Генеральному директору ООО “Группа компаний Синет”

Томскому Арсену Григорьевичу

от начальника отдела по разработке ПО

Муксунова Афанасия Сергеевича

05.12.2019 №1

г. Якутск

Служебная записка

Довожу до вашего сведения, что мне поручили внедрить программное средство (приложение) для удаленного доступа к возможностям банка.

Условия политики безопасности использования ПО

Политика информационной безопасности (далее - Политика) ООО «Группа компаний Синет» определяет высокоуровневые цели и задачи обеспечения информационной безопасности (далее — ИБ) настольного приложения для ПАО “Деньги в каждый карман” включая способы контроля реализации требований политики ИБ, а также определяет содержание, назначение и требования к деятельности по обеспечению ИБ.

* 1. Настоящая Политика разработана на основе:
  + накопленного в Банке опыта в области обеспечения ИБ;
  + результатов идентификации активов, подлежащих защите;
  + результатов оценки рисков, с учетом особенностей бизнеса и технологий;
  + требований законодательства Российской Федерации;
  + нормативных актов Банка России;
  + интересов и бизнес целей Банка.
  1. Политика учитывает современное состояние и ближайшие перспективы развития информационных технологий в Банке, цели, задачи и правовые основы их эксплуатации, режимы функционирования, а также содержит анализ угроз безопасности для объектов и субъектов информационных отношений Банка.
  2. Области действия настоящей Политики:
  + основные положения и требования настоящей Политики распространяются на все структурные подразделения Банка, включая филиалы и дополнительные офисы. Основные вопросы Политики также распространяются на другие организации и учреждения, взаимодействующие с Банком в качестве поставщиков и потребителей информационных ресурсов Банка в том или ином качестве.
  1. Настоящая Политика является методологической основой для:
  + формирования и проведения единой политики в области обеспечения безопасности информации в Банке;
  + принятия управленческих решений и разработки практических мер по воплощению политики безопасности информации и выработки комплекса согласованных мер, направленных на выявление, отражение и ликвидацию последствий реализации различных видов угроз безопасности информации;
  + координации деятельности структурных подразделений Банка при проведении работ по созданию, развитию и эксплуатации информационных технологий с соблюдением требований по обеспечению безопасности информации;
  + разработки предложений по совершенствованию правового, нормативного, технического и организационного обеспечения безопасности информации в Банке.
  1. Все владельцы информационных систем, обрабатывающих защищаемые информационные активы Банка обязаны обеспечить их защиту в соответствии с требованиями данного документа.
  2. В рамках реализации деятельности по обеспечению информационной безопасности в Банке осуществляется анализ инцидентов информационной безопасности, включающий:
     + сбор информации о событиях информационной безопасности;
     + выявление и анализ инцидентов информационной безопасности;
     + расследование инцидентов информационной безопасности;
     + оперативное реагирование на инцидент информационной безопасности;
     + минимизация негативных последствий инцидентов информационной безопасности;
     + оперативное доведение до руководства Банка информации по наиболее значимым инцидентам информационной безопасности и оперативное принятие решений по ним, включая регламентирование порядка реагирования на инциденты информационной безопасности;
     + выполнение принятых решений по всем инцидентам информационной безопасности в установленные сроки;
     + пересмотр применяемых требований, мер и механизмов по обеспечению информационной безопасности по результатам рассмотрения инцидентов информационной безопасности;
     + повышение уровня знаний персонала Банка в вопросах обеспечения информационной безопасности;
     + обеспечение регламентации и управления доступом к программным и программно-техническим средствам и сервисам автоматизированных систем Банка и информации, обрабатываемой в них;
     + применение средств криптографической защиты информации;
     + обеспечение бесперебойной работы автоматизированных систем и сетей связи;
     + обеспечение возобновления работы автоматизированных систем и сетей связи после прерываний и нештатных ситуаций;
     + применение средств защиты от вредоносных программ;
     + обеспечение информационной безопасности на стадиях жизненного цикла автоматизированных систем Банка, связанных с проектированием, разработкой, приобретением, поставкой, вводом в действие, сопровождением (сервисным обслуживанием);
     + обеспечение информационной безопасности при использовании доступа в сеть Интернет и услуг электронной почты;
     + контроль доступа в здания и помещения Банка.
  3. В целях совершенствования деятельности по обеспечению информационной безопасности в Банке осуществляется периодическое, а при необходимости оперативное, уточнение/пересмотр целей и задач обеспечения информационной безопасности (при изменениях целей и задач основной деятельности Банка).
  4. Соблюдение настоящей Политики является элементом корпоративной этики, в связи с чем на уровень ИБ Банка серьезное влияние оказывают отношения, как в коллективе, так и между коллективом и Руководством Банка. Понимая, что наиболее критичным элементом безопасности Банка является ее персонал, Руководство Банка поощряет заинтересованность и осведомленность персонала в решении проблем ИБ.
  5. Руководство Банка намерено обеспечить надлежащую защиту информационных активов Банка и настоятельно требует от всех должностных лиц и сотрудников четкого соблюдения норм и правил, установленных в настоящей Политике и Частных политиках ИБ;
  6. Руководство Банка проводит совещания, посвященные проблемам обеспечения информационной безопасности с целью формирования четких указаний по этому вопросу, осуществления контроля их выполнения, а также оказания административной поддержки инициативам по обеспечению ИБ.