия которого регламентируются правилами разграничения доступа.

Информационный актив — любая информация, независимо от вида её предоставления, имеющая ценность для Банка и находящаяся в его распоряжении.

Доступность информации (ресурсов автоматизированной системы) — состояние информации (ресурсов автоматизированной системы), при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Технические средства автоматизированной системы — средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, программные средства и средства защиты информации.

Целостность информации — состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.

Защита информации — деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

Инцидент информационной безопасности — любое непредвиденное или нежелательное событие, которое может нарушить деятельность или информационную безопасность.

Риск информационной безопасности — риск реализации угроз безопасности информации.

Информационная технология (ИТ) — процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления этих процессов и методов.

Конфиденциальность информации — обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

Несанкционированный доступ — доступ к информации или к ресурсам автоматизированной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

Вредоносный код — программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы автоматизированной системы;

Средства вычислительной техники — совокупность элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Средство защиты информации — техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенное или используемое для защиты информации.

3. Цели, задачи и принципы обеспечения информационной безопасности

3.1. Целями информационной безопасности являются:

– выполнение требований законодательства и нормативных документов Российской Федерации в области обеспечения информационной безопасности, нормативных актов Банка России и положений организационно-распорядительных документов Банка;

– обеспечение требуемого уровня защищенности информации, циркулирующей в Банке, и предотвращение ущерба от ее разглашения, утраты, утечки, блокирования, искажения, уничтожения, незаконного использования и/или нарушения работы АС;

– снижение уровня риска информационной безопасности путем выбора и применения мер и средств зашиты информации, их контроля и управления;

– обеспечение целостности, доступности и конфиденциальности информации, циркулирующей в АС Банка различного назначения.

3.2. Обеспечение информационной безопасности Банка направлено:

– на обеспечение защиты информации ограниченного доступа, предотвращения ее утечки по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию;

– повышение защищенности и устойчивости функционирования АС Банка, включая совершенствование механизмов предупреждения и обнаружения компьютерных атак и ликвидации последствий их проведения;

– противодействие деятельности, направленной на нанесение ущерба Банку.

3.3. Принципы и подходы к управлению и обеспечению функционирования системы обеспечения информационной безопасности Банка:

– управление системой обеспечения информационной безопасности Банка включает процесс планирования, реализации, контроля и совершенствования системы информационной безопасности Банка;

– Управление информационной безопасности Дирекции по безопасности Банка наделяется полномочиями и ресурсами, необходимыми для выполнения задач по обеспечению информационной безопасности Банка;

– для поддержания взаимосвязи целей обеспечения информационной безопасности с целями бизнес-деятельности из состава Правления Банка приказом назначается куратор Управления информационной безопасности Дирекции по безопасности. При этом Управление информационной безопасности Дирекции по безопасности и Дирекция информационных технологий Банка не должны иметь общего куратора;

– Правление Банка, Управление информационной безопасности Дирекции по безопасности и его куратор предпринимают необходимые экономически обоснованные меры для достижения требуемого уровня защиты информации;

– необходимый уровень ресурсного (кадрового и финансового) обеспечения системы обеспечения информационной безопасности Банк определяет на основании действующего законодательства Российской Федерации, государственных стандартов, стандартов и нормативных актов Банка России в области обеспечения информационной безопасности, результатов внешних и внутренних аудитов информационных технологий и информационной безопасности, а также оценок уровня рисков.

3.4. Требуемый уровень информационной безопасности достигается путем реализации следующих подходов к функционированию системы обеспечения информационной безопасности Банка:

– управление риском информационной безопасности Банка;

– прогнозирование (моделирование) угроз информационной безопасности в АС Банка различного назначения;

– предупреждение нарушения порядка доступа к информации;

– обнаружение фактов несанкционированного доступа к информации;

– предотвращение несанкционированного доступа к информации или передачи ее лицам, не имеющим права доступа к информации;

– предотвращение целенаправленного воздействия на технические средства АС, в результате которого нарушается конфиденциальность, целостность или доступность информации;

– предотвращение нарушений прав субъектов при обработке персональных данных;

– участие в ликвидации последствий реализации угроз информационной безопасности и восстановления актуального состояния АС;

– осуществление контроля за обеспечением требуемого уровня защищенности информации;

– обеспечение соответствия состояния информационной безопасности Банка требованиям законодательства Российской Федерации.

