

**Банк «Асака»
Регистрационный №**

**Утверждено
Правлением Банка «Асака»
Протокол № _____
от _____ 201 г.**

ПОРЯДОК ЭКСПЛУАТАЦИИ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ И БАНКОВСКОГО ОБОРУДОВАНИЯ В БАНКЕ «АСАКА»

Настоящий Порядок разработан на основании Закона Республики Узбекистан «О банках и банковской деятельности», «О банковской тайне», «Методических указаний об организации защиты информации между банками Республики Узбекистан по системе электронных платежей», утвержденных Центральным банком Республики Узбекистан за № 183 от 12 января 1996 г. и в целях повышения работоспособности и отказоустойчивости вычислительной техники и банковского оборудования (далее оборудование) в Банке «Асака», (далее – Банк).

I. Общие положения

1.1. Настоящий Порядок определяет правила эксплуатации вычислительной техники и банковского оборудования в Банке «Асака».

1.2. Целью настоящего Порядка является, повышение эффективности использования вычислительной техники и банковского оборудования в Банке.

II. Основные условия

Настоящим Порядком устанавливаются следующие требования по использованию оборудования в Банке.

2.1. При оснащении помещений, где размещается оборудование, руководствоваться Требованиями к помещениям для размещения средств вычислительной техники, приведенными в «Методических указаниях об организации защиты информации между банками Республики Узбекистан по системе электронных платежей», утвержденными Центральным банком Республики Узбекистан за № 183 от 12 января 1996 г., «Инструкцией об организации защиты электронной информации в банках Республики Узбекистан», зарегистрированной Министерством юстиции Республики Узбекистан за N 1047 от 9 июля 2001 года и «Инструкцией о мерах по обеспечению технической защиты информации в банке «Асака», утвержденными Председателем Правления банка «Асака» № 259 от 28 июня 2006 года.

2.2. Оборудование размещается в отдельных, изолированных, защищенных от обозрения посторонних лиц, надежно охраняемых помещениях. Эти помещения должны отвечать требованиям пожарной безопасности и должны иметь капитальные стены и надежные перекрытия, прочные двери, оборудованы замками, средствами защиты окон от возможного проникновения через них в помещение, а также шторы на окнах, защищающие от визуального наблюдения, и сигнализацию, связанную с подразделением охраны. В помещении должен быть создан и поддерживаться микроклимат (температура, влажность и запыленность), должно быть исключено протекание воды извне и из сети водопровода или отопления, а также наличие специальных средств пожаротушения (огнетушители с углекислым газом или галоидным углеводородом).

2.3. В целях поддержания оборудования в исправном состоянии и обеспечения сохранности данных требуется подключение оборудования исключительно к источникам бесперебойного сети гарантированного электропитания.

2.4. Пользователям категорически запрещается открывать корпуса оборудования, вытаскивать кабели подключения, самостоятельно менять конфигурацию, размещать другие предметы на оборудование сверху, загромождать тыльную сторону, делать надписи, наклейки и прочие отличительные знаки, вставлять скрепки, кнопки и другие предметы в открытые части оборудования, употреблять пищу на рабочем месте, над оборудованием и т.д.

2.5. В целях обеспечения сохранности данных на персональных компьютерах запрещается удалять файлы созданные другими пользователями, использовать нелегальные программные продукты, игровые, видео и аудио программы, использовать непроверенные на наличие вируса оптические и USB носители, оставлять без присмотра в доступных местах средства криптографической защиты, оптические и USB носители с данными.

III. Требования к эксплуатации вычислительной техники и оборудования

3.1. Распределение ответственности пользователей:

- каждое оборудование в Банке должно быть закреплено за конкретным сотрудником подразделения, ответственного за поддержание данного оборудования в рабочем состоянии и соблюдение мер безопасности при работе с ним. Распределение ответственности сотрудников оформляется внутренним распоряжением структурного подразделения;
- если оборудование снабжено дополнительными устройствами, то сотрудник, ответственный за оборудование, является ответственным и

за все дополнительные устройства, подключённые к данному оборудованию;

- фамилия, имя, отчество ответственных лиц, сетевое имя и вид оборудования, наименование подразделений и местоположение должны быть указаны в распоряжении по закреплению оборудования за ответственными сотрудниками подразделения;
- при увольнении ответственного сотрудника, при переходе его в другие подразделения или перераспределении ответственности внутри подразделения, не позднее чем в трехдневный срок требуется вносить изменения в распоряжения.
- при временном отсутствии ответственного сотрудника (болезнь, командировка и т.д.) ответственность за оборудование принимает на себя начальник данного подразделения (в его отсутствии исполняющий его обязанности) либо сотрудник, назначенный начальником подразделения;
- при работе на оборудовании двух или более сотрудников необходимо назначить одно ответственное лицо, все остальные сотрудники производят работы только с разрешения ответственного лица;
- решение о компетентности конкретного сотрудника принимает начальник структурного подразделения, при необходимости консультируясь со специалистами Департамента информационных технологий;
- при недостаточном уровне подготовленности сотрудников, начальник структурного подразделения должен принять меры к организации необходимых занятий и консультаций.

