**Приложение 1. Требования по информационной безопасности для работ по сервисному обслуживанию и ремонту ПТК САУГ «КЭР-АТ».**

Наличие у Исполнителя лицензии ФСТЭК РФ на техническую защиту конфиденциальной информации (ТЗКИ) с разрешенными к выполнению видами работ, определенными в подпунктах б), д) и е) пункта 4 Положения о лицензировании деятельности по технической защите конфиденциальной информации, утвержденного Постановлением Правительства РФ от 03.02.2012 № 79.

Исполнитель выполняет работы по обеспечению информационной безопасности (ИБ) в следующем составе и объеме:

1. Проводит анализ угроз безопасности информации в ПТК САУГ «КЭР-АТ» и рисков от их реализации, в том числе:

* анализ уязвимостей автоматизированной системы управления, возникших в ходе ее эксплуатации;
* анализ изменения угроз безопасности информации в автоматизированной системе управления, возникших в ходе ее эксплуатации;
* оценку последствий от реализации угроз безопасности информации в автоматизированной системе управления (анализ рисков).

1. По результатам анализа изменений угроз безопасности информации, возникших в ходе эксплуатации ПТК САУГ «КЭР-АТ», разрабатывает модель угроз или актуализирует (при необходимости) существующую модель угроз безопасности для котлоагрегата №2 и по согласованию с Заказчиком для котлоагрегата №3. Модель угроз разрабатывается (актуализируется) в соответствии с банком данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru), а также иными доступными источниками, содержащие сведения об уязвимостях и угрозах безопасности информации, и должна содержать описание автоматизированной системы управления и угроз безопасности информации для каждого из уровней автоматизированной системы управления, включающее описание возможностей нарушителей (модель нарушителя), возможных уязвимостей автоматизированной системы управления, способов (сценариев) реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (доступности, целостности, конфиденциальности) и штатного режима функционирования автоматизированной системы управления.
2. Производит оценку потенциального ущерба от реализации актуальных угроз информационной безопасности. Результаты оценки согласовывает с ответственными за эксплуатацию ПТК САУГ «КЭР-АТ» лицами.
3. Проводит мониторинг событий безопасности ПТК САУГ «КЭР-АТ».
   1. Проверку журналов регистрации и учета событий безопасности общесистемного, прикладного и специального ПО, включая:

* неудачные попытки входа (локального, сетевого) и блокировку учетных записей;
* создание новых учетных записей и смену паролей;
* попытки получения доступа к управлению компонентами обслуживаемой системы и программно-техническими средствами защиты информации (использование привилегированных учетных записей);
* внесение изменений в конфигурации компонентов обслуживаемой системы;
* факты изменения прав доступа субъектов доступа к объектам доступа;
* очистку содержимого журналов записей аудита (логов);
* переполнение журналов аудита с аномально высокой частотой регистрации событий;
* предупреждения, исходящие от антивирусных средств и средств обнаружения вторжений;
* отключение антивирусных средств и других средств защиты информации;
* применение обновлений программного обеспечения (ПО);
* перезагрузку (выключение) вычислительных средств обслуживаемой системы;
* подключение и попытки подключения съемных носителей информации;
* подключение и отключение периферийных устройств.
  1. В случае выявления инцидентов ИБ доводит информацию о выявленных инцидентах до специалиста Заказчика, ответственного за обеспечение ИБ ПТК САУГ «КЭР-АТ».
  2. Принимает меры по локализации инцидента ИБ и его последствий и, при необходимости, восстанавливает функционирования АСУ ТП после инцидента ИБ.

