Акционерное общество
«Национальные туристические технологии»

*info@aontt.ru http: www.aontt.ru*
*ОГРН 5177746199351*
*ИНН/КПП 9705112077 / 774301001*

**УТВЕРЖДАЮ:**
Генеральный директор

_____ /С.Р. Леви/

«22» ноября 2020 года

# ТРЕБОВАНИЯ

**по защите информации, предъявляемые к автоматизированным рабочим места пользователей и сегментам информационных систем туроператоров (турагентов), осуществляющих информационное взаимодействие с государственной информационной системой «Единая информационная система электронных путевок»**

Согласовано ФСТЭК России
№ 240/22/4820 от 19.11.2020

Москва
2020

# Оглавление

## 1. Общие положения

1.1. Настоящие требования разработаны оператором государственной информационной системы «Единая информационной системы электронных путевок» в целях организации защиты информации при ее обработке с использованием автоматизированных рабочих мест и организации информационного взаимодействия с сегментами информационных систем туроператоров (турагентов).

1.2. Требования разработаны в соответствии с нормативно-правовыми документами:

Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

Постановление Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановление Правительства Российской Федерации от 08 июня 2019 г. № 747 «Об утверждении Правил создания и функционирования единой информационной системы электронных путевок, структуры единой информационной системы электронных путевок и условий предоставления содержащейся в единой информационной системы электронных путевок информации»;

Постановление Правительства Российской Федерации от 08.06.2019 № 748 «Об утверждении требований к использованию документов в электронной форме туроператором, турагентом и туристом и (или) иным заказчиком при реализации туристского продукта и Правил обмена информацией в электронной форме между туроператором, турагентом и туристом и (или) иным заказчиком при реализации туристского продукта»;

Приказ ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

Приказ ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСТЭК России от 11 февраля 2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

Модель угроз и модель нарушителя безопасности информации в Единой информационной системе электронных путевок, согласована с ФСБ России № 149/3/2/1-1099 от 27.05.2020 и ФСТЭК России № 240/22/1913 от 06.05.2020.

## 2. Перечень сокращений

| Сокращение | Расшифровка сокращения |
|---|---|
| АРМ | Автоматизированное рабочее место |
| ПДн | Персональные данные |
| НСД | Несанкционированный доступ |
| ИС | Информационная система |
| ЕИС ЭП, Система | Государственная информационная система «Единая информационная система электронных путевок» |
| Сегмент ИС | Сегмент информационной системы внешнего пользователя |
| Оператор | АО «Национальные туристические технологии» |

## 3. Термины и определения

| Термин | Определение термина |
|---|---|
| Информационная обработка персональных данных | обработка персональных данных с помощью средств вычислительной техники |
| Доступ к информации | возможность получения информации и ее использования |
| Информационная система персональных данных | совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств |
| Обработка персональных данных | любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных |
| Персональные данные | любая информация, относящаяся к прямо или косвенно определенному, или определяемому физическому лицу (субъекту персональных данных) |
| Внешние пользователи | участники информационного взаимодействия, осуществляющие подключение автоматизированных рабочих мест к государственной информационной системе «Единая информационная система электронных путевок» |
| Сегмент ИС | Сегмент информационной системы внешнего пользователя, предназначенный для организации информационного взаимодействия с ЕИС ЭП |

## 4. Требования по обеспечению информационной безопасности автоматизированных рабочих мест и сегментов ИС внешних пользователей Системы

Состав настоящих требований основан на совокупности взглядов Оператора Системы на предотвращение актуальных угроз безопасности информации в ЕИС ЭП при организации доступа внешним пользователям к информации, содержащейся в Системе.

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации АРМ и (или) сегмента ИС должны быть направлены на исключение:

а) неправомерных доступа, копирования, предоставления или распространения информации (обеспечение конфиденциальности информации);

б) неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

в) неправомерного блокирования информации (обеспечение доступности информации).

Настоящие требования предъявляются ко всем АРМ и сегментам ИС внешних пользователей, осуществляющих информационное взаимодействие с ЕИС ЭП.

Требования по обеспечению информационной безопасности должны быть реализованы до момента подключения АРМ и (или) сегмента ИС внешнего пользователя к ЕИС ЭП.

### 4.1. Организационные требования к защите информации

Для выполнения требований по защите персональных данных при их обработке в ЕИС ЭП с использованием АРМ или сегмента ИС внешнему пользователю необходимо:

а) в соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ «О персональных данных» (Закон), самостоятельно определить состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных Законом и принятыми в соответствии с ним нормативными правовыми актами, в том числе:

- назначить ответственного за организацию обработки персональных данных;

- издать документы, определяющие политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- применять правовые, организационные и технические меры по обеспечению безопасности персональных данных в соответствии со ст. 19 Закона;

- осуществлять внутренний контроль и (или) аудит соответствия обработки персональных данных Закону и принятым в соответствии с ним нормативным правовым актам, требованиям к защите персональных данных, политик в отношении обработки персональных данных, локальным актам;

- ознакомить работников, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, локальными актами по вопросам обработки персональных данных и (или) организовать обучение указанных работников;

- выполнить иные мероприятия, предусмотренные Законом.

б) в соответствии с постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»:

- организовать режим обеспечения безопасности помещений, в которых размещены АРМ, подключаемые к ЕИС ЭП, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечить сохранность носителей персональных данных;

- утвердить документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым на АРМ подключенных к ЕИС ЭП, необходим для выполнения ими служебных (трудовых) обязанностей.

