«ТИНЬКОФФ КРЕДИТНЫЕ СИСТЕМЫ» БАНК (ЗАКРЫТОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО)
123060, РОССИЯ, МОСКВА, 1-Й ВОЛОКОЛАМСКИЙ ПРОЕЗД, 10, СТР. 1
ТЕЛ.: +7 (495) 648 1000, WWW.TCSBANK.RU

УТВЕРЖДЕНО:
решением Совета Директоров
протокол от 27 июня 2013г.

Политика информационной безопасности в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество)

редакция 3

Москва, 2013

Содержание

1. Общие положения

1.1. Политика информационной безопасности «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество) (далее - Банк) определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности, которыми руководствуется Банк в своей деятельности.

1.2. Настоящий документ разработан в соответствии с Федеральным законом № 86-ФЗ от 10.07.2002 г. «О Центральном банке Российской Федерации (Банке России)», письмом Банка России № 119-Т от 13.09.2005 г. «О современных подходах к организации корпоративного управления в кредитных организациях», раздел «Информационная политика» (п.п. 33-39), положениями Стандарта Центрального Банка Российской Федерации СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения», применяемыми в Российской Федерации международными стандартами банковской деятельности, иными нормативными документами, регламентирующими принципы информационной безопасности Банка.

1.3. Основными целями Политики информационной безопасности Банка являются защита информации Банка и обеспечение эффективной работы всего информационно-вычислительного комплекса Банка при осуществлении деятельности, указанной в его Уставе.

1.4. Общее руководство обеспечением информационной безопасности Банка осуществляет Председатель Правления Банка. Ответственность за организацию мероприятий по обеспечению информационной безопасности и контроль за соблюдением требований информационной безопасности несет руководитель Департамента Информационных технологий.

1.5. Руководители структурных подразделений Банка ответственны за обеспечение выполнения требований информационной безопасности в своих подразделениях.

1.6. Сотрудники Банка обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией Банка, соблюдать требования настоящей Политики и других документов информационной безопасности.

1.7. Перечень документов, входящих в состав документов базового уровня обеспечения информационной безопасности Банка, приведен в Приложении №2.

2. Область применения

2.1. Настоящая Политика распространяется на все структурные подразделения Банка и обязательна к исполнению всеми его сотрудниками и должностными лицами. Положения настоящей Политики применимы для использования во внутрибанковских документах Банка, а также в договорах.

2.2. Обеспечение информационной безопасности Банка

В ходе реализации своих бизнес-целей Банк широко вовлекает принадлежащие акционерам активы, в том числе информационные активы, в бизнес-процессы. Важнейшим условием реализации такой деятельности Банка является обеспечение необходимого и достаточного уровня информационной безопасности (ИБ) Банка, его активов (в т. ч. информационных), который во многом определяется уровнем ИБ информационной

инфраструктуры, обеспечивающей реализацию банковских технологических процессов (платежных, информационных и пр.), автоматизированных банковских систем, эксплуатирующихся в Банке.

3. Термины, определения и сокращения

В настоящем документе используются термины и определения, принятые в Стандарте Банка России. Полный перечень терминов и определений приведен в Приложении №1.

Ниже приводятся дополнительные термины, определения и сокращения.

Таблица 1

Термин/сокращение	Определение/расшифровка
АБС	Автоматизированная банковская система
Банк	«Тинькофф Кредитные Системы» Банк (закрытое акционерное общество)
Банковская информация	Информация, создаваемая, обрабатываемая и используемая Банком, доверенная Банку его клиентами и бизнес партнерами, а также информация, которую Банк должен защищать в соответствии с действующим законодательством Российской Федерации
Владелец информации	Организационная роль сотрудника Банка по обеспечению ИБ информации, создаваемой в рамках своего подразделения
ИБ	Информационная безопасность
НСД	Несанкционированный доступ
Организационная роль	Совокупность обязанностей сотрудника Банка, возлагаемых на него отдельными поручениями Руководства Банка или Руководителем подразделения, и уточняющие отдельные положения должностных обязанностей (например, участие в конкретной рабочей группе, кураторство нескольких конкретных филиалов, участие в разработке конкретного проекта и т. п.)
Политика	Настоящий документ
Руководитель, Руководитель подразделения	Руководитель Департамента, Управления, не входящего в структуру Департамента, Отдела, не входящего в структуру Управления или Департамента
СОИБ	Системы обеспечения информационной безопасности
Стандарт Банка России	Стандарт Центрального Банка Российской Федерации СТО БР ИББС-1.0-2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения»
СУБД	Система управления базами данных
Технологическая роль	Совокупность обязанностей сотрудника Банка, возлагаемых на него при эксплуатации информационных ресурсов Банка в ходе реализации своих должностных обязанностей (например, пользователь автоматизированной банковской системы, администратор информационной системы и т. п.)
УИБ	Управление информационной безопасности – структурное подразделение Банка, ответственное за проведение в жизнь политики обеспечения безопасности информации

4. Основные принципы обеспечения информационной безопасности Банка

4.1. Информационная безопасность Банка направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации.

4.2. Наибольшими возможностями для нанесения ущерба Банку обладает его собственный персонал. Действия персонала могут быть мотивированы злым умыслом (при этом злоумышленник может иметь сообщников как внутри, так и вне Банка) либо иметь непреднамеренный ошибочный характер. Риск аварий и технических сбоев определяется состоянием технического парка, надежностью систем энергоснабжения и телекоммуникаций, квалификацией персонала и его способностью к адекватным действиям в нештатной ситуации.

4.3. Стратегия обеспечения информационной безопасности Банка заключается в использовании заранее разработанных мер противодействия атакам злоумышленников, а также программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала Банка и других пользователей автоматизированных систем обработки информации и информационных систем.

4.4. Реализация стратегии информационной безопасности и защита информационной инфраструктуры Банка на разных уровнях должна гарантировать:

4.4.1. На физическом уровне:

- целостность и доступность помещений Банка на основе периметра защиты с использованием технических, организационных и административных мер;
- целостность и доступность линий связи и аппаратных средств за счет размещения внутри защищенного периметра, с одновременным обеспечением конфиденциальности информации на них при размещении оборудования. Кроме того, защита портативного оборудования должна предусматривать защиту от несанкционированного доступа к информации при возможных утратах и кражах оборудования.

4.4.2. На сетевом уровне:

- взаимодействие локальных и глобальных сетей должно осуществляться с использованием специализированных средств безопасности: межсетевых экранов, виртуальных частных сетей, специальных систем удаленного доступа и т. п., с применением систем обнаружения и предотвращения вторжений;
- типы, конфигурации, стандарты и правила настройки систем безопасности сетевого оборудования, межсетевых экранов и т. п. должны быть формализованы и утверждены;
- информационные ресурсы, доступ к которым необходим одновременно и из локальных и из глобальных сетей, должны размещаться в специальных демилитаризованных зонах;

- информация с различными классами конфиденциальности должна размещаться в различных сегментах корпоративной сети;
- сетевые узлы и их функционал должны быть защищены с одновременной регистрацией критических событий;
- удаленный доступ к сетевым ресурсам Банка должен быть строго регламентирован, необходимость доступа должна определяться ролью сотрудника, возможность доступа должна дополнительно авторизовываться, а реальный доступ должен контролироваться;
- проведение регулярного мониторинга и тестирования сети.

4.4.3. На системном уровне:

- настройки параметров безопасности на уровне операционных систем (ОС) и систем управления баз данных (СУБД), должны использоваться встроенные (штатные) средства безопасности и как минимум предоставлять следующие сервисы безопасности:
  1) идентификация и аутентификация;
  2) авторизация и контроль доступа;
  3) возможность формирования системных отчетов;
  4) возможность проведения аудита системы;
- в целях реализации централизованного управления разнородных (гетерогенных) систем, а так же, в случае недостаточности масштабируемости штатных средств безопасности, необходимо использовать специализированные программные средства сторонних разработчиков;
- типы, конфигурации, стандарты и правила настройки систем безопасности ОС и СУБД должны быть формализованы и утверждены;
- антивирусная защита информационных ресурсов Банка должна строиться эшелонировано, при этом должны контролироваться: информация, входящая из глобальных сетей во внутреннюю сеть Банка; информация, хранящаяся на файловых серверах Банка; и информация, хранящаяся на персональных компьютерах сотрудников Банка и ином оборудовании, входящем в состав информационной инфраструктуры Банка;
- использование средств криптографической защиты информации (СКЗИ) должно соответствовать требованиям законодательства РФ;
- для реализации архитектуры безопасности при распространении открытых ключей, управлении электронными сертификатами и ключами пользователей в Банке должна использоваться инфраструктура открытых ключей - Public Key Infrastructure (PKI).

4.4.4. На прикладном уровне:

- доступ к любого рода информационным ресурсам Банка должен предоставляться на основе:
  1) разработанных технологических и/или организационных ролей персонала Банка;
  2) Идентификации и Аутентификации;

3) строгой регламентации действий всех участников процесса;

- для формирования системных отчетов во всех информационных системах Банка должны использоваться средства протоколирования, регистрирующие как минимум: имя пользователя, тип события, описание события, дату и время события;
- для каждой информационной системы, банковской платежной системы и приложений должен быть определен владелец ресурсов, определяющий требования к уровню защиты и контролирующий достаточность существующих мер;
- технические профили и роли пользователей в банковских платежных системах и приложениях должны соответствовать основным принципам:
  1) разделения полномочий (Segregation of Duties);
  2) двойного контроля (Dual Control);
  3) минимум привилегий (Least Privileges);
  4) необходимо знать (Need to know);
- в банковских платежных системах и приложениях должны быть реализованы механизмы:
  1) защиты платежной информации от искажения, фальсификации, несанкционированного уничтожения, ложной авторизации электронных платежных сообщений;
  2) аутентификации входящих электронных платежных сообщений;
  3) двусторонней аутентификации автоматизированных рабочих мест (рабочих станций и серверов), участников обмена электронными платежными сообщениями;
- в системах дистанционного банковского обслуживания должны быть реализованы:
  1) механизмы, обеспечивающие невозможность отказа от авторства проводимых клиентами транзакций и операций (например, ЭЦП);
  2) механизмы информирования (регулярного, непрерывного или по требованию) клиентов обо всех операциях, совершаемых от их имен;
- все операции клиентов в течение всего сеанса работы с системами дистанционного банковского обслуживания должны выполняться только после выполнения процедур идентификации, аутентификации.

4.4.5. На уровне технологических процессов:

- технологические процессы должны быть документированы;
- для каждого технологического процесса должны быть:
  1) определены цели и задачи процесса;
  2) определен владелец используемой в процессе информации;
  3) определены перечни необходимого программного обеспечения и ресурсов информационных систем Банка;
  4) определены и документированы критичные для всего процесса элементы или функции, в том числе, с учетом процесса их восстановления (disaster recovery).

4.4.6. На уровне персонала:

- поддержание необходимого уровня квалификации сотрудников, с учетом требований Банка в сфере информационной безопасности и обеспечения высокого уровня безопасности в информационной банковской системе.

5. Цели и задачи информационной безопасности Банка

Меры безопасности, реализуемые в рамках системы обеспечения информационной безопасности Банка (СОИБ), и процессы эксплуатации этих мер нацелены на минимизацию любых выявленных угроз информационной безопасности и минимизацию банковских рисков.