3.5. Банком обеспечивается беспрепятственный доступ всех работников к тексту настоящей Политики и иным организационно-распорядительным документам Банка по вопросам информационной безопасности путем размещения документов в системе электронного документооборота Банка, а также доведение до сведения всех работников Банка об утверждении настоящей Политики или вносимых в Политику изменениях.

3.6. Каждым работником Банка или пользователем АС Банка должно быть подписано обязательство о соблюдении настоящей Политики (приложение 2 к настоящей Политике). Организацию подписания и хранение обязательств работников Банка обеспечивает отдел кадровой политики Управления по работе с персоналом Административно-хозяйственной дирекции.

4. Описание объектов защиты

4.1. Объектами защиты являются:

– любые носители, содержащие защищаемую информацию (бумажные, магнитные, оптические и иные типы носителей информации);

– информация, циркулирующая в АС Банка;

– средства вычислительной техники, телекоммуникационное оборудование, каналы передачи данных;

– прикладное, общесистемное и специальное программное обеспечение;

– средства защиты информации;

– помещения, в которых расположены технические средства и системы, непосредственно участвующие в обработке информации, а также обеспечивающие информационную безопасность.

5. Меры обеспечения информационной безопасности

5.1. Правовые меры обеспечения информационной безопасности:

– следование действующему законодательству Российской Федерации и требованиям Банка России;

– регламентация процессов обработки информации, подлежащей защите;

– определение персональной ответственности руководителей и работников Банка по вопросам информационной безопасности;

– разработка организационно-распорядительных, проектных и эксплуатационных документов по системам защиты информации.

5.2. Организационные меры обеспечения информационной безопасности:

– планирование работ в области информационной безопасности с учетом жизненного цикла АС;

– обучение работников соблюдению принятых политик безопасности и практическим действиям в нештатных ситуациях;

– проведение единой технической политики в области обеспечения информационной безопасности;

– оценка соответствия либо аттестация АС по требованиям безопасности информации;

– привлечение организаций, имеющих соответствующие лицензии на проведение работ, связанных с обеспечением информационной безопасности в ходе создания и эксплуатации АС Банка;

– применение там, где необходимо, сертифицированных средств защиты информации;

– использование, по мере возможности, в АС отечественного аппаратного и программного обеспечения с учетом рекомендаций федерального органа исполнительной власти в области обеспечения безопасности;

– мониторинг и оценка состояния информационной безопасности, моделирование угроз информационной безопасности, прогнозирование и выявление источников, а также предотвращение и нейтрализация этих угроз;

– проведение мероприятий, направленных на оценку состояния информационной безопасности;

– анализ АС Банка на наличие уязвимостей;

– выполнение требований по информационной безопасности при разработке, внедрении, модернизации или доработке АС и/или их компонентов.

5.3. Технические меры обеспечения информационной безопасности:

– внедрение средств управления, разграничения и контроля доступа пользователей к АС;

– использование Банком программного и аппаратного обеспечения, при внедрении которого проходила процедура согласования технических заданий с учетом требований по защите информации;

– защита машинных носителей информации;

– применение средств регистрации событий информационной безопасности;

– применение средств антивирусной защиты информации;

– защита АС, их средств, систем связи и каналов передачи данных от компьютерных атак;

– применение других целесообразных технических мер и средств защиты информации.

5.4. Меры обеспечения информационной безопасности предпринимаются на всех этапах жизненного цикла и ИР – создания, обработки, хранения и уничтожения.

6. Определение общих ролей и обязанностей, связанных с обеспечением информационной безопасности

6.1. Правление Банка:

– утверждает внесение изменений в настоящую Политику по представлению Управления информационной безопасности Дирекции по безопасности.

6.2. Куратор Управления информационной безопасности Дирекции по безопасности:

– осуществляет общий контроль состояния информационной безопасности Банка:

– курирует вопросы обеспечения информационной безопасности, системы управления информационной безопасности.

6.3. Управление информационной безопасности Дирекции по безопасности:

– разрабатывает и реализует стратегию развития информационной безопасности Банка;

– осуществляет мероприятия по планированию, реализации, мониторингу, анализу и совершенствованию системы обеспечения информационной безопасности Банка;

– разрабатывает, внедряет и актуализует внутренние нормативные акты в области информационной безопасности;

– организует и проводит мероприятия по выявлению нарушений нормативных актов в области информационной безопасности;

– организует и проводит мониторинг событий и иные мероприятия, направленные на предотвращение, выявление и пресечение инцидентов информационной безопасности, при необходимости проводит или участвует в их расследовании;

– в установленном порядке информирует об инцидентах информационной безопасности директора по безопасности Дирекции по безопасности и, при необходимости, Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере Банка России;

– участвует в процессе внедрения и эксплуатации АС, систем телекоммуникаций и связи, систем управления банковскими технологическими процессами в части обеспечения информационной безопасности;

– на регулярной основе организует и проводит внутренние и внешние аудиты с целью выявления имеющихся недостатков в области информационных технологий и информационной безопасности;

– участвует совместно со Службой управления рисками в оценке рисков информационной безопасности;

– выполняет другие действия, необходимые для обеспечения должного уровня информационной безопасности Банка;

– непосредственно подчиняется директору по безопасности Дирекции по безопасности и отчитывается перед ним о результатах работы.

