ПОРУЧЕНИЕ

Министерства экономического
развития
Российской Федерации от
«04» апреля 2024 г

Исх. №Д08и-10233

Требования к защите информации автоматизированных рабочих мест и информационных (автоматизированных) систем внешних пользователей (туроператоров), подключаемых к государственной информационной системе «Электронная путевка».

СОГЛАСОВАНО

ФСТЭК России

Исх. №240/22/1072

«07» марта 2024 г.

I.Общие положения

1. Настоящий Регламент разработан в соответствии нормативными правовыми актами Российской Федерации:

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

Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных» (Собрание законодательства Российской Федерации);

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»;

Постановлением Правительства Российской Федерации от 6 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;

Постановлением Правительства Российской Федерации от 18 марта 2023 г. № 417 “Об утверждении Правил функционирования единой информационной системы электронных путевок и о признании утратившими силу постановления Правительства Российской Федерации от 8 июня 2019 г. N 747 и пункта 18 изменений, которые вносятся в акты Правительства Российской Федерации, утвержденных постановлением Правительства Российской Федерации от 23 ноября 2020 г. N 1903”;

Постановлением Правительства Российской Федерации от 8 июня 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»;

Приказ ФСБ России от 24 октября 2022 г. № 24 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, с использованием шифровальных (криптографических) средств»;

Национальных стандартов Российской Федерации в области защиты информации и в области создания автоматизированных систем.

2. В Документе устанавливаются требования к обеспечению защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну (далее - информация), от несанкционированного доступа, специальных воздействий на такую информацию (носители информации) в целях ее добывания, уничтожения, искажения или блокирования доступа к ней (далее - защита информации) при обработке указанной информации на автоматизированных рабочих местах и в информационных (автоматизированных) системах внешних пользователей (туроператоров), подключающихся к государственной информационной системе «Электронная путевка».

3. Настоящие Требования являются обязательными при обработке информации на автоматизированных рабочих местах и в информационных (автоматизированных) системах персональных данных внешних пользователей (туроператоров), подключающихся к государственной информационной системе «Электронная путевка».

4. Настоящие Требования предназначены для обладателей информации, содержащей персональные данные, туроператоров - заказчиков, заключивших контракт на создание информационной системы (далее - заказчики) и операторов информационных (автоматизированных) систем туроператоров (далее - операторы).

Лицо, обрабатывающее информацию, содержащее персональные данные, являющуюся информационным ресурсом туроператора, по поручению обладателя информации (заказчика) или оператора и (или) предоставляющее им вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора (далее - уполномоченное лицо), обеспечивает защиту информации в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации. В договоре должна быть предусмотрена обязанность уполномоченного лица обеспечивать защиту информации, являющейся информационным ресурсом, в соответствии с настоящими Требованиями.

5. Защита информации, содержащейся на автоматизированных рабочих местах и в информационных (автоматизированных) системах персональных данных внешних

пользователей (туроператоров) (далее – ИС/АРМ внешнего пользователя), обеспечивается путем выполнения обладателем информации (заказчиком) и (или) оператором требований к организации защиты информации, содержащейся в информационной системе, и требований к мерам защиты информации, содержащейся в информационной системе персональных данных.

II. Требования к организации защиты информации, содержащейся в информационной системе

6. В ИС/АРМ внешних пользователей объектами защиты являются информация, содержащаяся в информационной системе, технические средства (в том числе средства вычислительной техники, машинные носители информации, средства и системы связи и передачи данных, технические средства обработки буквенно-цифровой, графической, видео- и речевой информации), общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

7. Для обеспечения защиты информации, содержащейся в ИС/АРМ внешнего пользователя, оператором назначается структурное подразделение или должностное лицо (работник), ответственные за защиту информации.

8. Для проведения работ по защите информации в ходе создания и эксплуатации ИС/АРМ внешнего пользователя обладателем информации (заказчиком) и оператором в соответствии с законодательством Российской Федерации при необходимости привлекаются организации, имеющие лицензию на деятельность по технической защите конфиденциальной информации в соответствии с Федеральным законом от 4 мая 2011 г. N 99-ФЗ «О лицензировании отдельных видов деятельности».

9. Для обеспечения защиты информации, содержащейся в ИС/АРМ внешнего пользователя, 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. N 184-ФЗ «О техническом регулировании».

10. Защита информации, содержащейся в ИС/АРМ внешнего пользователя, является составной частью работ по созданию и эксплуатации информационной системы и обеспечивается на всех стадиях (этапах) ее создания, в ходе эксплуатации и вывода из эксплуатации путем принятия организационных и технических мер защиты информации, направленных на блокирование (нейтрализацию) угроз безопасности информации в информационной (автоматизированной) системе, в рамках системы (подсистемы) защиты

информации ИС/АРМ внешнего пользователя (далее - система защиты информации ИС/АРМ внешнего пользователя).

Организационные и технические меры защиты информации, реализуемые в рамках системы защиты информации ИС/АРМ внешнего пользователя, в зависимости от информации, содержащейся в информационной системе, целей создания информационной системы и задач, решаемых этой информационной системой, должны быть направлены на исключение:

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

неправомерных уничтожения или модифицирования информации (обеспечение целостности информации);

неправомерного блокирования информации (обеспечение доступности информации).

11. Для обеспечения защиты информации, содержащейся в ИС/АРМ внешнего пользователя, проводятся следующие мероприятия:

формирование требований к защите информации, содержащейся в ИС/АРМ внешнего пользователя;

разработка системы защиты информации ИС/АРМ внешнего пользователя;

внедрение системы защиты информации ИС/АРМ внешнего пользователя;

аттестация ИС/АРМ внешнего пользователя по требованиям защиты информации (далее - аттестация информационной системы) и ввод ее в действие;

обеспечение защиты информации в ходе эксплуатации аттестованной ИС/АРМ внешнего пользователя;

обеспечение защиты информации при выводе из эксплуатации аттестованной ИС/АРМ внешнего пользователя или после принятия решения об окончании обработки информации.

12. Формирование требований к защите информации, содержащейся в информационной системе, осуществляется с учетом ГОСТ Р 51583 "Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения" (далее - ГОСТ Р 51583) и ГОСТ Р 51624 "Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования" (далее - ГОСТ Р 51624) и в том числе включает:

принятие решения о необходимости защиты информации, содержащейся в информационной системе;

классификацию информационной системы по требованиям защиты информации (далее - классификация информационной системы);

определение угроз безопасности информации, реализация которых может привести к

нарушению безопасности информации в ИС/АРМ внешнего пользователя, и разработку на их основе модели угроз безопасности информации;

определение требований к системе защиты информации ИС/АРМ внешнего пользователя не ниже третьего класса защищенности информационных систем (К3).

13. Принятие решения о необходимости защиты информации, содержащейся в ИС/АРМ внешнего пользователя, оформляется внешними пользователями ГИС «Электронная путевка» в виде приказа по организации.

14. Классификация ИС/АРМ внешнего пользователя по требованиям защиты информации (далее - классификация информационной системы), проводится с учетом требований безопасности информации, предъявляемых к информационным системам персональных данных не ниже третьего уровня защищенности персональных данных, содержащихся в системе и третьего класса защищенности информационных систем (К3).

Класс защищенности ИС/АРМ внешнего пользователя подлежит пересмотру при изменении масштаба информационной системы или значимости обрабатываемой в ней информации.

Результаты классификации ИС/АРМ внешнего пользователя оформляются актом классификации.

Класс защищенности ИС/АРМ внешнего пользователя, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, не должен быть выше класса защищенности информационно-телекоммуникационной инфраструктуры центра обработки данных.

15. Угрозы безопасности информации определяются по результатам оценки возможностей (потенциала) внешних и внутренних нарушителей, анализа возможных уязвимостей ИС/АРМ внешнего пользователя, возможных способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации (конфиденциальности, целостности, доступности).

При определении угроз безопасности информации в информационной системе, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, должны учитываться угрозы безопасности информации, актуальные для информационно-телекоммуникационной инфраструктуры центра обработки данных.

По результатам оценки разрабатывается Модель угроз безопасности информации ИС/АРМ внешнего пользователя, которая должна содержать описание информационной системы и ее структурно-функциональных характеристик, а также описание угроз безопасности информации, включающее описание возможностей нарушителей (модель

нарушителя), возможных уязвимостей информационной системы, способов реализации угроз безопасности информации и последствий от нарушения свойств безопасности информации.

16. Требования к системе защиты информации ИС/АРМ внешнего пользователя включаются в техническое задание на создание информационной системы и (или) техническое задание (частное техническое задание) на создание системы защиты информации информационной системы, разрабатываемые с учетом ГОСТ 34.602, ГОСТ Р 51583 и ГОСТ Р 51624, и, должны в том числе содержать:

цель и задачи обеспечения защиты информации в информационной системе;

класс защищенности информационной системы;

перечень нормативных правовых актов, методических документов и национальных стандартов, которым должна соответствовать информационная система;

перечень объектов защиты информационной системы;

требования к мерам и средствам защиты информации, применяемым в информационной системе;

стадии (этапы работ) создания системы защиты информационной системы;

требования к поставляемым техническим средствам, программному обеспечению, средствам защиты информации;

функции заказчика и оператора по обеспечению защиты информации в информационной системе;

требования к защите средств и систем, обеспечивающих функционирование информационной системы (обеспечивающей инфраструктуре);

требования к защите информации при информационном взаимодействии с иными информационными системами и информационно-телекоммуникационными сетями, в том числе с информационными системами уполномоченного лица, а также при применении вычислительных ресурсов (мощностей), предоставляемых уполномоченным лицом для обработки информации.

В случае создания ИС/АРМ внешнего пользователя, функционирование которой предполагается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных, дополнительно определяются требования по защите информации, подлежащие реализации в информационно-телекоммуникационной инфраструктуре центра обработки данных.

17. Разработка системы защиты информации ИС/АРМ внешнего пользователя организуется обладателем информации (туроператором) заказчиком.

Разработка системы защиты информации информационной системы осуществляется в соответствии с техническим заданием на создание информационной системы и (или)

техническим заданием (частным техническим заданием) на создание системы защиты информации информационной системы с учетом ГОСТ 34.601 "Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания" (далее - ГОСТ 34.601), ГОСТ Р 51583 и ГОСТ Р 51624 и в том числе включает:

проектирование системы защиты информации ИС/АРМ внешнего пользователя;

разработку эксплуатационной документации на систему защиты информации ИС/АРМ внешнего пользователя;

макетирование и тестирование системы защиты информации информационной системы (при необходимости).

18. Внедрение системы защиты информации ИС/АРМ внешнего пользователя организуется обладателем информации (туроператором) заказчиком.

Внедрение системы защиты информации ИС/АРМ внешнего пользователя осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает:

установку и настройку средств защиты информации в информационной системе;

разработку документов, определяющих правила и процедуры, реализуемые оператором для обеспечения защиты информации в ИС/АРМ внешнего пользователя в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации);

внедрение организационных мер защиты информации;

предварительные испытания системы защиты информации ИС/АРМ внешнего пользователя;

опытную эксплуатацию системы защиты информации ИС/АРМ внешнего пользователя;

анализ уязвимостей информационной системы и принятие мер защиты информации по их устранению;

приемочные испытания системы защиты информации ИС/АРМ внешнего пользователя.

19. Установка и настройка средств защиты информации в ИС/АРМ внешнего пользователя должна проводиться в соответствии с эксплуатационной документацией на систему защиты информации информационной системы и документацией на средства защиты информации. Форма акта установки / настройки СЗИ приведена в Приложении 1.

20. Разрабатываемые организационно-распорядительные документы по защите информации должны определять правила и процедуры:

управления (администрирования) системой защиты информации ИС/АРМ внешнего пользователя;

выявления инцидентов (одного события или группы событий), которые могут привести к сбоям или нарушению функционирования ИС/АРМ внешнего пользователя и (или) к возникновению угроз безопасности информации (далее - инциденты), и реагирования на них;

управления конфигурацией аттестованной информационной системы и системы защиты информации ИС/АРМ внешнего пользователя;

контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ИС/АРМ внешнего пользователя;

защиты информации при выводе из эксплуатации ИС/АРМ внешнего пользователя или после принятия решения об окончании обработки информации.

Перечень организационно-распорядительных документов, разрабатываемых туроператорами приведен в Приложение 2.

21. Предварительные испытания системы защиты информации ИС/АРМ внешнего пользователя проводятся с учетом ГОСТ 34.603 "Информационная технология. Виды испытаний автоматизированных систем" (далее - ГОСТ 34.603) и включают проверку работоспособности системы защиты информации информационной системы, а также принятие решения о возможности опытной эксплуатации системы защиты информации ИС/АРМ внешнего пользователя.

22. Опытная эксплуатация системы защиты информации ИС/АРМ внешнего пользователя проводится с учетом ГОСТ 34.603 и включает проверку функционирования системы защиты информации ИС/АРМ внешнего пользователя, в том числе реализованных мер защиты информации, а также готовность пользователей и администраторов к эксплуатации системы защиты информации ИС/АРМ внешнего пользователя.

23. Анализ уязвимостей ИС/АРМ внешнего пользователя проводится в целях оценки возможности преодоления нарушителем системы защиты информации ИС/АРМ внешнего пользователя и предотвращения реализации угроз безопасности информации.

24. Приемочные испытания системы защиты информации ИС/АРМ внешнего пользователя проводятся с учетом ГОСТ 34.603 и включают проверку выполнения требований к системе защиты информации ИС/АРМ внешнего пользователя в соответствии с техническим заданием на создание информационной системы и (или) техническим заданием (частным техническим заданием) на создание системы защиты информации ИС/АРМ внешнего пользователя.

III.Аттестация информационной системы и ввод ее в действие

25. Аттестация ИС/АРМ внешнего пользователя организуется обладателем информации (туроператором - заказчиком) или оператором и включает проведение комплекса организационных и технических мероприятий (аттестационных испытаний), в результате которых подтверждается соответствие системы защиты информации ИС/АРМ внешнего пользователя требованиям приказа ФСТЭК России приказа ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в соответствии с установленным третьем классом защищенности информационных систем (К3) и требования Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

26. Проведение аттестационных испытаний ИС/АРМ внешнего пользователя должностными лицами (работниками), осуществляющими проектирование и (или) внедрение системы защиты информации информационной системы, не допускается.

27. В качестве исходных данных, необходимых для аттестации ИС/АРМ внешнего пользователя, используются модель угроз безопасности информации, акт классификации ИС/АРМ внешнего пользователя, техническое задание на создание ИС/АРМ внешнего пользователя и (или) техническое задание (частное техническое задание) на создание системы защиты информации ИС/АРМ внешнего пользователя, проектная и эксплуатационная документация на систему защиты информации ИС/АРМ внешнего пользователя, организационно-распорядительные документы по защите информации, результаты анализа уязвимостей ИС/АРМ внешнего пользователя, материалы предварительных и приемочных испытаний системы защиты информации ИС/АРМ внешнего пользователя, а также иные документы, разрабатываемые в соответствии с требованиями приказа ФСТЭК России приказа ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в соответствии с установленным третьем классом защищенности информационных систем (К3) и требованиями Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

28. Аттестация ИС/АРМ внешнего пользователя организуется в соответствии с Порядком организации и проведения работ по аттестации объектов информатизации на соответствие требованиям о защите информации ограниченного доступа, не составляющей

государственную тайну, утвержденным приказом ФСТЭК России от 29 апреля 2021 г. № 77.

Для проведения аттестационных испытаний владелец ИС/АРМ внешнего пользователя привлекает организацию, имеющую лицензию на деятельность по технической защите конфиденциальной информации (с правом проведения работ и оказания услуг по аттестации (аттестационным испытаниям) на соответствие требованиям по защите информации), выданную ФСТЭК России в соответствии с Положением о лицензировании деятельности по технической защите конфиденциальной информации, утвержденным постановлением Правительства Российской Федерации от 3 февраля 2012 г. № 79.

Допускается аттестация ИС/АРМ внешнего пользователя на основе результатов аттестационных испытаний выделенного набора сегментов информационной системы, реализующих полную технологию обработки информации.

В этом случае распространение аттестата соответствия на другие сегменты ИС/АРМ внешнего пользователя осуществляется при условии их соответствия сегментам информационной системы, прошедшим аттестационные испытания.

Сегмент считается соответствующим сегменту ИС/АРМ внешнего пользователя, в отношении которого были проведены аттестационные испытания, если для указанных сегментов установлены одинаковые классы защищенности, угрозы безопасности информации, реализованы одинаковые проектные решения по информационной системе и ее системе защиты информации.

Соответствие сегмента, на который распространяется аттестат соответствия, сегменту ИС/АРМ внешнего пользователя, в отношении которого были проведены аттестационные испытания, подтверждается в ходе приемочных испытаний информационной системы или сегментов ИС/АРМ внешнего пользователя.

В сегментах информационной системы, на которые распространяется аттестат соответствия, оператором обеспечивается соблюдение эксплуатационной документации на систему защиты информации ИС/АРМ внешнего пользователя и организационно-распорядительных документов по защите информации.

Особенности аттестации ИС/АРМ внешнего пользователя на основе результатов аттестационных испытаний выделенного набора ее сегментов, а также условия и порядок распространения аттестата соответствия на другие сегменты информационной системы определяются в программе и методиках аттестационных испытаний, заключении и аттестате соответствия.

Ввод в действие ИС/АРМ внешнего пользователя осуществляется в соответствии с законодательством Российской Федерации об информации, информационных технологиях и о защите информации и с учетом ГОСТ 34.601 и при наличии аттестата соответствия.

29. ИС/АРМ внешнего пользователя, функционирующие на базе общей инфраструктуры (средств вычислительной техники, серверов телекоммуникационного оборудования) в качестве прикладных сервисов, подлежат аттестации в составе указанной инфраструктуры.

В случае если ИС/АРМ внешнего пользователя создается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных уполномоченного лица, такая инфраструктура центра обработки данных должна быть аттестована на соответствие требованиям приказа ФСТЭК России приказа ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

IV.Обеспечение защиты информации в ходе эксплуатации аттестованной информационной системы

30. Обеспечение защиты информации в ходе эксплуатации ИС/АРМ внешнего пользователя должно осуществляться оператором в соответствии с эксплуатационной документацией и организационно-распорядительными документами по защите информации и включать следующие мероприятия:

планирование мероприятий по защите информации в ИС/АРМ внешнего пользователя;

анализ угроз безопасности информации в ИС/АРМ внешнего пользователя;

управление (администрирование) системой защиты информации ИС/АРМ внешнего пользователя;

управление конфигурацией информационной системы и ее системой защиты информации;

реагирование на инциденты;

информирование и обучение персонала ИС/АРМ внешнего пользователя;

контроль за обеспечением уровня защищенности информации, содержащейся в ИС/АРМ внешнего пользователя.

31. В ходе планирования мероприятий по защите информации в информационной системе осуществляются:

определение лиц, ответственных за планирование и контроль мероприятий по защите информации в ИС/АРМ внешнего пользователя;

определение лиц, ответственных за выявление инцидентов и реагирование на них;

разработка, утверждение и актуализация плана мероприятий по защите информации в ИС/АРМ внешнего пользователя;

определение порядка контроля выполнения мероприятий по обеспечению защиты информации в ИС/АРМ внешнего пользователя, предусмотренных утвержденным планом.

План мероприятий по защите информации в ИС/АРМ внешнего пользователя утверждается вместе с правовым актом о вводе информационной системы в эксплуатацию.

Контроль выполнения мероприятий, предусмотренных планом мероприятий по защите информации в ИС/АРМ внешнего пользователя, осуществляется в сроки, определенные указанным планом.

32. В ходе анализа угроз безопасности информации в ИС/АРМ внешнего пользователя в ходе ее эксплуатации осуществляются:

выявление, анализ и устранение уязвимостей ИС/АРМ внешнего пользователя;

анализ изменения угроз безопасности информации в ИС/АРМ внешнего пользователя;

оценка возможных последствий реализации угроз безопасности информации в ИС/АРМ внешнего пользователя.

Периодичность проведения указанных работ определяется оператором в организационно-распорядительных документах по защите информации.

33. В ходе управления (администрирования) системой защиты информации ИС/АРМ внешнего пользователя осуществляются:

определение лиц, ответственных за управление (администрирование) системой защиты информации ИС/АРМ внешнего пользователя;

управление учетными записями пользователей и поддержание в актуальном состоянии правил разграничения доступа в ИС/АРМ внешнего пользователя;

управление средствами защиты информации ИС/АРМ внешнего пользователя;

управление обновлениями программных и программно-аппаратных средств, в том числе средств защиты информации, с учетом особенностей функционирования ИС/АРМ внешнего пользователя;

централизованное управление системой защиты информации ИС/АРМ внешнего пользователя (при необходимости);

мониторинг и анализ зарегистрированных событий в информационной системе, связанных с обеспечением безопасности (далее - события безопасности);

обеспечение функционирования системы защиты информации ИС/АРМ внешнего пользователя в ходе ее эксплуатации, включая ведение эксплуатационной документации и организационно-распорядительных документов по защите информации.

34. В ходе управления конфигурацией информационной системы и ее системы защиты информации осуществляются:

определение лиц, которым разрешены действия по внесению изменений в

конфигурацию информационной системы и ее системы защиты информации, и их полномочий;

определение компонентов информационной системы и ее системы защиты информации, подлежащих изменению в рамках управления конфигурацией (идентификация объектов управления конфигурацией): программно-аппаратные, программные средства, включая средства защиты информации, их настройки и программный код, эксплуатационная документация, интерфейсы, файлы и иные компоненты, подлежащие изменению и контролю;

управление изменениями информационной системы и ее системы защиты информации: разработка параметров настройки, обеспечивающих защиту информации, анализ потенциального воздействия планируемых изменений на обеспечение защиты информации, санкционирование внесения изменений в информационную систему и ее систему защиты информации, документирование действий по внесению изменений в информационную систему и сохранение данных об изменениях конфигурации;

контроль действий по внесению изменений в информационную систему и ее систему защиты информации.

35. В ходе реагирования на инциденты осуществляются:

обнаружение и идентификация инцидентов, в том числе отказов в обслуживании, сбоев (перезагрузок) в работе технических средств, программного обеспечения и средств защиты информации, нарушений правил разграничения доступа, неправомерных действий по сбору информации, внедрений вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

своевременное информирование пользователями и администраторами лиц, ответственных за выявление инцидентов и реагирование на них, о возникновении инцидентов в информационной системе;

анализ инцидентов, в том числе определение источников и причин возникновения инцидентов, а также оценка их последствий;

планирование и принятие мер по устранению инцидентов, в том числе по восстановлению информационной системы и ее сегментов в случае отказа в обслуживании или после сбоев, устранению последствий нарушения правил разграничения доступа, неправомерных действий по сбору информации, внедрения вредоносных компьютерных программ (вирусов) и иных событий, приводящих к возникновению инцидентов;

планирование и принятие мер по предотвращению повторного возникновения инцидентов.

36. В ходе информирования и обучения персонала информационной системы осуществляются:

информирование персонала информационной системы о появлении актуальных угрозах безопасности информации, о правилах безопасной эксплуатации информационной системы;

доведение до персонала информационной системы требований по защите информации, а также положений организационно-распорядительных документов по защите информации с учетом внесенных в них изменений;

обучение персонала информационной системы правилам эксплуатации отдельных средств защиты информации;

проведение практических занятий и тренировок с персоналом информационной системы по блокированию угроз безопасности информации и реагированию на инциденты;

контроль осведомленности персонала информационной системы об угрозах безопасности информации и уровня знаний персонала по вопросам обеспечения защиты информации.

Периодичность проведения практических занятий и тренировок с персоналом, мероприятий по обучению персонала и контролю осведомленности персонала устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационной системы, но не реже 1 раза в два года.

37. В ходе контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, осуществляются:

контроль (анализ) защищенности информации с учетом особенностей функционирования информационной системы;

анализ и оценка функционирования информационной системы и ее системы защиты информации, включая анализ и устранение уязвимостей и иных недостатков в функционировании системы защиты информации информационной системы;

документирование процедур и результатов контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе;

принятие решения по результатам контроля за обеспечением уровня защищенности информации, содержащейся в информационной системе, о необходимости доработки (модернизации) ее системы защиты информации.

Контроль за обеспечением уровня защищенности информации, содержащейся в информационной системе, проводится оператором самостоятельно и (или) с привлечением организации, имеющей лицензию на деятельность по технической защите конфиденциальной информации.

Периодичность проведения контроля за обеспечением уровня защищенности

информации, содержащейся в информационных системах 2 и 3 классов защищенности, устанавливается оператором в организационно-распорядительных документах по защите информации с учетом особенностей функционирования информационных систем, но не реже 1 раза в два года.

V.Организационные требования, предъявляемые к информационным (автоматизированным) системам внешних пользователей (туроператоров), подключаемых к государственной информационной системе «Электронная путевка»

38. Организация подключения ИС/АРМ внешних пользователей к государственной информационной системе «Электронная путевка» осуществляется в соответствии с:

− требованиями нормативно-правовых актов Российской Федерации в сфере защиты информации;

− требованиями нормативно-технических и методических документов уполномоченных органов исполнительной власти Российской Федерации в сфере обеспечения безопасности информации (федеральная служба по техническому и экспортному контролю России (далее – ФСТЭК России), федеральная служба безопасности России (далее – ФСБ России);

− настоящими Требованиями.

39. Для организации взаимодействия ИС/АРМ внешних пользователей с ГИС «Электронная путевка», подключаемые ИС/АРМ внешних пользователей должны соответствовать требованиям приказа ФСТЭК России от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в соответствии с установленным третьем классом защищенности информационных систем (К3) и требования Постановления Правительства Российской Федерации от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных».

40. Для организации взаимодействия ИС/АРМ внешних пользователей с ГИС «Электронная путевка», подключаемая ИС должна иметь действующий аттестат, подтверждающий ее соответствие требованиям безопасности информации, предъявляемым к государственным информационным системам третьего класса защищенности, а также действующий аттестат (результаты проведенной оценки эффективности), подтверждающий

соответствие требованиям безопасности информации, предъявляемым к информационным системам персональных данных третьего уровня защищенности.

41. Внешним пользователям необходимо предоставить в адрес эксплуатирующей ГИС «Электронная путевка» Организации скан-копии документов, подтверждающих наличие необходимых средств защиты и выполнение условий согласно настоящим Требованиям в составе:

– технические паспорта на информационные системы;

– действующие аттестаты соответствия ИС/АРМ внешних пользователей туроператоров требованиям по безопасности информации;

– акты установки/настройки средств защиты информации.

По запросу эксплуатирующей ГИС «Электронная путевка» Организации предоставляются иные сведения, подтверждающие выполнение условий согласно настоящим Требованиям.

42. В случае проведения повторной аттестации (оценки эффективности) ИС, подключенной к ГИС, владелец ИС обязан предоставить в эксплуатирующую ГИС «Электронная путевка» Организацию скан-копию действующего аттестата соответствия (результаты проведенной оценки эффективности) в течение пяти рабочих дней с даты выдачи, а так же сведения о внесенных изменениях, повлекших за собой необходимость проведения повторной аттестации.

VI. Требования к мерам защите информации, предъявляемые к информационным (автоматизированным) системам внешних пользователей (туроператоров), подключаемых к государственной информационной системе «Электронная путевка»

43. Организационные и технические меры защиты информации, реализуемые в ИС/АРМ внешних пользователей в рамках ее системы защиты информации, в зависимости от угроз безопасности информации, используемых информационных технологий и структурно-функциональных характеристик ИС/АРМ внешних пользователей должны обеспечивать:

идентификацию и аутентификацию субъектов доступа и объектов доступа;

управление доступом субъектов доступа к объектам доступа;

ограничение программной среды;

защиту машинных носителей информации;

регистрацию событий безопасности;

антивирусную защиту;

обнаружение (предотвращение) вторжений;

контроль (анализ) защищенности информации;

целостность информационной системы и информации;

доступность информации;

защиту среды виртуализации;

защиту технических средств;

защиту информационной системы, ее средств, систем связи и передачи данных.

Состав мер защиты информации и их базовые наборы для соответствующих классов защищенности информационных систем приведены в приложении N 2 к Требованиям о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах, утвержденных приказом ФСТЭК России от 11 февраля 2013г. № 17.

44. Меры по идентификации и аутентификации субъектов доступа и объектов доступа должны обеспечивать присвоение субъектам и объектам доступа уникального признака (идентификатора), сравнение предъявляемого субъектом (объектом) доступа идентификатора с перечнем присвоенных идентификаторов, а также проверку принадлежности субъекту (объекту) доступа предъявленного им идентификатора (подтверждение подлинности).

45. Меры по управлению доступом субъектов доступа к объектам доступа должны обеспечивать управление правами и привилегиями субъектов доступа, разграничение доступа субъектов доступа к объектам доступа на основе совокупности установленных в информационной системе правил разграничения доступа, а также обеспечивать контроль соблюдения этих правил.

46. Меры по ограничению программной среды должны обеспечивать установку и (или) запуск только разрешенного к использованию в информационной системе программного обеспечения или исключать возможность установки и (или) запуска запрещенного к использованию в информационной системе программного обеспечения.

47. Меры по защите машинных носителей информации (средства обработки (хранения) информации, съемные машинные носители информации) должны исключать возможность несанкционированного доступа к машинным носителям и хранящейся на них информации, а также несанкционированное использование съемных машинных носителей информации.

48. Меры по регистрации событий безопасности должны обеспечивать сбор, запись, хранение и защиту информации о событиях безопасности в информационной системе, а также

возможность просмотра и анализа информации о таких событиях и реагирование на них.

49. Меры по антивирусной защите должны обеспечивать обнаружение в информационной системе компьютерных программ либо иной компьютерной информации, предназначенной для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирование на обнаружение этих программ и информации.

50. Меры по обнаружению (предотвращению) вторжений должны обеспечивать обнаружение действий в информационной системе, направленных на преднамеренный несанкционированный доступ к информации, специальные воздействия на информационную систему и (или) информацию в целях ее добывания, уничтожения, искажения и блокирования доступа к информации, а также реагирование на эти действия.

51. Меры по контролю (анализу) защищенности информации должны обеспечивать контроль уровня защищенности информации, содержащейся в информационной системе, путем проведения мероприятий по анализу защищенности информационной системы и тестированию ее системы защиты информации.

52. Меры по обеспечению целостности информационной системы и информации должны обеспечивать обнаружение фактов несанкционированного нарушения целостности информационной системы и содержащейся в ней информации, а также возможность восстановления информационной системы и содержащейся в ней информации.

53. Меры по обеспечению доступности информации должны обеспечивать авторизованный доступ пользователей, имеющих права по такому доступу, к информации, содержащейся в информационной системе, в штатном режиме функционирования информационной системы.

54. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

55. Меры по защите технических средств должны исключать несанкционированный доступ к стационарным техническим средствам, обрабатывающим информацию, средствам, обеспечивающим функционирование информационной системы (далее - средства

обеспечения функционирования), и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий, а также защиту информации, представленной в виде информативных электрических сигналов и физических полей.

56. Меры по защите информационной системы, ее средств, систем связи и передачи данных должны обеспечивать защиту информации при взаимодействии информационной системы или ее отдельных сегментов с иными информационными системами и информационно-телекоммуникационными сетями посредством применения архитектуры информационной системы, проектных решений по ее системе защиты информации, направленных на обеспечение защиты информации.

57. Меры защиты информации выбираются и реализуются в информационной системе в рамках ее системы защиты информации с учетом угроз безопасности информации применительно ко всем объектам и субъектам доступа на аппаратном, системном, прикладном и сетевом уровнях, в том числе в среде виртуализации и облачных вычислений.

58. Организационные меры и средства защиты информации, применяемые в информационной системе, должны обеспечивать в ИС/АРМ внешних пользователей не ниже 3 класса защищенности - защиту от угроз безопасности информации, связанных с действиями нарушителей с потенциалом не ниже базового.

59. Технические меры защиты информации реализуются посредством применения средств защиты информации, в том числе программных (программно-аппаратных) средств, в которых они реализованы, имеющих необходимые функции безопасности. При этом в ИС/АРМ внешних пользователей 3 класса защищенности применяются средства защиты информации 6 класса, а также средства вычислительной техники не ниже 5 класса.

В ИС/АРМ внешних пользователей применяются средства защиты информации, сертифицированные на соответствие обязательным требованиям по безопасности информации, установленным ФСТЭК России, или на соответствие требованиям, указанным в технических условиях (заданиях по безопасности).

60. Базовый состав средств защиты информации для нейтрализации актуальных угроз безопасности информации при подключении ИС/АРМ внешних пользователей к ГИС «Электронная путевка».

К базовому составу средств защиты информации, необходимому для обеспечения информационной безопасности при взаимодействии ИС/АРМ внешних пользователей с ГИС «Электронная путевка» 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 владельца ГИС «Электронная путевка».

61. Требования к средствам защиты от НСД

Средства защиты ИС/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 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 поискаи 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.

62. 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.

63. 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.

64. 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.

65. 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 к 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 применяемых средств криптографической защиты в ИС внешних пользователь при подключении к ГИС «Электронная путевка» в соответствии с требованиями ФСБ России не ниже КС3.

Приложение 1

Форма акта настройки средств защиты информации на автоматизированном рабочем месте или в информационной (автоматизированной) системе внешнего пользователя (туроператора, подключаемого к государственной информационной системе «Электронная путевка»

ФОРМА 1

УТВЕРЖДАЮ
Руководитель
_____
ФИО
«_____» _____ 20___ г.

АКТ
настройки средств защиты на автоматизированном рабочем месте внешнего пользователя (туроператора), подключаемого к государственной информационной системе «Электронная путевка»

1. Наименование подключаемого автоматизированного рабочего места

Наименование АРМ	Учетный (инвентарный) номер	ФИО работника	Должность работника
АРМ № 1	4102501445652	Сидоров Евгений Андреевич Ведущий	специалист отдела сопровождения

2. Состав средств защиты информации

Тип СЗИ	Наименование	Версия	Дата настройки	Серийный номер (СЗЗ)	Сертификат соответствия ФСТЭК России (ФСБ России)
АРМ № 1					
Средство защиты информации от несанкционированного доступа	Dallas Lock 8.0- K	8.0.565.2	12.12.2023	13306-2075- 448 (З 989991)	Сертификат соответствия ФСТЭК России № 4068
Средство межсетевого экранирования	Dallas Lock 8.0- K	8.0.565.2	12.12.2023	13306-2075- 448 (З 989991)	Сертификат соответствия ФСТЭК России № 4068
Средство обнаружения	Dallas Lock 8.0- K	8.0.565.2	12.12.2023	13306-2075- 448	Сертификат соответстви

вторжения				(З 989991)	я ФСТЭК России № 4068
Средство антивирусной защиты	Kaspersky Endpoint Security 11	11.1.1.126	12.12.2023	СМП8067-29444 (Н 450182)	Сертификат соответствия ФСТЭК России № 4068
Средство криптографической защиты информации	ViPNet PKI Client	4.5.1	12.12.2023	отсутствует	Сертификат соответствия ФСБ России № СФ/124-3430

Ответственный за обеспечение
защиты подключаемых АРМ _____ ФИО

ФОРМА 2

УТВЕРЖДАЮ
Руководитель
_____
ФИО
«_____» _____ 20___ г.

АКТ
настройки средств защиты в информационной (автоматизированной) системе внешнего пользователя (туроператора), подключаемой к государственной информационной системе «Электронная путевка»

1.Наименование подключаемой информационной (автоматизированной) системы.

2. Состав программно-технических средств информационной (автоматизированной) системы

Наименование АРМ	Учетный (инвентарный) номер	ФИО работника	Должность работника
Сервер № 1	4102501556512	Егоров Виталий Андреевич	Отдел технического обеспечения
АРМ № 1	4102501445652	Сидоров Евгений Андреевич Ведущий	специалист отдела сопровождения

2. Состав средств защиты информации

Тип СЗИ	Наименование	Версия	Дата настройки	Серийный номер (СЗЗ)	Сертификат соответствия ФСТЭК России (ФСБ России)
Сервер № 1					
Средство защиты информации от несанкционированного доступа	Dallas Lock 8.0- K	8.0.565.2	12.12.2023	13306-2075- 448 (З 989991)	Сертификат соответствия ФСТЭК России № 4068
Средство межсетевого экранирования	Dallas Lock 8.0- K	8.0.565.2	12.12.2023	13306-2075- 448 (З 989991)	Сертификат соответствия ФСТЭК России № 4068
Средство обнаружения вторжения	Dallas Lock 8.0- K	8.0.565.2	12.12.2023	13306-2075- 448 (З 989991)	Сертификат соответствия ФСТЭК России №

					4068
Средство антивирусной защиты	Kaspersky Endpoint Security 11	11.1.1.126	12.12.2023	СМП8067-29444 (Н 450182)	Сертификат соответствия ФСТЭК России № 4068
Средство криптографической защиты информации	ViPNet PKI Client	4.5.1	12.12.2023	отсутствует	Сертификат соответствия ФСБ России № СФ/124-3430
Отдельно установленные средства защиты информации					
Средство анализа защищенности	Сканер-ВС	v5-1.0.10-1.0.13	12.12.2023	100002693 (Н 255432)	Сертификат соответствия ФСТЭК России № 2204
Средство межсетевого экранирования	ViPNet Coordinator	HW1000 Q5	12.12.2023	030-35711 (Л 995878)	Сертификат соответствия ФСТЭК России № 3692
Средство криптографической защиты	ViPNet Coordinator	HW1000 Q5	12.12.2023	отсутствует	Сертификат соответствия ФСБ России № СФ/124-3674

Ответственный за обеспечение
защиты подключаемой ИС _____ ФИО

Приложение 2

Примерный перечень
организационно-распорядительных документов по защите информации владельца объекта информатизации

1. Приказ об организации обработки и защиты персональных данных;

2. Приказ о назначении ответственного за организацию обработки персональных данных;

3. Приказ о назначении ответственных за обеспечение безопасности информации персональных данных;

4. Приказ о назначении администратора безопасности;

5. Приказ о комиссии по определению уровней защищенности персональных данных, обрабатываемых в информационных системах персональных данных;

6. Приказ об утверждении списка лиц, которым необходим доступ к персональным данным, обрабатываемым в информационных системах персональных данных, для выполнения трудовых обязанностей;

7. Приказ о выделении помещений, в котором производится обработка персональных данных;

8. Правила рассмотрения запросов субъектов персональных данных или их представителей;

9. Правила осуществления внутреннего контроля соответствия обработки персональных данных требованиям к защите персональных данных;

10. Положение об организации режима безопасности помещений, где осуществляется работа с персональными данными;

11. Порядок резервного копирования информации;

12. Положение о порядке организации и проведения работ по защите персональных данных при их обработке;

13. Положение о защите персональных данных;

14. Правила обработки персональных данных;

15. Положение о порядке хранения и уничтожения носителей персональных данных;

16. План мероприятий по обеспечению защиты персональных данных;

17. Форма журнала по учету применяемых средств защиты информации, эксплуатационной и технической документации к ним;

18. Руководство пользователя;

19. Руководство администратора информационной безопасности;

20. Инструкция администратора;

21. Инструкция по антивирусной защите;

22. Инструкция по парольной защите;

23. Инструкция о порядке обращения с носителями конфиденциальной информации;

24. Форма журнала учета машинных носителей информации;

25. Форма журнала по учету мероприятий по контролю обеспечения защиты персональных данных;

26. Приказ о ведении электронного журнала обращений пользователей;

27. Перечень персональных данных;

28. Перечень информационных систем;

29. Правила работы с обрабатываемыми обезличенными персональными данными;

30. Перечень должностей, ответственных за проведение мероприятий по обезличиванию персональных данных;

31. Типовая форма согласия на обработку персональных данных;

32. Типовая форма обязательства о неразглашении;

33. Типовая форма разъяснения субъекту персональных данных
юридических последствий отказа предоставить свои данные;

34. Памятка по обеспечению режима безопасности в помещении, в котором осуществляется обработка персональных данных;

35. Инструкция по обработке персональных данных без использования средств автоматизации;

36. Политика в отношении обработки персональных данных;

37. Должностная инструкция ответственного за организацию обработки персональных данных.

39. Организация эксплуатации средств криптографической защиты информации

40. Приказ о назначении ответственного за эксплуатацию СКЗИ,
утверждении инструкций и журналов, касающихся использования средств
криптографической защиты информации;

41. Инструкция ответственного за эксплуатацию средств криптографической защиты информации;

42. Инструкция по порядку обращения с сертифицированными средствами криптографической защиты информации, предназначенными для защиты информации

ограниченного доступа, не содержащей сведения,

составляющие государственную тайну;

43. Форма журнала поэкземплярного учета средств криптографической защиты информации, эксплуатационной и технической документации к ним, ключевых документов;

44. Типовая форма акта об уничтожении криптографических ключей, содержащихся на ключевых носителях, и ключевых документов;

45. Перечень работников, допущенных к работе с сертифицированными СКЗИ, предназначенными для защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну;

46. Перечень мест хранения СКЗИ;

47. Приказ о назначении лиц, допущенных к работе в информационной системе.