5.1. Основными целями обеспечения ИБ являются:

- соответствие требованиям законодательства, требованиям надзорных и регулирующих органов, включая соответствие положениям Стандарта Банка России;
- повышение стабильности функционирования Банка в целом;
- достижение адекватности мер по защите от реальных угроз информационной безопасности;
- предотвращение и/или снижение ущерба от инцидентов информационной безопасности;
- обеспечение стабильности функционирования Банка (обеспечение непрерывности его бизнеса) посредством обеспечения необходимой доступности информационных активов и информационной инфраструктуры Банка;
- повышение доверия к Банку со стороны клиентов, контрагентов, партнеров, инвесторов и общественности в целом, повышение рейтинга Банка и его инвестиционной привлекательности;
- предотвращение или снижение ущерба от инцидентов ИБ посредством обеспечения целостности информационных активов и информационной инфраструктуры Банка и обеспечения конфиденциальности чувствительных информационных активов Банка;
- защита законных прав Банка и его работников, в случаях неправомерного использования или злоупотребления информационной инфраструктурой и информационными активами;
- защита капиталовложений в информационную инфраструктуру и реализуемые посредством ее технологические процессы Банка;
- формирование взвешенного подхода к защите от угроз ИБ посредством применения экономически и технически обоснованных, а также необходимых и достаточных защитных мер информационной безопасности.

5.2. Основные принципы информационной безопасности Банка:

- одним из наиболее ценных активов Банка является информация, создаваемая, обрабатываемая и используемая Банком, доверенная Банку его клиентами и бизнес партнерами, а также информация, которую Банк должен защищать в соответствии с действующим законодательством РФ;

- Банк должен обеспечить конфиденциальность, целостность и доступность банковской информации и защитить ее от повреждения, изменения, разглашения и утраты;
- безопасность информационных ресурсов Банка должна быть обеспечена как от нарушителей (внутренних и внешних), так и от естественных (природных и техногенных) угроз;
- для оценки угроз информационной безопасности в Банке должен быть реализован процесс управления рисками информационной безопасности. При этом, реализация процесса управления рисками информационной безопасности возлагается на Управление информационной безопасности;
- информационные активы Банка должны быть защищены на всех этапах их жизненного цикла: разработка технических заданий – проектирование - создание и тестирование - приемка и ввод в действие – эксплуатация - сопровождение и модернизация - снятие с эксплуатации;
- требования настоящей Политики должны быть реализованы на всех уровнях информационной инфраструктуры - во всех банковских продуктах, системах, сервисах, процессах и технологиях, при этом ответственность за бюджетирование, внедрение и использование мер безопасности возлагается на Руководителей подразделений, в зоне ответственности которых находятся информационные ресурсы, подлежащие защите.

5.3. Принципы, декларированные в настоящем пункте, должны быть уточнены и детализированы соответствующими частными Политиками/ Положениями/ Правилами, входящими в состав документов базового уровня обеспечения ИБ Банка (Приложении №2).

5.4. Основными задачами деятельности по обеспечению информационной безопасности Банка являются:

- разработка требований по обеспечению информационной безопасности;
- контроль выполнения установленных требований по обеспечению информационной безопасности;
- повышение эффективности мероприятий по обеспечению и поддержанию информационной безопасности;
- разработка и совершенствование нормативной базы Банка по обеспечению информационной безопасности;
- выявление, оценка и прогнозирование угроз информационной безопасности;
- организация антивирусной защиты информационных активов;
- защита информации от несанкционированного доступа и утечки по техническим каналам связи.

6. Объекты защиты

6.1. Объектами защиты с точки зрения информационной безопасности в Банке являются:

- платежная информация;
- персональные данные клиентов Банка;

- данные платежных карт;
- банковский информационный технологический процесс;
- различного рода носители защищаемой информации.

7. Требования по информационной безопасности

7.1. Требования информационной безопасности формулируются для следующих областей:

- назначения и распределения ролей и доверия к персоналу;
- стадий жизненного цикла автоматизированных систем обработки информации и информационных систем;
- защиты от несанкционированного доступа, управления доступом и регистрацией в автоматизированных системах обработки информации и информационных системах;
- антивирусной защиты;
- использования ресурсов Интернет;
- использования средств криптографической защиты информации;
- защиты банковских платежных и информационных технологических процессов;
- защиты от аварийных сбоев в электроснабжении и телекоммуникационных каналах связи.

8. Управление рисками информационной безопасности

8.1. Основные принципы управления рисками информационной безопасности.

8.1.1. Меры безопасности, реализуемые в рамках СОИБ, и процессы их эксплуатации нацелены на минимизацию любых выявленных угроз информационной безопасности и минимизацию связанных с ними операционных рисков основной деятельности Банка (бизнеса).

8.1.2. С целью снижения рисков нарушения ИБ и управления ими в Банке должен существовать уполномоченный на выполнение мероприятий в области ИБ орган, организовано создание и эксплуатация СОИБ, а также организована эксплуатация АБС в соответствии с правилами и требованиями, задаваемыми СОИБ. Одна из задач службы ИБ – выявление следов активности нарушителя.

8.1.3. Снижение рисков нарушения ИБ должно осуществляться до определенного остаточного уровня. Оставшаяся (остаточная) часть риска должна быть признана приемлемой и принята, либо отклонена. В этом случае от риска следует либо уклониться (изменить среду деятельности), либо перевести на кого-нибудь (например, застраховать). Таким образом, уровень защищенности интересов Банка определяется, во–первых, величиной принятых остаточных рисков, а во-вторых, эффективностью работ по поддержанию принятых рисков на допустимом, низком (остаточном) уровне.

8.1.4. Риски нарушения ИБ должны быть согласованы и связаны с рисками основной деятельности Банка.

8.1.5. Анализ и оценка рисков нарушения ИБ должны основываться на идентификации активов Банка, на их ценности для целей и задач Банка, на моделях угроз и нарушителей ИБ.

8.1.6. Анализ и оценка рисков нарушения ИБ должны проводиться не реже 1 раза в 12 месяцев.

8.2. Реализация процесса управления рисками информационной безопасности.

Реализация процесса управления рисками информационной безопасности возлагается на Управление информационной безопасностью (УИБ), при этом:

- УИБ должно быть независимо от подразделений, ответственных за реализацию и обеспечение информационных технологий в Банке;
- организационная структура и подчинение УИБ должны соответствовать подходу и рекомендациям Банка России и лучшим мировым и отечественным практикам;
- в функциональные обязанности УИБ входит разработка, контроль выполнения и обновление данной Политики;
- для реализации требований Политики могут быть назначены специальные роли – Администраторы безопасности из числа сотрудников структурных подразделений.