1. Проводит проверку текущего уровня защищенности обслуживаемой системы.
   1. Проводит инструментальный анализ защищенности при помощи специализированных сканеров безопасности, сертифицированных ФСТЭК России, всех устройств сетевой инфраструктуры ПТК АСУ ТП. В рамках инструментального анализа защищенности при помощи специализированных сканеров безопасности должно быть проведено в том числе: инвентаризация компонентов ПТК САУГ «КЭР-АТ» и установленного ПО на них, сканирование в части обнаружения сетевых уязвимостей, уязвимостей операционной системы, уязвимостей прикладного и специализированного ПО, уязвимостей ПЛК, сканирование в части соответствия стандартам безопасности производителей ПТК САУГ «КЭР-АТ» (если применимо). Инструментальный анализ защищенности проводится по программе, заранее согласованной с Заказчиком, в том числе и с главным специалистом по ИБ АСУ ТП УРиТП ИА, а также с подрядной организацией, которая проводит сервисное или техническое обслуживание проверяемого ПТК САУГ «КЭР-АТ».
   2. Устраняет выявленные в ходе анализа защищенности недостатки в соответствии с рекомендациями производителя ПО.
   3. После устранения недостатков проводит повторный инструментальный анализ защищенности при помощи специализированных сканеров безопасности, сертифицированных ФСТЭК России, согласно требованиям, указанных в п. 5.1, на предмет устранения, выявленных ранее недостатков.
   4. Проводит тестирование программно-технического комплекса (ПТК) обслуживаемой системы на предмет корректности функционирования после устранения выявленных недостатков. При возникновении неполадок в работе компонентов ПТК обслуживаемой системы обеспечивает возврат ПО в первоначальное состояние и устраняет неполадки.
   5. Результаты инструментальных анализов защищённости предоставляются Заказчику в форме отчета с приложениями технических отчетов из сканеров безопасности. В отчете должны быть отражены обнаруженные недостатки и уязвимости, рекомендации по их устранению, выполнение данных рекомендаций Подрядчиком (при необходимости совместно с Производителем ПТК) или мотивированное обоснование о невозможности их выполнения, и вывод по всему отчету.»
2. Управление конфигурацией системы защиты информации ПТК.
   1. Контроль соответствия состава ПТК приведенному в эксплуатационной документации с целью поддержания актуальной (установленной в соответствии с эксплуатационной документацией) конфигурации ПТК. При выявлении несоответствий, принятие мер по внесению необходимых изменений в текущую конфигурацию ПТК.
   2. Проверка состава ПО, установленного на компонентах ПТК обслуживаемой системы. По согласованию с Заказчиком удаление неиспользуемого и нецелевого ПО. Создание списка, разрешенного к использованию на ПТК ПО, согласованного с Заказчиком.
   3. Контроль сроков действия лицензий на применяемое ПО. При обнаружении, что у лицензий заканчивается срок действия, незамедлительно оповестить об этом Заказчика.
3. По результатам анализа уязвимостей и угроз безопасности ПТК САУГ «КЭР-АТ», возникших в ходе эксплуатации, согласовывает с Производителем ПТК и выполняет мероприятия по обеспечению информационной безопасности, направленные на поддержание требуемого уровня защищенности обслуживаемой системы в части настройки штатных механизмов защиты (параметров настройки операционной системы, прикладного и специализированного программного обеспечения, средств антивирусной защиты, оборудование ЛВС ПТК САУГ «КЭР-АТ» и т.д.), включая, но не ограничиваясь:
   1. Проверка и при отсутствии выполнение установки паролей на BIOS автоматизированного рабочего места (далее - АРМ) и серверов для администраторов.
   2. Проверка и при отсутствии выполнение настройки автоматической блокировки экрана на АРМ и серверах, не используемых оперативным персоналом для постоянной работы.
   3. Проверка и при наличии выполнение физического отключения флоппи-дисководов, CD/DVD приводов.
   4. Проверка и при наличии отключение на программном уровне (в BIOS) загрузки со сменных носителей.
   5. Проверка и при наличии отключение на программном уровне (в BIOS) неиспользуемых встроенных сетевых карт, звуковых карт, LPT и СОМ портов.
   6. Проверка и при необходимости отключение на программном уровне (в BIOS) или физически неиспользуемых USB портов.
   7. Проведение анализа и при наличии отключение неиспользуемых системой учетных записей пользователей.
   8. Проведение ревизии открытых сетевых ресурсов и при наличии проведение настройки доступа только авторизированным пользователям.
   9. Проверка установки, настройки и работоспособности антивирусного ПО. При необходимости выполнение обновления сигнатур угроз.
   10. Проведение полной антивирусной проверки компонентов ПТК обслуживаемой системы в режиме обнаружения, исключающем автоматические действия при обнаружении вредоносного кода. В случае обнаружения заражений, принятие мер по локализации заражения и его последствий и, при необходимости, восстановлению функционирования обслуживаемой системы после заражения
   11. Проведение анализа и при отсутствии настройка функции разграничения доступа к файловой системе и функциям операционной системы.
   12. Проведение анализа и при отсутствии настройка политик для учетных записей, не обладающих правами «Администратор» (запуск только разрешенных программ).
   13. Проведение анализа и при отсутствии настройка функции разграничения доступа к ПрК, сетевым ИБП, активному сетевому оборудованию. Установка разрешения на изменение настроек и файлов конфигураций только пользователям с правами «Администратор». Установка запрета на вход в интерфейс без аутентификации или с идентификаторами по умолчанию («root», «admin», «user», «superuser» и т.п.).
   14. Проверка и при наличии отключение на программном уровне неиспользуемых портов на активном сетевом оборудовании (далее - АСО).
   15. Проведение анализа и при наличии отключение неиспользуемых сетевых протоколов. Установка запрета доступа к устройствам АСО по незащищенным протоколам.
   16. Проведение анализа и при отсутствии настройка функции разграничения доступа к системе управления базами данных (далее - СУБД). Установка запрета на вход в интерфейс без аутентификации.
   17. Проведение анализа и при отсутствии настройка функции разграничения доступа к специализированному ПО, позволяющему вносить изменения в конфигурации ПТК АСУТП. Установка запрета на вход в интерфейс без аутентификации.
   18. По результатам письменных рекомендаций производителя, специализированного ПО, установленного в ПТК САУГ «КЭР-АТ», и письменно оформленных результатов тестирования на совместимость в тестовой зоне Подрядчика, установить рекомендуемые обновления безопасности ОС Windows, MS SQL Server, MS Office, опубликованных Microsoft, на момент проведения работ.
   19. По результатам письменных рекомендаций Производителя, специализированного ПО, установленного в ПТК САУГ «КЭР-АТ», и письменно оформленных результатов тестирования на совместимость в тестовой зоне Подрядчика, установить рекомендуемые обновления специализированного ПО на момент проведения работ.
   20. Проверка и при отсутствии выполнение установки паролей на режим администрирования в панели управления операторов, на вход на приборы учета, иные электронные датчики и приборы, имеющие функционал разграничения доступа.
   21. Проверка и при отсутствии опечатывание пломбами (наклейками) корпусов АРМ и серверов, сетевого оборудования.
4. Резервное копирование и восстановление данных.
   1. Исполнитель обязуется снять образы аварийного восстановления АРМ, серверов, баз данных, конфигурации контроллеров и сетевого оборудования до начала и после полного окончания работ на переносной жесткий диск Заказчика.
   2. Выполнение выборочных проверок целостности, сохранности и достаточности резервных копий образов аварийного восстановления путем проведения восстановления данных.
   3. В случае обнаружения ошибок восстановления данных проведение мероприятий по устранению ошибок, а при невозможности их устранения - замена носителей с проведением повторного резервного копирования образов аварийного восстановления обслуживаемой системы.
   4. Фиксация информации о проведенных работах в журнале учета создания и использования резервных копий.
5. Обеспечение ИБ при проведении работ.
   1. При исполнении Договора Подрядчик несет ответственность за соблюдение его работниками и работниками привлеченных им субподрядчиков требований по обеспечению информационной безопасности (ИБ), предусмотренных нормативно-правовыми актами Российской Федерации и внутренними требованиями Заказчика в сфере обеспечения ИБ.
   2. Заказчик принимает следующие меры для обеспечения ИБ при проведении работ персоналом Подрядчика:

* предоставляет Подрядчику для ознакомления организационно-распорядительную документацию Заказчика в сфере обеспечения ИБ, область действия которой распространяется на обслуживаемые Подрядчиком системы и проводимые работы;
* проводит с персоналом Подрядчика вводный инструктаж по обеспечению ИБ, надлежащему и безопасному обращению с обслуживаемыми Подрядчиком системами и их компонентами;
* проводит с персоналом Подрядчика дополнительный инструктаж по обеспечению ИБ в случае внесения изменений в организационно-распорядительную документацию Заказчика в сфере обеспечения ИБ, область действия которой распространяется на обслуживаемые Подрядчиком системы и проводимые работы.
  1. Доступ персонала Подрядчика к оборудованию ПТК обслуживаемой системы допускается только в периоды останова соответствующих энергоблоков.
  2. При выполнении работ Подрядчику запрещено:
* подключать к ПТК ноутбуки, переносные жесткие диски, usb-модемы, внешние CD/DVD-приводы, мобильные телефоны, любые съемные носители информации без их предварительной регистрации и полной антивирусной проверки у инженера по ИБ;
* использовать компоненты программного и аппаратного обеспечения ПТК обслуживаемой системы в неслужебных (личных) целях;
* передавать свои учетные данные другим лицам, не имеющим санкционированный доступ к компонентам обслуживаемой системы;
* записывать учетные данные (логин, пароль) на листках, календарях, корпусах оборудования, в записных книжках, в электронных документах и т.п. и/или хранить в потенциально доступном для ознакомления другими лицами месте;
* сохранять учетные данные (логин, пароль) в полях ввода логина и пароля;
* останавливать или изменять режим работы ПТК обслуживаемой системы, если это не предусмотрено эксплуатационной документацией на ПТК и составом работ, выполняемых в рамках Договора;
* оставлять рабочее место, не активировав временную блокировку экрана;
* оставлять без личного присмотра служебные носители информации.
  1. При выполнении работ Подрядчик обязан:
* строго соблюдать требования по ИБ, установленные в организационно-­распорядительных документах Заказчика;
* использовать технические средства обработки информации, системные и прикладные программные средства ПТК обслуживаемой системы исключительно в служебных целях в соответствии с выполняемыми работами;
* незамедлительно оповещать Заказчика при обнаружении несанкционированных (произведенных с нарушением установленного порядка) изменений в конфигурации программных или аппаратных средств ПТК обслуживаемой системы, отклонений в нормальной работе системных и прикладных программных средств ПТК, выхода из строя, перезагрузки или неустойчивого функционирования аппаратных средств ПТК, предупреждений и ошибок в работе программных и аппаратных средств защиты информации, нарушения целостности пломб (наклеек), нарушения или несоответствия номеров печатей на сетевом оборудовании, серверах и АРМ или иных фактов совершения попыток несанкционированного доступа.
  1. Перед началом выполнения работ по Техническому заданию Подрядчик обязан подписать Соглашение о передаче, неразглашении и охране информации, составляющей коммерческую тайну по форме Заказчика.

1. Мониторинг и контроль качества.
   1. Контроль над исполнением обязательств осуществляется специалистом Заказчика, ответственным за обеспечение ИБ.
   2. Заказчик вправе в любое время проводить проверку соблюдения персоналом Подрядчика требований по обеспечению ИБ, в том числе с привлечением внешних сторон, в целях обеспечения контроля качества проводимых работ и текущего уровня защищенности обслуживаемых Подрядчиком систем.
2. Документация, предъявляемая Заказчику:
   1. План аварийного восстановления ПТК САУГ «КЭР-АТ» в случае реализации инцидентов ИБ Бл.№2.
   2. План аварийного восстановления ПТК САУГ «КЭР-АТ» в случае реализации инцидентов ИБ Бл.№3
   3. Модель угроз информационной безопасности для ПТК САУГ «КЭР-АТ» Бл. №2.
   4. Модель угроз информационной безопасности для ПТК САУГ «КЭР-АТ» Бл.№3. (по согласованию с Заказчиком)
   5. Анализ рисков информационной безопасности ПТК САУГ «КЭР-АТ» Бл.№2. с оценкой потенциального ущерба.
   6. Анализ рисков информационной безопасности ПТК САУГ «КЭР-АТ» Бл.№3. с оценкой потенциального ущерба.
   7. Программа инструментального анализа защищенности при помощи специализированных сканеров безопасности.
   8. Перечень выявленных уязвимостей в ПТК САУГ «КЭР-АТ» Бл.№2 и возможных рисков от их реализации (с предоставлением технических отчетов из сканеров безопасности).
   9. Перечень выявленных уязвимостей в ПТК САУГ «КЭР-АТ» Бл.№3 и возможных рисков от их реализации (с предоставлением технических отчетов из сканеров безопасности).
   10. Перечень выявленных инцидентов по информационной безопасности в ПТК САУГ «КЭР-АТ» Бл.№2 и мер по локализации.
   11. Перечень выявленных инцидентов по информационной безопасности в ПТК САУГ «КЭР-АТ» Бл.№3 и мер по локализации.
   12. Перечень реализованных технических и организационных мероприятий по обеспечению информационной безопасности ПТК САУГ «КЭР-АТ» Бл.№2.
   13. Перечень реализованных технических и организационных мероприятий по обеспечению информационной безопасности ПТК САУГ «КЭР-АТ» Бл.№3.
   14. Перечень установленных обновлений безопасности ОС и прикладного ПО, с письменно оформленными результатами тестирования на совместимость в тестовой зоне Подрядчика.
   15. Перечень установленных обновлений специализированного ПО, с письменно оформленными результатами тестирования на совместимость в тестовой зоне Подрядчика.
   16. Перечень снятых образов аварийного восстановления средств вычислительной техники (СВТ) ПТК САУГ «КЭР-АТ».
   17. Описание настроек штатных механизмов защиты (параметров настройки операционной системы, прикладного и специализированного программного обеспечения, средств антивирусной защиты и т.д.) ПТК САУГ «КЭР-АТ» Бл.№2 и ее компонентов, включая оборудования ЛВС ПТК.
   18. Описание настроек штатных механизмов защиты (параметров настройки операционной системы, прикладного и специализированного программного обеспечения, средств антивирусной защиты и т.д.) ПТК САУГ «КЭР-АТ» Бл. №3 и ее компонентов, включая оборудования ЛВС ПТК.
   19. Перспективные рекомендации по повышению уровня ИБ в программной и аппаратной частях ПТК САУГ «КЭР-АТ».