6.4. Владельцы информационных ресурсов:

– определяют степень конфиденциальности информационных ресурсов;

– определяют требования по доступу к АС, в которых хранятся и обрабатываются их информационные ресурсы;

– определяют целесообразность предоставления доступа пользователей к их информационным ресурсам и контролируют актуальность предоставленных прав.

6.5. Пользователи:

– выполняют требования Банка по обеспечению информационной безопасности;

– информируют Управление информационной безопасности Дирекции по безопасности об обнаруженных нарушениях информационной безопасности или возникших подозрениях о возможности таких нарушений;

– несут ответственность за нарушение установленного в Банке режима информационной безопасности в соответствии с действующим законодательством и нормативными документами Банка.

7. Актуальные угрозы безопасности информации

7.1. Основными угрозами безопасности информации являются:

– нарушение конфиденциальности информации, циркулирующей в АС Банка различного назначения;

– нарушение доступности АС Банка и отдельных ее компонентов, приводящие к блокированию доступа пользователей к АС;

– нарушение целостности (модификация, удаление) информации, отдельных компонентов АС Банка.

7.2. Угрозы безопасности информации подразделяются на преднамеренные и непреднамеренные.

7.2.1. Непреднамеренные угрозы безопасности информации:

– непреднамеренные нарушения пользователями АС политики информационной безопасности, утвержденных приказов, распоряжений, положений, инструкций и процедур сбора, обработки и хранения информации;

– уязвимость в программном обеспечении или технических средствах объектов АС;

– отказы в работе технических средств объектов АС и защиты информации.

7.2.2. Преднамеренные угрозы безопасности информации:

– физическое воздействие на объекты АС, приводящее к нарушению их функционирования;

– действия администраторов или пользователей АС, противоречащие организационно-распорядительным документам Банка;

– использование «чужих» идентификационных данных для доступа к АС;

– угрозы, исходящие от сторонних организаций, осуществляющих доступ к АС Банка в рамках исполнения договорных обязательств;

– угрозы, исходящие из сети Интернет, с целью несанкционированного доступа к информации или ее перехвата;

– целенаправленные компьютерные атаки на информационные ресурсы и АС Банка;

– угроза несанкционированного доступа к информации клиентов Банка;

– угрозы, связанные с применением вредоносного кода и/или не декларированных возможностей программного обеспечения;

– подключение работниками к сети Банка незарегистрированных средств вычислительной техники;

– действия либо бездействие должностных лиц по информированию и ознакомлению под роспись работников Банка, а также отказ работника от ознакомления с нормативными правовыми актами Банка в области защиты информации.

8. Модель нарушителя информационной безопасности

8.1. Нарушителем является субъект доступа, в результате действий которого возникает угроза или предпосылки к угрозе безопасности информации и АС Банка.

8.2. Все нарушители по наличию права доступа к информации делятся на внутренних и внешних.

8.2.1. Внутренними нарушителями могут быть:

– работники Банка, имеющие доступ к данным АС различного назначения;

– зарегистрированные пользователи АС, имеющие различные права доступа к АС со своего рабочего места;

– пользователи, осуществляющие удаленный доступ к информационным ресурсам Банка;

– программисты-разработчики прикладного ПО и лица, обеспечивающие его сопровождение;

– разработчики и лица, обеспечивающие поставку и сопровождение АС.

8.2.2. Внешними нарушителями могут быть:

– работники внешних организаций, осуществляющих доступ к АС (их эксплуатацию) в рамках исполнения договорных обязательств;

– работники Банка, с которыми расторгнут трудовой договор;

– конкурирующие организации, преступные сообщества, а также специальные службы и подконтрольные общественные организации отдельных государств;

– лица, проникшие в АС из сетей международного информационного обмена, в том числе сети Интернет;

– иные лица, осуществившие доступ к информации и АС Банка с нарушением требований информационной безопасности.