в) в соответствии с приказом ФСБ России от 10 июля 2014 г. № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»:

- обеспечить режим, препятствующий возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые для организации защищенного соединения с ЕИС ЭП средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения), лиц, не имеющих права доступа в Помещения, который достигается путем оборудования Помещений входными дверьми с замками, обеспечения постоянного закрытия дверей Помещений на замок и их открытия только для санкционированного прохода, а также опечатывания Помещений по окончании рабочего дня или оборудование Помещений соответствующими техническими устройствами, сигнализирующими о несанкционированном

вскрытии Помещений;

- утвердить правила доступа в Помещения в рабочее и нерабочее время, а также в нештатных ситуациях;

- утвердить перечь лиц, имеющих право доступа в Помещения;

- осуществлять хранение съемных машинных носителей персональных данных в сейфах (металлических шкафах), оборудованных внутренними замками с двумя или более дубликатами ключей и приспособлениями для опечатывания замочных скважин или кодовыми замками. В случае если на съемном машинном носителе персональных данных хранятся только персональные данные в зашифрованном с использованием СКЗИ виде, допускается хранение таких носителей вне сейфов (металлических шкафов);

- осуществлять поэкземплярный учет машинных носителей персональных данных, который достигается путем ведения журнала учета носителей персональных данных с использованием регистрационных (заводских) номеров;

- поддерживать в актуальном состоянии документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым на АРМ и (или) сегмента ИС, необходим для выполнения ими служебных (трудовых) обязанностей.

Кроме перечисленных выше требований в сегменте ИС внешнего пользователя с учетом актуальных угроз безопасности персональных данных должны выполняться меры по обеспечению безопасности персональных данных, необходимые для обеспечения, установленного для сегмента ИС уровня защищенности персональных данных[1].

### 4.2. Технические требования к защите информации

Технические меры защиты информации при организации информационного взаимодействия АРМ и (или) сегмента ИС внешних пользователей с ЕИС ЭП достигаются посредством применения внешним пользователем средств защиты информации, в том числе программных (программно-аппаратных) средств в которых реализованы необходимые функции безопасности.

Для обеспечения защиты информации, при осуществлении информационного взаимодействия с ЕИС ЭП в АРМ и (или) сегменте ИС, внешними пользователями должны применяются средства защиты информации, прошедшие оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации в соответствии со статьей 5 Федерального закона от 27 декабря 2002 г. № 184-ФЗ «О техническом регулировании».

---

[1] Утверждены приказом ФСТЭК России от 18.02.2013 г. № 21.

а) Базовый состав средств защиты информации для нейтрализации актуальных угроз безопасности персональных данных при подключении АРМ внешних пользователей к ЕИС ЭП.

К базовому составу средств защиты информации, необходимому для обеспечения информационной безопасности при взаимодействии АРМ внешних пользователей с ЕИС ЭП относятся:

- средство защиты от НСД;
- средство антивирусной защиты;
- средство обнаружения вторжений;
- средства межсетевого экранирования;
- средство криптографической защиты информации.

Данный набор средств минимально необходим, но в отдельных случаях может быть дополнен в соответствии с принятыми внешними пользователями моделями угроз и нарушителя безопасности информации, а также по решению оператора ЕИС ЭП.

4.2.1. Требования к средствам защиты от НСД

Средства защиты АРМ внешних пользователей от НСД должны обеспечивать следующие функции:

- защиту от НСД;
- контроль входа пользователя в систему, в том числе и с использованием дополнительных аппаратных средств защиты;
- сквозную аутентификацию по аппаратным идентификаторам;
- возможность блокировки сессии пользователя по периоду неактивности;
- разграничение доступа пользователей к устройствам и контроль аппаратной конфигурации АРМ, ИС;
- разграничение доступа пользователей к информации;
- контроль утечек информации;
- избирательное (дискреционное) управление доступом:
    - возможность назначения прав доступа на файлы, каталоги, принтеры, устройства;
    - возможность наследования прав доступа для файлов и каталогов;
    - возможность установки индивидуального аудита доступа

для объектов, указания учетных записей пользователей или групп, чей доступ подвергается аудиту;

- полномочное (мандатное) управление доступом:
  - возможность выбора уровня конфиденциальности сессии для пользователя;
  - возможность назначения мандатных меток файлам, каталогам, внешним устройствам, принтерам, сетевым интерфейсам;
  - возможность изменения количества мандатных меток в системе и их названий;
  - контроль потоков конфиденциальной информации в системе;
  - возможность контроля потоков информации в системах терминального доступа при передаче информации между клиентом и сервером по протоколу RDP;
- Контроль вывода конфиденциальных данных на печать;
- Контроль аппаратной конфигурации компьютера и подключаемых устройств;
- поддержка персональных идентификаторов iButton; USB-ключей eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ, iKey 2032, Rutoken/Rutoken S, Rutoken ЭЦП, Rutoken Lite; смарт-карт eToken PRO, eToken PRO (Java), JaCarta PKI, JaCarta ГОСТ, ESMART Token для входа в систему и разблокировки компьютера;
- Возможность ограничить работу сетевого интерфейса заданными уровнями конфиденциальности сессий;
- Возможность блокирования входа в систему локальных пользователей;
- Возможность блокирования операций вторичного входа в систему в процессе работы пользователей;
- Контроль целостности файлов, каталогов, элементов системного реестра;
- Возможность блокировки компьютера при подключении или отключении заданных устройств;
- Возможность обновления ПО с электронной подписью без необходимости корректировки настроек контроля целостности;
- Блокировка запуска при нарушении целостности контролируемых модулей;

- Затирание файлов небольшого размера;
- Затирание данных в файловой системе ReFS;
- Возможность интеграции компьютеров, работающих под управлением ОС GNU/Linux, в общую инфраструктуру управления и мониторинга;
- Регистрацию событий безопасности в журнале;
    - Должна быть возможность формирования отчетов по результатам аудита;
    - Должна быть возможность поиска и фильтрации при работе с данными аудита;
    - Разделение событий НСД на просмотренные и новые.

Используемые средства защиты от НСД должно соответствовать требованиям руководящего документа «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) – не ниже 5 класса защищенности.

4.2.2. Требования к средствам антивирусной защиты

Антивирусные средства защиты АРМ внешних пользователей должны обеспечивать следующие функции:

- автоматическую проверку наличия вредоносных программ по типовым сигнатурам и с помощью эвристического анализа;
- сканирование локальных дисков, подключаемых дисков, отчуждаемых носителей, в том числе по команде и по расписанию;
- удаление вредоносного программного обеспечения и его блокировку (перемещение в «карантин»);
- откат операций удаления программного обеспечения, воспринятого как вредоносное;
- должно обеспечивать кэширование данных сканирования для сокращения времени обнаружения вредоносного программного обеспечения;
- должен обеспечиваться контроль целостности компонентов для защиты модулей продукта, включая антивирусные базы и базы правил от подмены;
- возможность обновления антивирусных баз;
- регистрацию событий безопасности.

