Технические и организационные требования к защите Рабочей станции удаленного доступа к Информационной системе

1. Общие положения:

Установлены Системой безопасности «Автоматизированной информационной системы оформления воздушных перевозок» АО «Сирена-Трэвел» (далее – АИС ОВП), разработанной в соответствии с Приказом ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования», Приказом ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», Постановлением Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» и Приказом ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

Система безопасности АИС ОВП направлена на обеспечение устойчивого функционирования АИС ОВП при проведении в отношении нее компьютерных атак, а также на предотвращение неправомерного доступа к информации, обрабатываемой в АИС ОВП, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации.

Согласно п. 24 Приказа ФСТЭК России от 21.12.2017 № 235 организационно-распорядительные документы по безопасности значимых объектов разрабатываются исходя из особенностей деятельности Субъекта КИИ на основе требований по безопасности, иных нормативных правовых актов в области обеспечения безопасности критической информационной инфраструктуры и защиты информации.

Особенность деятельности АО «Сирена-Трэвел» заключается в использовании АИС ОВП контрагентами, заключившими договора с АО «Сирена-Трэвел» в отношении Информационных систем (далее - Контрагент), являющихся частью АИС ОВП, со стороны Рабочих станций которых при недостаточной защищенности могут быть реализованы некоторые угрозы безопасности.

В связи с чем настоящие «Технические и организационные требования к защите Рабочей станции удаленного доступа к Информационной системе» АО «Сирена-Трэвел обязательны к выполнению всеми Контрагентами АО «Сирена-Трэвел».

2. Определения:

Информационная система (Система) – Объект КИИ, программно-технический комплекс, входящий в состав «Автоматизированной информационной системы оформления воздушных перевозок», которая на основании Постановления Правительства Российской Федерации от 08.08.2022 № 1393 «Об утверждении требований к автоматизированной информационной системе оформления воздушных перевозок, к базам данных, входящим в ее состав, к информационно-телекоммуникационной сети, обеспечивающей работу указанной автоматизированной информационной системы, к ее оператору, а также мер по защите информации, содержащейся в ней, и порядка ее функционирования и изменении и признании утратившими силу некоторых актов Правительства Российской Федерации» отнесена к объектам критической информационной инфраструктуры (далее по тексту «КИИ») и в соответствии с Постановлением Правительства Российской Федерации от 08.02.2018 № 127 «Об утверждении Правил категорирования объектов КИИ Российской Федерации, а также перечня показателе критериев значимости объектов КИИ Российской Федерации и их значений» является объектом КИИ 1 (первой) категории значимости. Одновременно с этим АИС ОВП является информационной системой персональных данных 3-го уровня защищенности, в отношении которой применяется законодательство в области защиты персональных данных.

Перечень Систем, входящих в состав АИС ОВП / Объекты КИИ:
- ПС / ИС «Леонардо», ЦБА
- Инвенторная система бронирования, Инвенторная система бронирования / Продающий хост, CRS
- АС «Астра»/Astra DCS
- СЭБ-2000
- ПСС ТрансХост

Рабочая станция - Совокупность устройств на стороне Контрагента, включающая видеодисплейное оборудование с центральным процессором или без него, клавиатуру и/или другие устройства ввода, программные средства, дополнительные принадлежности, периферийное оборудование, такие как: компьютер, компьютерный терминал, тонкий клиент и т.п., на которой установлен один или несколько программных / программно-аппаратных комплексов, для взаимодействия с Информационной системой посредством удаленного доступа.

