Приложение №3
к Правилам о дистанционном банковском обслуживании юридических лиц, индивидуальных предпринимателей и физических лиц, занимающихся в установленном законодательством РФ порядке частной практикой в системе «Интернет-Банк» в АКБ «Энергобанк» (АО)

Требования по обеспечению информационной безопасности при работе в системе Интернет-Банк
Рекомендациии по снижению рисков осуществления перевода денежных средств без согласия клиента.

В целях обеспечения информационной безопасности Клиент наделяется следующими обязанностями по выполнению Требований по обеспечению информационной безопасности при работе в системе Интернет-Банк

1. Требования, предъявляемые к компьютеру и мобильному устройству, с которого осуществляется доступ к системе Интернет-Банк (далее-Система):

1.1. Компьютер, мобильное устройство должны быть защищены с помощью средств защиты информации, а именно средств антивирусной защиты и сетевой защиты (персональный фаервол), разрешающие доступ в сеть Интернет только тем программам, которые необходимы для работы с Системой и запрещающие любое иные обращение к компьютеру из сети Интернет.

1.2. Должно быть исключено подключение переносного компьютера(ноутбука), мобильного устройства к сетям общего доступа в местах свободного доступа в Интернет (офисные центры, кафе и пр.)

1.3. Включенный компьютер мобильное устройство не должены оставаться без контроля. Не отлучаться от компьютера, мобильного устройства пока происходит сеанс связи с Банком. Время до автоматической блокировки экрана во время бездействия пользователя должно составлять не более 3 минут. Разблокировка экрана должна происходить по паролю.

1.4. На компьютере, мобильном устройстве, на котором осуществляется доступ к Системе:

- должна быть установлена только одна операционная система и только те программы, которые необходимы для работы в Системе;
- запрещается устанавливать на него иные программы и электронную почту, не должно быть установлено программное обеспечение, содержащее средства разработки и отладки приложений, а также средств, позволяющих осуществлять несанкционированный доступ к системным ресурсам;
- должны быть отключены все неиспользуемые для связи с Банком службы и процессы операционной системы Windows (в т.ч. службы удаленного администрирования и управления, службы общего доступа к ресурсам сети и др.);
- производить только работы в Системе и не использовать компьютер для иных целей;
- операционная система, как и любое другое программное обеспечение, должно быть только лицензионным и в актуальной версии;
- должны своевременно устанавливаться обновления операционной системы, а также обновления по безопасности прикладного программного обеспечения;
- должна производиться регулярная (перед каждым запуском Системы) проверка целостности дистрибутива Клиента с использованием программного средства контроля целостности согласно инструкции по эксплуатации (эксплуатационную документацию) такого программного средства, полученного от Банка;
- должно быть установлено лицензионное средство антивирусной защиты (предпочтительно российского производителя) со своевременно обновляемыми антивирусными базами данных и проверкой по расписанию всех объектов системы;
- должна быть активирована подсистема регистрации событий информационной безопасности;
- пользователи не должны обладать правами локального администратора;
- на учетные записи пользователей операционной системы, должны быть установлены пароли, удовлетворяющие настоящим Требованиям;
- не допускать модификацию программного обеспечения;
- должен быть исключено подключение сменных носителей не участвующих в работе Системы.

1.5. Настройку компьютера (управление привилегиями, квотами, установка прав доступа пользователей и т.п.) должен выполнять специалист, обладающий необходимыми навыками по администрированию компьютерной техники и сети.

2. Требования по обеспечению информационной безопасности, предъявляемые к паролям:

2.1. На компьютере, мобильном устройстве должна быть установлена парольная защита на вход в Операционную систему.