9. Владение информацией

9.1. Руководители подразделений, для банковской информации находящейся в зоне их ответственности (используемой подразделением), должны определить Владельцев информации.

9.2. Владелец информации должен классифицировать информацию в зоне своей ответственности следующим образом:

- КОНФИДЕНЦИАЛЬНАЯ;
- ДЛЯ СЛУЖЕБНОГО ИСПОЛЬЗОВАНИЯ (ВНУТРЕННЯЯ);
- ОБЩЕДОСТУПНАЯ.

9.3. Каждый Руководитель, в рамках своей ответственности, является Владельцем информации, создаваемой в рамках своего подразделения, при этом, для одной и той же информации может быть определен только один владелец.

9.4. На основе процесса управления рисками и классификации информации, Руководитель должен определить необходимый уровень защиты для банковской информации и убедиться, что существующих мер защиты достаточно, чтобы соответствовать утвержденному уровню приемлемого риска.

9.5. Руководители подразделений должны убедиться, в рамках своих полномочий, что в Банке ведется инвентаризация всех информационных активов, банковских систем, приложений и технологических процессов. Результаты инвентаризации должны, как минимум содержать: название ресурса (актива/системы/приложения/процесса), имя Владельца информации, Классификацию информации, Уровень риска.

10.Модель угроз и нарушителей

10.1. Безопасность информационных ресурсов Банка должна быть обеспечена как от нарушителей (внутренних и внешних), так и от естественных (природных и техногенных) угроз.

10.1.1. Модели угроз и нарушителей должны быть основным инструментом Банка при развертывании, поддержании и совершенствовании СОИБ.

10.1.2. Модели угроз и нарушителей должны быть разработаны для Банка в целом, а также, при необходимости, для отдельных банковских процессов и систем.

10.1.3. При построении адекватной модели нарушителя необходимо классифицировать нарушителя по следующим параметрам:

- по отношению к системе (внутренний, внешний);
- по правам доступа;
- по мотивам нарушения;
- по уровню знаний о системе;
- по уровню возможностей (используемым методам и средствам);
- по времени действия;
- по месту действия.

10.1.4. При построении адекватной модели угроз необходимо исходить из того, что основными источниками угроз ИБ являются:

- работники Банка, реализующие угрозы ИБ с использованием легально предоставленных им прав и полномочий (внутренние нарушители ИБ);
- работники Банка, реализующие угрозы ИБ вне легально предоставленных им прав и полномочий, а также субъекты, не являющиеся работниками Банка, но осуществляющие попытки НСД и НРД (внешние нарушители ИБ);
- неблагоприятные события природного, техногенного и социального характера;
- террористы и криминальные элементы;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- сбои, отказы, разрушения/повреждения программных и технических средств;
- несоответствие требованиям действующего законодательства РФ.

11.Полномочия и обязанности по обеспечению информационной безопасности

11.1. В рамках деятельности по обеспечению информационной безопасности указанные ниже работники и подразделения Банка выполняют следующие функции:

Таблица 2

Работник / Подразделение	**Функции по обеспечению информационной безопасности**
Председатель Правления	общее руководство обеспечением информационной безопасности Банка

Работник / Подразделение	Функции по обеспечению информационной безопасности
Банка	организация своевременного и качественного обучения и проверки знаний по информационной безопасности в целом по Банку
Правление Банка	организация, оценка и анализ функционирования системы обеспечения информационной безопасности, в том числе путем проведения соответствующих совещаний и обработки полученных отчетов и информации по Информационной безопасности с ответственным работником, Управлением информационной безопасности и иными специалистами в области информационной безопасности
Ответственный работник и Управление информационной безопасности	поддержание и совершенствование системы обеспечения информационной безопасности
	управление планами по обеспечению информационной безопасности
	разработка документов по обеспечению информационной безопасности, а также контроль исполнения данных документов
	определение требований к защитным мерам обеспечения информационной безопасности
	контроль доступа и использования средств обеспечения информационной безопасности (средств антивирусной защиты, межсетевых экранов, блокировки портов, обнаружения сетевых атак и т.д.)
	мониторинг событий, связанных с обеспечением информационной безопасности
	расследование событий, связанных с инцидентами информационной безопасности и в случае необходимости вынесение предложений по применению санкций в соответствии с законодательством Российской Федерации в отношении лиц, осуществивших противоправные действия
	контроль уровня информационной безопасности Банка
	участие в восстановлении работоспособности информационной инфраструктуры после сбоев и аварий
	взаимодействие по вопросам обеспечения информационной безопасности с регулирующими и надзорными органами
	разработка программ обучения сотрудников Банка
	контроль своевременности обучения по информационной безопасности сотрудников Банка
Департамент информацион-ных технологий	внедрение и эксплуатация защитных мер системы информационной безопасности
	организация мероприятий по обеспечению информационной безопасности
	контроль за соблюдением требований информационной безопасности
Руководители структурных подразделений Банка	выполнение работниками возглавляемого подразделения требований и правил Банка по обеспечению информационной безопасности
	информирование Ответственного работника и Управления

Работник / Подразделение	Функции по обеспечению информационной безопасности
	информационной безопасности об инцидентах информационной безопасности
	соблюдение принципа минимальности при предоставлении доступа к информационным активам и компонентам информационной инфраструктуры
	ознакомление с документами и требованиями по обеспечению информационной безопасности работников возглавляемых подразделений
	организация своевременного и качественного обучения и проверки знаний по информационной безопасности в структурных подразделениях
Все работники Банка	соблюдение требований законодательных и нормативных документов, в том числе внутренних нормативных документов Банка по вопросам информационной безопасности
	обеспечение целостности и конфиденциальности информационных активов и компонентов информационной инфраструктуры, при этом условие о соблюдении конфиденциальности должно распространяться на всю защищаемую от разглашения информацию, доверенную работнику или ставшую ему известной в процессе выполнения им своих служебных обязанностей
	соблюдение прав Банка на информационные активы, информационную инфраструктуру и интеллектуальную собственность
	использование только тех информационных активов и компонентов информационной инфраструктуры, которые необходимы для выполнения служебных обязанностей, и только в целях, для которых они предназначены
	своевременное уведомление непосредственных руководителей, Ответственного работника и Управления информационной безопасности о фактических или потенциально возможных инцидентах информационной безопасности, угрозах и уязвимости, а также о несанкционированных действиях и обращениях неуполномоченных лиц

11.2. Все работники Банка в соответствии с законодательством Российской Федерации несут дисциплинарную и материальную ответственность за неисполнение или ненадлежащее исполнение требований по обеспечению информационной безопасности, определенных Политикой и иными внутренними документами Банка.