9. Механизм реализации политики информационной безопасности

9.1. Реализация политики информационной безопасности Банка осуществляется на основе утвержденных планов и объемов финансирования, которые с периодичностью один раз в год актуализируются на соответствие:

– федеральному законодательству и нормативной базе в области ИБ;

– организационно-распорядительным документам Банка;

– потребностям в средствах защиты информации и организационным мерам обеспечения ИБ при выявлении новых актуальных угроз и уязвимостей.

9.2. Банком организуются и финансируются мероприятия по обеспечению информационной безопасности, в том числе направленные:

– на организацию и поддержание в актуальном состоянии управление системой защиты информации;

– повышение уровня осведомленности работников Банка в вопросах обеспечения информационной безопасности;

– разработку и актуализацию организационно-распорядительных документов по информационной безопасности;

– проведение контроля соблюдения требований настоящей Политики и иных нормативных правовых актов в области информации, информационных технологий и защиты информации;

– ликвидацию последствий нарушения установленных требований информационной безопасности;

– поддержание установленного уровня защищенности АС.

10. Ответственность за соблюдение положений настоящей Политики

10.1. Ответственность за поддержание настоящей Политики в актуальном состоянии, координацию работ и внесение изменений в процессы обеспечения информационной безопасности Банка лежит на начальнике Управления информационной безопасности Дирекции по безопасности.

10.2. Работники Банка и пользователи АС несут ответственность за соблюдение требований информационной безопасности, установленную законодательством Российской Федерации.

11. Санкции и последствия нарушений настоящей Политики

11.1. По фактам выявленных нарушений требований по обеспечению информационной безопасности, порядка и правил пользования АС Банка проводятся проверки. На время проверки доступ к АС Банка работника, допустившего нарушение, может быть приостановлен.

11.2. По результатам проверки работник может быть привлечен к ответственности в рамках действующего законодательства.

11.3. Мера ответственности работников за действия, совершенные в нарушение установленных правил по обеспечению информационной безопасности, порядка и правил пользования АС Банка, определяется нанесенным ущербом, либо угрозой его возникновения в результате допущенного нарушения и другими факторами по усмотрению руководства Банка.

12. Контроль за соблюдением положений настоящей Политики

12.1. Общий контроль состояния информационной безопасности Банка осуществляется Куратором Управления информационной безопасности Дирекции по безопасности.

12.2. Текущий контроль соблюдения положений настоящей Политики (контроль в ходе проведения работ) осуществляет директор по безопасности Дирекции по безопасности.

12.3. В целях контроля проводятся мониторинг и управление инцидентами информационной безопасности, а также другие контрольные мероприятия.

13. Заключительные положения

13.1. Для развития и детализации положений настоящей Политики в Банке введены: Политика в отношении обработки персональных данных и сведения о реализуемых требованиях к защите персональных данных Банка, Частная политика предоставления прав доступа к информационным системам Банка, другие частные политики, положения, регламенты, стандарты и инструкции в области информационной безопасности. Перечисленные организационно-распорядительные документы содержат указания на подразделения Банка, ответственные за их соблюдение и реализацию.

13.2. При изменении действующего законодательства Российской Федерации, нормативных актов Банка России и иных нормативных правовых актов по вопросам защиты информации, а также Устава Банка настоящая Политика и изменения к ней применяются в части, не противоречащей принятым документам. В этом случае Управление информационной безопасности Дирекции по безопасности инициирует внесение соответствующих изменений.

13.3. В случае вступления отдельных пунктов в противоречие с новыми законодательными актами эти пункты утрачивают юридическую силу до момента внесения изменений в настоящую Политику.

13.4. Внесение изменений в настоящую Политику регламентировано и осуществляется:

– в связи с изменениями требований в законодательных и иных нормативных документах Российской Федерации, стандартов и нормативных актов Банка России в области обеспечения

информационной безопасности, а также в случае изменения целей и задач Банка и особенностей его деятельности;

– по результатам анализа инцидентов безопасности, актуальности, достаточности и эффективности используемых мер и средств обеспечения информационной безопасности и других контрольных мероприятий.

