Политика информационной безопасности

1. Общие положения

1.1. Настоящая Политика разработана в соответствии с действующим законодательством, нормативными актами и соотносимыми с ними положениями внутренних документов ОАО «Гамма». Она регламентирует порядок организации с целью обеспечения сохранности информации и ее безопасности в Гамма как в осуществлении текущей деятельности, так и в обозримом будущем.

1.2. Предметом настоящего документа является:

* порядок доступа к конфиденциальной информации;
* работа с криптографическими системами;
* физическая безопасность (доступ в помещения);
* разграничение прав доступа;
* работа в глобальной сети Интернет;
* дублирование, резервирование и раздельное хранение конфиденциальной информации.

2. Порядок доступа к конфиденциальной информации

2.1. В целях обеспечения защиты информации в Гамма, устанавливается следующий порядок допуска к работе с конфиденциальными источниками:

* Решение о доступе работника к определенному разделу банковской информации принимается руководством Гамма.
* Отдел банковских и информационных технологий обеспечивает защиту отдельных файлов и программ от чтения, удаления, копирования лицами, не допущенными к этому.
* Доступ к компьютерной сети Гамма осуществляется только с персональным паролем. Пользователь должен держать в тайне свой пароль. Сообщать свой пароль другим лицам, а также пользоваться чужими паролями запрещается. Имя пользователя и пароль на вход в АБС должны быть отличны от имени пользователя и пароля в общую компьютерную сеть Гамма.
* Категорически запрещается снимать несанкционированные копии с носителей банковской информации, знакомить с содержанием электронной информации лиц, не допущенных к этому.

3. Работа с криптографическими системами

3.1. К работе с криптографическими системами допускаются только сотрудники Гамма, имеющие соответствующее разрешение от руководства Гамма.

3.2. Секретные ключи электронно-цифровых подписей и шифрования должны храниться в сейфах под ответственностью лиц на то уполномоченных. Доступ неуполномоченных лиц к носителям секретных ключей и шифрования должен быть исключен.

3.3. Категорически запрещается:

* выводить секретные ключи и шифрования на дисплей компьютера или принтер;
* устанавливать в дисковод компьютера носитель секретных ключей и шифрования в непредусмотренных режимах функционирования;
* записывать на носитель секретных ключей и шифрования постороннюю информацию.

3.4. При компрометации секретных ключей, шифрования и прочей электронной информации Управлением банковских и информационных технологий принимаются меры для прекращения любых операций с использованием этих ключей и прочей информации; принимаются меры для смены ключей и шифрования, паролей. По факту компрометации организуется служебное расследование, результаты которого отражаются в акте и доводятся до сведения руководства Гамма.

4. Физическая безопасность

4.1. Все объекты критичные с точки зрения информационной безопасности (все сервера баз данных, телефонная станция, основной маршрутизатор, файервол) находятся в отдельном помещении, доступ в которое разрешен только сотрудникам, имеющими соответствующее разрешение от руководства Гамма.

4.2. Вход в помещение осуществляется через металлическую дверь, оснащенную замками (не менее двух) и переговорным устройством. Копии ключей находятся в службе безопасности банка.

4.3. Помещение оборудовано принудительной вентиляцией и пожарной сигнализацией. Вход в помещение контролируется системой видео наблюдения с выходом на мониторы охраны.

4.4. Ключевые дискеты, пароли и прочая конфиденциальная информация хранится в сейфах.

4.5. Доступ в помещение посторонним лицам запрещен. Технический персонал, осуществляющий уборку помещения, ремонт оборудования, обслуживание кондиционера и т.п. может находится в помещении только в присутствии работников, имеющих право находится в помещении в связи с выполнением своих должностных обязанностей.

4.6. Доступ в помещение в неурочное время или в выходные и праздничные дни осуществляется с письменного разрешения Председателя Правления (его заместителей).

5. Разграничение прав доступа к программному обеспечению и системам хранения данных

5.1. Для входа в компьютерную сеть Гамма сотрудник должен ввести имя и пароль. Не допускается режимы беспарольного (гостевого) доступа к какой-либо банковской информации.

5.2. В целях защиты конфиденциальной информации Гамма организационно и технически разделяются подразделения банка, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности, секретности и смысловой направленности). Данная задача решается с использованием сетевой операционной системы, где в целях обеспечения защиты данных доступ и права пользователей ограничивается персональными каталогами. Права назначаются в соответствии с производственной необходимостью, определяемой начальником подразделения.

5.3. Параметры входа в сеть, имя и пароль, пользователем не разглашаются. Копии на бумажном носителе держатся в недоступном для посторонних месте. В случае компрометации пароля пользователь должен незамедлительно обратиться в Управление информационных технологий с заявкой о замене.

5.4. При работе с АБС имя пользователя и пароль должны быть отличны от имени пользователя и пароля в при входе общую компьютерную сеть Гамма. Пароль должен быть не менее пяти символов. Категорически запрещается сообщать свой пароль другим лицам, а также пользоваться чужими паролями. Все действия пользователя, работающего с АБС протоколируются. Журнал операций храниться не менее шести месяцев.

6. Работа в глобальной сети Интернет

6.1. К работе с ресурсами сетью Интернет допускаются сотрудники, получившие соответствующее разрешение от руководства Гамма (достаточна устная форма).

6.2. Работа сотрудников Гамма с электронной почтой сети Интернет допускается на основании отдельного разрешения от руководства Гамма (достаточна устная форма).

6.3. При работе с сетью Интернет сотрудникам запрещено:

* Скачивать и устанавливать на компьютер программное обеспечение.
* Посещать ресурсы, не имеющие непосредственного отношения к работе и служебным обязанностям.
* Осуществлять подписку на рассылку информации непроизводственного характера.
* Сообщать адрес электронной почты в непроизводственных целях.

7. Дублирование, резервирование и раздельное хранение конфиденциальной информации

7.1. В целях защиты банковской информации от преднамеренного или же непреднамеренного ее уничтожения, фальсификации или разглашения обеспечить

* ежедневное обязательное резервирование всей информации, имеющей конфиденциальный характер.
* Дублирование информации с использованием различных физических и аппаратных носителей.

7.2. Ответственность за хранение и резервирование информации в электронном виде возложить на Отдел банковских и информационных технологий.