3.2. Обязанности пользователей:

- ответственный сотрудник, должен обладать знаниями, достаточными для того, чтобы поддерживать оборудование в работоспособном состоянии;
- ответственное лицо должно следить за работоспособностью данного оборудования, при любых сомнениях в корректности функционирования устройства, обращаться к начальнику своего подразделения для консультаций со специалистами Департамента информационных технологий;
- сотрудник, отвечающий за данное оборудование, несет ответственность за решение об установке нового программного обеспечения или удаления какой-либо информации со своего оборудования. Соответственно он несет ответственность за наличие на компьютере программного обеспечения, не разрешённого к использованию и установленное не специалистами Департамента информационных технологий.
- сотрудник, ответственный за данное оборудование, обязан, производить необходимые профилактические работы на вверенном

ему оборудовании, периодический запуск антивирусных программ, удаление ненужной информации и процедуры проверки целостности и чистки жесткого диска. При необходимости обращаться за консультациями к специалистам Департамента информационных технологий;

- ответственный сотрудник должен присутствовать при любых работах, производимых на его оборудование специалистами Департамента информационных технологий или другими сотрудниками Банка;
- твердо знать и неукоснительно выполнять установленные требования по обеспечению режима защиты информации при использовании оборудования;
- соблюдать установленный порядок учета проводимых на оборудовании работ, включая подготовку данных, их ввод, обработку и выдачу результатов обработки, проведение ремонтно-профилактических работ;
- обеспечивать надежное хранение машинных носителей информации и машинных документов;
- соблюдать установленный режим разграничения доступа к конфиденциальной информации.

3.3. Для защиты данных хранимых на персональных компьютерах должны быть выполнены следующие меры безопасности:

3.3.1. Аппаратно-технические меры безопасности:

- перед включением компьютера и началом работы необходимо произвести внешний осмотр места его установки. Категорически запрещается загромождать специальные вентиляционные отверстия на задней и передней панелях системного блока, верхней части монитора;
- включение осуществляется в следующем порядке: монитор (кнопка включения питания расположен на лицевой панели); системный блок (кнопка включения питания расположен на лицевой панели); принтер или другое периферийное устройство. (Выключение должно осуществляться в обратном порядке, т.е. принтер, монитор, системный блок);
- максимально исключить контакт с кабелями, подключенными к вычислительной технике. Не допускать повреждения розеток при перемещении мебели в помещении;
- не ставить посторонние предметы (скрепки, чашки, сумки и т.п.) на корпус компьютера или периферийного оборудования;
- самостоятельно не перемещать компьютер и отдельные его блоки. При необходимости перемещения техники, вызывать специалистов Департамента информационных технологий;

- не размещать рядом с компьютером нагревательных приборов и любое другое электронное оборудование, кроме оборудования установленного специалистами Департамента информационных технологий;
- не курить в помещениях, где установлены компьютеры.

3.3.2. Системно-технические меры безопасности:

- оборудование должно быть опломбировано сотрудниками Департамента информационных технологий. Ответственный за оборудованием должен ежедневно, перед началом работы проверить целостность пломбы, а при её повреждении докладывать начальнику подразделения и сотрудникам Департамента информационных технологий.
- при входе в систему на персональном компьютере должен стоять пароль для входа в сеть. Сетевой пароль меняется каждые 30 дней. При выходе сообщения о смене пароля ответственный сотрудник должен выполнить следующие действия: ввести старый пароль; новый пароль; подтверждение нового пароля. Устанавливать старый пароль как новый система не пропустит, как и предыдущие 12. Если ответственный сотрудник набрал три раза неправильный пароль, то системная политика блокирует пользователя. При блокировке пароля ответственный сотрудник должен позвонить в Департамент информационных технологий и сообщить о проблеме входа в систему. Ответственный сотрудник не имеет права разглашать свой пароль другим сотрудникам Банка. В случае отсутствия ответственного сотрудника по причине болезни, командировки или отпуска допуск к данным может получить начальник данного структурного подразделения с согласованием с Департаментом информационных технологий.

IV. Нарушение порядка эксплуатации вычислительной техники и оборудования в Банке “Асака”

4.1. При нарушении порядка эксплуатации оборудования, приведшие к его временной или полной не работоспособности, а также порче или утере какой-либо части устройства, ответственное лицо за данное оборудование несет материальную ответственность в соответствии с нормами действующего законодательства Республики Узбекистан.

V. Прочие положения

- 5.1. Настоящий Порядок вступает в силу со дня его утверждения.
- 5.2. С вступлением в силу настоящего Порядка утрачивают свою силу «Порядок эксплуатации вычислительной техники и банковского

оборудования в банке «Асака» за №071, утвержденный Протоколом
Правления Банка «Асака» № 8 от 31 марта 2001 года.