12.Порядок пересмотра Политики

12.1. Настоящая Политика и соответствующие частные Политики/ Положения/Порядки должны ежегодно пересматриваться и, при необходимости, обновляться, при этом ответственность за пересмотр и обновление возлагается на Управление информационной безопасности.

12.2. Проект Политики представляется на утверждение Совету Директоров Банка.

12.3. В случае изменения действующего законодательства РФ, внесения изменений в нормативные документы Банка России и иных органов, а также внутренние документы Банка, настоящая Политика действует в части, не противоречащей действующему законодательству и действующим внутренним документам Банка, до приведения ее в соответствие с такими изменениями.

Приложение №1
к Политике информационной безопасности в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество

Сокращения, термины и определения, применяемые в Стандарте СТО БР ИББС–1.0–2010

Настоящий документ содержит выдержки из Стандарта СТО БР ИББС–1.0–2010 «Обеспечение информационной безопасности организаций банковской системы российской Федерации. Общие положения» (далее - Стандарт).

Термины и определения

Ниже приводятся термины и определения, принятые в разделе 3 Стандарта, за исключением ссылок на нормативные документы.

Все подразделения ТКС Банк (ЗАО) при разработке внутрибанковских документов, затрагивающих вопросы информационной безопасности, обязаны применять термины и их определения, установленные настоящим приложением.

Термин	Определение
Банковская система Российской Федерации	Банк России и кредитные организации, а также филиалы и представительства иностранных банков.
Стандарт	Документ, в котором в целях добровольного многократного использования устанавливаются характеристики продукции, правила осуществления и характеристики процессов производства, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг. Стандарт также может содержать требования к терминологии, символике, упаковке, маркировке или этикеткам и правилам их нанесения.
Рекомендации в области стандартизации	Документ, содержащий советы организационно-методического характера, которые касаются проведения работ по стандартизации и способствуют применению основополагающего стандарта.
Комплекс БР ИББС	Комплекс документов в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации».
Менеджмент	Скоординированная деятельность по руководству и управлению.

Система	Множество (совокупность) материальных объектов (элементов) любой, в том числе различной физической природы и информационных объектов, взаимодействующих между собой для достижения общей цели, обладающее системным свойством (свойствами), т.е. свойством, которого не имеет ни один из элементов и ни одно из подмножеств элементов при любом способе членения. Системное свойство не выводимо непосредственно из свойств элементов и частей.
Информация	Сведения (сообщения, данные) независимо от формы их представления.
Инфраструктура	Комплекс взаимосвязанных обслуживающих структур, составляющих основу для решения проблемы (задачи).
Информационная инфраструктура	Система организационных структур, обеспечивающих функционирование и развитие информационного пространства и средств информационного взаимодействия. Примечание. Информационная инфраструктура: включает совокупность информационных центров, банков данных и знаний, систем связи; обеспечивает доступ потребителей к информационным ресурсам.
Документ	Зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Примечание. Под материальным носителем подразумевается изделие (материал), на котором записана информация и которое обеспечивает возможность сохранения этой информации и снятие ее копий, например, бумага, магнитная лента или карта, магнитный или лазерный диск, фотопленка и т.п.
Процесс	Совокупность взаимосвязанных ресурсов и деятельности, преобразующая входы в выходы.
Технология	Совокупность взаимосвязанных методов, способов, приемов предметной деятельности.
Технологический процесс	Процесс, реализующий некоторую технологию.

Автоматизированная система	Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.
Авторизация	Предоставление прав доступа.
Идентификация	Процесс присвоения идентификатора (уникального имени); сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.
Аутентификация	Подтверждение подлинности.
Регистрация	Фиксация данных о совершенных действиях (событиях).
Роль	Заранее определенная совокупность правил, устанавливающих допустимое взаимодействие между субъектом и объектом. Примечания. 1. К субъектам относятся лица из числа руководителей организации банковской системы Российской Федерации, ее персонала, клиентов или инициируемые от их имени процессы по выполнению действий над объектами. 2. Объектами могут быть аппаратное средство, программное средство, программно-аппаратное средство, информационный ресурс, услуга, процесс, система, над которыми выполняются действия.
Угроза	Опасность, предполагающая возможность потерь (ущерба).
Риск	Мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.
Актив	Все, что имеет ценность для организации банковской системы Российской Федерации и находится в ее распоряжении. Примечание. К активам организации банковской системы Российской Федерации могут относиться: работники (персонал), финансовые (денежные) средства, средства вычислительной техники, телекоммуникационные средства и пр.; различные виды банковской информации – платежная, финансово-аналитическая, служебная, управляющая и пр.;

	банковские процессы (банковские платежные технологические процессы, банковские информационные технологические процессы); банковские продукты и услуги, предоставляемые клиентам.
Информационный актив	Информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для организации банковской системы Российской Федерации; находящаяся в распоряжении организации банковской системы Российской Федерации и представленная на любом материальном носителе в пригодной для ее обработки, хранения или передачи форме.
Классификация информационных активов	Разделение существующих информационных активов организации банковской системы Российской Федерации по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.
Объект среды информационного актива	Материальный объект среды использования и(или) эксплуатации информационного актива (объект хранения, передачи, обработки, уничтожения и т.д.).
Ресурс	Актив организации банковской системы Российской Федерации, который используется или потребляется в процессе выполнения некоторой деятельности.
Банковский технологический процесс	Технологический процесс, реализующий операции по изменению и(или) определению состояния активов организации банковской системы Российской Федерации, используемых при функционировании или необходимых для реализации банковских услуг. Примечания. 1. Операции над активами организации банковской системы Российской Федерации могут выполняться вручную или быть автоматизированными, например, с помощью автоматизированных банковских систем. 2. В зависимости от вида деятельности выделяют: банковский платежный технологический процесс, банковский информационный технологический процесс и др.