Приложение 1
к Политике
информационной безопасности
АО «РОСКОСМОСБАНК»

Перечень нормативных правовых актов

1. Указ Президента РФ от 31.12.2015 N 683 «О Стратегии национальной безопасности Российской Федерации»;
2. Указ Президента РФ от 05.12.2016 N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации»;
3. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
4. Указ Президента РФ от 06.03.1997 N 188 «Об утверждении Перечня сведений конфиденциального характера»;
5. Федеральный закон от 10.07.2002 N 86-ФЗ «О Центральном банке Российской Федерации (Банке России)»;
6. «Трудовой кодекс Российской Федерации» от 30.12.2001 N 197-ФЗ;
7. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне»;
8. Федеральный закон от 02.12.1990 N 395-1 «О банках и банковской деятельности»;
9. Федеральный закон от 07.07.2003 N 126-ФЗ «О связи»;
10. Федеральный закон от 26.07.2017 N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;
11. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных»;
12. Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
13. Федеральный закон от 07.08.2001 N 115-ФЗ «О противодействии легализации (отмыванию) доходов, полученных преступным путем, и финансированию терроризма»;
14. Федеральный закон от 27.06.2011 N 161-ФЗ «О национальной платежной системе»;
15. Указание Банка России от 14.09.2011 N 2695-У «О требованиях к обеспечению бесперебойности осуществления перевода электронных денежных средств» (Зарегистрировано в Минюсте РФ 23.09.2011 N 21877);
16. «Положение о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств и о порядке осуществления Банком России контроля за соблюдением требований к обеспечению защиты информации при осуществлении переводов денежных средств» (утв. Банком России 09.06.2012 N 382-П) (Зарегистрировано в Минюсте России 14.06.2012 N 24575);
17. «Положение о требованиях к защите информации в платежной системе Банка России» (утв. Банком России 09.01.2019 N 672-П) (вместе с «Правилами материально-технического обеспечения формирования электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре участника ССНП, а также правила материально-технического обеспечения обработки электронных сообщений и контроля реквизитов электронных сообщений в информационной инфраструктуре ОПКЦ») (Зарегистрировано в Минюсте России 21.03.2019 N 54109):
18. Указание Банка России от 08.10.2018 N 4926-У «О форме и порядке направления операторами по переводу денежных средств, операторами платежных систем, операторами услуг

платежной инфраструктуры в Банк России информации обо всех случаях и (или) попытках осуществления переводов денежных средств без согласия клиента и получения ими от Банка России информации, содержащейся в базе данных о случаях и попытках осуществления переводов денежных средств без согласия клиента, а также о порядке реализации операторами по переводу денежных средств, операторами платежных систем, операторами услуг платежной инфраструктуры мероприятий по противодействию осуществлению переводов денежных средств без согласия клиента» (Зарегистрировано в Минюсте России 12.12.2018 N 52988);

19. «Положение об установлении обязательных для кредитных организаций требований к обеспечению защиты информации при осуществлении банковской деятельности в целях противодействия осуществлению переводов денежных средств без согласия клиента» (утв. Банком России 17.04.2019 N 683-П) (Зарегистрировано в Минюсте России 16.05.2019 N 54637);

20. СТО БР ИББС-1.0-2014 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения;

21. РС БР ИББС-2.0-2007 Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0;

22. РС БР ИББС-2.5-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности;

23. РС БР ИББС-2.6-2014. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных банковских систем;

24. РС БР ИББС-2.7-2015. Ресурсное обеспечение информационной безопасности;

25. РС БР ИББС-2.9-2016. Предотвращение утечек информации;

26. СТО БР БФБО-1.5-2018 О Формах и сроках взаимодействия Банка России с участниками информационного обмена при выявлении инцидентов, связанных с нарушением требований к обеспечению защиты информации;

27. ГОСТ Р 57580.1-2017 Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер.

Приложение 2
к Политике
информационной безопасности
АО «РОСКОСМОСБАНК»

ОБЯЗАТЕЛЬСТВО
О СОБЛЮДЕНИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ
АО «РОСКОСМОСБАНК»

Я, _____
(фамилия, имя, отчество полностью)

ознакомлен(а) с содержанием Политики информационной безопасности АО «РОСКОСМОСБАНК». Принципы и требования АО «РОСКОСМОСБАНК» в отношении соблюдения норм информационной безопасности мне разъяснены, беру на себя обязательство выполнять требования этой Политики и руководствоваться ею при принятии решений в своей профессиональной деятельности.

Я осознаю персональную ответственность за нарушение мной действующего законодательства Российской Федерации, принципов и требований Политики информационной безопасности АО «РОСКОСМОСБАНК» и других организационно-распорядительных документов АО «РОСКОСМОСБАНК», направленных на защиту информационных активов, обязуюсь уведомить непосредственного руководителя и Управление информационной безопасности Дирекции по безопасности о нарушении требований указанных документов.

«____» _____20___г. _____ _____
(подпись) (расшифровка подписи)