Средство антивирусной защиты должно соответствовать требованиями руководящего документа «Требования к средствам антивирусной защиты»

(утвержден приказом ФСТЭК России от 20 марта 2012 г. № 28) не ниже 5-го класса защиты.

4.2.3. Требования к средствам обнаружения вторжений.

В системе обнаружения вторжений (СОВ), установленной на АРМ внешних пользователи должны быть реализованы следующие функции безопасности системы обнаружения вторжений:

- разграничение доступа к управлению системой обнаружения вторжений;
- управление работой системы обнаружения вторжений;
- управление параметрами системы обнаружения вторжений;
- управление установкой обновлений (актуализации) базы решающих правил системы обнаружения вторжений; анализ данных системы обнаружения вторжений; аудит безопасности системы обнаружения вторжений;
- сбор данных о событиях и активности в контролируемой информационной системе; реагирование системы обнаружения вторжений.

В среде, в которой СОВ функционирует, должны быть реализованы следующие функции безопасности среды:

- обеспечение доверенного маршрута;
- обеспечение доверенного канала; обеспечение условий безопасного функционирования; управление атрибутами безопасности.

Средство обнаружения (предотвращения) вторжений должно иметь действующий сертификат ФСТЭК в соответствии с требованиями руководящего документа «Требования к системам обнаружения вторжений», утвержденного приказом ФСТЭК России от 6 декабря 2011г. № 638 не ниже, чем по 5 классу защиты.

4.2.4. Требования к средствам межсетевого экранирования

Средства межсетевого экранирования, должны быть сертифицированы на соответствие Требованиям к межсетевым экранам, утвержденным приказом ФСТЭК России от 9 февраля 2016 г. № 9 и соответствовать Требованиям по безопасности информации, устанавливающим уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденным приказом ФСТЭК России от 2 июня 2020 г. № 76.

4.2.5. Функции средств криптографической защиты информации

Криптографические средства защиты информации (СКЗИ), установленные на АРМ внешних пользователей должны обеспечивать следующие функции:

- реализация TLS-аутентификации (в том числе односторонней) на основе технологии открытых ключей (используются сертификаты квалифицированных открытых ключей электронной подписи формата X.509);
- установление защищенного соединения с сервером на базе протокола HTTPS, в том числе по выделенному TLS-туннелю;
- возможность работы с серверами, поддерживающими протокол TLS v. 1.0, TLS v 1.2;
- хранение ключевой информации в защищенном контейнере;
- проверка сертификатов ключей по списку отозванных сертификатов;
- регистрация событий, связанных с настройкой и функционирование средств защиты АРМ пользователей;
- контроль целостности программного обеспечения, передаваемой и хранимой информации;
- очистка сессионной, включая криптографическую, информацию при разрыве соединения.

СКЗИ при доступе ресурсам ЕИС ЭП должно соответствовать требованиям ГОСТ 28147-89, ГОСТ Р 34.11.-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.10-2012, ГОСТ Р 34.11.2012.

Класс средств криптографической защиты в соответствии с требованиями ФСБ России определяется внешним пользователем с учетом модели угроз безопасности информации, обрабатываемой в подключаемом АРМ.

б) Состав мер по обеспечению безопасности персональных данных при организации информационного взаимодействия сегмента ИС и ЕИС ЭП.

Состав мер по обеспечению безопасности персональных данных при организации информационного взаимодействия сегмента ИС внешнего пользователя и ЕИС ЭП определяется внешними пользователями с учетом требований приказа ФСТЭК России от 11 февраля 2013г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Меры по обеспечению безопасности персональных данных внешними пользователями ЕИС ЭП реализуются в рамках системы защиты персональных данных, создаваемой ими в соответствии с Требованиями к защите

персональных данных при их обработке в информационных системах персональных данных, утвержденными постановлением Правительства Российской Федерации от 1 ноября 2012 г. № 1119, и должны быть направлены на нейтрализацию актуальных угроз безопасности персональных данных.

## 5. Заключительные положения

5.1. После выполнения организационных и технических требований комиссией внешнего пользователя ЕИС ЭП (далее – комиссия) проводится оценка эффективности, принимаемых мер по обеспечению безопасности персональных данных.

5.2. По результатам оценки эффективности, принимаемых мер по обеспечению безопасности персональных данных комиссией составляются отчетные документы:

а) Акт о готовности подключения АРМ к ЕИС ЭП - приложение № 1 – при подключении отдельного АРМ.

б) Заключение по результатам оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных – при подключении сегмента ИС.

5.3. Информация, содержащаяся в документах, указанных в подпунктах а), б), пункта 5.2 должна быть достоверна и не противоречить законодательству Российской Федерации.

5.4. Ответственность за достоверность информации, содержащейся в документах, указанных в подпунктах а), б), пункта 5.2 возлагается на внешнего пользователя.

5.5. Электронные копии заключения или акта прикладываются внешним пользователем к заявке на подключение в процессе регистрации в ЕИС ЭП.

Акционерное общество
«Национальные туристические технологии»

Приложение №1

Утверждаю
Руководитель организации

_____

« » _____ 202__г.

М.П.

# Образец

АКТ
о готовности подключения автоматизированного рабочего места (наименование организации) к ГИС «Единая информационная система электронных путевок»

«___» _____ 202_ года г. _____

Комиссия (наименования организации) в составе:

_____
_____
_____

составила настоящий акт о готовности автоматизированного (ых) рабочего (их) места (т) №_____ к информационному взаимодействию с Единой информационной системной электронных путевок (далее -ЕИС ЭП).