Банковский платежный технологический процесс	Часть банковского технологического процесса, реализующая банковские операции над информационными активами организации банковской системы Российской Федерации, связанные с перемещением денежных средств с одного счета на другой и(или) контролем данных операций.
Банковский информационный технологический процесс	Часть банковского технологического процесса, реализующая операции по изменению и(или) определению состояния информационных активов, необходимых для функционирования организации банковской системы Российской Федерации и не являющихся платежной информацией. Примечания. Платежная информация – информация, содержащаяся в документах, на основании которой совершаются операции, связанные с перемещением денежных средств с одного счета на другой. Неплатежная информация, необходимая для функционирования организации банковской системы Российской Федерации, может включать в себя, например, данные статистической отчетности и внутри хозяйственной деятельности, аналитическую, финансовую, справочную информацию.
Автоматизированная банковская система	Автоматизированная система, реализующая технологию выполнения функций организации банковской системы Российской Федерации.
Комплекс средств автоматизации автоматизированной банковской системы	Совокупность всех компонентов автоматизированной банковской системы организации банковской системы Российской Федерации, за исключением людей.
Безопасность	Состояние защищенности интересов (целей) организации банковской системы Российской Федерации в условиях угроз.
Информационная безопасность, ИБ	Безопасность, связанная с угрозами в информационной сфере. Примечания. 1. Защищенность достигается обеспечением совокупности свойств ИБ – доступности, целостности, конфиденциальности информационных активов. Приоритетность свойств ИБ определяется ценностью

	указанных активов для интересов (целей) организации банковской системы Российской Федерации. 2. Информационная сфера представляет собой совокупность информации, информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение, хранение и использование информации, а также системы регулирования возникающих при этом отношений.
Доступность информационных активов	Свойство ИБ организации банковской системы Российской Федерации, состоящее в том, что информационные активы предоставляются авторизованному пользователю, причем в виде и месте, необходимых пользователю, и в то время, когда они ему необходимы.
Целостность информационных активов	Свойство ИБ организации банковской системы Российской Федерации сохранять неизменность или обнаруживать факт изменения в своих информационных активах.
Система информационной безопасности; СИБ	Совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.
Система менеджмента информационной безопасности; СМИБ	Часть менеджмента организации банковской системы Российской Федерации, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.
Система обеспечения информационной безопасности; СОИБ	Совокупность СИБ и СМИБ организации банковской системы Российской Федерации.
Область действия системы обеспечения информационной безопасности; область действия СОИБ	Совокупность информационных активов и элементов информационной инфраструктуры организации банковской системы Российской Федерации.
Осознание необходимости обеспечения информационной безопасности; осознание ИБ	Понимание руководством организации банковской системы Российской Федерации необходимости самостоятельно на основе принятых в этой организации ценностей и накопленных знаний формировать и учитывать в рамках основной деятельности (бизнеса) прогноз результатов от деятельности по

	обеспечению ИБ, а также поддерживать эту деятельность адекватно прогнозу. Примечание. Осознание ИБ является внутренней побудительной причиной для руководства банковской системы Российской Федерации инициировать и поддерживать деятельность по обеспечению ИБ, в отличие от побуждения или принуждения, когда решение об инициировании и поддержке деятельности по обеспечению ИБ определяется соответственно либо возникшими проблемами организации, либо внешними факторами, например, требованиями законов.
Защитная мера	Сложившаяся практика, процедура или механизм, которые используются для уменьшения риска нарушения ИБ организации банковской системы Российской Федерации.
Угроза информационной безопасности; угроза ИБ	Угроза нарушения свойств ИБ – доступности, целостности или конфиденциальности информационных активов организации банковской системы Российской Федерации.
Уязвимость информационной безопасности; уязвимость ИБ	Слабое место в инфраструктуре организации банковской системы Российской Федерации, включая СОИБ, которое может быть использовано для реализации или способствовать реализации угрозы ИБ.
Ущерб	Утрата активов, повреждение (утрата свойств) активов и(или) инфраструктуры организации или другой вред активам и(или) инфраструктуре организации банковской системы Российской Федерации, наступивший в результате реализации угроз ИБ через уязвимости ИБ.
Инцидент информационной безопасности; инцидент ИБ	Событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ, т.е. реализацию нарушения свойств ИБ информационных активов организации банковской системы Российской Федерации. Примечание. Нарушение может вызываться источниками угроз ИБ: либо случайными факторами (ошибкой персонала, неправильным функционированием технических средств,

	природными факторами, например, пожаром или наводнением), либо преднамеренными действиями, приводящими к нарушению доступности, целостности или конфиденциальности информационных активов.
Нарушитель информационной безопасности; нарушитель ИБ	Субъект, реализующий угрозы ИБ организации банковской системы Российской Федерации, нарушая предоставленные ему полномочия по доступу к активам организации банковской системы Российской Федерации или по распоряжению ими.
Модель нарушителя информационной безопасности; модель нарушителя ИБ	Описание и классификация нарушителей ИБ, включая описание их опыта, знаний, доступных ресурсов, необходимых для реализации угрозы, возможной мотивации их действий, а также способы реализации угроз ИБ со стороны указанных нарушителей.
Модель угроз информационной безопасности; модель угроз ИБ	Описание источников угроз ИБ; методов реализации угроз ИБ; объектов, пригодных для реализации угроз ИБ; уязвимостей, используемых источниками угроз ИБ; типов возможных потерь (например, нарушение доступности, целостности или конфиденциальности информационных активов); масштабов потенциального ущерба.
Риск нарушения информационной безопасности; риск нарушения ИБ	Риск, связанный с угрозой ИБ.
Оценка риска нарушения информационной безопасности	Систематический и документированный процесс выявления, сбора, использования и анализа информации, позволяющей провести оценивание рисков нарушения ИБ, связанных с использованием информационных активов организации банковской системы Российской Федерации на всех стадиях их жизненного цикла.
Обработка риска нарушения информационной безопасности	Процесс выбора и осуществления защитных мер, снижающих риск нарушения ИБ, или мер по переносу, принятию или уходу от риска.
Остаточный риск нарушения информационной безопасности	Риск, остающийся после обработки риска нарушения ИБ.
Допустимый риск нарушения информационной безопасности	Риск нарушения ИБ, предполагаемый ущерб от которого организация банковской системы Российской Федерации в данное

