УТВЕРЖДЕНО:
Решением Совета Директоров
ЗАО АКБ «ЦентроКредит»
(протокол № 43/13
от 21 октября 2013 г.)

ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЗАО АКБ «ЦЕНТРОКРЕДИТ»

г. Москва

ЛИСТ СОГЛАСОВАНИЯ

№ п/п	Должность	ФИО	Подпись
1	Начальник Правового Управления	Музыка А.Ч.	
2	Начальник Управления автоматизации	Авилкин И.А.	
3	Начальник Отдела сетевой и информационной безопасности	Шапцов В.Э.	
4	ВРИО Руководителя Службы внутреннего контроля	Стриганина О.С.	

© 2013 ЗАО АКБ “ЦетроКредит”

ОГЛАВЛЕНИЕ

© 2013 ЗАО АКБ “ЦетроКредит”

1. ОБЩИЕ ПОЛОЖЕНИЯ

1.1 Политика информационной безопасности ЗАО АКБ «ЦентроКредит» (далее – Политика) разработана в соответствии с законодательством Российской Федерации и нормами права в части обеспечения ИБ, требованиями нормативных актов Центрального банка Российской Федерации, федерального органа исполнительной власти, уполномоченного в области безопасности, федерального органа исполнительной власти, уполномоченного в области противодействия техническим разведкам и технической защиты информации, и основывается на Стандарте Банка России СТО БР ИББС–1.0–2010 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения» и Рекомендаций в области стандартизации Банка России "Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Методические рекомендации по документации в области обеспечения информационной безопасности в соответствии с требованиями СТО БР ИББС-1.0" (РС БР ИББС-2.0-2007).

1.2 Политика является высокоуровневым документом, определяющим общие цели и задачи обеспечения ИБ в Банке, включая способы контроля реализации требований Политики. Политика определяет содержание, назначение и требования к деятельности по обеспечению ИБ Банка.

1.3 Политика является доступным для работников и клиентов Банка документом, и представляет собой официально принятую руководством Банка позицию по отношению к проблемам обеспечения информационной безопасности Банка, построения СМИБ. Политика обязательная для применения всеми работниками и руководством Банка, а также пользователями информационных ресурсов Банка.

1.4 Руководство Банка осознает важность совершенствования мер и средств обеспечения ИБ в контексте развития законодательства и норм регулирования банковской деятельности, а также развития реализуемых банковских технологий и ожиданий клиентов Банка и других заинтересованных сторон. Соблюдение требований ИБ позволит создать конкурентные преимущества Банку, обеспечить его финансовую стабильность, рентабельность, соответствие правовым, регулятивным и договорным требованиям и повышение имиджа.

1.5 Банк является собственником документов, массивов документов, информационных систем, технологий и средств их обеспечения, которые созданы, произведены за счет его средств, приобретены им на законных основаниях, получены в порядке дарения, наследования или иным законным способом.

1.6 Банк, как собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения в полном объеме реализует полномочия владения, пользования, распоряжения указанными объектами и определяет условия использования этой продукции.

1.7 Банк, как собственник информации, составляющей коммерческую тайну Банка, имеет право передавать и продавать ее другим юридическим и физическим лицам в качестве товара при условии, что данная сделка не противоречит обязательствам Банка, не ущемляет права и не наносит вред самому Банку, его работникам, клиентам или корреспондентам.

1.8 При функционировании Банка существуют реальные угрозы несанкционированного получения и использования информации, являющейся собственностью Банка, в результате чего может быть нанесен ощутимый материальный, моральный или другой ущерб Банку, его клиентам и корреспондентам.

1.9 Для предотвращения реализации угроз и их последствий документированная информация, информационные системы, технологии и средства их обеспечения подлежат защите.

© 2013 ЗАО АКБ “ЦетроКредит”

1.10 Частные политики, детализирующие положения настоящей Политики применительно к различным областям информационной безопасности, оформляются в виде отдельных внутренних нормативных документов Банка.

