ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 70669— 2023

Дистанционное зондирование Земли из космоса

ДАННЫЕ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ ИЗ КОСМОСА

Требования к информационной безопасности при хранении

Издание официальное

Москва
Российский институт стандартизации
2023

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Акционерным обществом «Российская корпорация ракетно-космического приборостроения и информационных систем» (АО «Российские космические системы») по заказу Государственной корпорации по космической деятельности «Роскосмос»

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 321 «Ракетно-космическая техника»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 13 июля 2023 г. № 525-ст

4 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (*gost.e-ecolog.ru

© Оформление. ФГБУ «Институт стандартизации», 2023

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Сокращения 3
5 Общие положения 3
6 Виды нарушителей информационной безопасности архива данных дистанционного зондирования Земли из космоса 4
7 Требования к системе (комплексу) информационной безопасности архива данных дистанционного зондирования Земли из космоса 5
8 Требования к нормативному обеспечению архива данных дистанционного зондирования Земли из космоса 7
Приложение А (справочное) Средства защиты информации архива данных дистанционного зондирования Земли из космоса, их назначение и предъявляемые требования 9
Приложение Б (справочное) Типовой состав комплекта документов обеспечения информационной безопасности архива данных дистанционного зондирования Земли из космоса 10
Библиография 11

Введение

Первичные данные дистанционного зондирования Земли из космоса, получаемые с космических комплексов (космических систем) являются уникальными и невоспроизводимыми, поэтому необходимо обеспечить их защиту от несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения. Реализация мер обеспечения информационной безопасности данных дистанционного зондирования Земли из космоса осуществляется в процессе их хранения в архиве данных дистанционного зондирования Земли из космоса.

Целью данного стандарта является определение унифицированного подхода к организации системы (комплекса) информационной безопасности архива данных дистанционного зондирования Земли из космоса, рассмотрение видов угроз и нарушителей безопасности, определение основных требований к средствам защиты информации, состав и требования к нормативным документам по обеспечению информационной безопасности.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Дистанционное зондирование Земли из космоса

ДАННЫЕ ДИСТАНЦИОННОГО ЗОНДИРОВАНИЯ ЗЕМЛИ ИЗ КОСМОСА

Требования к информационной безопасности при хранении

Remote sensing of the Earth from space. Remote sensing data of the Earth from space.
Requirements for information security during storage

Дата введения — 2024—01—01

1 Область применения

Настоящий стандарт устанавливает требования к обеспечению информационной безопасности архива данных дистанционного зондирования Земли, а также положения по реализации технического обеспечения информационной защиты архива данных дистанционного зондирования Земли из космоса.

Настоящий стандарт предназначен для организаций, непосредственно осуществляющих получение (прием) первичных данных дистанционного зондирования Земли из космоса, предназначенных для архивного хранения.

Настоящий стандарт не распространяется на данные дистанционного зондирования Земли из космоса, получаемые с космических комплексов (космических систем) гидрометеорологического, океанографического и гелиогеофизического назначения.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 15408-3 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности

ГОСТ Р 50922 Защита информации. Основные термины и определения

ГОСТ Р 59753 Данные дистанционного зондирования Земли из космоса. Термины и определения

ГОСТ Р 59754 Данные дистанционного зондирования Земли из космоса. Обработка данных дистанционного зондирования Земли из космоса. Термины и определения

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.

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ГОСТ Р 50922, ГОСТ Р 59753, ГОСТ Р 59754, а также следующие термины с соответствующими определениями:

3.1 **администратор информационной безопасности:** Руководитель или уполномоченный специалист, осуществляющий функции организации защиты информации и контроля над предотвращением несанкционированного доступа, использования, раскрытия, искажения, изменения, исследования, записи или уничтожения информации.

3.2

архив данных дистанционного зондирования Земли из космоса: Совокупность программно-технических средств, а также данных дистанционного зондирования Земли из космоса, хранение, управление, миграция и безопасность которых обеспечивается посредством использования программно-технических средств.

Примечание — Постоянный архив обеспечивает постоянное хранение данных дистанционного зондирования Земли из космоса, оперативный архив обеспечивает оперативное хранение данных дистанционного зондирования Земли из космоса.

[ГОСТ Р 70666—2023, пункт 3.8]

3.3 **оператор архива данных дистанционного зондирования Земли из космоса:** Организация, осуществляющая ведение архива данных дистанционного зондирования Земли из космоса, в том числе получение данных дистанционного зондирования Земли из космоса, их учет, хранение, а также обеспечение целостности, конфиденциальности и доступности.

