



Студенттер мен жас ғалымдардың  
**«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»**  
XIII Халықаралық ғылыми конференциясы

**СБОРНИК МАТЕРИАЛОВ**

XIII Международная научная конференция  
студентов и молодых ученых  
**«НАУКА И ОБРАЗОВАНИЕ - 2018»**

The XIII International Scientific Conference  
for Students and Young Scientists  
**«SCIENCE AND EDUCATION - 2018»**



12<sup>th</sup> April 2018, Astana

**ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ  
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ**

**Студенттер мен жас ғалымдардың  
«Ғылым және білім - 2018»  
атты XIII Халықаралық ғылыми конференциясының  
БАЯНДАМАЛАР ЖИНАҒЫ**

**СБОРНИК МАТЕРИАЛОВ  
XIII Международной научной конференции  
студентов и молодых ученых  
«Наука и образование - 2018»**

**PROCEEDINGS  
of the XIII International Scientific Conference  
for students and young scholars  
«Science and education - 2018»**

**2018 жыл 12 сәуір**

**Астана**

**УДК 378**

**ББК 74.58**

**Ғ 96**

Ғ 96

«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: <http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/>, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

**ISBN 978-9965-31-997-6**

Жинаққа студенттердің, магистранттардың, докторанттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

©Л.Н. Гумилев атындағы Еуразия  
ұлттық университеті, 2018

MathLab с чертежными программами вроде AutoCAD. Если после проектирования космического аппарата необходимо рассчитать смету и передать данные в бухгалтерскую программу, то программы должны быть взаимосвязаны. Такая интеграция может позволить облегчить и улучшить автоматизацию технологического процесса производства и работать в одной среде.

#### Список использованных источников

1. Официальный сайт Autodesk. Сайт-источник: <https://www.autodesk.ru/>
2. Выбор системы САПР. Сайт-источник: <http://www.automationlabs.ru/index.php/sw/134-2008-06-23-14-40-17>
3. Михайлов А. Что нового в AutoCAD 2018. Март 2017. Сайт-источник: <https://mikhailov-andrey-s.blogspot.com/2017/03/что-нового-v-autocad-2018-1.html>
4. Бутяга С. Creo 3: игра по новым правилам // Control Engineering Россия, Май 2015, стр. 86-88.
5. Выбираем программу САПР: Inventor или Solidworks. Сайт-источник: <http://glavconstructor.ru/articles/programs/inventor-solidworks/>
6. Официальный сайт Solidworks. Сайт-источник: <http://www.solidworks.com/>
7. PTC Creo Parametric // Сайт-источник: <http://www.ptc.ru.com/cad/creo>
8. SWR-Технология. Система подготовки технологической документации. Сайт-источник: <http://solidworks.tpu.ru/chapter.php?cid=85>
9. Официальный сайт Kompas. Сайт-источник: <http://kompas.ru/>
10. Основы систем автоматизированного проектирования. Сайт-источник: <http://bourabai.kz/cm/cad.htm>

УДК 654.1

### КОМПЛЕКС РЕШЕНИЙ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ЭЛЕМЕНТОВ НАЗЕМНОГО СЕГМЕНТА КОСМИЧЕСКОЙ СИСТЕМЫ ИССЛЕДОВАНИЯ ЗЕМЛИ

**Бакашев Галым Юсупжанович, Талбаев Мирас Канатович**

Студенты ЕНУ им. Л.Н. Гумилева, Астана, Казахстан

Научный руководитель - Муханбеткалиева А.К.

#### Введение

Важную роль в корректном функционировании и развитии элементов наземного сегмента космической системы ДЗЗ (КС ДЗЗ) играет эффективное использование, своевременное получение, безопасная передача и надежное хранение служебной информации. Наземный сегмент, связанный информационными и управляющими радиолиниями с космическим аппаратом требует обеспечения комплексной защиты, так как выполняет функцию по координированию функционирования всех элементов спутниковой системы.

В состав наземного сегмента космической системы дистанционного зондирования Земли обычно входят:

- наземный комплекс управления космическим аппаратом и приема данных;
- комплекс обработки данных;
- комплекс хранения данных.

Некоторые операторы космических систем ДЗЗ включают в наземные сегменты дополнительные комплексы и системы, такие как комплекс тематической обработки, комплекс обработки информации детального разрешения, комплекс взаимодействия с потребителями данных ДЗЗ. Некоторые космические агентства используют сети приемных станций глобального размещения, например USGS (США), Европейское космическое

агентство (ESA), Индийское космическое агентство (ISRO).

