

**Сведения о реализуемых АО БАНК «СНГБ» требованиях к защите
персональных данных согласно Федерального закона
от 27.07.2006 № 152-ФЗ «О персональных данных»**

АО БАНК «СНГБ» для обеспечения безопасности персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных, принимаются следующие меры:

- назначение ответственного за организацию обработки персональных данных;
- утверждение документов по вопросам обработки персональных данных: положения о сведениях ограниченного распространения, политики обработки персональных данных, положения о порядке обработки персональных данных, осуществляемой без использования средств автоматизации, положения по уничтожению персональных данных;
- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных Федеральному закону от 27.07.2006 № 152-ФЗ «О персональных данных» и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политике обработки персональных данных, локальным нормативным актам АО БАНК «СНГБ»;
- управление операционными и правовыми рисками в сфере обработки персональных данных;
- ознакомление работников АО БАНК «СНГБ», непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе с требованиями к защите персональных данных, политикой обработки персональных данных, локальными нормативными актами АО БАНК «СНГБ» по вопросам обработки персональных данных, и (или) обучение указанных работников;
- определение угроз безопасности персональных данных при их обработке в информационных системах персональных данных АО БАНК «СНГБ»;
- применение организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах Банка, включая криптографическую защиту персональных данных и их обезличивание (псевдонимизацию);
- применение организационных и технических мер по обеспечению конфиденциальности, целостности, доступности информационных систем АО БАНК «СНГБ», обеспечивающих обработку персональных данных;
- применение прошедших в установленном порядке процедур оценки соответствия средств защиты информации;
- проведение оценки эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных АО БАНК «СНГБ»;
- осуществление учета материальных носителей персональных данных;
- выявление фактов несанкционированного доступа к персональным данным и принятие соответствующих мер, в том числе восстановление персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним, природного или технического инцидента;
- установление правил доступа к персональным данным, в том числе обрабатываемым в информационной системе персональных данных АО БАНК «СНГБ», а также обеспечение регистрации и учета всех действий, совершаемых с персональными данными в информационной системе персональных данных АО БАНК «СНГБ»;
- осуществление контроля за принимаемыми мерами по обеспечению безопасности персональных данных и уровня защищенности информационных систем персональных данных АО БАНК «СНГБ» и совершенствование указанных мер;

- осуществление поэкземплярного учета используемых средств криптографической защиты информации, а также учета средств защиты информации от несанкционированного доступа в электронном журнале;
- повышение осведомленности/компетентности работников АО БАНК «СНГБ», контроля знаний и соблюдения требований информационной безопасности;
- классификация информационных систем персональных данных АО БАНК «СНГБ» по уровню защищенности;
- осуществление хранения материальных носителей персональных данных с соблюдением условий, обеспечивающих сохранность персональных данных и исключающих несанкционированный доступ к ним.

АО БАНК «СНГБ» применяются следующие технические меры по защите персональных данных от несанкционированного доступа и неправомерных действий (средства обеспечения безопасности):

- используются аппаратные, программные и программно-аппаратные средства защиты, выполняющие (самостоятельно или в комплексе с другими средствами) функции системы защиты персональных данных;
- используются как наложенные, так и встроенные в операционные системы защиты от несанкционированного доступа;
- обеспечивается защита от несанкционированного доступа к серверам, автоматизированным рабочим местам пользователей и прикладных сервисов;
- обеспечивается регистрация событий информационной безопасности в журналах средств защиты информации, системного и прикладного программного обеспечения, регистрация входа (выхода) пользователей в систему (из системы), регистрация загрузки и инициализации операционной системы и ее программного останова;
- обеспечивается целостность посредством использования средств операционных систем и средств мониторинга событий информационной безопасности;
- проводится анализ защищенности, который реализован на основе использования средств выявления уязвимостей (сканер безопасности) и контроля настроек безопасности (аудит);
- обеспечивается безопасное межсетевое взаимодействие. Подключения к сетям общего доступа контролируются средствами межсетевого экрана. Разграничение доступа к ресурсам информационных систем персональных данных при межсетевом взаимодействии реализовано программно-аппаратными межсетевыми экранами;
- обеспечивается обнаружение вторжений для информационных систем персональных данных, подключенных к сетям общего пользования. Применяются системы обнаружения вторжений, использующие наряду с сигнатурными методами анализа методы выявления аномалий;
- используются комплексы антивирусных средств, устанавливаемых на серверы и рабочие станции и обеспечивающих централизованное управление функционированием средств антивирусной защиты с рабочего места администратора безопасности, автоматизированное обновление сигнатур, защиту от вредоносного программного обеспечения, распространяющегося по сети или через подключаемые носители, обнаружение и удаление вирусов;
- обеспечивается защита открытых каналов связи при помощи их шифрования, а также при помощи шифрования передаваемых данных (как встроенными средствами, так и наложенными);
- используются решения для защиты данных, предотвращения утечек и контроля перемещения конфиденциальной информации за пределы АО БАНК «СНГБ», а также защиты АО БАНК «СНГБ» от внутренних угроз.