Перечень программных / программно-аппаратных комплексов, взаимодействующих с Объектами КИИ и установленных на Рабочих станциях Контрагента, которые обязательны к защите в соответствии с настоящими требованиями:

- Клиентские приложения ПС / ИС «Леонардо» (терминалы, GUI и другие пользовательские интерфейсы АО «Сирена-Трэвел»)

- Криптический, графический и web терминалы Инвенторной системы бронирования, Инвенторной системы бронирования / Продающего хоста, CRS

- WEB-интерфейс (приложение) MyCharter

- Графические терминалы JXT для доступа в СЭБ-2000 и для ввода тарифной информации в Инвенторную систему бронирования, Инвенторную систему бронирования / Продающий хост, CRS

- Клиентские приложения АС «Астра»/Astra DCS

- Клиентские приложения ПСС ТрансХост – GUI, Мобильное Приложение

3. Требования к защите Рабочей станции:

3.1. К рабочим станциям Контрагентов, с которых осуществляется работа с объектом КИИ Системой, предъявляются повышенные требования защиты информации.

3.2. При удаленной работе в Системе Рабочая станция Контрагента должна быть оснащена сертифицированной ФСТЭК России операционной системой или сертифицированным ФСТЭК России 6 уровня доверия и выше средством от несанкционированного доступа (SecretNet, DallasLock, иное), средством антивирусной защиты (SecretNet. Kaspersky, Dr.Web).

3.3. Контрагент обязан:

3.3.1. Обеспечить следующие настройки парольной политики на защищенной Рабочей станции:
- ✓ применение сочетания букв верхнего и нижнего регистра, цифр и специальных символов;
- ✓ минимальное количество символов – 12;
- ✓ минимальное количество измененных символов при создании нового пароля – 4 символов;
- ✓ максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки - 5 попыток;
- ✓ блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации - 10 минут
- ✓ смена паролей не более чем через 90 дней.

3.3.2. Обеспечить следующие правила управления доступом к защищенной Рабочей

станции:

- ✓ запрет использования одной учетной записи (логина и пароля) разными пользователями,

✓ разделение роли пользователя и администратора (установка программного обеспечения, настройка средств защиты, установленных на Рабочей станции, должна осуществляться администратором и должна быть недоступна пользователю, работа в Системе должна быть недоступна администратору Рабочей станции, но доступна пользователю);

✓ запрет удаленного подключения к защищенной Рабочей станции из сети Интернет;

✓ отсутствие на защищенной Рабочей станции программного обеспечения удаленного доступа (TeamViewer, Ammy admin, подобные);

✓ блокирование защищенной Рабочей стации при ее неиспользовании автоматически через 5 минут или по запросу пользователя;

✓ исключение присутствия посторонних лиц в помещении при включенной Рабочей станции без присмотра.

3.3.3. Обеспечить следующие правила безопасной работы в Системе:

✓ запрет на применение защищенной Рабочей станции для использования сети Интернет, не предусмотренного должностными функциями,

✓ применение Рабочей станции только для выполнения должностных обязанностей, исключение использования в иных целях,

✓ запрет или контроль вывода информации на съемные носители информации, или контроль подключения съемных носителей информации,

✓ обеспечение постоянной работы и обновления антивируса, установленного на Рабочей станции,

✓ блокирование Рабочей станции пользователем при покидании рабочего места.

3.3.4. Обеспечить следующие правила безопасной эксплуатации защищенной Рабочей станции:

✓ настройка межсетевого экранирования, запрещающего доступ к Рабочей станции со стороны других компьютеров в сети,

✓ запрет загрузки операционной системы Рабочей станции с внешнего съемного носителя информации с защитой настроек BIOS паролем, известным только уполномоченному лицу,

✓ проверка защищенной Рабочей станции на уязвимости и их устранение не реже 1 раза в месяц,

✓ проверка состава установленного на Рабочей станции программного обеспечения не реже 1 раза в месяц (должен подтверждаться установленный состав программного обеспечения, отсутствовать избыточное для выполнения функционального назначения Рабочей станции программное обеспечение),

✓ регистрация событий безопасности на Рабочей станции, анализ событий безопасности администратором ежемесячно (при отсутствии SIEM-системы) или автоматизировано (при наличии SIEM).