2.2. При выборе пароля необходимо соблюдать следующие требования:

- пароль должен содержать не менее 8 символов;
- содержать как минимум по одному символу из букв нижнего и верхнего регистра, цифры и знаки препинания;
- не использовать в качестве пароля один и тот же повторяющийся символ, либо комбинацию из нескольких рядом стоящих символов;
- не использовать в качестве пароля имя, фамилию, день рождения и другие памятные даты, номер телефона, автомобиля, девичью фамилию матери и другие данные, которые могут быть подобраны злоумышленником путем анализа информации о пользователе.

2.3. Пароль от операционной системы необходимо менять один раз в 60 дней. Пароль от Системы необходимо менять каждые 30 дней. Запрещено ставить один и тот же пароль на операционную систему и Систему.

2.4. Строго запрещается записывать пароли на бумажных носителях или в текстовых файлах на рабочем месте, оставлять их в легкодоступных местах, передавать неуполномоченным лицам.

3. Требования по обеспечению информационной безопасности, предъявляемые к сменным носителям ключевой информации, используемым в Системе для канала доступа Интернет-Банк:

3.1. Ключевая информация (ключ ЭЦП/ЭП для работы в Системе) должна размещаться на сменном носителе информации (USB Token). Размещение ключевой информации на жестком диске компьютера (на котором установлена Система) или на внешних незащищенных накопителях, запрещается.

3.2. Сменный носитель с ключевой информацией должен быть установлен в считывающее устройство только во время работы в Системе. Размещение сменного носителя в считывающем устройстве вне сеансов работы в Системе должно быть исключено.

3.3. Сменный носитель с ключевой информацией должен использоваться только владельцем сертификата ключа проверки ЭЦП\ЭП либо лицом, уполномоченным на использование такого сменного носителя.

3.4. Хранить ключевой носитель необходимо в защищаемой комнате, в сейфе, исключающим доступ неуполномоченных лиц и повреждение материального носителя. Вся ответственность за конфиденциальность секретных ключей ЭЦП/ЭП Клиента лежит на Клиенте, как на единственном владельце секретных ключей ЭЦП/ЭП.

3.5. Не допускается:

- снимать несанкционированные копии с носителей ключевой информации;
- передавать носители ключевой информации лицам, к ним не допущенным;
- записывать на носители ключевой информации постороннюю информацию.

4. Требования к рабочему месту и работе

4.1. Компьютер должен располагаться в отдельном запирающемся помещении, в котором исключен несанкционированный доступ. В таком помещении должно быть установлено средство регистрации и контроля доступа в виде электронного замка и видеофиксации.

4.2. Категорически запрещается пользоваться Системой в Интернет-кафе, библиотеках и других местах с публичным доступом в сеть Интернет из-за отсутствия должной системы безопасности в вышеперечисленных заведениях.

4.3. Исключить попадание на компьютер, мобильное устройство вредоносных программ и неправомерного доступа неуполномоченных лиц.

4.4. Обеспечить регулярное получение, доведение до уполномоченных лиц и исполнение рекомендаций и требований по вопросам безопасности, включая изучение рассылки Банка по вопросам защиты информации, от воздействия вредоносного кода, о возможных рисках и мерах по их снижению, в том числе информации о:

- рекомендуемых мерах по предотвращению несанкционированного доступа к защищаемой информации, в том числе при утрате (потере, хищении) устройства, с использованием которого клиентом осуществлялся перевод денежных средств;
- рекомендуемых мерах по контролю конфигурации устройства, с использованием которого клиентом осуществляется перевод денежных средств, и своевременному обнаружению воздействия вредоносного кода;
- появлении в сети "Интернет" ложных (фальсифицированных) ресурсов и программного обеспечения, имитирующих программный интерфейс используемых оператором по переводу денежных средств систем Интернет-банкинга, и (или) использующих зарегистрированные товарные знаки и наименование оператора по переводу денежных средств, и рекомендуемых мерах по обнаружению указанных ресурсов и программного обеспечения

4.5. При осуществлении доступа к Системе необходимо удостовериться в правильности указанного адреса в адресной строке браузера (должно быть https://dbo.energobank.ru/) и значок защищенного соединения (замок), исключая выход на сайты, внешне маскирующиеся под Интернет-Банк.

4.6. Отправление ЭПД производить только с использованием идентификационной информации, используемой для адресации устройства, с использованием которого осуществлен доступ к автоматизированной системе, программному обеспечению с целью осуществления переводов денежных средств, которой в зависимости от технической возможности является IP-адрес, MAC-адрес и (или) иной идентификатор устройства.

4.7. Не допускать при использовании носителей секретных ключей следующих ситуаций:
несанкционированного копирования носителей секретных ключей ЭЦП/ЭП;

4.8. Соблюдать требования информационной безопасности при работе в Системе дистанционного банковского обслуживания Интернет-Банк, и рекомендации Банка, сообщениях об угрозах и иные документы, размещенные на официальном сайте Банка.

5. Действия пользователя при получении сообщений из Банка и компрометации ключевой информации

5.1. Ни при каких случаях не отвечать на письма, якобы от имени Системы, с требованиями (просьбами, предложениями) зайти на сайт, не принадлежащий домену energobank.ru, прислать секретный ключ или пароль доступа к нему, а немедленно сообщить о подобном факте специалистам Банка.
Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать секретный ключ ЭЦП/ЭП или пароли. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры.

5.2. В случае поступления на мобильный номер телефона SMS-оповещение или электронного сообщения о совершенной операции, Клиент обязан немедленно связаться с Банком по соответствующим каналам и телефонам или лично для сообщения, что операция не была осуществлена Клиентом.

5.3. При подозрении на компрометацию ключевой информации, в случаях кадровых перестановок лиц, имевших доступ к Системе, компьютеру и ключам, при опасениях в несанкционированном доступе, при случаях обнаружения вируса, при утери мобильного устройства с сим-картой необходимо немедленно обратиться в Банк для блокирования Системы и последующей замены ключевой информации.

5.4. По всем случаям п.5. следует незамедлительно сообщить специалистам Отдела удаленного обслуживания клиентов УИТ по телефону (843) 231-60-80, Отдела обеспечения информационной безопасности (843) 231-60-78 или сообщить Вашему обслуживающему операционисту.

6. Дополнительные меры защиты.

6.1. Клиент вправе ограничить работу Системы с одного или нескольких устройств, с использованием которых может осуществляться доступ к Системе с целью осуществления переводов ЭПД/ЭД, на основе идентификаторов MAC-адресов, если такое ограничение предусмотрено для используемого канала доступа к Системе. При осуществлении режима работы с любых MAC-адресов Клиент понимает и принимает на себя все риски, связанные с возможностью доступа к серверу Системы с любого компьютера при наличии доступа к ключам ЭЦП/ЭП и паролям.

6.2. Клиент вправе дополнительно выбрать, предоставляемую Банком возможность, услугу по дополнительному информированию по альтернативному системе каналу связи о каждой отправке ЭПД в Банк. Заявление намерение Клиента, использовать дополнительную услугу по альтернативным каналам связи и номера мобильных телефонов для приема SMS-сообщений, оформляются в соответствующем Соглашении по форме Банка и подлежит оплате в соответствии с Тарифами Банка.

6.3. Клиент вправе на, основании заявления, выбрать предоставляемую Банком возможность определять дополнительные ограничения (параметры) операций, которые могут осуществляться Клиентом с использованием Системы, устанавливать ограничение:

- на максимальную сумму перевода денежных средств за одну операцию;
- на общую сумму переводов денежных средств фактически отправленных за календарную дату;
- времени приема платежных документов, с указанием периода начала и окончания обслуживания

6.4. Клиент вправе, на основании специального заявления, выбрать предоставляемую Банком возможность использования одноразового кода подтверждения, в целях аутентификации платежного документа Клиентом, реализованного в виде подключения специального технического устройства eTokenPass, с оплатой согласно Тарифов Банка.