© 2013 ЗАО АКБ “ЦетроКредит”

2. ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Автоматизированная банковская система – автоматизированная система, реализующая технологию выполнения функций Банка.

Актив - все, что имеет ценность для Банка и находится в её распоряжении.

Аудит информационной безопасности Банка – периодический, независимый и документированный процесс получения свидетельств аудита и объективной их оценки с целью установления степени выполнения Банком установленных требований по обеспечению информационной безопасности.

Банк – ЗАО АКБ «ЦентроКредит».

Банковский технологический процесс – технологический процесс, реализующий операции по изменению и (или) определению состояния активов Банка, используемых при функционировании или необходимых для реализации банковских услуг.

Банковский информационный технологический процесс – часть банковского технологического процесса, реализующая операции по изменению и (или) определению состояния информационных активов, необходимых для функционирования Банка и не являющихся платежной информацией.

Банковский платежный технологический процесс – часть банковского технологического процесса, реализующая банковские операции над информационными активами Банка, связанные с перемещением денежных средств с одного счета на другой и (или) контролем данных операций.

Информация – сведения (сообщения, данные) независимо от формы их представления.

Информационный актив – информация с реквизитами, позволяющими ее идентифицировать; имеющая ценность для Банка.

Информационная система персональных данных – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств.

Информационная безопасность Банка – состояние защищенности интересов (целей) Банка в условиях угроз в информационной сфере.

Инцидент информационной безопасности – событие, указывающее на свершившуюся, предпринимаемую или вероятную реализацию угрозы ИБ.

Классификация информационных активов – разделение существующих информационных активов Банка по типам, выполняемое в соответствии со степенью тяжести последствий от потери их значимых свойств ИБ.

Мониторинг информационной безопасности Банка (мониторинг ИБ) – постоянное наблюдение за событиями мониторинга ИБ, сбор, анализ и обобщение результатов наблюдения.

© 2013 ЗАО АКБ “ЦетроКредит”

Политика информационной безопасности – документация, определяющая высокоуровневые цели, содержание и основные направления деятельности по обеспечению ИБ в Банке.

Персональные данные – любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).

Риск – мера, учитывающая вероятность реализации угрозы и величину потерь (ущерба) от реализации этой угрозы.

Риск нарушения информационной безопасности (риск нарушения ИБ) – Риск, связанный с угрозой ИБ.

Самооценка информационной безопасности Банка – систематический и документированный процесс получения свидетельств самооценки в деятельности Банка по обеспечению информационной безопасности и установления степени выполнения в Банке установленных критериев самооценки информационной безопасности.

Система информационной безопасности – совокупность защитных мер, защитных средств и процессов их эксплуатации, включая ресурсное и административное (организационное) обеспечение.

Система менеджмента информационной безопасности – часть менеджмента Банка, предназначенная для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и совершенствования системы обеспечения ИБ.

Система обеспечения информационной безопасности – совокупность СИБ и СМИБ Банка.

Ущерб – утрата активов, повреждение (утрата свойств) активов и (или) инфраструктуры Банка или другой вред активам и (или) инфраструктуре Банка, наступивший в результате реализации угроз ИБ через уязвимости ИБ.

Угроза – опасность, предполагающая возможность потерь (ущерба).

Угроза информационной безопасности (угроза ИБ) – угроза нарушения свойств ИБ — доступности, целостности или конфиденциальности информационных активов Банка.

© 2013 ЗАО АКБ “ЦетроКредит”

3. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

АБС — автоматизированная банковская система;

ИБ — информационная безопасность;

ИСПДн — информационная система персональных данных;

НСД — несанкционированный доступ;

НРД — нерегламентированные действия в рамках предоставленных полномочий;

ПДн — персональные данные;

РФ — Российская Федерация;

СМИБ — система менеджмента информационной безопасности;

СИБ — система информационной безопасности;

СОИБ — система обеспечения информационной безопасности;

ФСБ — Федеральная служба безопасности;

ФСТЭК — Федеральная служба по техническому и экспортному контролю;

ЭВМ — электронная вычислительная машина.