	время и в данной ситуации готова принять.
Документация	Совокупность взаимосвязанных документов, объединенных общей целевой направленностью.
План работ по обеспечению информационной безопасности	Документ, устанавливающий перечень намеченных к выполнению работ или мероприятий по обеспечению ИБ организации банковской системы Российской Федерации, их последовательность, объем (в той или иной форме), сроки выполнения, ответственных лиц и конкретных исполнителей.
Свидетельства выполнения деятельности по обеспечению информационной безопасности	Документ или элемент документа, содержащий достигнутые результаты (промежуточные или окончательные), относящиеся к обеспечению ИБ организации банковской системы Российской Федерации.
Политика информационной безопасности; политика ИБ	Документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ, предназначенная для организации банковской системы Российской Федерации в целом.
Частная политика информационной безопасности; частная политика ИБ	Документация, детализирующая положения политики ИБ применительно к одной или нескольким областям ИБ, видам и технологиям деятельности организации банковской системы Российской Федерации.
Мониторинг	Постоянное наблюдение за объектами и субъектами, влияющими на ИБ организации банковской системы Российской Федерации, а также сбор, анализ и обобщение результатов наблюдений.
Аудит информационной безопасности; аудит ИБ	Систематический, независимый и документируемый процесс получения свидетельств деятельности организации банковской системы Российской Федерации по обеспечению ИБ, установления степени выполнения в организации банковской системы Российской Федерации критериев ИБ, а также допускающий возможность формирования профессионального аудиторского суждения о состоянии ИБ организации банковской системы Российской Федерации.

	Примечание. Аудит ИБ выполняется работниками организации, являющейся внешней по отношению к организации банковской системы Российской Федерации.
Критерии оценки (аудита) информационной безопасности; критерии оценки (аудита) ИБ	Совокупность требований в области ИБ, определенных стандартом Банка России СТО БР ИББС_1.0 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» или его частью.
Свидетельства оценки соответствия (аудита) информационной безопасности установленным критериям; свидетельства оценки соответствия (аудита) ИБ	Записи, изложение фактов или другая информация, которые имеют отношение к критериям оценки соответствия (самооценки соответствия, аудита) ИБ и могут быть проверены. Примечание. Свидетельства оценки соответствия (самооценки соответствия, аудита) ИБ могут быть качественными или количественными.
Выводы аудита информационной безопасности; выводы аудита ИБ	Результат оценки собранных свидетельств аудита ИБ.
Заключение по результатам аудита информационной безопасности (аудиторское заключение); заключение по результатам аудита ИБ	Качественная или количественная оценка соответствия установленным критериям аудита ИБ, представленная аудиторской группой после рассмотрения всех выводов аудита ИБ в соответствии с целями аудита ИБ.
Область аудита информационной безопасности; область аудита ИБ	Содержание и границы аудита ИБ. Примечание. Область аудита ИБ обычно включает местонахождение, организационную структуру, виды деятельности проверяемой организации и процессы, которые подвергаются аудиту ИБ, а также охватываемый период времени.
Программа аудита информационной безопасности; программа аудита ИБ	План деятельности по проведению одного или нескольких аудитов ИБ (и других проверок ИБ), запланированных на конкретный период времени и направленных на достижение конкретной цели. Примечание. Программа аудита ИБ включает всю деятельность, необходимую для планирования, проведения, контроля, анализа и совершенствования аудитов ИБ

	(и других проверок ИБ).

Сокращения

Ниже приводятся сокращения, принятые в разделе 4 Стандарта.

Сокращение	Расшифровка сокращения
АБС	автоматизированная банковская система
БС	банковская система
ЖЦ	жизненный цикл
ИБ	информационная безопасность
НСД	несанкционированный доступ
НРД	нерегламентированные действия в рамках предоставленных полномочий
РФ	Российская Федерация
СКЗИ	средство криптографической защиты информации
СМИБ	система менеджмента информационной безопасности
СИБ	система информационной безопасности
СОИБ	система обеспечения информационной безопасности
ЭВМ	электронная вычислительная машина
ЭЦП	электронная цифровая подпись

Приложение №2
к Политике информационной безопасности в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество), редакция 3.

Перечень документов, входящих в состав документов базового уровня обеспечения ИБ[1]

№	Ориентировочное название	Краткое содержание/описание
1.	Политика информационной безопасности	Общие принципы обеспечения ИБ в Банке. Излагаются основные правила, уточнение которых осуществляется в Стандартах
2.	Положение по обеспечению защиты информации от вредоносного программного обеспечения в подразделениях Банка	Требования по архитектуре системы, порядок и режим обновлений вирусных баз, порядок действий при вирусной атаке, распределение зон ответственности
3.	Порядок предоставления, реорганизации и закрытия доступа к информационным и вычислительным ресурсам	Требования по разграничению доступа к информационным ресурсам. Принципы управления доступом. Принципы оформления доступа. Требования по контролю за действующими уровнями доступов и за порядком предоставления доступа. Определение (фиксация) владельцев ресурсов. Категорирование информационных ресурсов. Распределение зон ответственности.
4.	Правила использования ресурсов глобальной сети Интернет в Банке	Требования по архитектуре межсетевого взаимодействия. Определение информационных ресурсов подлежащих размещению в ДМЗ. Требования по межсетевому экранированию. Требования по категорированию Web-ресурсов, порядок доступа к отдельным категориям Web-ресурсов. Контроль за использованием Интернет-ресурсов. Распределение зон ответственности.
5.	Инструкция о порядке учета, обращения и хранения документов и дел, содержащих конфиденциальные сведения в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество	Перечень сведений, составляющих коммерческую тайну Банка. Права и обязанности работника Банка в отношении информации, составляющей коммерческую тайну.
6.	Положение по основным правилам работы пользователей корпоративной вычислительной сети	Права и обязанности пользователей корпоративной вычислительной сети. Порядок подключения пользователей и основные правила работы в сети

