ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПНСТ 199— 2017

Глобальная навигационная спутниковая система

РЕГИОНАЛЬНЫЕ НАВИГАЦИОННО-ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Назначение, состав и характеристики системы обеспечения информационной безопасности

Издание официальное

Москва
Стандартинформ
2018

Предисловие

1 РАЗРАБОТАН Федеральным государственным унитарным предприятием «ЗащитаИнфоТранс Министерства транспорта Российской Федерации» (ФГУП «ЗащитаИнфоТранс»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 363 «Радионавигация»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 23 ноября 2017 г. № 49-пнст

4 ПЕРЕИЗДАНИЕ. Ноябрь 2018 г.

Правила применения настоящего стандарта и проведения его мониторинга установлены в ГОСТ Р 1.16—2011 (разделы 5 и 6).

Федеральное агентство по техническому регулированию и метрологии собирает сведения о практическом применении настоящего стандарта. Данные сведения, а также замечания и предложения по содержанию стандарта можно направить не позднее чем за 4 мес до истечения срока его действия разработчику настоящего стандарта по адресу: 105082 Москва, ул. Бакунинская, д. 71, стр. 10 и/или в Федеральное агентство по техническому регулированию и метрологии по адресу: 109074 Москва, Китайгородский проезд, д. 7, стр. 1.

В случае отмены настоящего стандарта соответствующая информация будет опубликована в ежемесячном информационном указателе «Национальные стандарты» и также будет размещена на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Настоящий стандарт входит в комплекс стандартов «Глобальная навигационная спутниковая система. Региональные навигационно-информационные системы» и определяет назначение, состав и требования к характеристикам системы обеспечения информационной безопасности.

Система создается в составе региональной навигационно-информационной системы и должна обеспечивать предотвращение несанкционированного доступа к информационным ресурсам РНИС и обеспечение безопасности информации при информационном обмене между компонентами РНИС и с внешними автоматизированными системами (аппаратно-программными комплексами) потребителей в соответствии с Постановлением Правительства Российской Федерации от 21 декабря 2012 г. № 1367 «Об утверждении правил предоставления и распределения в 2013—2014 годах субсидий из федерального бюджета бюджетам субъектов Российской Федерации на информационно-навигационное обеспечение автомобильных маршрутов по транспортным коридорам «СЕВЕР—ЮГ» и «ВОСТОК—ЗАПАД» (с изменениями на 29 декабря 2015 г.).

ПРЕДВАРИТЕЛЬНЫЙ НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Глобальная навигационная спутниковая система

РЕГИОНАЛЬНЫЕ НАВИГАЦИОННО-ИНФОРМАЦИОННЫЕ СИСТЕМЫ

Назначение, состав и характеристики системы обеспечения информационной безопасности

Global navigation satellite system.
Regional navigation and information systems.
Purpose, composition and characteristics of information security system

Срок действия — с 2018—03—01
до 2020—03—01

1 Область применения

Настоящий стандарт распространяется на систему обеспечения информационной безопасности (далее — система), входящую в состав региональной навигационно-информационной системы, и устанавливает требования к ее назначению, составу и характеристикам.

Положения настоящего стандарта могут быть использованы для обеспечения унификации и совместимости аппаратных и программных средств, функционирующих в рамках автоматизированных систем управления (диспетчеризации), мониторинга и контроля, создаваемых на основе применения глобальных навигационных спутниковых систем [1].

Примечание — Назначение, архитектура РНИС и общие требования к региональному навигационно-информационному центру и его компонентам установлены в ПНСТ 194.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ПНСТ 193 Глобальная навигационная спутниковая система. Региональные навигационно-информационные системы. Термины и определения

ПНСТ 194 Глобальная навигационная спутниковая система. Региональные навигационно-информационные системы. Назначение и архитектура

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте применены термины по ПНСТ 193.

Издание официальное

4 Сокращения

В настоящем стандарте применены следующие сокращения:
АВЗ — антивирусная защита;
АНЗ — контроль (анализ) защищенности информации;
ГЛОНАСС — глобальная навигационная спутниковая система Российской Федерации;
ЗИС — защита информационной системы, ее средств, систем связи и передачи данных;
ЗНИ — защита машинных носителей информации;
ЗСВ — защита среды виртуализации;
ЗТС — защита технических средств;
ИАФ — идентификация и аутентификация субъектов доступа и объектов доступа;
ОПС — ограничение программной среды;
ОЦЛ — обеспечение целостности информационной системы и информации;
РНИС — региональная навигационно-информационная система;
РСБ — регистрация событий безопасности;
УПД — управление доступом субъектов доступа к объектам доступа.

5 Назначение системы

5.1 Система предназначена для предотвращения несанкционированного доступа к информационным ресурсам РНИС и обеспечения безопасности информации при информационном обмене между компонентами РНИС и с внешними автоматизированными системами (аппаратно-программными комплексами).

5.2 Целью создания системы является предотвращение или минимизация ущерба (прямого или косвенного), наносимого компонентам РНИС посредством нежелательного воздействия на информацию, ее носители и процессы обработки.

5.3 Класс защищенности РНИС (не ниже К3) и меры по защите информации определяются на стадии проектирования при создании (модернизации) РНИС и ее компонентов в соответствии с требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [2], и зависят от уровня значимости информации, которая обрабатывается в РНИС.

5.4 Порядок мероприятий по созданию системы в РНИС определяется в соответствии с требованиями о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [2].

6 Состав системы

6.1 Система должна создаваться и функционировать как система, все или некоторые компоненты которой должны размещаться на базе технологической инфраструктуры РНИС [3].

6.2 Система должна включать в свой состав следующие основные модули (при минимально возможном классе защищенности К3) или их функционал:

- идентификации и аутентификации субъектов доступа и объектов доступа;
- управления доступом субъектов доступа к объектам доступа;
- ограничения программной среды;
- защиты машинных носителей информации;
- регистрации событий безопасности;
- антивирусной защиты;
- контроля (анализа) защищенности информации;
- обеспечения целостности информационной системы и информации;
- защиты среды виртуализации;
- защиты технических средств;
- защиты информационной системы, ее средств, систем связи и передачи данных.

6.3 В состав системы дополнительно могут быть включены и другие модули (в зависимости от класса защищенности РНИС) или их функционал.

Примечание — Назначение и состав дополнительных модулей, включаемых в систему, определяются решением субъекта Российской Федерации.

7 Характеристики системы

7.1 Требования к функционалу системы

Система должна обеспечивать выполнение следующих функциональных задач:
- 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;
- контроль (анализ) защищенности информации;
- обеспечение целостности информационной системы и информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

7.2 Требования к основным модулям системы и их функциям

7.2.1 Модуль ИАФ должен обеспечивать следующие меры защиты информации:
- идентификацию и аутентификацию пользователей, являющихся работниками оператора (ИАФ.1);
- управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов (ИАФ.3);
- управление средствами аутентификации, в том числе хранение, выдачу, инициализацию, блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации (ИАФ.4);
- защиту обратной связи при вводе аутентификационной информации (ИАФ.5);
- идентификацию и аутентификацию пользователей, не являющихся работниками оператора (внешних пользователей) (ИАФ.6).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.2 Модуль УПД должен обеспечивать следующие меры защиты информации:
- управление (заведение, активацию, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей (УПД.1);
- реализацию необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа (УПД.2);
- разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование информационной системы (УПД.4);
- назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы (УПД.5);
- ограничение неуспешных попыток входа в информационную систему (доступа к информационной системе) (УПД.6);
- блокирование сеанса доступа в информационную систему после установленного времени бездействия (неактивности) пользователя или по его запросу (УПД.10);
- разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации (УПД.11);
- реализацию защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети (УПД.13);
- регламентацию и контроль использования в информационной системе технологий беспроводного доступа (УПД.14);
- регламентацию и контроль использования в информационной системе мобильных технических средств (УПД.15);
- управление взаимодействием с информационными системами сторонних организаций (внешние информационные системы) (УПД.16).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.3 Модуль ОПС должен обеспечивать следующие меры защиты информации:

- установку (инсталляцию) только разрешенного к использованию программного обеспечения и (или) его компонентов (ОПС.3).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.4 Модуль ЗНИ должен обеспечивать следующие меры защиты информации:

- учет машинных носителей информации (ЗНИ.1);
- управление доступом к машинным носителям информации (ЗНИ.2);
- уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания) (ЗНИ.8).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.5 Модуль РСБ должен обеспечивать следующие меры защиты информации:

- определение событий безопасности, подлежащих регистрации, и сроков их хранения (РСБ.1);
- определение состава и содержания информации о событиях безопасности, подлежащих регистрации (РСБ.2);
- сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения (РСБ.3);
- реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти (РСБ.4);
- мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них (РСБ.5);
- генерирование временных меток и (или) синхронизацию системного времени в информационной системе (РСБ.6);
- защиту информации о событиях безопасности (РСБ.7).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.6 Модуль АВЗ должен обеспечивать следующие меры защиты информации:

- реализацию антивирусной защиты (АВЗ.1);
- обновление базы данных признаков вредоносных компьютерных программ (вирусов) (АВЗ.2).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [3].