© 2013 ЗАО АКБ “ЦетроКредит”

4. ИСХОДНАЯ КОНЦЕПТУАЛЬНАЯ СХЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

4.1 Концептуальная схема информационной безопасности 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 и обеспечение нормального функционирования технологических процессов.

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 Для противодействия угрозам ИБ в Банке на основе имеющегося опыта составляется прогностическая модель предполагаемых угроз и модель нарушителя. Чем точнее сделан прогноз (составлены модель угроз и модель нарушителя), тем ниже риски нарушения ИБ в Банке при минимальных ресурсных затратах.

4.4 Разработанная на основе прогноза политика ИБ и в соответствии с ней построенная система обеспечения ИБ является наиболее правильным и эффективным способом добиться минимизации рисков нарушения ИБ для Банка. Банком периодически на основании данных мониторинга и аудита, обновляются модели угроз и нарушителя.

4.5 Соблюдение политики ИБ в значительной степени является элементом корпоративной этики, поэтому в Банке серьезное внимание уделяется вопросам управления отношениями, как в коллективе, так и между коллективом и собственником или руководством Банка, представляющим интересы собственника.

4.6 В ЗАО АКБ «ЦентроКредит» за обеспечение ИБ отвечает структурное подразделение, в функциональные обязанности которого входит реализация выработанной Руководством и собственниками политики ИБ, координация процессов по управлению ИБ, выявление и предотвращение инцидентов ИБ.

4.7 Работники Банка соблюдают требования действующего законодательства РФ и внутренних документов Банка по ИБ, а также информируют своих непосредственных руководителей обо всех событиях, связанных с нарушениями (могущими повлечь нарушения) ИБ. Руководитель структурного подразделения любого уровня соблюдает требования действующего законодательства РФ и внутренних документов Банка по ИБ, а также обеспечивает контроль за выполнением таких требований сотрудниками своего подразделения.

4.8 Стратегия обеспечения ИБ в Банке заключается как в эффективном использовании по имеющемуся плану заранее разработанных мер по обеспечению ИБ, противостоящих атакам злоумышленников, так и в регулярном пересмотре моделей и политик ИБ, а также корректировке СОИБ.

4.9 Основой для построения СОИБ Банка являются требования законодательства РФ, нормативные акты Банка России, контрактные требования Банка, а также условия ведения бизнеса, выраженные на основе идентификации активов Банка, построения модели нарушителей и угроз.

5. ЦЕЛИ И ЗАДАЧИ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

5.1 Главной целью обеспечения ИБ является обеспечение устойчивого функционирования Банка и защита информационных активов, принадлежащих Банку, его акционерам, инвесторам и клиентам от случайных (ошибочных) и направленных противоправных посягательств, разглашения, утраты, утечки, искажения, модификации и уничтожения охраняемых сведений.

5.2 Основными задачами обеспечения ИБ в Банке являются:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, Банку;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы;
- обеспечение правового режима документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах.

5.3 Организационные, технологические и технические мероприятия по защите информации в Банке проводятся в соответствии с требованиями действующего законодательства, нормативных и иных документов ФСТЭК, ФСБ, Центрального банка Российской Федерации (ЦБ РФ), а также нормативно-методическими материалами и организационно-распорядительными документами Банка по вопросам обеспечения ИБ.

© 2013 ЗАО АКБ “ЦентроКредит”

6. ОБЪЕКТЫ ЗАЩИТЫ

6.1 Основными объектами защиты в Банке являются:

- информационные ресурсы с ограниченным доступом, составляющие коммерческую, банковскую тайну, иные чувствительные по отношению к случайным и несанкционированным воздействиям и нарушению их безопасности информационные ресурсы, в том числе открытая (общедоступная) информация, представленные в виде документов и массивов информации, независимо от формы и вида их представления (носителя);
- информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал банка;
- информационная инфраструктура, включающая системы обработки, хранения и анализа информации, технические и программные средства ее передачи, хранения, обработки и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации.

© 2013 ЗАО АКБ “ЦентроКредит”

7. МОДЕЛИ УГРОЗ И НАРУШИТЕЛЕЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

7.1 Для успешного осуществления мер по обеспечению ИБ Банка необходимо иметь представление о возможных угрозах для него.

7.2 Модели угроз и нарушителей (прогноз ИБ) являются определяющими при развертывании, поддержании и совершенствовании системы обеспечения ИБ Банка.

7.3 Деятельность Банка поддерживается входящей в его состав информационной инфраструктурой, которая обеспечивает реализацию банковских технологий и может быть представлена в виде иерархии следующих основных уровней:

- физического (линии связи, аппаратные средства и пр.);
- сетевого (сетевые аппаратные средства: маршрутизаторы, коммутаторы, концентраторы и пр.);
- сетевых приложений и сервисов;
- операционных систем (ОС);
- систем управления базами данных (СУБД);
- банковских технологических процессов и приложений;
- бизнес-процессов Банка.

7.4 Главной целью злоумышленника является получение контроля над активами на уровне бизнес процессов. Другими целями злоумышленника могут являться, например, нарушение функционирования бизнес-процессов Банка путем нарушения доступности или целостности информационных активов, например, посредством распространения вредоносных программ или нарушения правил эксплуатации ЭВМ или их сетей.

7.5 В качестве основных источников угроз ИБ Банком рассматриваются:

- внешние нарушители ИБ (бывшие сотрудники Банка, представители организаций, взаимодействующих по вопросам технического обеспечения Банка, клиенты Банка, посетители зданий и помещений Банка, конкуренты, террористы и криминальные структуры, хакеры);
- внутренние нарушители ИБ (зарегистрированные пользователи систем Банка, обслуживающий персонал, администраторы, администраторы информационной безопасности и др.);
- комбинированные источники угроз: внешние и внутренние, действующие совместно и/или согласованно (в сговоре);
- сбои, отказы, разрушения/повреждения программных и технических средств;
- зависимость от поставщиков/провайдеров/партнеров/клиентов;
- несоответствие требованиям надзорных и регулирующих органов, действующему законодательству.

7.6 Реализация угроз возможна на различных уровнях информационной инфраструктуры. При этом для внешних нарушителей угрозы на двух верхних уровнях труднореализуемы (однако внешний злоумышленник может иметь сообщника внутри Банка), а вероятность нанесения ущерба внутренним нарушителем тем выше, чем выше уровень инфраструктуры, на котором он действует, чем больше объем ресурсов, к которым он имеет доступ (концентрация информационных ресурсов), и чем выше квалификация работника (в случае преднамеренных действий).

© 2013 ЗАО АКБ “ЦентроКредит”

8. СИСТЕМА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

8.1 Выполнение требований по информационной безопасности является основой для обеспечения должного уровня ИБ.

8.2 Система информационной безопасности Банка формируются для нескольких областей ИБ.

8.3 Обеспечение ИБ при назначении и распределении ролей обеспечения доверия к персоналу:

- при приеме на работу проводится проверка идентичности личности, заявляемой квалификации, точности и полноты биографических фактов, наличия рекомендаций;
- компетенция персонала Банка соответствует выполняемым функциям. Компетентность персонала обеспечивается с помощью процессов обучения в области ИБ, осведомленности персонала и периодической проверкой уровня компетентности;
- весь персонал Банка дает письменное обязательство о соблюдении конфиденциальности, приверженности правилам корпоративной этики, включая требования по недопущению конфликта интересов;
- для внешних организаций требования по ИБ регламентируются положениями, включаемыми в договоры (соглашения).

8.4 Обеспечение ИБ АБС на всех стадиях жизненного цикла:

8.4.1 Требования по обеспечению ИБ в Банке устанавливаются на всех стадиях модели ЖЦ АБС, в том числе:

- приемка и ввод в действие;
- эксплуатация;
- сопровождение и модернизация;
- снятие с эксплуатации.

8.5 Защита от НСД и НРД, управления доступом и регистрацией всех действий в АБС, в телекоммуникационном оборудовании, автоматических телефонных станциях и т.д. обеспечивается посредством:

- предоставления прав доступа к информационным системам на основе действующих ролей, в соответствии с принципом минимально необходимого уровня доступа, т.е. пользователи получают доступ к тем и только тем операциям и данным, которые им необходимы для выполнения своих должностных обязанностей и предусмотрены ролью данного сотрудника;
- предоставление/лишение и изменение прав доступа возможно только после предварительного согласования администратором информационной безопасности, осуществляющим, кроме того, контроль (мониторинг и аудит) правильности устанавливаемых прав доступа.

8.6 Обеспечение ИБ средствами антивирусной защиты;

- на всех АРМ и серверах установлены средства антивирусной защиты. Версии и базы данных средств антивирусной защиты периодически обновляются уполномоченным лицом;

© 2013 ЗАО АКБ “ЦентроКредит”

- в случае обнаружения вируса или другого вредоносного программного обеспечения информация о факте обнаружения доводится до администратора безопасности и принимаются меры по предотвращению его распространения по сети Банка.

8.7 Обеспечение ИБ при использовании ресурсов сети Интернет:

- ресурсы сети Интернет используются для получения и распространения информации, связанной с банковской деятельностью, информационно-аналитической работы в интересах Банка, обмена почтовыми сообщениями исключительно с внешними организациями, а также ведения хозяйственной деятельности Банка. Использование сети Интернет в неустановленных целях запрещается;
- для осуществления безопасного электронного почтового обмена через сеть Интернет применяются защитные меры.

8.8 Обеспечение ИБ при использовании средств криптографической защиты информации:

- конфиденциальная информация хранится в АБС и передается по открытым каналам связи в зашифрованном виде. Используемые алгоритмы шифрования соответствуют российским или международным стандартам;
- при необходимости подтверждения авторства документов, экспортируемых или импортируемых в АБС, используются средства ЭЦП. Для вычисления ЭЦП применяются алгоритмы соответствующие российским или международным стандартам;
- для АБС, в которых применяются средства криптографической защиты информации, документально определяются правила управления ключами, включая процедуры создания, смены, хранения, распространения, использования и уничтожения ключей, а также действия при их компрометации.

8.9 Обеспечение ИБ банковских платежных технологических процессов;

- Банк принимает необходимые организационные и технические меры, для защиты платежной информации.

8.10 Обеспечение ИБ банковских информационных технологических процессов:

- Банк проводит классификацию неплатежной информации и принимает необходимые организационные и технические меры, для ее защиты.

8.11 Обработка персональных данных в Банке:

- Банк при обработке персональных данных принимает необходимые организационные и технические меры, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий.

8.12 Обеспечение ИБ банковских технологических процессов, в рамках которых обрабатываются персональные данные:

© 2013 ЗАО АКБ “ЦентроКредит”

– Банк принимает необходимые организационные и технические меры, для защиты персональных данных в банковских технологических процессах.

8.13 Детализация требований к СИБ оформляется отдельными внутренними документами Банка – частными политиками.

8.14 На основе сформированных требований выбираются меры по обеспечению ИБ Банка.

© 2013 ЗАО АКБ “ЦентроКредит”

9. СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ БАНКА

9.1 Обеспечение ИБ предполагает развертывание, эксплуатацию и совершенствование системы менеджмента ИБ (СМИБ), под которой понимается система скоординированной деятельности по руководству и управлению ИБ в Банке.

9.2 Область применения правил ИБ (область действия СМИБ) к информационным ресурсам определяется на основе классификации ресурсов. При этом учитываются состав (перечень) информационных активов и их значимость, обязательность непрерывности процессов деятельности Банка.

9.3 Развертывание, реализацию и эксплуатацию СМИБ осуществляет Отдел сетевой и информационной безопасности.

9.4 СМИБ можно представить в виде систематических непрерывных процессов на базе процессного подхода циклической модели менеджмента ИБ (модель Деминга): "планирование – реализация – проверка – совершенствование - планирование-…".

