Приложение № 2 к Политике информационной безопасности ПАО Сбер

# ПОЛОЖЕНИЕ

**О РЕАГИРОВАНИИ НА ИНЦИДЕНТЫ ИБ**

# Назначение и область действия

# Настоящее Положение о порядке выявления и реагирования на инциденты информационной безопасности (далее - Положение) устанавливает порядок управления инцидентами (одним событием или группой событий), способными привести к сбоям или нарушению функционирования информационной системы персональных данных Банка ПАО Сбер и (или) возникновению угроз безопасности конфиденциальной информации Банка (далее - инциденты ИБ), а также регулирует порядок проведения служебного расследования нарушений режима служебной тайны (далее - служебное расследование) в Банке.

# Настоящее Положение распространяется на сотрудников Банка.

# Процесс управления инцидентами ИБ включает:

# − учет и регистрацию инцидентов ИБ;

# − оповещение ответственного лица о возникновении инцидентов ИБ;

# − расследование обнаруженных инцидентов ИБ;

# − устранение причин и последствий инцидентов ИБ;

# − определение плана корректирующих и превентивных мероприятий.

# 1.4. Требования настоящего Положения являются обязательными для выполнения всеми сотрудниками Банка.

# Основные требования

* 1. Для выявления инцидентов ИБ должны использоваться встроенные механизмы регистрации и учета событий безопасности операционных систем, систем управления базами данных, прикладного программного обеспечения и средств защиты информации, а также специализированные средства анализа защищенности информационных систем Банка.
  2. В обязательном порядке должны регистрироваться следующие события безопасности:

**−** попытки входа (выхода) пользователей в операционную систему (из операционной системы);

**−** загрузка и инициализация операционной системы рабочих станций и серверов;

**−** попытка доступа к средствам виртуализации;

**−** факт изменения конфигурации средств виртуализации;

**-** запуск и остановка служб (системных сервисов) средств виртуализации;

**-** попытки подключения к рабочим станциям и серверам мобильных устройств и внешних носителей информации.

* 1. В параметрах регистрации событий безопасности в обязательном порядке должны указываться следующие параметры:

**−** тип события;

**−** дата и время события;

**−** результат события;

**−** источник события;

**-** идентификатор пользователя информационной системы, предъявленный при попытке доступа.

* 1. Хранение информации об инцидентах ИБ должно осуществляться в течение срока, достаточного для проведения служебного расследования.
  2. Учет инцидентов ИБ осуществляется работниками службы по противодействию угроз информационной безопасности, назначенными приказом Банка. Допускается ведение учета инцидентов ИБ как в бумажном виде, так и в электронном виде.
  3. При обнаружении инцидента ИБ администратор информационной безопасности проводит его классификацию в соответствии с Приложением к настоящему Положению. Инциденты ИБ и их последствия классифицируются по значимости на текущие, значимые и имеющие признаки преступления.

# Роли и ответственность

* 1. Ответственность за проведение служебного расследования и за контроль своевременного и качественного выполнения работ по проведению корректирующих и превентивных мероприятий несет ответственный по защите информации.
  2. Ответственность за обеспечение своевременной регистрации инцидентов ИБ несет руководитель службы по противодействию угроз информационной безопасности.