Требования по обеспечению информационной безопасности автоматизированного рабочего места Клиента

Настоящие требования определяют перечень мер, обязательных для применения Клиентом и предназначенных для обеспечения защиты конфиденциальной информации на стороне Клиента при использовании системы «Интернет-банк».

Выполнение настоящих требований по информационной безопасности позволит обеспечить защиту юридически значимого электронного документооборота Клиента с Банком и минимизировать риски возможных финансовых потерь.

Форма и порядок реализации приведенных требований информационной безопасности устанавливается Клиентом самостоятельно.

Клиент обязан учитывать то, что:

- информационно-телекоммуникационная сеть Интернет не имеет единого органа управления (за исключением службы управления пространством имен и адресов) и не является юридическим лицом, с которым можно было бы заключить договор (соглашение). Провайдеры (посредники) информационно-телекоммуникационной сети Интернет могут обеспечить только те услуги, которые реализуются непосредственно ими;
- существует вероятность несанкционированного доступа, потери и искажения информации, передаваемой посредством информационно-телекоммуникационной сети Интернет;
- существует вероятность атаки Злоумышленников на оборудование, программное обеспечение и информационные ресурсы Клиента, подключенные/доступные из информационно-телекоммуникационной сети Интернет;
- гарантии по обеспечению Информационной безопасности при использовании сети Интернет никаким органом/учреждением/организацией не предоставляются;
- меры по нейтрализации Злоумышленных действий могут быть эффективными только в течение первых часов после Инцидента;
- расследованием Злоумышленных действий и поиском Злоумышленников занимаются правоохранительные органы.
- Банк никогда не осуществляет рассылку писем, содержащих ссылки для перехода на страницы в сети Интернет, или для загрузки какого-либо программного обеспечения или данных. Необходимое для работы системы «Интернет-банк» программное обеспечение размещено на веб-сайте Faktura.ru в разделе «Настройка и поддержка».
- Банк никогда не запрашивает у клиентов конфиденциальную информацию по собственной инициативе!

Информационная безопасность автоматизированного рабочего места Клиента в системе «Интернет-банк» (далее по тексту АРМ) обеспечивается применением совокупности организационных и технических мер и средств защиты информации.

Организационные меры

Клиент разрабатывает и документально фиксирует правила подготовки, ввода в эксплуатацию и использования АРМ.

Клиент определяет и документально фиксирует (например, приказом) перечень лиц из числа своих работников, имеющих доступ к рабочему месту, с закреплением за каждым из них допустимых полномочий. В этот перечень включаются:

- лицо, непосредственно осуществляющее работу на АРМ в системе «Интернет-банк»;
- лицо, осуществляющее системное администрирование АРМ;

- лицо, ответственное за обеспечение информационной безопасности АРМ и администрирующее установленные на АРМ средства защиты информации;
- лица, замещающие вышеперечисленных на время их отсутствия.

Остальным работникам Клиента должен быть установлен запрет на доступ к АРМ.

Лица, допущенные к конфигурированию и эксплуатации АРМ, обязаны ознакомиться под подпись с установленными для Клиента правилами, инструкциями, размещенными на сайте Faktura.ru, а также настоящими требованиями.

Размещение оборудования АРМ осуществляется способом, исключающим возможность его несанкционированного использования, и производится в служебном помещении, для которого обеспечен режим ограниченного доступа (защищаемые помещения).

Защищаемое помещение необходимо оборудовать прочной входной дверью с замками, гарантирующими надежное закрытие в нерабочее время. По окончании рабочего дня защищаемое помещение и установленные в нем хранилища закрывают.

Для предотвращения наружного наблюдения за деятельностью сотрудников окна помещения необходимо защитить.

Окна помещения, расположенного на первом или последнем этаже здания, а также окна, находящиеся около пожарных лестниц и других мест, откуда возможно проникновение посторонних лиц, необходимо оборудовать охранной сигнализацией, или другими средствами, препятствующими неконтролируемому проникновению в защищаемое помещение.

Клиент устанавливает режим охраны, предусматривающий периодический контроль за состоянием технических средств охраны.

Ключи от защищаемого помещения подлежат учету и выдаются только лицам, имеющим право допуска в защищаемые помещения, согласно перечню.

При обнаружении признаков, указывающих на возможное несанкционированное проникновение в защищаемое помещение посторонних лиц, Клиент обязан оценить возможность несанкционированного доступа к системе или компрометации ключа электронной подписи и при необходимости максимально быстро уведомить об инциденте Банк с последующим направлением письменного заявления.

Клиент устанавливает порядок хранения и использования носителей ключевой информации, исключающий возможность несанкционированного доступа третьих лиц.

Клиент определяет и документально фиксирует (например, приказом) перечень лиц из числа своих работников, имеющих право использования ключа электронной подписи.

Во время работы с носителями ключевой информации необходимо исключить доступ к АРМ посторонних лиц.

Хранение носителей ключевой информации осуществляется в сейфах или запираемых металлических шкафах (хранилищах), исключающих возможность несанкционированного доступа, неправомерного использования или утраты (хищения).

По окончании рабочего дня, а также между сеансами работы с системой носители ключевой информации убираются в хранилище.

В отношении носителей ключевой информации необходимо установить запрет на:

- передачу другим работникам и посторонним лицам;
- использование не по назначению;
- подключение к другим компьютерам или иному оборудованию;
- оставление без присмотра на рабочем месте.

При смене лица, наделенного правом использования ключей электронной подписи, Клиент обязан признать его компрометацию и уведомить об этом Банк, с дальнейшим изготовлением новых ключей на вновь назначенных лиц.

Технические меры и средства

Для осуществления работы в системе «Интернет-банк» необходимо использовать отдельное, специально выделенное для этих целей АРМ, на котором в обязательном порядке обеспечиваются меры защиты от несанкционированного доступа и защиты от вредоносного программного обеспечения.

Защита АРМ от несанкционированного доступа осуществляется с целью исключения возможностей:

- внесения несанкционированных изменений в технический или программный состав АРМ;
- несанкционированного вмешательства в электронный документооборот Клиента с Банком.

Клиент предпринимает меры, препятствующие несанкционированному доступу и вскрытию технических средств АРМ.

Необходимо установить запрет на несанкционированное подключение к АРМ внешних устройств, в том числе съёмных носителей информации, а также автозапуск программ со всех устройств хранения, в том числе съемных.

На АРМ устанавливают только одну операционную систему, а также исключают возможность загрузки с внешних носителей (CD/DVD, USB flash).

Клиентом осуществляются мероприятия по ограничению программной среды АРМ, обеспечивающие:

- установку и (или) запуск только разрешенного к использованию программного обеспечения;
- невозможность установки стороннего программного обеспечения;
- отсутствие средств разработки и отладки программного обеспечения.

Клиентом регламентируются процедуры мониторинга и установки обновлений системного и прикладного программного обеспечения.

Необходимо предусмотреть процедуры контроля целостности программного обеспечения, обнаружения фактов её несанкционированного нарушения и последующего восстановления при необходимости.

Клиентом исключается возможность использования на АРМ нелицензионных копий и свободно распространяемого программного обеспечения.

Клиентом определяется порядок идентификации и аутентификации пользователей на АРМ, а также разграничения доступа и предоставления полномочий. Устанавливаемый порядок исключает возможность наделения какого-либо пользователя максимальными полномочиями (администрирования АРМ, администрирования средств защиты, осуществления работы в системе «Интернет-банк»). Доступ к изменению настроек BIOS также сопровождается процедурой аутентификации (защита паролем). Учетную запись «Гость» необходимо выключить.

Длина используемых паролей составляет не менее восьми символов, включая заглавные, строчные буквы и специальные символы. Сложность пароля выбирают достаточной для исключения возможности подбора. Срок действия паролей необходимо ограничить.

Клиентом предусматриваются меры по защите АРМ при взаимодействии с информационно-телекоммуникационными сетями. Для этого рекомендуется установить и настроить соответствующим образом персональный межсетевой экран.

Меры устанавливают запрет сетевого доступа к ресурсам АРМ с других рабочих станций локальной сети или с использованием внешних сетей общего пользования, в том числе в режимах удаленного рабочего стола и удаленного администрирования.

Необходимо установить строгое ограничение на использование ресурсов сети Интернет пользователями АРМ, что означает определение законченного списка доступных для соединения адресов (например, разрешить только соединение с серверами системы «Интернет-банк»).

При использовании на АРМ систем обмена сообщениями или электронной почты пользователи информируются о мерах предосторожности при работе с электронными письмами или сообщениями, получаемыми от неизвестных источников.

В случае если при включении или в процессе работы с системой «Интернет-банк» будут обнаружены какие-то не имевшие ранее места события: самопроизвольные движения указателя мыши, нештатные информационные окна, несанкционированные платежи или сообщения об ошибках, о неверном ключе или пароле, и т.п. – Клиент обязан незамедлительно прекратить работу в системе, зафиксировать суть события и сопутствующую информацию и уведомить о событии сотрудников Банка.

Меры по защите АРМ от вредоносного кода (ВК) обеспечивают обнаружение компьютерных программ, предназначенных для внедрения в информационные системы, программное обеспечение, средства вычислительной техники, телекоммуникационное оборудование, участвующее в дистанционном банковском обслуживании, приводящего к уничтожению, созданию, копированию, блокированию, модификации и (или) передаче информации, а также реагирование на обнаружение этих программ и информации.

На АРМ организуют непрерывное функционирование средств защиты от ВК в автоматическом режиме с регулярным контролем целостности и работоспособности защитного ПО.

Обновление баз сигнатур средств защиты от ВК необходимо производить в автоматическом режиме по мере их размещения (выпуска) разработчиком.

Рекомендуется осуществлять полную еженедельную проверку АРМ на наличие ВК.

Средства защиты от ВК осуществляют фильтрацию всех сообщений электронной почты, интернет-мессенджерах и т.д.

На АРМ обеспечивается обязательная проверка подключаемых съемных носителей информации на наличие ВК.

Средство защиты от ВК настраивают таким образом, чтобы при обнаружении признаков присутствия ВК на АРМ автоматически реализовывался комплекс мер по блокированию нежелательной активности и устранению последствий, а также происходило уведомление пользователя об инциденте. А в случае обнаружения атаки ВК в сетевом трафике с внешнего по отношению к АРМ источника, средство защиты от ВК автоматически блокирует обмен данными с этим источником.

При возникновении инцидентов, связанных с воздействием вредоносного кода на АРМ, Клиент обязан незамедлительно прекратить работу в системе «Интернет-банк», выяснить и устранить возможные последствия, зафиксировать всю доступную информацию об инциденте и уведомить сотрудников Банка.

Клиент предусматривает использование средств анализа наличия на АРМ уязвимостей системного и прикладного программного, особенно в части защиты от ВК.

Средства защиты от ВК предусматривают средства обобщения и анализа информации, фиксируемой в журналах протоколирования работы защитного ПО.

При выборе средств защиты от ВК рекомендуется отдавать предпочтение известным, хорошо зарекомендовавшим себя в течение продолжительного времени компаниям-разработчикам, предлагающим продукты, использующие зарегистрированные товарные знаки. Целесообразно предусматривать приобретение средств защиты от ВК у авторизованных партнеров компаний - разработчиков.