|  |
| --- |
|  |
| **Политика информационной безопасности**  Банка ПАО Сбер |
|  |
| г. Москва  2023 г. |

# СОДЕРЖАНИЕ

1. [ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ](#_TOC_250009)
2. [ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ](#_TOC_250008)
3. [ОБЛАСТЬ ПРИМЕНЕНИЯ](#_TOC_250007)
4. [НОРМАТИВНЫЕ ССЫЛКИ](#_TOC_250006)
5. [ОБЩИЕ ПОЛОЖЕНИЯ](#_TOC_250005)
6. [ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ](#_TOC_250004)
7. [ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ](#_TOC_250003)
8. [РЕАЛИЗАЦИЯ](#_TOC_250002)
9. [КОНТРОЛЬ](#_TOC_250001)
10. [СОВЕРШЕНСТВОВАНИЕ](#_TOC_250000)

# ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

В настоящем документе использованы следующие сокращения:

|  |  |  |
| --- | --- | --- |
| **ИБ** | - | Информационная безопасность |
| **ИС** | - | Информационная система |
| **СУИБ** | - | Система управления информационной безопасностью |

# ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Термины и определения, используемые в настоящей Политике и рекомендуемые к использованию в нормативных и организационно- распорядительных документах, созданных на ее основе, приведены в Приложении № 1 «Термины и определения».

# ОБЛАСТЬ ПРИМЕНЕНИЯ

* 1. Настоящая Политика информационной безопасности (далее – «Политика») предназначена для установления единых норм, правил и требований к системе управления информационной безопасностью Банка ПАО Сбер.
  2. Система обеспечения ИБ представляет собой совокупность правил, требований и руководящих принципов в области ИБ, которыми руководствуется Банк в своей деятельности.
  3. Система управления ИБ является составной частью общей системы управления Сбер, обеспечивает поддержку и управление процессами обеспечения ИБ на всех этапах деятельности корпоративной информационной системы.
  4. Банк разрабатывает и внедряет систему управления ИБ, отвечающую требованиям и рекомендациям нормативных документов Российской Федерации.
  5. Основные цели внедрения системы управления ИБ Банка Сбер:

– обеспечить конфиденциальность своей информации, предотвращая несанкционированный доступ и разглашение чувствительных данных.

– обеспечить целостность данных, предотвращая их несанкционированное изменение или повреждение.

– гарантировать доступность информации для легитимных пользователей, предотвращая атаки на отказ в обслуживании (DDoS) и другие события, которые могут привести к недоступности данных.

– помочь организации соблюдать законодательные и регуляторные требования, связанные с информационной безопасностью. Это может включать в себя соблюдение законов о защите данных (например, GDPR, HIPAA), стандартов (например, ISO 27001) и других нормативных актов.

– разработать стратегии и меры для выявления, предотвращения и митигации угроз информационной безопасности, таких как вирусы, вредоносные программы, фишинг и другие атаки.

– обучить персонал основам информационной безопасности и о том, как соблюдать меры безопасности в повседневной работе.

– использовать систему для оценки и управления рисками информационной безопасности. Это включает в себя идентификацию рисков, их приоритизацию и внедрение мер для уменьшения рисков до приемлемого уровня.

– проводить процедуры для управления инцидентами информационной безопасности, что позволяет быстро реагировать на угрозы и восстанавливать работоспособность системы после инцидентов.

– произвести оптимизацию использование ресурсов (включая финансовые, человеческие и технические ресурсы), сосредотачивая их на ключевых областях защиты информации.

* 1. Положения настоящей Политики распространяются на все виды информации в Сбер, хранящейся либо передающейся любыми способами, в том числе информацию, зафиксированную на материальных носителях.
  2. Положения настоящей Политики также распространяются на средства приема, обработки, передачи, хранения и защиты информации Организации.
  3. Политика применяется ко всем сотрудникам Сбер.
  4. Область применения настоящей Политики распространяется на все подразделения Сбер, в которых обрабатывается информация, не составляющая государственную тайну.

# НОРМАТИВНЫЕ ССЫЛКИ

При разработке настоящей Политики учтены требования и рекомендации следующих документов:

- Федерального закона «О банках и банковской деятельности» от 02.12.1990 №395-1;

- Федерального закона «Об информации, информационных технологиях и о защите информации» от 27.07.2006 №149-ФЗ;

- Федерального закона «О коммерческой тайне» от 29.07.2004 г. №98-ФЗ;

- Федерального закона «О персональных данных» от 27.07.2006 г. №152-ФЗ;

- Федерального закона «О национальной платежной системе» от 27.06.2011г. №161-ФЗ;

- Постановления Правительства РФ от 01.11.2012 г. №1119 об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных;

- Постановления Правительства РФ «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» от 15.09.2008 г. №687;

- Положения Банка России от 09.06.2012 г. №382-П «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»;

- Положения Банка России от 17.04.2019 г. №683-П «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»;

- Положения Банка России от 09.01.2019 г. №672-П «О требованиях к защите информации в платежной системе Банка России»;

- Национальные стандарты РФ ГОСТ Р 57580.1-2017 и ГОСТ Р 57580.2-2018;

- Стандарты Банка России.

# ОБЩИЕ ПОЛОЖЕНИЯ

* + 1. Для защиты ресурсов своей корпоративной информационной системы и связанных с нею существенных данных от случайного или несанкционированного изменения, раскрытия или уничтожения, а также для обеспечения конфиденциальности, целостности и доступности информации и средств еѐ обработки, банк применяет меры по организационной безопасности и физической защите, технические меры безопасности, в том числе контроль доступа, криптографические технологии и другие технологии защиты информации. При этом мероприятия по охране и защите являются достаточными, законными и отвечают требованиям банка в части законности деловых операций и соблюдения деловой этики. Настоящая Политика соответствует законодательству Российской Федерации, руководящим документам ФСБ и ФСТЭК России, внутренним документам в области безопасности.
    2. Любое лицо, работающее на Банке, обязано поддерживать конфиденциальность и целостность деловой информации Сбер и защищать эту информацию от несанкционированного, незаконного или случайного раскрытия, искажения или уничтожения.
    3. Защита информационных ресурсов Банка является обязанностью всех работников Сбер. Лица, работающие в Сбере, несут персональную ответственность за выполнение внутренних требований и правил информационной безопасности.

# ПОЛОЖЕНИЯ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

* + 1. Положения по информационной безопасности Банка ПАО Сбер (далее – «Положения») разрабатываются на основании Политики информационной безопасности Банка в целях создания, развития и совершенствования общей системы защиты информации Банка.
    2. Положения по ИБ являются приложениями к настоящей Политике.

6.3. Правила доступа к информационным ресурсам Сбер определены в «Положении о доступе к информационным ресурсам».

6.4. Правила использования паролей определены в «Положении об использовании паролей».

6.5. Программное обеспечение в Сбер используется в соответствии с «Положением об использовании программного обеспечения».

6.6. Правила пользования ресурсами сети Сбера указаны в «Положении об использовании сети интернет».

6.7. Правила пользования электронной почтой Сбера указаны в «Положении об использовании электронной почты».

6.8. Правила защиты от вредоносных программ определены в «Положении о защите от вредоносного программного обеспечения».

6.9. Правила использования средств беспроводного доступа приведены в «Положении об использовании средств беспроводного доступа».

6.10. Правила и порядок организации рабочих мест определены в «Положении об организации рабочих мест».

6.11. Общие правила технического обслуживания элементов информационных систем указаны в «Положении о техническом обслуживании»

6.12. Правила классификации информационных ресурсов Сбера в целях обеспечения соответствующего уровня их защиты определены в «Положении о классификации информации».

6.13. Инвентаризация информационных систем Сбера проводится в соответствии с «Положением об инвентаризации информационных ресурсов и систем».

6.15. Перечень ролей информационной безопасности и правила управления ролями ИБ приведены в «Положении об управлении ролями информационной безопасности».

6.16. Мониторинг информационной безопасности в Сбере выполняется в соответствии с «Положением о мониторинге событий информационной безопасности».

# ЗАДАЧИ СИСТЕМЫ УПРАВЛЕНИЯ ИБ

* 1. Основной целью управления ИБ является защита информации Банка и обеспечение стабильной и эффективной работы всего информационно-вычислительного комплекса Банка при осуществлении деятельности, указанной в Уставе, достижение адекватных мер при защите от реальных угроз ИБ, предотвращение и/или снижение ущерба от инцидентов ИБ.
  2. Основными задачами управления ИБ являются:

– разработка требований по обеспечению ИБ;

− контроль выполнения установленных требований по обеспечению ИБ; − повышение эффективности мероприятий по обеспечению и поддержанию ИБ;

− разработка и совершенствование нормативно-правовой базы обеспечения ИБ;

− выявление, оценка и прогнозирование угроз ИБ;

− организация антивирусной защиты информационных активов;

− защита информации от НСД и утечки по техническим каналам

– бесконтрольного выхода конфиденциальной информации за пределы Банка или круга лиц, которым она была доверена.

* 1. В основе управления ИБ Банка лежит подход, отраженный в модели деятельности в виде циклического процесса «планирование – реализация – контроль – совершенствование» (по ГОСТ Р ИСО/МЭК 27001-2021).
  2. Банк Сбер осуществляет деятельность по управлению рисками, повышению осведомленности сотрудников и реагированию на инциденты в области ИБ. Регулярно, не реже одного раза в два года, производится анализ состояния рисков, связанных с ИБ. Защитные меры должны основываться на всесторонней оценке этих рисков и должны быть им соразмерны.
  3. Всю ответственность за защиту своей информации и информационных ресурсов Банка ПАО Сбер возлагается на руководители структурных подразделений Банка. Сотрудники Сбера обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией Банка, соблюдать требования настоящей Политики ИБ и других документов СОИБ.

# РЕАЛИЗАЦИЯ

Реализация системы управления ИБ осуществляется на основе четкого распределения ролей и ответственности в области информационной безопасности.

# Структура и ответственность

* + 1. Ответственное лицо, назначенное приказом Президента председателя правления Сбера, руководит работами по внедрению и совершенствованию СУИБ, в том числе организует выполнение Положений по ИБ.

# 8.1.2. Руководство всеми видами деятельности по управлению ИБ в структурных подразделениях Банка осуществляют руководители этих

# подразделений. Они же несут ответственность за выполнение обязательств Положений по ИБ.

# 8.1.3. Функции администраторов по ИБ возлагаются на штатных работников подразделений Банка, которые осуществляет свою деятельность во взаимодействии с другими подразделениями Сбера. Координацию их деятельности по защите информации осуществляет ответственное лицо, назначенное президентом председателем правления Сбера.

# 8.1.4. Ответственность работников Сбера за надлежащее выполнение требований и правил ИБ определена в положениях, правилах, регламентах и другие внутренних нормативных и организационно распорядительных документах Банка.

# Осведомленность и информирование

# 8.2.1. Для обеспечения эффективного функционирования СУИБ первостепенное значение имеет осведомленность работников Сбера по вопросам информационной безопасности.

# 8.2.2. Перед началом работы в информационных системах работники Сбера получают у своего руководителя и знакомятся с «Инструкцией пользователя информационных систем Банка ПАО Сбер».

# 8.2.3. Доведение правил ИБ до персонала всех уровней проводится: при приеме на работу; в ходе производственных совещаний, собраний, профессиональной подготовки персонала, тренингов по информационной безопасности.

# 8.3. Реагирование на инциденты безопасности

* + 1. Для определения возможных сценариев восстановления информационной системы Организации в чрезвычайных ситуациях, конкретизации технических средств и действий работников и структурных подразделений по локализации инцидентов ИБ должны быть разработаны планы восстановительных работ для важных информационных ресурсов.
    2. Реагирование на инциденты ИБ осуществляется в соответствии с «Положением о реагировании на инциденты информационной безопасности» (Приложение № 2).

# КОНТРОЛЬ

# 9.1. Контроль соблюдения требований настоящей Политики возлагается на ответственное лицо, назначенное приказом президента председателя правления Сбера.

# 9.2. Контроль за актуальностью Политики осуществляет ответственное лицо, назначенное приказом президента председателя правления Сбера.

# 9.3. Контроль в области информационной безопасности является частью работ по обеспечению ИБ Сбера. Целью контроля ИБ является выявление угроз, предотвращение их реализации, минимизация возможного ущерба.

# 9.4. Объектами контроля ИБ являются информационные ресурсы Сбера (информация, работники, системы и средства информационных технологий).

# СОВЕРШЕНСТВОВАНИЕ

# 10.1. Для совершенствования системы управления ИБ в Банке ПАО Сбер выполняется систематический анализ и оценивание действующей ситуации в области информационной безопасности.

# 10.2. Анализ ИБ осуществляется на основе данных мониторинга в соответствии с «Положением о мониторинге событий ИБ».

# 10.3. В ситуациях, требующих оперативного реагирования, работа ведется согласно «Положению о реагировании на инциденты ИБ».

# 10.4. Нормативные и организационно-распорядительные документы по информационной безопасности разрабатываются в строгом соответствии с Концепцией и Политикой информационной безопасности Института.

# 10.5 Нормативные и организационно-распорядительные документы по информационной безопасности утверждаются приказами по Сберу и рассылаются членам правления Сбера и руководителям подразделений

# Банк ПАО Сбер будет применять следующий системный подход к обеспечению исполнения требований и правил по информационной безопасности:

# 10.6.1. Настоящая Политика информационной безопасности Банка ПАО Сбер считается официально принятым документом после его утверждения приказом президента председателя правления Сбера.

# 10.6.2. Разработка и внедрение нормативных и организационно распорядительных документов по информационной безопасности проводится поэтапно.

# 10.6.3. Все нормативные и организационно-распорядительные документы по информационной безопасности могут быть приняты, отменены и пересмотрены отдельными приказами по Сберу, а также уточнены и дополнены распоряжениями по отдельному структурному подразделению.