Наземный комплекс управления космическим аппаратом и приема данных состоит из центра управления спутником, центра управления миссией спутника, приемо-передающей наземной станции. Центр управления спутником служит для контроля и управления космическим аппаратом посредством приема и передачи служебной информации, центр управления миссией планирует работу полезной нагрузки спутника, приемно-передающая наземная станция служит для приема и передачи служебной в S-диапазоне и полезной информации со спутника на наземный сегмент в X-диапазоне. Схема элементов наземного сегмента космической системы ДЗЗ приведена на рисунке 1.



Рисунок 1 –Схема наземного сегмента космической системы ДЗЗ

Данные полезной нагрузки могут передаваться на Землю сразу в процессе съемки, если спутник находится в зоне радиовидимости приемной станции, или сохраняются в бортовом накопителе и передаются при ближайшем контакте с наземной приемной станцией.

При выполнении задач наземного сегмента важную роль играет обеспечение конфиденциальности, достоверности и целостности передаваемых данных между элементами системы наземного сегмента. Для обеспечения защиты передаваемых и обрабатываемых данных между элементами систем наземного сегмента требуется комплекс решений позволяющих снизить риск возникновения угроз информационной безопасности, которые могут привести к выводу из строя программно-аппаратных средств.

В работе планируется проведение анализа существующих угроз, рассмотрение методов и средств противодействия данным угрозам в комплексе предварительной и стандартной обработки наземного сегмента.

Объектами защиты в комплексе обработки данных наземного сегмента являются спутниковые изображения, их метаданные в сыром виде и после различных видов обработки, промежуточные папки хранения в процессе обработки, базы данных каталогов, непосредственно сами программы обработки.

1. Особенности защиты информации в комплексе обработки данных наземного сегмента КС ДЗЗ

В комплексе предварительной и стандартной обработки данных наземного сегмента спутниковые изображения, полученные непосредственно со спутника приемной станцией проходят предварительную обработку, радиометрическую и геометрическую коррекцию, затем данные о снимках (квиклуки и метаданные) заносятся в локальный каталог, и в случае наличия во внешний интернет-каталог для публикации данных. Космические снимки – это набор данных, включающие непосредственно спутниковые изображения, метаданные, квиклуки.

Информационная система комплекса предварительной и стандартной обработки данных состоит из нескольких обрабатывающих блоков (программ, или приложений), базы данных локальных каталогов «сырых» (необработанных) и обработанных данных (рисунок2). Движение данных из одного блока в другой осуществляется в соответствии с технологической схемой обработки. Система приема данных отвечает за распаковку данных полезной нагрузки, корреляции метаданных с «сырыми» данными, затем в программе радиометрической коррекции проводится обработка для снижения неточностей и ошибок

вносимых датчиками съемочного прибора, сбойными пикселями, радиометрическая калибровка с использованием данных телеметрии, поступающих со спутника вместе с изображением и калибровочных коэффициентов, рассчитываемых для каждого съемочного прибора по результатам наземных и летных испытаний. Далее проводится геометрическая коррекция данных, которая включает в себя устранение на изображении геометрических искажений (вследствие кривизны Земли, неровности рельефа) и географическую привязку. Затем информация по принятым снимкам заносится во внутренний и внешний каталоги, сами снимки размещаются в архиве данных.

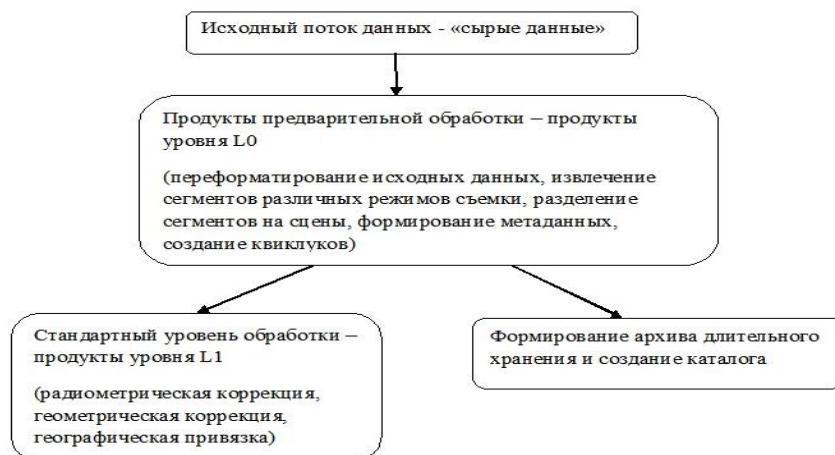


Рисунок 2 –Технологическая схема предварительной и стандартной обработки данных ДЗЗ

Спутниковые изображения имеют различную степень секретности в зависимости от пространственного разрешения, разную информативность в зависимости от стадии обработки, различную значимость в зависимости от оперативности информации. Хранимую и обрабатываемую в комплексе обработки информацию можно разделить на: необработанные данные («сырые данные»), принимаемые со спутников ДЗЗ, и продукты стандартной обработки снимков.

## 2. Классификация потенциальных угроз комплекса обработки данных

Система защиты информации представляет собой комплекс программных, программно-аппаратных и технических средств защиты информации (антивирусов, межсетевых экранов, систем обнаружения вторжений, систем контроля доступа и т.п.). При построении такой системы защиты информации в большинстве случаев учитываются **технологические угрозы информационной безопасности**, кроме того существуют антропогенные и техногенные угрозы и форс-мажорные обстоятельства.

В качестве антропогенного источника угроз рассматривают субъекта, имеющего доступ (санкционированный или несанкционированный) к работе со штатными средствами защищаемого объекта.

Техногенные угрозы содержат источники угроз, вызванных физическим и моральным устареванием технического парка используемого оборудования, а также отсутствием материальных средств на его обновление. Технические средства, являющиеся источниками потенциальных угроз безопасности информации, могут быть внешними (средства связи; сети инженерных коммуникаций; транспорт) и внутренними (некачественные технические средства обработки информации; некачественные программные средства обработки информации; вспомогательные средства и т.д.).

К форс-мажорным обстоятельствам относятся стихийные источники потенциальных угроз информационной безопасности, являющиеся внешними по отношению к защищаемому объекту: пожары; землетрясения; наводнения; различные непредвиденные обстоятельства.

## 3. Обеспечение безопасности программно-техническими методами

### 3.1 Многоуровневое разграничение доступа субъектов к информации

В зависимости от секретности и ценности спутниковых изображений и продуктов на их основе необходимо определить многоуровневое разграничение доступа субъектов к информации баз данных каталогов и хранилищу данных. Для обеспечения наиболее гибкого подхода необходимо разграничить права субъектов на уровнях разрешения или запрета работы:

- с семантикой объектов снимка;
- с объектами снимка определенного уровня секретности;
- с векторными слоями снимка и его продуктов в зависимости от уровня секретности объектов снимка группирующихся в определенные слои;
- с электронными снимками и его продуктами, к которым он допущен по назначенным правам;
- с районами работ (участок местности с граничными значениями широты и долготы, к которому разрешен доступ субъекту);
- со снимками определенного уровня секретности в зависимости от пространственного разрешения.

### 3.2 Обеспечение безопасности WEB-серверов (сервер публикации космических снимков), защита информации при передаче

Для решения вопроса о разграничении доступа к объектам Web-сервиса (внешний каталог) необходимо определить объекты защиты, идентифицировать субъекты разного уровня доступа и выбрать модель управления доступом - принудительную или произвольную.

Конфигурация сетевой инфраструктуры значительно влияет на обеспечение безопасности web-сервера. При разработке конфигурации сети, необходимо обязательно учитывать требований обеспечения безопасности web-сервера. Безопасность web-сервера должна обеспечиваться с помощью многоуровневых и распределенных механизмов обороны. Учитывая, важность защищаемой информации следует применять демилитаризованную зону (DMZ) с двумя межсетевыми экранами.

Демилитаризованная зона применяется для предотвращения доступа из внешней сети к хостам внутренней сети, что осуществляется путем выноса из локальной сети в особую зону всех сервисов, требующих доступа извне. DMZ будет отдельной подсетью с публичными адресами, защищенной (или - отделенной) от публичных и корпоративных сетей межсетевыми экранами.

При этом возникает необходимость обеспечения разграниченного доступа к ресурсам и серверам, расположенным в DMZ, конфиденциальности информации, передаваемой при работе пользователей с этими ресурсами, контроля за действиями пользователей. Так как публичные сервисы могут быть взломаны, на них должна находиться наименее важная информация, а любая ценная информация должна размещаться исключительно в локальной сети, которая не будет доступна с публичных серверов.

Выбор DMZ с двумя межсетевыми экранами обеспечит достаточную защиту, так как выделенные межсетевые экраны могут иметь более сложные и сильные наборы правил безопасности. Выделенный межсетевой экран может анализировать входящий и исходящий HTTP-трафик, определить атаки прикладного уровня, направленные на web-сервер, и защитить от них.

Преимущества создания DMZ для обеспечения безопасности: оптимизированная поддержка и защита web-сервера и возможность анализа сетевого трафика от и к web-серверу. Компрометация web-сервера непосредственно не угрожает внутренней сети предприятия.

Недостатки DMZ при обеспечении безопасности: DoS-атаки, направленные на web-сервер, могут воздействовать на внутреннюю сеть.

Для решения проблем защиты информации при передаче применяются защищенные информационные каналы. Реализация защиты осуществляется дополнительными приложениями – межсетевыми экранами: и со стороны сервера, и со стороны клиента

добавляются программы, обеспечивающие обмен ключами (паролями) и шифрование/дешифрование данных. Межсетевой экран проводит фильтрацию потока данных, шифрование и имитозащиту данных при передаче, идентификацию и аутентификацию сетевых узлов, обнаружение несанкционированного доступа (НСД) со стороны внешних сетей, антивирусную защиту, скрытие топологии сети, протоколирование, оповещение о НСД.

#### **Выводы**

В результате проделанной работы выявлены особенности защиты информации в комплексе обработки данных, определены объекты защиты и потенциальные угрозы, рассмотрены методы защиты при публикации данных ДЗЗ в сети Интернет.

Предложенные решения могут быть использованы при организации защиты информации комплекса обработки данных наземного сегмента и организации работы внешнего каталога оператора космических снимков.

#### **Список использованных источников**

1. Дворкин Б.А., Элердова М.А. Особенности наземных сегментов современных космических систем ДЗЗ // ГЕОМАТИКА №3, 2010, стр.19-24.
2. Федоткин Д.И. Технологии предварительной обработки данных ДЗЗ: опыт ИТЦ «СканЭкс» в создании программного обеспечения и организации обработки данных в составе приемных комплексов // Пространственные данные. 2006, №1.
3. Шатунов С.В. Особенности защиты информации в географических информационных системах // Информационное противодействие угрозам терроризма. 2007, №6, стр. 20-24.
4. Вихорев С.В. Как оценить угрозы безопасности // Технологии и средства связи. 2000, №5.
5. Быстров В.В., Маслобоев А.В., Путилов В.А. Применение проектного менеджмента в задачах управления региональной безопасностью: подход и формальный аппарат // Надежность и качество сложных систем. 2017, №4, стр. 73-84.
6. Иванкова М.В., Бростилов С.А., Куличенко И.В., Бростилова Т.Ю., Баннов В.Я. Система автоматизированного хранения и выдачи ключей // Труды международного симпозиума «Надежность и качество», 2017, т.2, стр.5-6.

УДК 629.78.01

### **ҒАРЫШТЫҚ АППАРАТТАРДЫҢ ТЕРМОРЕТТЕУ ЖҮЙЕСІН ЖЕТІЛДІРУ**

<sup>1</sup>Баткульдинова Камила Канатовна, <sup>2</sup>Әбдірашев Өмірзақ Көптілеуұлы,

<sup>3</sup>Жебеген Гулдана Аршынбекқызы, <sup>3</sup>Жомартбекқызы Дильназ

Л.Н. Гумилев атындағы ЕҰУ, Физика-техникалық факультет,

<sup>1</sup>Ғарыштық техника және технологиялар кафедрасының 3-курс студенті,

<sup>2</sup>Ғарыштық техника және технологиялар кафедрасының оқытушысы

<sup>3</sup>Ырғыз гимназиясының оқушысы

Ғылыми жетекшісі – Тасболат Айнұр Қазтайқызы

Ғарыштық аппараттардың (ҒА) сапасының негізгі көрсеткіштеріне олардың сенімділігі мен орбитадағы белсенді өмір сүру уақыты (БӨС) болып табылады. 1957 жылғы 4 қазанда ұшырылған ПС-1 алғашқы серіктің сенімді жұмыс істеуін қамтамасыз ету үшін, диаметрі 580 мм болатын сфералық контейнер түрінде жасалған, 2 мм қалыңдығы АМgб парағының қорытпасынан жасалған екі сфералық жартылай қабықтан тұратын (спутниктің көлеміндегі жылу режимі термостатта 30 ° С тең немесе одан жоғары температурада қосылған желдеткіш арқылы қамтамасыз етілген термиялық реттеу жүйесі пайдаланылды.