Комиссия подтверждает выполнение в (наименование организации), ИНН_____, требований по информационной безопасности, предъявляемым к автоматизированным рабочим местам пользователей ЕИС ЭП, а именно:

1. Организационные мероприятия

- назначено ответственное лицо за организацию обработки персональных данных в ЕИС ЭП;

- изданы, документы, определяющие политику обработки персональных данных, а также локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;

- применяются правовые, организационные и технические меры по обеспечению безопасности персональных;

- в (наименование организации) осуществляется внутренний контроль и (или) аудит соответствия обработки персональных данных;

- работники (наименование организации), непосредственно осуществляющие обработку персональных данных в ЕИС ЭП, ознакомлены с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, локальными актами по вопросам обработки персональных данных;

- в (наименование организации) организован режим обеспечения безопасности помещений, в которых размещены АРМ, подключаемые к ЕИС ЭП, препятствующий возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;

- обеспечена сохранность носителей персональных данных, используемых для работы в ЕИС ЭП;

- руководителем (наименование организации) утвержден документ, определяющий перечень лиц, доступ которых к персональным данным, обрабатываемым на АРМ подключенных к ЕИС ЭП, необходим для выполнения ими служебных (трудовых) обязанностей;

- обеспечен режим, препятствующий возможности неконтролируемого проникновения или пребывания в помещениях, где размещены используемые для организации защищенного соединения с ЕИС ЭП средства криптографической защиты информации (СКЗИ), хранятся СКЗИ и (или) носители ключевой, аутентифицирующей и парольной информации СКЗИ (далее - Помещения), лиц, не имеющих права доступа в Помещения.

2. Технические мероприятия

На АРМ установлены и настроены в соответствии с эксплуатационными документами средства защиты информации:

| Тип СЗИ | Наименование | Версия/ Исполнение | Сертификат соответствия |
|---|---|---|---|
| Средство защиты от несанкционированного доступа (программное средство) | *Средство защиты информации Secret Net Studio* | *8.5* | *ФСТЭК России №3745 выдан 16.05.2017* |
| Средство обнаружения вторжения (программное средство) | *Средство защиты информации Secret Net Studio* | *8.5* | *ФСТЭК России №3745 выдан 16.05.2017* |
| Средство антивирусной защиты (программное изделие) | *Программное изделие «Kaspersky Endpoint Security для Windows (11.0.0.6499)»* | *11.0.0.6499* | *ФСТЭК России № 4068 выдан 22.01.2019* |
| Средство межсетевого экранирования | *Средство защиты информации Secret Net Studio* | *8.5* | *ФСТЭК России №3745 выдан 16.05.2017* |
| Средство криптографической защиты информации | *ViPNet PKI Client* | *Исполнение 1* | *ФСБ России №СФ/124-3676 выдан 12.04.2019* |

| | | |
|---|---|---|
| (должность) | (роспись) | (инициалы, фамилия) |
| (должность) | (роспись) | (инициалы, фамилия) |
| (должность) | (роспись) | (инициалы, фамилия) |

Акционерное общество
«Национальные туристические технологии»

Приложение № 2

**УТВЕРЖДАЮ**
Директор

« ___» _____ 2020 года
м.п.

Образец

**ЗАКЛЮЧЕНИЕ**
по результатам оценки эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных

**сегмент информационной системы обработки персональных данных** *ООО «Мотылек»*

г. Москва
2020

Акционерное общество
«Национальные туристические технологии»

**1. Общие положения**

В соответствии с пунктом 6 Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденного приказом ФСТЭК России от 18.02.2013 № 21 на объекте информатизации: сегмент информационной системы ***«Информационная система обработки персональных данных туроператора ООО «Мотылек»*** (далее – ИС ПДн), расположенном по адресу: ***г. Москва, ул. Маши Порываевой д. 18, стр. 1, Бизнес центр «Орион», офис № 22*** ***проведена оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных***, которая предусматривала:

- проверку соответствия исходных о сегменте ИС ПДн данных реальным условиям размещения объекта вычислительной техники;
- изучение технологического процесса обработки и хранения персональных данных и определение состава используемых средств вычислительной техники в сегменте ИС ПДн;
- проверку состояния организации работ и выполнения организационно-технических требований по защите информации в сегменте ИС ПДн;
- проверку сегмента ИС ПДн на соответствие требованиям по защите информации от несанкционированного доступа (НСД);
- подготовку отчетной документации, протоколов измерений и заключения по результатам оценки с выводами комиссии о соответствии или несоответствии сегмента ИС ПДн установленным требованиям по безопасности информации.

При проведении испытаний комиссия руководствовалась требованиями следующих нормативных документов:

- "Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)", Гостехкомиссия России, 2001 год;
- "Положение по аттестации объектов информатизации по требованиям безопасности информации", Гостехкомиссия России, 1994 год;
- Руководящий документ "Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации", Гостехкомиссия России, 1998 год;
- ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию".

**2. Результаты оценки соответствия информационной системы организационно-техническим требованиям по защите информации.**

**По результатам оценки соответствия комиссией установлено:**

- представленные документы полностью соответствуют требуемому составу, не содержат противоречивых сведений и оформлены в соответствии с установленными требованиями;
- состав, номенклатура, структура программно-технических средств сегмента ИС ПДн и их размещение соответствуют представленной документации на сегмент ИС ПДн;
- описание технологического процесса обработки, хранения и передачи защищаемой информации в сегменте ИС ПДн соответствует реальному технологическому процессу обработки;
- уровень защищенности персональных данных в сегменте ИС ПДн соответствует представленному на оценку акту определения уровня защищенности персональных от «___» _____ 2020 №_____;
- уровень подготовки пользователей сегмента ИС ПДн обеспечивает выполнение требований безопасности информации;
- требования к помещениям, в которых производится обработка персональных данных, соответствуют руководящим документам.

Проведённый анализ результатов оценки на предмет выполнения **организационно–технических требований** показал, что условия эксплуатации сегмента ИС ПДн **соответствуют**

---

[2] Если информационная система персональных данных состоит из нескольких сегментов, то указываются адреса всех сегментов информационной системы, где размещаются технические средства (ПЭВМ, сервер и т.д.)

требованиям руководящих документов. Подробные результаты приведены в приложении №1.

**3. Результаты контроля выполнения требований по защите информации от несанкционированного доступа.**

- сертификаты на СЗИ от НСД **соответствуют** требованиям безопасности информации на все используемые в сегменте ИС ПДн средства защиты информации от НСД;
- используемые СЗИ от НСД **соответствуют** уровню защищенности персональных данных в ИС ПДн и используемой технологии обработки информации;
- результаты контрольного суммирования программных модулей СЗИ от НСД полностью **соответствуют** значениям, указанным в формуляре средства защиты;
- система антивирусной защиты информации работоспособна, доверенный канал получения обновлений антивирусных баз и механизм обновления в наличии, антивирусные базы на момент проведения контроля актуальны, требования по антивирусному контролю ресурсов сегмента ИС ПДн **выполняются**;
- технологический процесс обработки и хранения персональных данных **соответствует** требованиям безопасности информации;
- описание технологического процесса обработки и хранения персональных данных **соответствует** реальному процессу;

Проведённый анализ результатов контроля организационно-техническим требованиям по защите персональных данных показал её соответствие требованиям РД, предъявляемым к информационным системам персональных данных _____[3] уровня защищённости. Подробные результаты приведены в приложении № 2.

**Выводы по результатам оценки**

Оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных сегменте ИС ПДн показала, что сегмент информационной системы ***«Информационная система обработки персональных данных туроператора ООО «Мотылек»*** удовлетворяет требованиям по безопасности информации, предъявляемым к информационным системам персональных данных ***3 уровня защищённости.***

Приложения:

Приложение 1. «Протокол соответствия сегмента ***информационной системы обработки персональных данных туроператора ООО «Мотылек»*** организационно–техническим требованиям по результатам оценки, № _____ от ___.___.2020;

Приложение 2. «Протокол соответствия сегмента ***информационной системы обработки персональных данных туроператора ООО «Мотылек»*** требованиям по защите информации от несанкционированного доступа», № _____ от ___.___.2020.

**Председатель комиссии:**

_____ *(подпись)*

« ____» _____ 2020 года

**Эксперты комиссии:**

Специалист

_____ *(подпись)*

« ____» _____ 2020 года

Специалист

_____ *(подпись)*

« ____» _____ 2020 года

[3] Указывается уровень защищенности персональных данных в соответствии с постановлением Правительства Российской Федерации от 25.11.2012 № 1119

Акционерное общество
«Национальные туристические технологии»

Приложение №1
к заключению

**Протокол соответствия**
**Сегмента информационной системы персональных данных *ООО «Мотылек»***
**организационно–техническим требованиям по результатам оценки эффективности**

**1. Наименование объекта оценки**

Сегмент информационной системы персональных данных ***ООО «Мотылек»*** (далее – сегмент ИС ПДн).

**2. Цель оценки эффективности**

Определение соответствия принятых в сегменте ИС ПДн мер требованиям безопасности информации.

**3. Порядок проведения испытаний**

**3.1. Организация проведения**

Оценка эффективности принятых мер проводятся комиссией ***ООО «Мотылек»***, назначенной приказом директора от «  »  2020 г. № _____ в соответствии с приказом ФСТЭК России от 18.02.2013 № 21.

**3.2. Перечень использованных нормативных документов и методик испытаний**

1. «Специальные требования и рекомендаций по защите конфиденциальной информации (СТР-К)», Гостехкомиссия России, 2001 год.
2. ГОСТ РО 0043-003-2012 «Защита информации. Аттестация объектов информатизации. Общие положения».
3. ГОСТ РО 0043-004-2013 «Защита информации. Аттестация объектов информатизации. Программы и методики аттестационных испытаний».
4. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», Гостехкомиссия России, 1998 год.
5. ГОСТ Р 51275-99 "Защита информации. Объект информатизации. Факторы, воздействующие на информацию".

**4. Проверка состояния организации работ и выполнения требований безопасности информации**

**4.1. Проверка соответствия содержания представленных документов установленным требованиям**

Комиссии представлены следующие документы:

Акционерное общество
«Национальные туристические технологии»

Таблица №1

| № п/п | Наименование документа | Учётный (инв.) номер, дата документа |
|---|---|---|
| *1.* | *«Перечень сведений конфиденциального характера…»* | |
| *2.* | *Приказ об организации контролируемой зоны объекта информатизации* | |
| *3.* | *«Описание технологического процесса …»* | |
| *4.* | *«Разрешительная система доступа …»* | |
| *5.* | *«Акт определения уровня защищенности персональных данных»* | |
| *6.* | *«Инструкция пользователям …»* | |
| *7.* | *«Инструкция администратору безопасности …»* | |
| *8.* | *«Инструкция по антивирусной защите»* | |
| *9.* | *«Парольная политика…»* | |
| *10.* | *«Технический паспорт …»* | |
| *11.* | *Сертификаты соответствия требованиям по безопасности информации используемых средств защиты информации* | |
| *12.* | *Приказ о назначении администратора безопасности* | |
| *13.* | *Приказ о назначении ответственного по защите информации* | |
| *14.* | *Приказ о назначении комиссии по определению уровня защищенности ИСП Дн* | |

**4.2. Проверка соответствия состава и структуры программно-технических средств сегмента ИС ПДн представленной документации**

Фактический состав технических средств сегмента ИС ПДн соответствует составу, представленному в «Техническом паспорте сегмента ИС ПДн…».

В «Техническом паспорте сегмента ИС ПДн…» представлен следующий состав программных средств ИС ПДн.

Состав программных средств сегмента ИС ПДн:

Таблица №2

| № п/п | Тип программы | Наименование | Место установки |
|---|---|---|---|
| 1. | Операционная система | *Microsoft Windows 10* | *НЖМД Kingston SA400S37240G, зав № 50026B768354C308* |
| 2. | Офисный пакет | *Microsoft Office Standard2019Volume* | |
| 3. | Архиватор | *Архиватор 7-Zip* | |
| 4. | Список настольных инструментов разработчика | *JetBains Toolbox Subscription Certificate* | |

### 4.3. Проверка технологического процесса обработки

Обобщенная технологическая схема сегмента ИС ПДн с существующими и возможными информационными потоками, возможностями доступа к обрабатываемой и передаваемой информации представлена в «Описании технологического процесса обработки информации в…» и на рис. 1.

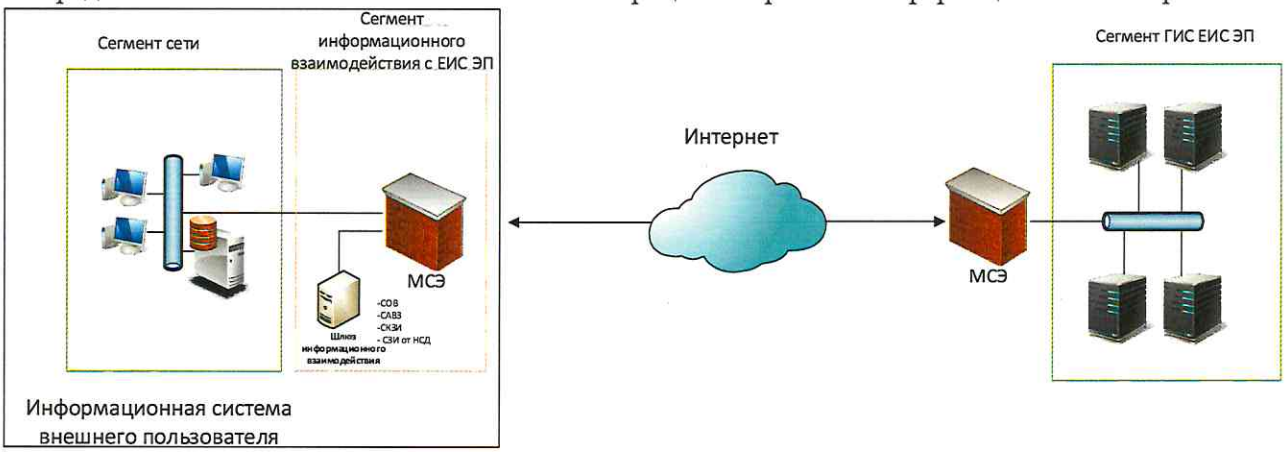


*Рис. 1. Технологическая схема информационного обмена*

### 4.4. Проверка правильности определения уровня защищенности сегмента ИС ПДн

В соответствии с постановлением Правительства Российской Федерации от 01 ноября 2012 г. № 1119 сегмент ИС ПДн является:

- информационной системой, обрабатывающей ***иные категории персональных данных;***
- для сегмента ИС ПДн актуальны угрозы безопасности персональных данных ***3-го типа.***
- в сегменте ИС ПДн обрабатываются персональные данные ***более чем 100 000 субъектов персональных данных***, не являющихся сотрудниками ***ООО «Мотылек».***

В соответствии с «Актом определения уровня защищённости персональных данных сегмента ИС ПДн (название)» для сегмента ИС ПДн установлена необходимость обеспечения 3-го уровня защищенности персональных данных – ***УЗ3,*** что соответствует требованиям нормативно-правовых документов по защите персональных данных.

### 4.5. Проверка уровня подготовки специалистов и распределения ответственности пользователей сегмента ИС ПДн

Опрос пользователей сегмента ИС ПДн на предмет знания требований руководящих документов по безопасности информации показал удовлетворительный уровень подготовки пользователей.

***Список пользователей, допущенных к работе в сегменте ИС ПДн; Приказ о назначении администратора безопасности сегмента ИС ПДн; «Инструкция пользователя сегмента ИС ПДн…»; «Инструкция администратора безопасности сегмента ИСПДн…» доведены работникам под роспись.***

**4.6. Проверка выполнения требований к помещениям, в которых производится обработка персональных данных**

Размещение технических средств сегмента ИС ПДн ***исключает возможность несанкционированного просмотра информации с экранов мониторов, с распечаток принтеров и с других устройств ввода-вывода информации лицами, не имеющими права доступа к обрабатываемой информации.***

***В соответствии с «Планом контролируемой зоны…» помещение находятся в границах контролируемой зоны.***

***Двери помещений оборудованы автоматическими замками. Окна помещений оборудованы защитными жалюзи, исключающими несанкционированный просмотр отображаемой информации.***

**5. Выводы:**

- представленные документы полностью соответствуют требуемому составу, не содержат противоречивых сведений и оформлены в соответствии с установленными требованиями;
- состав, номенклатура, структура программно-технических средств сегмента ИС ПДн и их размещение соответствуют представленной документации;
- описание технологического процесса обработки, хранения и передачи персональных данных соответствует реальному технологическому процессу обработки;
- уровень защищенности персональных данных в сегменте ИС ПДн соответствует представленному на оценку акту от «  »_____ 2020 № _____;
- уровень подготовки пользователей сегмента ИС ПДн обеспечивает выполнение требований безопасности информации;
- требования к помещениям, в которых производится обработка персональных данных, выполняются.

***Проведённый анализ результатов оценки эффективности принятых мер, реализованных в рамках системы защиты персональных данных в сегменте информационной системе персональных данных ООО «Мотылек» показала, что эффективность принятых мер позволяет обеспечить защиту персональных данных в сегменте ИС ПДн, взаимодействующим с ГИС «Единая информационная система электронных путевок» в соответствии с требованиями руководящих документов по 3 уровню защищенности.***

Члены комиссии:

специалист _____
*(подпись)*
«____» _____ 2020 года

специалист _____
*(подпись)*
«____» _____ 2020 года

Акционерное общество
«Национальные туристические технологии»

Приложение 2

**Протокол**
**оценки соответствия сегмента информационной системы персональных данных *ООО «Мотылек»* требованиям по защите информации от несанкционированного доступа**

**1. Наименование объекта оценки**

Сегмент информационной системы персональных данных *ООО «Мотылек»* (далее – сегмент ИС ПДн).

**2. Цель оценки**

Оценка эффективности принятых мер по защите информации от несанкционированного доступа (НСД) для ИС ПДн *3-го уровня* защищенности персональных данных (УЗ3).

**3. Порядок проведения оценки**

**3.1. Организация проведения**

Оценка проводится комиссией оператора информационной системы персональных данных *ООО «Мотылек»*, назначенной приказом генерального директора от «  » _____ 2020 г. № _____.

Основанием для проведения оценки является приказ ФСТЭК России от 18.02.2013 № 21.

**3.2. Перечень использованных нормативных документов и методик испытаний**

1. ГОСТ Р 50739-95 «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования» (введен в действие постановлением Госстандарта России от 09.02.1995г. №49);

2. Руководящий документ. «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (утв. решением Гостехкомиссии России, 1992г.);

3. Руководящий документ «Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей» (утв. решением Гостехкомиссии России от 04.06.1999г. №114);

4. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (утв. решением Гостехкомиссии России от 30.03.1992г.);

**3.3. Перечень используемых средства контроля защищенности от НСД к информации**

Таблица № 1

| № | Используемые средства | Сведения о сертификате, знаке соответствия |
|---|---|---|
| 1. | *Программа фиксации и контроля исходного программного комплекса «ФИКС» версия 2.0.2* | *ФСТЭК России № 1548, действителен до 15.01.2021* |
| 2. | *Средство создания модели системы разграничения доступа «Ревизор 1 XP»* | *ФСТЭК России № 989, действителен до 08.02.2020, лицензия № _____* |
| 3. | *Программа контроля полномочий доступа к информационным ресурсам доступа «Ревизор 2 XP»* | *ФСТЭК России № 990, действителен до 08.02.2020, лицензия № _____* |
| 4. | *Программа поиска и гарантированного уничтожения информации на дисках «Terrier» версия 3.0* | *ФСТЭК России № 1193, действителен до 16.05.2021, лицензия № _____* |

**4. Проверка наличия сертификатов на средства защиты информации, выполнения правил их эксплуатации**

В сегменте ИС ПДн применяются программные средства защиты информации от НСД:

Акционерное общество
«Национальные туристические технологии»

Таблица № 2

| № п/п | Наименование и тип технического средства | Заводской номер защитная марка | Сведения о сертификате | Место установки |
|---|---|---|---|---|
| 1. | *Система защиты информации от несанкционированного доступа Secret Net Studio 8* | | *Сертификат ФСТЭК России № 3745 от 16.05.2017 (действителен до 16.05.2025 г.)* | *АРМ № _____ C:\Program Files\Secret Net Studio* |
| 2. | *Средство антивирусной защиты информации Kaspersky Endpoint Security* | | *Сертификат ФСТЭК России № 3025 от 25.11.2013 г. (действителен до 01.11.2021 г.)* | *АРМ № _____ C:\Program Files\Kaspersky En dpoint Security* |
| 3. | *Средство криптографической защиты информации ViPNet PKI Client , исполнение 1* | | *ФСБ России №СФ/124-3676 выдан 12.04.2019* | *Сервер № _____ C:\Program Files\VipNet* |

Фиксация исходного состояния СЗИ от НСД осуществлялась программой фиксации и контроля исходного программного комплекса *«ФИКС» версия 2.0.2.* Контрольные суммы рассчитывались по алгоритму контрольного суммирования *«Уровень-3»* (Таблица № 3).

Таблица № 3

| № пп | Имя файла | Дата создания | Длина, байт | Длина, строк | КС |
|---|---|---|---|---|---|
| 1 | Admshell.exe | 05.10.18 17-09 | 16062096 | - | 33651224 |
| 2 | BlockIcon.exe | 05.10.18 17-09 | 10977936 | - | e4a2f172 |
| 3 | DlAutP.dll | 05.10.18 17-09 | 7446160 | - | 7fe852a7 |
| 4 | DlClipboard.dll | 05.10.18 17-09 | 4592784 | - | ff8eaadd |
| 5 | DlCloud.dll | 05.10.18 17-09 | 4533392 | - | c50180db |
| 6 | DlCredProv.dll | 05.10.18 17-09 | 6632592 | - | 8e8350e5 |
| 7 | DlCrypt.sys | 05.10.18 15-00 | 47960 | - | 6925559b |
| **итого: файлов - 7** | | | **179610008** | **0** | **d3441694** |
| **ВСЕГО: файлов - 7** | | | **179610008** | **0** | **d3441694** |

Контроль соответствия результатов контрольного суммирования проведен путем сравнения со значениями, указанными в формуляре СЗИ от НСД.

Работоспособность системы антивирусной защиты информации (САВЗ) проверена. Обновление антивирусных баз осуществляется администратором безопасности АС в режиме «офлайн» путем копирования антивирусных баз в автоматизированную систему.

**5. Проверка соответствия описания технологического процесса обработки и хранения защищаемой информации реальному процессу**

Согласно представленному «Описанию технологического процесса …» (уч.№ _____), сегмент ИС ПДн (наименование системы ) предназначен для обработки персональных данных.

Субъекты доступа сегмента ИС ПДн имеют разные уровни полномочий на доступ к персональным данным. Доступ пользователей к работе в сегменте ИС ПДн осуществляется в утверждённом порядке.

**6. Оценка подсистемы управления доступом**

**6.1. Оценка подсистемы идентификации и аутентификации субъектов и объектов доступа**

В рамках оценки подсистемы управления доступом проверке были подвергнуты:

Механизм идентификации и проверки подлинности субъектов доступа при входе в систему.

В ходе оценки выявлено:

Идентификация и проверка подлинности субъектов доступа осуществляется применением СЗИ от НСД при входе в систему по имени пользователя и паролю условно-постоянного действия длинной не

менее **шести** буквенно-цифровых символов. Настройки СЗИ от НСД при задании или смене пароля не позволяют ввести пароль длиной менее шести символов.

Надёжность аутентификации оценивалась возможностью подбора или несанкционированного получения пароля посторонним субъектом доступа в период действия этого пароля с учётом временной блокировки ПЭВМ после превышения, заданного в СЗИ от НСД предела попыток неправильного ввода пароля. После троекратного введения неверного пароля СЗИ от НСД полностью блокируют ПЭВМ (при этом разблокировка осуществляется только спустя 15 минут или администратором безопасности информации сегмента ИСП Дн) и делает запись в журнале регистрации входов/выходов.

Пользователи не имеют доступа к основным органам настройки СЗИ от НСД. Таким образом, возможность изменения прав доступа пользователей к ресурсам сегмента ИС ПДн доступна только для администратора безопасности.

**6.2. Оценка подсистемы регистрации и учета**

При проведении испытаний проверялись:

1) Результаты регистрации и учёта событий на всех этапах работы информационной системы;

2) Порядок регистрации и учёта носителей персональных данных;

В ходе проверки моделировались стандартные процессы обработки информации, после чего просматривались результаты учёта в журнале регистрации событий.

В ходе испытаний выявлено:

1) В информационной системе средствами СЗИ от НСД регистрируются все события, к которым предъявлены требования п. 2.12. Руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа. Классификация автоматизированных систем и требования по защите информации». Параметры регистрации также соответствуют требованиям п. 2.12. Кроме того, при наличии попыток несанкционированного доступа либо нарушениях целостности системы, помимо фиксации данных событий, СЗИ извещает о них администратора безопасности информационной системы.

2) СЗИ от НСД не осуществляет автоматическую регистрацию, учёт и маркировку защищаемых носителей информации. Однако выполнение соответствующих требований обеспечивается организационными мерами.

**6.3. Оценка подсистемы обеспечения целостности**

В ходе испытаний осуществлялись проверки:

1) Обеспечения целостности программных средств СЗИ от НСД, а также неизменности программной среды;

2) Наличия физической охраны сегмента ИС ПДн;

3) Проведения периодического тестирования СЗИ от НСД;

4) Наличия средств восстановления используемой программной среды и приложений, а также СЗИ от НСД.

При оценке выявлено:

1) При загрузке информационной системы средствами СЗИ от НСД осуществляется автоматический контроль целостности CMOS ПЭВМ, загрузочных записей НЖМД, файлов СЗИ от НСД, а также основных конфигурационных файлов операционной системы.

При обнаружении нарушений СЗИ от НСД блокирует вход пользователей и сигнализирует об этом администратору безопасности.

2) Помещения, в которых расположена информационная система, расположены в пределах контролируемой зоны.

3) Производится периодическое тестирование функций СЗИ от НСД при смене персонала и программной среды, предусмотренное инструкциями администратору безопасности.

4) Восстановить СЗИ от НСД возможно при помощи дистрибутива, хранящегося на носителе у администратора безопасности информационной системы.

**6.4. Оценка функционирования СКЗИ**

В ходе испытаний осуществлялись проверки:

1) Обеспечения целостности программных средств СКЗИ, а также неизменности программной среды;

2) Наличия физической охраны СКЗИ и ограничение прав доступа работников;

3) Проведения периодического тестирования СКЗИ;

4) Правильности выбора класса СКЗИ.

При оценке выявлено:

1) При загрузке информационной системы средствами осуществляется автоматический контроль целостности СКЗИ.

2) Помещения, в которых эксплуатируются СКЗИ, расположены в пределах контролируемой зоны.

3) Производится периодическое тестирование функций СКЗИ при смене персонала и программной среды, предусмотренное инструкциями администратору безопасности.

4) Восстановить СКЗИ возможно при помощи дистрибутива, хранящегося на носителе у администратора безопасности информационной системы.

5) Класс СКЗИ определен исходя из актуальности актуальных угроз безопасности информации КС__[4].

**7. Выводы:**

- сертификаты на СЗИ и СКЗИ **соответствуют** требованиям безопасности информации на все используемые в ИС ПДн средства защиты информации;
- используемые СЗИ **соответствуют** уровню защищенности персональных данных в ИСП Дн и используемой технологии обработки информации;
- результаты контрольного суммирования программных модулей СЗИ полностью **соответствуют** значениям, указанным в формулярах средств защиты информации;
- система антивирусной защиты информации работоспособна, доверенный канал получения обновлений антивирусных баз и механизм обновления в наличии, антивирусные базы на момент проведения контроля актуальны, требования по антивирусному контролю ресурсов ИС ПДн **выполняются**;
- применяемые в ИС ПДн СКЗИ соответствуют требованиям приказа ФСБ России от 10.07.2014 № 378, КС___;
- технологический процесс обработки и хранения персональных данных в ИС ПДн **соответствует** требованиям безопасности информации;
- описание технологического процесса обработки и хранения защищаемой информации **соответствует** реальному процессу.

Члены комиссии:

специалист _____
*(подпись)*
«____» _____ 2020 года

специалист _____
*(подпись)*
«____» _____ 2020 года

[4] Определяется в соответствии с требованиями приказа ФСБ России от 10.07.2014 № 378

Акционерное общество
«Национальные туристические технологии»

ПОЯСНЕНИЯ:

В соответствии с Требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденными приказом ФСТЭК России от 18.02.2013 № 17 Оператор ЕИС ЭП – АО «Национальные туристические технологии» осуществляет и обеспечивает управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) (требование УПД.16 состава мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы).

В соответствии с методическим документом «Меры защиты информации в государственных информационных системах», утвержденным ФСТЭК России от 14.02.2014 ) оператор предоставляет доступ к информационной системе авторизованным (уполномоченным) пользователям внешних информационных систем или разрешает обработку, хранение и передачу информации с использованием внешней информационной системы при выполнении следующих условий:

а) при наличии договора (соглашения) об информационном взаимодействии с оператором (обладателем, владельцем) внешней информационной системы;

б) при наличии подтверждения выполнения во внешней информационной системе предъявленных к ней требований о защите информации (наличие аттестата соответствия требованиям по безопасности информации или иного подтверждения).

Правила и процедуры управления взаимодействием с внешними информационными системами регламентируются в организационно распорядительных документах оператора по защите информации.

В соответствии с пунктом 6 Состава и содержания мер, утвержденных приказом ФСТЭК России от 18 февраля 2013 г. № 21, оценка эффективности реализованных в рамках системы защиты персональных данных мер по обеспечению безопасности персональных данных проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц и индивидуальных предпринимателей, имеющих лицензию на осуществление деятельности по технической защите конфиденциальной информации.

Требования к формам и содержанию материалов оценки эффективности приятных оператором персональных данных мер выработаны оператором ЕИС ЭП с учетом обеспечения защиты информации в государственной информационной системе, отнесенной к 2 классу защищенности (К2), в которой обрабатывается информация, содержащая персональные данные с необходимостью обеспечения 3 уровня их защищенности (УЗ3).