9.5 В Банке реализуются основные процессы СМИБ, связанные:

- с планированием процессов выполнения требований ИБ;
- с реализацией и эксплуатацией защитных мер;
- с проверкой процессов выполнения требований ИБ;
- с совершенствованием процессов выполнения требований ИБ.

9.6 Руководство Банка регулярно осуществляет анализ СМИБ и анализ соответствия реализации и/или эксплуатации СМИБ политике ИБ, как правило, после внешнего или внутреннего аудита (самооценки) ИБ.

9.7 По предоставленным материалам, а также используя практику работы СМИБ, в Банке принимаются (утверждаются) нормативно-распорядительные документы (приказы, распоряжения, решения, протоколы и т. п.), содержащие положения и указания, определяющие требования:

- по совершенствованию СМИБ;
- по изменению процедур, влияющих на СМИБ;
- по реализации корректирующих и превентивных действий в отношении СМИБ;
- по выделению ресурсов для целей СМИБ.

9.8 На основе нормативных документов, в том числе внутренних документов Банка, на основе анализа и применения моделей угроз и нарушителей, оценки рисков, уточняется область действия СМИБ, выбираются приоритеты обеспечения ИБ.

9.9 Требования к СМИБ Банка конкретизируются внутренними документами Банка – частными политиками.

© 2013 ЗАО АКБ “ЦентроКредит”

10. ПОРЯДОК ВВОДА В ДЕЙСТВИЕ И ПЕРЕСМОТР ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

10.1 Настоящая Политика утверждается Правлением Банка.

10.2 Поводом для пересмотра Политики могут являться:

- изменения политики ИБ Банка;
- изменения в действующем законодательстве РФ, а также в отраслевых стандартах Банка России в области обеспечения ИБ.

10.3 Настоящая Политика подлежит обязательному пересмотру не реже одного раза в три года.

© 2013 ЗАО АКБ “ЦентроКредит”

11. ОТВЕТСТВЕННОСТЬ

11.1 По степени опасности нарушения, связанные с несоблюдением локальных нормативных актов по обеспечению ИБ Банка, делятся на две группы:

- нарушения, повлекшие за собой наступление нежелательных для Банка последствий (утечку или уничтожение информации);
- нарушения, в результате которых созданы предпосылки, способные привести к нежелательным для банка последствиям (угроза уничтожения или утраты информации).

11.2 Нарушение требований локальных нормативных актов Банка по обеспечению ИБ является чрезвычайным происшествием и влечет за собой последствия, предусмотренными действующим законодательством РФ, локальными нормативными актами, договорами, заключенными между Банком и работниками и договорами, заключенными между Банком и контрагентами.

11.3 Степень ответственности за нарушение требований локальных нормативных актов в области ИБ определяется исходя из размера ущерба причинённого Банку.

11.4 Действие настоящей Политики распространяется на всех контрагентов, работников и должностных лиц Банка.

11.5 Руководители всех уровней несут персональную ответственность за соблюдение положений настоящей Политики и поддержание уровня ИБ в подконтрольных им подразделениях.

11.6 Ответственность за разглашение конфиденциальных сведений несет руководство структурных подразделений, а также персонально каждый работник Банка, имеющий доступ к информации, составляющей коммерческую тайну и допустивший ее утечку.

11.7 За разглашение конфиденциальных сведений, утерю носителей, содержащих такие сведения, а также за иные нарушения в работе с конфиденциальной информацией, виновные привлекаются к ответственности, вплоть до увольнения с работы.

11.8 Виды ответственности, предусмотренные отдельными федеральными законами об обращении с информацией ограниченного доступа:

- гражданско-правовая ответственность;
- дисциплинарная ответственность;
- административная ответственность;
- уголовная ответственность.

11.9 За разглашение сведений, составляющих банковскую тайну, работники могут быть привлечены к уголовной ответственности в соответствии с действующим законодательством Российской Федерации (ст.183 Уголовного кодекса Российской Федерации).

© 2013 ЗАО АКБ “ЦентроКредит”