[1] Перечень документов не является исчерпывающим и может быть изменен и/или дополнен.

7.	Порядок приобретения, установки и использования программного обеспечения в Банке	Регулирует вопросы упорядочения процесса приобретения, установки и использования программного обеспечения.
8.	Требования по обеспечению информационной безопасности при использовании паролей в подразделениях Банка	Требования к необходимому уровню информационной безопасности при использовании паролей для защиты средств вычислительной техники, программного обеспечения, информации от несанкционированного доступа; Технические и организационные меры, обеспечивающие исполнение указанных требований.
9.	Правила использования электронной почты	Правила обмена электронными сообщениями.
10.	Порядок управления информационными потоками	Устанавливает основные принципы управления информационными потоками, в том числе получением и передачей информации, их основные виды.
11.	Положение по управлению сбоями «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество)	Определяет совокупность правил, требований по управлению сбоями, которыми руководствуется ТКС Банк (ЗАО) в повседневной деятельности. Порядок реагирования на обнаруженные сбои.
12.	Положение о системе резервного копирования и архивирования	Устанавливает принципы организации резервного копирования в Банке. Требования к системе, аппаратному обеспечению, порядок хранения и сроки хранения копий. Правила использования (восстановления) резервных копий.
13.	Положение об обучении и проверке знаний сотрудников ТКС Банк (ЗАО) вопросам информационной безопасности	Определяет цели, задачи обучения, основные виды обучения, порядок взаимодействия структурных подразделений Банка, полномочия и обязанности сотрудников при организации обучения вопросам информационной безопасности.
14.	Порядок использования мобильных устройств и беспроводных технологий в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество),	Устанавливает основополагающие принципы обеспечения информационной безопасности при использовании беспроводных технологий, определяет минимальный набор защитных механизмов, направленных на снижение рисков, связанных с несанкционированным использованием беспроводных технологий
15.	Регламент организации межсетевого экранирования в «Тинькофф Кредитные Системы» Банк	Определяет основные принципы и правила организации сетевой защиты информационной инфраструктуры процессингового центра Банка.

16.	Процедуры физической защиты электронных носителей в «Тинькофф Кредитные Системы» Банк	Устанавливает правила учета, хранения, использования и очистки (уничтожения) электронных носителей информации, применяемых для хранения и передачи данных банковских карт в ТКС Банк в процессе выпуска, хранения, учета и передачи клиенту, а также последующего обслуживания карт.
17.	Процедура проведения сканирования уязвимостей и организации внутренних и внешних тестов на проникновение в «Тинькофф Кредитные Системы» Банк	Определяет процесс проведения сканирований уязвимостей внутренней сети, ежеквартальных внешних ASV-сканирований, а также ежегодного проведения внешних и внутренних тестов на проникновение.
18.	Процедура выявления и анализа несанкционированного использования беспроводных сетей ТКС Банк (ЗАО)	Регламентирует процессы, направленные на выявление факта несанкционированного использования беспроводных сетей и анализа выявленных устройств, в том числе методику определения местоположения несанкционированных точек доступа в пределах обследуемой территории.
19.	Процедура обеспечения информационной безопасности при разработке программного обеспечения в «Тинькофф Кредитные Системы» Банк	Определяет требования к процессу разработки программного обеспечения в ТКС Банк с учетом требований информационной безопасности, в том числе при планировании, написании исходного кода, тестировании безопасности, анализе исходного кода, выпуске и поддержке.
20.	Положение по хранению и передаче данных платежных карт в «Тинькофф Кредитные Системы» Банк	Определяет требования к обеспечению информационной безопасности при хранении и уничтожении данных платежных карт на бумажных и электронных носителях в ТКС Банк.
21.	Положение по управлению уязвимостями в «Тинькофф Кредитные Системы» Банк	Определяет общий подход к процессу выявления новых уязвимостей, а также по управлению уязвимостями.
22.	Положение по управлению изменениями в «Тинькофф Кредитные Системы» Банк	Определяет требования по обновлению безопасности и изменениям в конфигурации системных компонентов АБС.
23.	Положение по предоставлению удаленного доступа в «Тинькофф Кредитные Системы» Банк	Определяет требования по предоставлению удаленного доступа к АБС.
24.	Положение по оценке защищенности общедоступных веб-приложений в «Тинькофф Кредитные Системы» Банк	Определяет общий подход к процессу оценки защищенности веб-приложений, доступ к которым обычно осуществляется через веб-браузер или веб-службы.
25.	Политика мониторинга и управления инцидентами	Определяет требования к осуществлению мониторинга и управления инцидентами ИБ в

	информационной безопасности в «Тинькофф Кредитные Системы» Банк	ТКС Банк.
26.	Перечень файлов, подлежащих контролю целостности в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество)	Содержит перечень конфигурационных, системных и исполняемых файлов операционных систем и систем управления базами данных, для которых должен выполняться периодический контроль целостности.
27.	Инструкция по управлению ключами при использовании Oracle TDE в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество)	Определяет порядок иифрования данных платежных карт
28.	Процедура синхронизации времени в «Тинькофф Кредитные Системы» Банк (закрытое акционерное общество)	Определяет требования к синхронизации времени