3.4

доступность: Свойство объекта находиться в состоянии готовности и возможности использования по запросу авторизованного логического объекта.

[ГОСТ Р ИСО 7498-2—99, пункт 3.3.11]

3.5

конфиденциальность: Свойство, позволяющее не давать права на доступ к информации или не раскрывать ее неполномочным лицам, логическим объектам или процессам.

[ГОСТ Р ИСО 7498-2—99, пункт 3.3.16]

3.6

модель угроз (безопасности информации): Физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

[ГОСТ Р 53114—2008, статья 3.3.3]

3.7

нарушитель информационной безопасности организации; нарушитель ИБ организации: Физическое лицо или логический объект, случайно или преднамеренно совершивший действие, следствием которого является нарушение информационной безопасности организации.

[ГОСТ Р 53114—2008, статья 3.3.5]

3.8

несанкционированный доступ: Доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый с нарушением установленных прав и (или) правил доступа.

[ГОСТ Р 53114—2008, статья 3.3.6]

3.9 **система [комплекс] информационной безопасности архива данных дистанционного зондирования Земли из космоса:** Программно-технический комплекс, обеспечивающий информационную безопасность архива данных дистанционного зондирования Земли из космоса.

3.10

средство защиты информации: Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

[ГОСТ 50922—2006, статья 2.7.2]

3.11

угроза безопасности информации: Совокупность факторов и условий, создающих опасность нарушения информационной безопасности организации, вызывающую или способную вызвать негативные последствия (ущерб/вред) для организации.

[Адаптировано из ГОСТ Р 53114—2008, статья 3.3.2]

3.12

целостность: Способность данных не подвергаться изменению или аннулированию в результате несанкционированного доступа.

[ГОСТ Р ИСО 7498-2—99, пункт 3.3.31]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ДЗЗ — дистанционное зондирование Земли;
ИС — информационная система;
КА — космический аппарат;
КС — космическая система;
МЭ — межсетевой экран;
ПО — программное обеспечение;
СЗИ — средство защиты информации;
СОВ — средство обнаружения вторжений;
IT — информационные технологии (information technologies).

5 Общие положения

5.1 В архиве данных ДЗЗ из космоса, должна обеспечиваться конфиденциальность, доступность и целостность следующих категорий информации:

- данных ДЗЗ из космоса;
- метаданных данных ДЗЗ из космоса;
- служебно-технологической информации архива данных ДЗЗ из космоса;
- идентификационной/аутентификационной информации пользователей и администраторов архива данных ДЗЗ (логические имена, сетевые адреса коммутационного и серверного оборудования, настройки СЗИ и т.д.).

Примечания:

1 Данные ДЗЗ из космоса, получаемые с КА ДЗЗ и их метаданные могут не относиться к конфиденциальной информации.

2 Полный перечень конфиденциальной информации устанавливается в соответствии с регламентирующим документом хранения данных и продуктов ДЗЗ из космоса.

5.2 Основными видами угроз информационной безопасности при хранении являются:

- нарушение конфиденциальности информации в архиве данных ДЗЗ из космоса — несанкционированный доступ к информации, содержащей сведения, которые относятся к информации ограниченного доступа в соответствии с [1] или отнесенные собственником (заказчиком) КС ДЗЗ и оператором архива данных ДЗЗ из космоса к конфиденциальной информации;
- нарушение целостности данных ДЗЗ из космоса — несанкционированная модификация, дополнение или уничтожение информации архива данных ДЗЗ из космоса;
- нарушение доступности информационных ресурсов архива данных ДЗЗ из космоса — ограничение или блокирование доступа к информации архива данных ДЗЗ из космоса.

5.3 Объектами защиты в составе архива данных ДЗЗ из космоса являются:

- информационные ресурсы (архивные данные ДЗЗ из космоса и др. согласно 5.1);
- виртуальные серверы;
- программное обеспечение ИС;
- программно-технические средства (физические серверы), сетевое оборудование;
- СЗИ;
- каналы информационного обмена.

5.4 Основными мерами обеспечения информационной безопасности архива данных ДЗЗ из космоса являются:

- постоянный и всесторонний анализ информационного пространства с целью выявления угроз для информационных ресурсов;
- своевременное обнаружение технических проблем, потенциально способных повлиять на информационную безопасность;
- разработка и корректировка модели угроз и типов нарушителей информационной безопасности;
- анализ необходимости и планирование модернизации (доработки) комплекса информационной безопасности архива данных ДЗЗ из космоса в соответствии с характером выявленных угроз, а также изменениями законодательства и руководящих документов в области безопасности информации для объектов критической информационной инфраструктуры;
- распределение полномочий, обязанностей персонала по обеспечению информационной безопасности.

Определение перечня необходимых мер обеспечения информационной безопасности архива данных ДЗЗ из космоса должно осуществляться на стадии проектирования.

Примечание — При разработке модели угроз может быть использован информационный ресурс [2].

6 Виды нарушителей информационной безопасности архива данных дистанционного зондирования Земли из космоса

6.1 Степень воздействия угроз, факторов и источников, влияющих на информационную безопасность средств архива данных ДЗЗ из космоса, зависит от возможностей нарушителя информационной безопасности.

6.2 В зависимости от наличия прав и уровня возможностей нарушители информационной безопасности архива данных ДЗЗ из космоса подразделяются на две категории:

- внешние — субъекты, не имеющие законных оснований для пребывания в месте размещения технических средств архива данных ДЗЗ из космоса и полномочий для доступа к информационным ресурсам и компонентам ИС;
- внутренние — субъекты, имеющие законные основания для пребывания в месте размещения технических средств архива данных ДЗЗ из космоса и полномочия для доступа к информационным ресурсам и компонентам ИС.

6.3 К основным видам внешних нарушителей информационной безопасности архива данных ДЗЗ из космоса в соответствии с [3] относят:

- специальные службы иностранных государств;
- террористические, экстремистские группировки;
- преступные группы (криминальные структуры);
- отдельных физических лиц (хакеров);
- конкурирующие организации;
- бывших (уволенных) работников;
- пользователей;
- и др.

6.4 К основным видам внутренних нарушителей информационной безопасности архива данных ДЗЗ из космоса относят:

- администраторов архива данных ДЗЗ из космоса (специалисты, выполняющие функции системного администратора, администратора безопасности информации);
- администраторов подсистем или баз данных архива данных ДЗЗ из космоса (специалисты, являющиеся администраторами прикладного ПО и осуществляющие ввод данных в ИС, редактирование их структуры и содержания, удаление, настройку прикладного ПО);

- обслуживающий персонал (служба охраны, инженерно-техническая служба и т.д.);
- персонал разработчиков ПО и оборудования, который на договорной основе имеет право на техническое обслуживание и модификацию компонентов ИС;
- и др.

6.5 Перечни внешних и внутренних нарушителей информационной безопасности архива данных ДЗЗ из космоса могут быть дополнены иными видами нарушителей с учетом особенностей информационной системы и системы защиты информации архива данных ДЗЗ из космоса.

6.6 Уровень возможностей нарушителя информационной безопасности архива данных ДЗЗ из космоса в соответствии с [3] определяется его компетентностью и оснащенностью, требуемыми для реализации угроз информационной безопасности архива данных ДЗЗ из космоса. Выделяются следующие уровни возможностей нарушителя информационной безопасности архива данных ДЗЗ из космоса:

- нарушитель, обладающий базовыми возможностями, — имеет возможность реализовывать только известные угрозы, направленные на известные (документированные) уязвимости, с использованием общедоступных инструментов. Предполагается, что такими возможностями обладают, например, пользователи ИС либо не имеющие отношения к ИС физические лица;
- нарушитель, обладающий базовыми повышенными возможностями, — имеет возможность реализовывать угрозы, в т.ч. направленные на неизвестные (недокументированные) уязвимости, с использованием специально созданных для этого инструментов, свободно распространяемых в сети Интернет. Не имеет возможностей реализации угроз на физически изолированные сегменты ИС и сетей;
- нарушитель, обладающий средними возможностями, — имеет возможность реализовывать угрозы, в том числе на выявленные ими неизвестные уязвимости, с использованием самостоятельно разработанных для этого инструментов. Не имеет возможностей реализации угроз на физически изолированные сегменты ИС и сетей;
- нарушитель, обладающий высокими возможностями, — имеет практически неограниченные возможности реализовывать угрозы, в том числе с использованием недекларированных возможностей, программных, программно-технических закладок, встроенных в компоненты ИС и сетей.

7 Требования к системе (комплексу) информационной безопасности архива данных дистанционного зондирования Земли из космоса

7.1 Система информационной безопасности архива данных ДЗЗ из космоса должна реализовывать функции обеспечения защиты архива данных ДЗЗ из космоса от всех существующих видов угроз, способных привести к возникновению рисков (ущерба).

7.2 Основными требованиями обеспечения безопасности информации архива данных ДЗЗ из космоса являются:

- предотвращение неправомерного доступа к информации, обрабатываемой значимым объектом критической информационной инфраструктуры, уничтожения такой информации, ее модифицирования, блокирования, копирования, предоставления и распространения, а также иных неправомерных действий в отношении такой информации;
- недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено и (или) прекращено функционирование значимого объекта критической информационной инфраструктуры;
- восстановление функционирования значимого объекта критической информационной инфраструктуры, обеспечиваемого в том числе за счет создания и хранения резервных копий информационных ресурсов;
- непрерывное взаимодействие с государственной системой обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы значимого объекта критической информационной инфраструктуры в соответствии с [4].

7.3 К СЗИ архива данных ДЗЗ из космоса, входящим в состав системы информационной безопасности, относят:

- технические — сигнализация, решетки на окнах, генераторы помех воспрепятствования передаче данных по радиоканалам, вход в здание или помещение по ключ-карте, электронные ключи и т.д.;
- программные — программы-шифровальщики данных, антивирусы, брандмауэры, бэкап-системы, системы аутентификации пользователей и т.п.;
- смешанные — комбинация технических и программных средств.

7.4 Для обеспечения функционирования системы информационной безопасности архива данных ДЗЗ из космоса применяют следующие организационные меры:

- разработку комплекта документов обеспечения информационной безопасности архива данных ДЗЗ из космоса;
- обеспечение соответствия законодательным актам в сфере защиты информации;
- подготовку помещений с компьютерной техникой и прокладку сетевых кабелей с учетом требований по ограничению доступа к информации.

7.5 В зависимости от категории значимости и угроз информационной безопасности архива данных ДЗЗ из космоса должны быть реализованы следующие организационные и технические меры в соответствии с [5], приведенные в таблице 1.

Таблица 1

Наименование	Назначение
Идентификация и аутентификация	Идентификация и аутентификация пользователей (операторов, администраторов), являющихся работниками оператора архива данных ДЗЗ из космоса. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных. Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов
Управление доступом	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 обеспечение контроля за соблюдением этих правил
Антивирусная защита	Комплекс профилактических и диагностических мер, применяемых для защиты информационных систем от заражения вирусами
Предотвращение вторжений	Обнаружение вторжений или нарушений безопасности и автоматическая защита от них
Обеспечение целостности	Обеспечение обнаружения фактов несанкционированного нарушения целостности информационной системы и содержащихся в ней данных, а также возможность восстановления информационной системы и содержащихся в ней данных
Обеспечение доступности	Обеспечение авторизованного доступа пользователей, имеющих права по доступу, в штатном режиме функционирования информационной системы
Защита технических средств и систем	Исключение несанкционированного доступа к стационарным техническим средствам, средствам, обеспечивающим функционирование информационной системы, и в помещения, в которых они постоянно расположены, защиту технических средств от внешних воздействий
Управление конфигурацией	Обеспечение управления изменениями конфигурации информационной системы и системы защиты, анализ потенциального воздействия планируемых изменений на обеспечение безопасности персональных данных, а также документирование этих изменений
Реагирование на инциденты информационной безопасности	Обеспечение обнаружения, идентификации, анализа инцидентов в информационной системе, а также принятие мер по устранению и предупреждению инцидентов
Регистрация событий безопасности	Сбор, запись, хранение информации о событиях безопасности в течение установленного времени хранения. Реагирование на сбои при регистрации событий безопасности, в том числе технические и программные ошибки, сбои в механизмах сбора информации и достижении предела или переполнения объема (емкости) памяти. Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них
Примечание — Полный перечень мер защиты информации, необходимый для выполнения всех требований безопасности информации, формируют на основании модели угроз.	

7.6 Состав системы (комплекса) информационной безопасности архива данных ДЗЗ формируют в соответствии с категорией значимости архива данных ДЗЗ из космоса, определенной собственником (заказчиком) КС ДЗЗ, и потенциальными угрозами его информационной безопасности.

Примеры средств защиты информации приведены в приложении А.

8 Требования к нормативному обеспечению архива данных дистанционного зондирования Земли из космоса

8.1 В процессе проектирования архива данных ДЗЗ из космоса должен быть разработан комплект документов, который определяет цели и задачи системы обеспечения информационной безопасности и устанавливает совокупность правил, требований и руководящих принципов в области информационной безопасности архива данных ДЗЗ из космоса.

8.2 В состав комплекта документов обеспечения информационной безопасности архива данных ДЗЗ из космоса могут входить:

- приказы — требуются для утверждения лиц, ответственных за информационную безопасность архива данных ДЗЗ из космоса, и подразделений, осуществляющих эксплуатацию архива данных ДЗЗ из космоса, а также для утверждения нормативных актов, регламентирующих деятельность по обеспечению информационной безопасности архива данных ДЗЗ из космоса;
- положения — требуются для определения прав, обязанностей, ответственности, порядка и правил организации работы подразделений, осуществляющих эксплуатацию архива данных ДЗЗ из космоса;
- перечни — содержат сведения о защищаемых программно-технических средствах архива данных ДЗЗ из космоса, имеющихся СЗИ, их типах, уязвимостях и др.;
- списки — содержат сведения о допущенных к программно-техническим средствам архива данных ДЗЗ из космоса лицах;
- инструкции — обеспечивают пользователей и администраторов необходимой информацией для соблюдения информационной безопасности при эксплуатации архива данных ДЗЗ из космоса.

Типовой состав документов, которые могут входить в комплект документов обеспечения информационной безопасности архива данных ДЗЗ из космоса, представлен в приложении Б.

Примечание — При необходимости состав комплекта документов обеспечения информационной безопасности архива данных ДЗЗ из космоса может быть расширен.

8.3 Комплект документов обеспечения информационной безопасности архива данных ДЗЗ из космоса разрабатывается оператором архива данных ДЗЗ из космоса по согласованию с собственником (заказчиком) КС ДЗЗ.

8.4 Ответственность за реализацию правил, требований и руководящих принципов, установленных в комплекте документов обеспечения информационной безопасности архива данных ДЗЗ из космоса возлагают на сотрудников, взаимодействующих с архивом данных ДЗЗ из космоса согласно должностным и функциональным обязанностям.

Примечание — Ответственность за реализацию правил, требований и руководящих принципов, установленных в комплекте документов обеспечения информационной безопасности архива данных ДЗЗ из космоса, является персональной, разделяется по видам и возлагается на основании и в порядке, предусмотренном [6] — [9].

8.5 Допуск сотрудника оператора архива данных ДЗЗ к работе с защищаемыми информационными ресурсами архива данных ДЗЗ из космоса осуществляют только после его ознакомления с соответствующими положениями по обеспечению информационной безопасности архива ДЗЗ из космоса.

8.6 При пересмотре положений по обеспечению информационной безопасности или при возникновении инцидента нарушения информационной безопасности архива данных ДЗЗ из космоса среди сотрудников оператора архива данных ДЗЗ из космоса проводят внеплановую разъяснительную работу, а также инструктаж по соблюдению требований комплекта документов обеспечения информационной безопасности архива данных ДЗЗ из космоса.

8.7 Профилактику нарушений информационной безопасности выполняют посредством проведения регламентных работ по защите архива данных ДЗЗ из космоса, предупреждения возможных нарушений информационной безопасности и проведения разъяснительной работы по информационной безопасности среди пользователей архива данных ДЗЗ из космоса.

8.8 При проведении регламентных работ по защите архива данных ДЗЗ из космоса выполняют процедуры контрольного тестирования (проверки) функций СЗИ. Контрольное тестирование функций СЗИ может быть полным или частичным. Контрольное тестирование функций СЗИ должно быть проведено на основе положений комплекта документов обеспечения информационной безопасности архива данных ДЗЗ из космоса.

Приложение А
(справочное)

Средства защиты информации архива данных дистанционного зондирования Земли из космоса, их назначение и предъявляемые требования

Таблица А.1

Подсистема	Назначение	Класс СЗИ	Требования
Защиты каналов связи	Средство криптографической защиты информации	Комплекс шифрования	ГОСТ Р ИСО/МЭК 15408-3 (оценочный уровень доверия 3). Профиль защиты МЭ [10]. Профиль защиты СОВ [11]. Задание по безопасности
Межсетевого экранирования	Фильтрация трафика между сетями или узлами сети	МЭ	Профиль защиты МЭ [12]
Межсетевого экранирования	Защита веб-приложений за счет фильтрации трафика на прикладном уровне	МЭ для защиты веб-приложений	Профиль защиты МЭ [13]
Регистрации событий безопасности	Мониторинг IT-инфраструктуры и выявление инцидентов информационной безопасности	Средства мониторинга информационной безопасности	ГОСТ Р ИСО/МЭК 15408-3 (оценочный уровень доверия 4)
Анализа защищенности	Контроль защищенности и соответствия стандартам	Средства контроля защищенности	ГОСТ Р ИСО/МЭК 15408-3 (оценочный уровень доверия 4)
Обнаружения и предотвращения вторжений	Глубокий анализ сетевого трафика для выявления атак на периметре и внутри сети	СОВ	ГОСТ Р ИСО/МЭК 15408-3 (оценочный уровень доверия 3). Профиль защиты СОВ [14]