7.2.7 Модуль АНЗ должен обеспечивать следующие меры защиты информации:

- выявление, анализ уязвимостей информационной системы и оперативное устранение вновь выявленных уязвимостей (АНЗ.1);
- контроль установки обновлений программного обеспечения, включая обновление программного обеспечения средств защиты информации (АНЗ.2);
- контроль работоспособности, параметров настройки и правильности функционирования программного обеспечения и средств защиты информации (АНЗ.3);
- контроль состава технических средств, программного обеспечения и средств защиты информации (АНЗ.4);
- контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступа, полномочий пользователей в информационной системе (АНЗ.5).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.8 Модуль ОЦЛ должен обеспечивать следующие меры защиты информации:

- возможность восстановления программного обеспечения, включая программное обеспечение средств защиты информации, при возникновении нештатных ситуаций (ОЦЛ.3).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.9 Модуль ЗСВ должен обеспечивать следующие меры защиты информации:

- идентификацию и аутентификацию субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации (ЗСВ.1);

- управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин (ЗСВ.2);
- регистрацию событий безопасности в виртуальной инфраструктуре (ЗСВ.3);
- реализацию и управление антивирусной защитой в виртуальной инфраструктуре (ЗСВ.9).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.10 Модуль ЗТС должен обеспечивать следующие меры защиты информации:
- организацию контролируемой зоны, в пределах которой постоянно размещаются стационарные технические средства, обрабатывающие информацию, и средства защиты информации, а также средства обеспечения функционирования (ЗТС.2);
- контроль и управление физическим доступом к техническим средствам, средствам защиты информации, средствам обеспечения функционирования, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ к средствам обработки информации, средствам защиты информации и средствам обеспечения функционирования информационной системы и в помещения и сооружения, в которых они установлены (ЗТС.3);
- размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр (ЗТС.4).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

7.2.11 Модуль ЗИС должен обеспечивать следующие меры защиты информации:
- обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи (ЗИС.3);
- запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств (ЗИС.5);
- защиту беспроводных соединений, применяемых в информационной системе (ЗИС.20);
- защиту мобильных технических средств, применяемых в информационной системе (ЗИС.30).

Примечание — Условное обозначение и номер мер защиты информации приведены в соответствии с [2].

Требования к модулю ЗИС (в том числе к средствам криптографической защиты информации в случае их необходимости) определяются на стадии проектирования при создании (модернизации) РНИС и ее компонентов в зависимости от класса защищенности внешних автоматизированных систем, с которыми необходима интеграция.

7.3 Требования к аппаратным средствам и общему программному обеспечению, необходимым для обеспечения эффективного функционирования системы

7.3.1 В РНИС должны применяться [2] (при минимально возможном классе защищенности К3):
- средства вычислительной техники не ниже 5 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 4 класса;
- межсетевые экраны не ниже 4 класса.

Примечание — Класс применяемых средств и систем может быть пересмотрен в зависимости от класса защищенности РНИС.

7.3.2 Средства защиты информации, применяемые в РНИС, должны быть сертифицированы Федеральной службой по техническому и экспортному контролю и содержаться в Государственном реестре сертифицированных средств защиты информации N РОСС RU.0001.01БИ00.

7.3.3 Общее программное обеспечение, применяемое в РНИС, должно быть сертифицировано Федеральной службой по техническому и экспортному контролю и содержаться в Государственном реестре сертифицированных средств защиты информации N РОСС RU.0001.01БИ00.

7.3.4 Функционирование системы должно осуществляться в непрерывном режиме работы.

Библиография

[1] Указ Президента Российской Федерации от 17 мая 2007 г. № 638 «Об использовании глобальной навигационной спутниковой системы ГЛОНАСС в интересах социально-экономического развития Российской Федерации»

[2] Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

[3] Постановление Правительства Российской Федерации от 21 декабря 2012 г. № 1367 «Об утверждении правил предоставления и распределения в 2013—2014 годах субсидий из федерального бюджета бюджетам субъектов Российской Федерации на информационно-навигационное обеспечение автомобильных маршрутов по транспортным коридорам «СЕВЕР—ЮГ» и «ВОСТОК—ЗАПАД» (с изменениями на 29 декабря 2015 г.)

УДК 621.396.931:006.354 ОКС 35.240.60

Ключевые слова: региональные навигационно-информационные системы, ГЛОНАСС, информационная безопасность, защита информации

Редактор *Л.В. Коретникова*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Р. Ароян*
Компьютерная верстка *Ю.В. Поповой*

Сдано в набор 14.11.2018. Подписано в печать 21.11.2018. Формат 60 × 84 1/8. Гарнитура Ариал.
Усл. печ. л. 1,40. Уч.-изд. л. 1,26.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

ИД «Юриспруденция», 115419, Москва, ул. Орджоникидзе, 11.
www.jurisizdat.ru y-book@mail.ru

Создано в единичном исполнении ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru