Рекомендации по обеспечению информационной безопасности при работе в УРМ

Важнейшим фактором, способствующим обеспечению безопасности, является личная заинтересованность Участника. Центр считает необходимым соблюдение Участниками следующего комплекса мер по защите информации:

1. **Обеспечение безопасности компьютера, с использованием которого осуществляется работа в УРМ:**

- Установите и регулярно обновляйте лицензионное программное обеспечение, а также антивирусное программное обеспечение на Вашем компьютере. Действие вредоносных программ может быть направлено на перехват Вашей персональной информации и передачу её третьим лицам.
- Своевременно устанавливайте обновления операционной системы своего компьютера, рекомендуемые компанией-разработчиком в целях устранения выявленных в ней уязвимостей.
- Установите и настройте персональный брандмауэр (firewall) на Вашем компьютере**.** Это позволит Вам запретить несанкционированный удаленный доступ к Вашему компьютеру из сети Интернет и Вашей локальной сети с использованием удаленного управления компьютером и терминального доступа.
- Используйте дополнительное программное обеспечение, позволяющее повысить уровень защиты Вашего компьютера – программы поиска шпионских компонент, программы защиты от «спам» - рассылок.
- В обязательном порядке следует отключать Автозапуск в операционной системе (для OS Windows: «Панель управления» -> «Администрирование» -> «Службы»; необходимо найти в закладке «Расширенный» службу «Определение оборудования оболочки» и установить «Отключено»).

□

Для предотвращения возможности несанкционированного доступа к компьютеру с использованием которого осуществляется работа в системе, рекомендуется использовать программные комплексы или программное обеспечение, обеспечивающие предотвращение возможности несанкционированного доступа.

- Исключите посещение с компьютеров сайтов сомнительного содержания и любых других Интернет-ресурсов (социальные сети, форумы, чаты, телефонные сервисы и т.д.), а также чтение почты и открытие почтовых документов от недостоверных источников.
- Категорически не рекомендуется работать с УРМ с компьютеров, не заслуживающих доверия (интернет-кафе) или с использованием общественных каналов связи (бесплатный Wi-Fi и т.п.), т.к. это существенно увеличивает риск кражи Ваших данных.
- Регулярно контролируйте состояние своих счетов и незамедлительно сообщайте работникам Центра обо всех подозрительных или несанкционированных операциях.
- На компьютере не рекомендуется устанавливать иное программное обеспечение, кроме необходимого для работы в УРМ. Рекомендуется использовать для работы с УРМ выделенный компьютер.
- Перечень пользователей, имеющих доступ к компьютеру, должен быть строго ограничен. Права пользователя, работающего с УРМ, на данном компьютере должны быть минимально необходимыми (наличие прав администратора должно быть запрещено).
- Исключите запуск и работу сервисов (как встроенных в ОС, так и сторонних), позволяющих получить удаленный доступ к компьютеру, в том числе и с целью администрирования и обслуживания.

2. **Соблюдение правил безопасности при работе с ключевыми носителями:**

- Храните ключи только на съемном носителе. По возможности используйте съемные защищенные носители. Хранение ключевых носителей должно быть организовано в месте, недоступном для посторонних лиц. Установка ключевых носителей на рабочее место допускается только непосредственно на время работы с УРМ.

□

ВАЖНО: После окончания сеанса работы в УРМ съемный ключевой носитель должен быть незамедлительно извлечен из компьютера!

- Если Вы используете несколько ключей ЭП при работе в УРМ, не переносите эти ключи ЭП на один ключевой носитель, а также не подключайте одновременно различные ключевые носители к компьютеру.

  Для контроля доступа к съемному ключевому носителю рекомендуется установить на него пароль.

  ВАЖНО: Не сообщайте никому пароль для доступа к съемному ключевому носителю (включая работников Центра и работников Вашей организации или Ваших родственников)!
- Генерацию ключей ЭП осуществляйте лично с записью ключевой информации на съемный носитель. Не допускайте копирования сгенерированных ключей ЭП.
- После окончания работы в УРМ обязательно корректно завершите работу (выйдите из УРМ с использованием кнопки «Выход») и/или закройте браузер.

  ВАЖНО: Извлеките из компьютера съемный ключевой носитель!
- Производите замену ключей ЭП до истечения срока их действия. Кроме того, проводите замену ключей ЭП во всех случаях увольнения и/или смены лиц, имеющих доступ к УРМ, а также руководителей с правом подписи доверенностей на получение ключей ЭП, и в случае подозрений на их компрометацию.

3. **Выполнение правил безопасности при работе в УРМ:**

- В случае сбоев в работе компьютера или его поломки во время работы в УРМ или сразу после сеанса (проблемы с загрузкой операционной системы, выход из строя жесткого диска, и т.п.), следует НЕМЕДЛЕННО извлечь ключи ЭП и выключить компьютер, а также обратиться в Центр и убедиться, что от Вашего имени не производились несанкционированные операции (путём сверки операций за день).

□

- Обращайте внимание на любые изменения в привычных для Вас процессах установления соединения с УРМ или в функционировании УРМ. При возникновении любых сомнений в правильности функционирования УРМ незамедлительно обратитесь в Центр.
- При использовании механизма импорта документов из каталогов общего доступа необходимо обеспечить безопасность данных каталогов. Права доступа к данным каталогам должны быть минимально необходимыми для обеспечения транспортного функционала. Документы, загруженные из каталогов общего доступа, должны ОБЯЗАТЕЛЬНО проходить стадию визуального контроля пользователем.
- В случае появления предупреждений браузера о перенаправлении Вас на другой сайт при подключении к УРМ Центра, отложите совершение операций и обратитесь в службу поддержки Центра.

В случае утраты ключевого носителя, утраты ключей от хранилища в момент нахождения в нем ключевого носителя, а также в случае возникновения ситуации, связанной с временным доступом посторонних лиц к ключевому носителю либо в связи с подозрением, что такой доступ имел место, необходимо незамедлительно обратиться в Центр в связи с компрометацией ключа ЭП.

Рекомендации по организационному обеспечению безопасности средств защиты информации (СЗИ):

- в организации Клиента выделяются (определяются) должностные лица, ответственные за обеспечение безопасности информации и эксплуатации СЗИ;
- в организации Клиента разрабатываются нормативные документы, регламентирующие вопросы безопасности информации и эксплуатации СЗИ;
- к работе с СЗИ допускаются сотрудники, имеющие навыки работы на персональном компьютере, ознакомленные с правилами эксплуатации СЗИ.

Рекомендации по размещению СЗИ и режиму охраны:

- помещения, в которых размещаются технические средства клиентского рабочего места со встроенными СЗИ, являются режимными и должны обеспечивать конфиденциальность проводимых работ;
- размещение режимных помещений и их оборудование должны исключать возможность бесконтрольного проникновения в них посторонних лиц и обеспечивать сохранность находящихся в этих помещениях конфиденциальных документов и технических средств;
- размещение оборудования, технических средств, предназначенных для обработки конфиденциальной информации, должно соответствовать требованиям техники безопасности, санитарным нормам и требованиям пожарной безопасности;
- входные двери режимных помещений должны быть оборудованы замками, обеспечивающими надежное закрытие помещений в нерабочее время;
- окна и двери должны быть оборудованы охранной сигнализацией, связанной с пультом централизованного наблюдения за сигнализацией;
- размещение технических средств в режимном помещении должно исключать возможность визуального просмотра конфиденциальных документов и экранов мониторов, на которых она отражается, через окна;
- в режимные помещения допускаются руководители организации Клиента, сотрудники подразделения безопасности и исполнители, имеющие прямое отношение к обработке, передаче и приему конфиденциальных документов;
- системные блоки компьютеров с СЗИ оборудуются средствами контроля вскрытия;

- ремонт и/или последующее использование системных блоков осуществляется после удаления с них программного обеспечения СЗИ.

Рекомендации по обеспечению безопасности ключевой информации:

- ключевые носители в организации Клиента берутся на поэкземплярный учет в выделенных для этих целей журналах;
- учет и хранение ключей поручается руководством Клиента специально выделенным сотрудникам;
- для хранения ключевых носителей с ключами ЭЦП выделяется сейф или иное хранилище, обеспечивающее сохранность ключевой информации;
- хранение ключей допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное применение, не предусмотренное правилами пользования СЗИ;
- ключевые носители с рабочими ключами (копиями рабочих ключей) хранятся раздельно с обеспечением условия невозможности их одновременной компрометации;
- при транспортировке ключевых носителей с секретной ключевой информацией создаются условия, обеспечивающие защиту от физических повреждений и внешнего воздействия на записанную ключевую информацию.

ВНИМАНИЕ!

Незамедлительное обращение в Центр с предоставлением полной информации о несанкционированном списании денежных средств со счетов может позволить оперативно приостановить транзакцию и предотвратить финансовые потери.