Приложение Б
(справочное)

Типовой состав комплекта документов обеспечения информационной безопасности архива данных дистанционного зондирования Земли из космоса

Таблица Б.1

Тип документа	Наименование документа
Приказ	Приказ об определении лиц и подразделений, ответственных за эксплуатацию архива данных ДЗЗ из космоса. Приказ о назначении ответственного за информационную безопасность. Приказ о назначении ответственного за обеспечение безопасности информации ограниченного доступа. Приказ об утверждении Положения о порядке резервного копирования информации. Приказ об утверждении Положения об отделе информационной безопасности
Положение	Положение о порядке организации и проведения работ по защите информации ограниченного доступа в архиве данных ДЗЗ из космоса. Положение о порядке управления доступом пользователей к информационным ресурсам архива данных ДЗЗ из космоса. Положение о порядке резервного копирования информации. Положение об отделе информационной безопасности. Положение о порядке учета, хранения и уничтожения носителей информации. Положение о порядке проведения ремонта и обслуживания технических средств. Положение о порядке управления инцидентами информационной безопасности. Правила и процедуры управления установкой (инсталляцией) компонентов программного обеспечения архива данных ДЗЗ из космоса. Правила взаимодействия архива данных ДЗЗ из космоса с внешними информационными системами
Перечень	Перечень защищаемых ресурсов. Перечень неисправностей, которые могут возникнуть в процессе эксплуатации системы, и рекомендации в отношении действий при их возникновении
Список	Перечень субъектов доступа к защищаемым ресурсам. Матрица доступа или полномочий субъектов доступа по отношению к защищаемым ресурсам архива данных ДЗЗ из космоса
Инструкция	Инструкция администратора информационной безопасности. Инструкция по антивирусной защите. Инструкция по парольной защите. Процедуры контроля работоспособности системы и компонентов, обеспечивающих защиту информации

Библиография

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

[2] Банк данных угроз безопасности информации [Электронный ресурс] URL: gost.e-ecolog.ru

[3] Методический документ «Методика оценки угроз безопасности информации» (утвержден ФСТЭК России 5 февраля 2021 г.)

[4] Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»

[5] Методический документ «Меры защиты информации в государственных информационных системах» (утвержден ФСТЭК России 11 февраля 2014 г.)

[6] Уголовно-процессуальный кодекс Российской Федерации от 18 декабря 2001 г. № 174-ФЗ

[7] Арбитражный процессуальный кодекс Российской Федерации от 24 июля 2002 г. № 95-ФЗ

[8] Гражданский процессуальный кодекс Российской Федерации от 14 ноября 2002 г. № 138-ФЗ

[9] Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ

[10] Методический документ «Профиль защиты межсетевых экранов типа «А» третьего класса защиты» ИТ.МЭ.А3.ПЗ (утвержден ФСТЭК России 12 сентября 2016 г.)

[11] Методический документ «Профиль защиты систем обнаружения вторжений уровня сети третьего класса защиты» ИТ.СОВ.С3.ПЗ (утвержден ФСТЭК России 3 февраля 2012 г.)

[12] Методический документ «Профиль защиты межсетевых экранов типа «А» четвертого класса защиты» ИТ.МЭ.А4.ПЗ (утвержден ФСТЭК России 12 сентября 2016 г.)

[13] Методический документ «Профиль защиты межсетевых экранов типа «Г» четвертого класса защиты» ИТ.МЭ.Г4.ПЗ (утвержден ФСТЭК России 12 сентября 2016 г.)

[14] Методический документ «Профиль защиты систем обнаружения вторжений уровня сети четвертого класса защиты» ИТ.СОВ.С4.ПЗ (утвержден ФСТЭК России 3 декабря 2012 г.)

УДК 528.8:006.354

ОКС 35.240.70
49.140

Ключевые слова: данные дистанционного зондирования Земли, архив данных, информационная безопасность, защита информации, угрозы информационной безопасности

Редактор *Е.Ю. Митрофанова*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 17.07.2023. Подписано в печать 27.07.2023. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 1,86. Уч.-изд. л. 1,23.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru