СТРУКТУРА ЗАЩИТЫ ИНФОРМАЦИИ В МЕЖДУНАРОДНОЙ ГИДРОГРАФИЧЕСКОЙ ОРГАНИЗАЦИИ

Михайлов С., Шевцов Ю.

Публикация «S-63 IHO Data Protection Scheme» («Схема защиты данных Международной гидрографической организации»), далее называемая «схемой», описывает рекомендуемый стандарт защиты информации электронной навигационной карты (ЭНК). Он определяет конструкции безопасности и рабочие процедуры, которые должны соблюдаться для обеспечения правильной работы схемы защиты данных и предоставления спецификаций, позволяющих участникам создавать системы, совместимые с S-63, и распространять данные безопасным и коммерчески жизнеспособным способом.

Стандарт «Защита информации электронных картографических навигационных систем» был принят в качестве официального стандарта МГО государствами-членами МГО в декабре 2002 года (IHO CL 66, 2002). Он определяет роли и обязанности по защите данных электронной навигационной карты (ЭНК), созданных Национальными гидрографическими службами, и распространяется среди клиентов с системами ECS/ ECDIS (Система отображения электронных карт и информации).

Ключевые слова. Стандарт защиты информации, электронная навигационная карта, гидрографическая служба.

ОБЩЕЕ ОПИСАНИЕ

В этом документе описывается метод защиты информации электронных навигационных карт (ЭНК) и поддержания целостности службы ЭНК с несколькими службами данных, обслуживающими большую клиентскую базу. Защита данных имеет три раздела: 1.Защита от пиратства: для предотвращения несанкционированного использования данных путем шифрования информации электронной навигационной карты(ЭНК); 2.Селективный доступ: для ограничения доступа к информации электронных навигационных карт (ЭНК) только тех клиентов, которые поставлены на учет; 3.Аутентификация: обеспечить уверенность в том, что данные электронной навигационной карты (ЭНК) поступают из официальных источников.

Защита от пиратства и выборочный доступ достигаются за счет шифрования информации электронных навигационных карт (ЭНК) и предоставления разрешений ячеек для их расшифровки. Серверы данных будут шифровать данные электронных навигационных карт (ЭНК), предоставленные странами-производителями, прежде чем отправлять их клиенту данных. Зашифрованная электронная навигационная карта (ЭНК) затем дешифруется ECS / ECDIS до того, как будет переформатирована и импортирована в системную электронную

навигационную карту (SENC). Аутентификация обеспечивается посредством цифровых подписей в данных. В схеме конкретно не рассматривается способ защиты информации электронной навигационной карты (ЭНК) или системной электронной навигационной карты (SENC), когда она находится в приложении конечного пользователя. Это ответственность производителя оригинального оборудования. Схема позволяет для массовой рассылки зашифрованных электронных навигационных карт (ЭНК) на жестком носителе (например, CD-ROM или DVD) и может быть использована для всех клиентов с действующей лицензией, содержащей набор разрешений. Избирательный доступ к отдельным ячейкам поддерживается за счет предоставления пользователям с лицензированным пакетом разрешающих документов, содержащий зашифрованные ключи. Эта лицензия создана с использованием уникального идентификатора оборудования системы и является уникальным для каждого клиента данных. Следовательно, лицензии не могут быть обменены между индивидуальными клиентами информации. В схеме используется алгоритм сжатия для уменьшения размера набора данных. Незашифрованные данные электронных навигационных карт содержат много повторяющихся шаблонов информации, например, координатная информация. Поэтому сжатие всегда применяется до того, как информация электронных навигационных карт зашифрована и не сжата после дешифрования в клиентской системе данных (как правило, электронная навигационная карта (ECS) или система отображения электронных карт и информации(ECDIS). Существует несколько типов пользователей схемы: администратор схемы (АС), который всегда один; сервер данных (СД), которых может быть много; клиент данных (КД), которых может быть много; производитель оригинального оборудования, которых может быть много. Более подробное объяснение этих терминов приведено ниже.

Администратор схемы.

Администратор несет полную ответственность за поддержание и координацию схемы. Роль администратора схемы реализуется Международным гидрографическим бюро (IHB) в качестве секретариата МГО от имени государств-членов МГО. Администратор схемы отвечает за контроль членства в схеме и обеспечение того, чтобы все участники работали в соответствии с определенными процедурами. Администратор схемысохраняет цифровой сертификат верхнего уровня, используемый для работы со «Схемой защиты данных», и является единственным органом, который может подтвердить личность других участников схемы. Администратор схемы также является хранителем всей документации, относящейся к схеме защиты данных.

Серверы данных.

Серверы данных отвечают за шифрование и подпись данных электронной навигационной картыв соответствии с процедурами и процессами, определенными в схеме. Серверы данных выдают лицензии электронной навигационной карты т.е разрешения, чтобы клиенты данных с действительными разрешениями пользователей могли расшифровать данные электронной навигационной карты. Серверы данных будут использовать информацию уникального идентификационного ключа (M_KEY) и уникального идентификатора (HW_ID), предоставленную администратору схемы, для выдачи зашифрованных ключей ячейки электронной навигационной карты для каждой конкретной установки. Несмотря на то, что ключи ячейки, используемые для шифрования каждой ячейки, идентичны, они будут зашифрованы с использованием уникального идентификатора(HW_ID) и поэтому не могут быть переданы между другими системами отображения электронных карт и информации (ECDIS) от того же производителя. Примерами серверов данных являются гидрографические офисы, реселлеры с добавленной стоимостью и региональным координационным центром электронной навигационной карты.

Клиенты данных.

Клиенты данных являются конечными пользователями информации электронной навигационной картыи получают защищенную информацию от серверов данных. Программное обеспечение клиента данных отвечает за аутентификацию цифровых подписей электронной навигационной картыи дешифрование информации электронной навигационной карты в соответствии с процедурами, определенными в схеме. Эта схема не мешает агентам или дистрибьюторам предоставлять услуги передачи данных своим клиентам.

Оригинальный производитель оборудования.

Производители оборудования и программного обеспечения должны создавать программное приложение и самостоятельно проверять и проверять его в соответствии с условиями, предусмотренными администратором схемы. Стандарт S-63 содержит тестовые данные для проверки и проверки приложений. Администратор схемы предоставит успешным OEM-производителям собственный уникальный ключ производителя и идентификацию (M_KEY и M_ID). Изготовитель должен обеспечить безопасный механизм в своих программных системах для уникальной идентификации каждой установки конечного пользователя. Схема требует, чтобы каждая установка имела уникальный идентификатор оборудования (HW_ID). Программное приложение сможет расшифровывать ключи ячейки с помощью уникального

идентификатора оборудования (HW_ID), хранящегося в аппаратных или программных средствах, подключенных или запрограммированных в приложении, чтобы впоследствии расшифровать и открыть данные электронной навигационной карты. Затем значение циклической проверки избыточности(CRC), содержащееся в электронной навигационной карте (ENC), может быть проверено для установления целостности базовых данных.

Взаимодействие участников схемы.

Администратор схемы, который может быть только один, аутентифицирует личность других участников схемы. Все серверы данных и системные производители должны обратиться к администратору схемы, чтобы стать участниками схемы и при приеме им назначается уникальной для них конфиденциальной информацией. Клиенты данных являются клиентами серверов данных и OEM-производителей, где серверы данных предоставляют услуги передачи данных и OEM-производители оборудование для дешифрования и отображения этих сервисов.

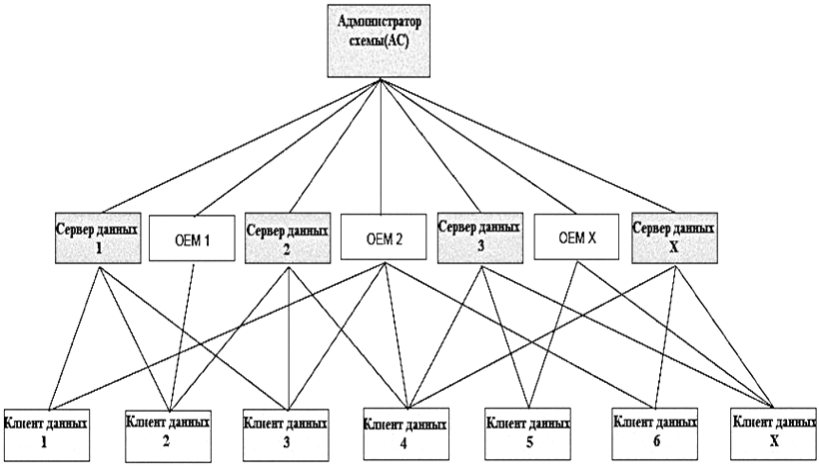

Рис.1– Совместимость с предыдущими версиями

Версия 1.1 стандарта была подготовлена с учетом опыта, накопленного серверами данных и производителями ECS / ECDIS во время работы схемы согласно версии 1.0. Эта версия пытается более четко определить стандарт, удалив дублирование и возможную неопределенность. Она также содержит дополнительные механизмы, которые позволят производителям сделать их системы более интуитивными для пользователей ECS / ECDIS. Перечень изменений в

стандарте. 1. Удаление ненужного дублирования. 2. Спецификация того, как и при каких условиях должны использоваться определенные файлы.

3. Удаление зависимости получения доступа разрешения от редакции ячейки. 4. Дополнительная информация, позволяющая клиентам данных управлять данными ENC более эффективно и эффективно. 5. Идентификация стратегии загрузки для обеспечения более эффективной загрузки зашифрованных ЭНК.

Структура документа

Основная часть документа обычно может быть разбита на четыре части. В первой части подробно описываются компоненты, которые являются фундаментальными для схемы и описывают их назначение и конструкцию. Второй определяет, как все компоненты объединяются в набор обмена электронной навигационной карты(ENC) S-63. Третий описывает роли и обязанности каждого типа пользователей, участвующих в схеме. Наконец, есть раздел, который определяет различные сообщения об ошибках и предупреждениях, которые должны отображаться на клиенте данных при возникновении определенных условий.

ОСНОВНОЙ ДОКУМЕНТ.

1.СЖАТИЕ ДАННЫХ

1.1 Обзор

Файл электронной навигационной карты(ENC) из-за своей структуры содержит повторяющиеся шаблоны информации. Примерами этого являются последовательная нумерация идентификатора объекта (FOID) или небольшие изменения в координатной информации в файле электронной навигационной карты (ENC). Поэтому данные электронной навигационной карты (ENC) хорошо реагируют на сжатие с уменьшением в размере от 30% до 60%, что значительно снижает стоимость передачи данных электронной навигационной карты (ENC) в конечный пункт назначения. Сжаты только файлы электронной навигационной карты ENC (база и обновление). Файлы ENC всегда сжимаются до того, как они зашифрованы, поскольку эффективность любого алгоритма сжатия основана на существовании структурированных данных.

1.2 Алгоритм сжатия

В схеме безопасности используется алгоритм ZIP1 для сжатия и распаковки данных электронной навигационной карты(ENC). Он идентичен алгоритму, используемому во многих коммерческих приложениях, например. WinZip, PKZIP. Потенциальные серверы данных и OEM-производители должны знать, что в прошлом произошли ошибки, когда серверы данных сжимают данные и интерпретируются популярными реализациями алгоритма ZIP как «текстовые» данные.

Если данные не сжаты с неправильными параметрами, это может привести к повреждению файла электронной навигационной карты(ENC), ведущего к ошибкам проверки целостности. Серверу данных и OEM-производителям рекомендуется тщательно выполнять (архивирование) сжатие / несжатие в своих системах.

1.3 Сжатые файлы

Схема безопасности сжимает только базовую ячейку электронной навигационной карты(ENC) и файлы обновлений. Никакие другие файлы в наборе обмена S-57 не будут сжаты.

2.ШИФРОВАНИЕ И ОБРОБОТКА ДАННЫХ

2.1 Какие данные зашифрованы?

В рамках Схемы используется только один алгоритм шифрования. Только данные в файлах электронной навигационной карты (ENC) база или обновленная ячейка внутри набора обмена S-57, то есть текстовых или графических файлов, остаются незашифрованными. Схема шифрует полное содержимое базы данных электронной навигационной карты (ENC) или обновляет файлы данных. Другая информация в шифрованной схеме включает в себя системный идентификатор (HW_ID) OEM-системы, который зашифрован и предоставлен клиенту данных в форме пользовательского ввода. Клавиши соты, используемые для шифрования файлов данных электронной навигационной карты (ENC), сами зашифровываются сервером данных и предоставляются клиентам данных в качестве разрешений сотовой сети.

2.2. Алгоритм шифрования

Каждый отдельный файл ячейки электронной навигационной карты(ENC) шифруется с использованием уникального ключа ячейки. Один и тот же ключ ячейки используется для шифрования всех обновлений, выпущенных для ячейки. Тем не менее, эта схема позволяет увеличивать и изменять ключи ячеек по усмотрению сервера данных. Ключи соты доставляются клиентам данных в виде разрешений на ячейки. Информация электронной навигационной карты ENC(базовые ячейки и обновления) шифруется с использованием 40-битного ключа.

Пользовательское разрешение и содержимое разрешений для ячеек шифруются с использованием 48-битного ключа. Схема шифрует всю информацию, используя алгоритм Blowfish. Алгоритм непатентован и доступен в общественном достоянии (www.counterpane.com). Blowfish - это алгоритм блочного шифрования, который работает с 64-разрядными (8 байт) данными. Это требуется, чтобы источники данных были дополнены, если они не кратны 8 байтам. Схема защиты использует алгоритм заполнения «DESinCBCMode», когда любые источники данных должны быть дополнены. Это соответствует режиму ЭКК (электронная кодовая книга) DES.

3. ЛИЦЕНЗИРОВАНИЕ ДАННЫХ

3.1 Введение

Лицензирование – это метод, которым серверы данных пользуются, чтобы предоставить выборку клиентов, данных современным элементам электронной навигационной карты (ENC) в течение данного периода времени. Чтобы взаимно действовать со схемой фактически должны быть средства, где установки клиента данных могут открыть кодируемые элементы электронной навигационной карты (ENC). Чтобы открыть данные, установка клиента данных должна иметь доступ к кнопочным переключателям с самовозвратом, которые используются, чтобы кодировать элементы электронной навигационной карты (ENC).

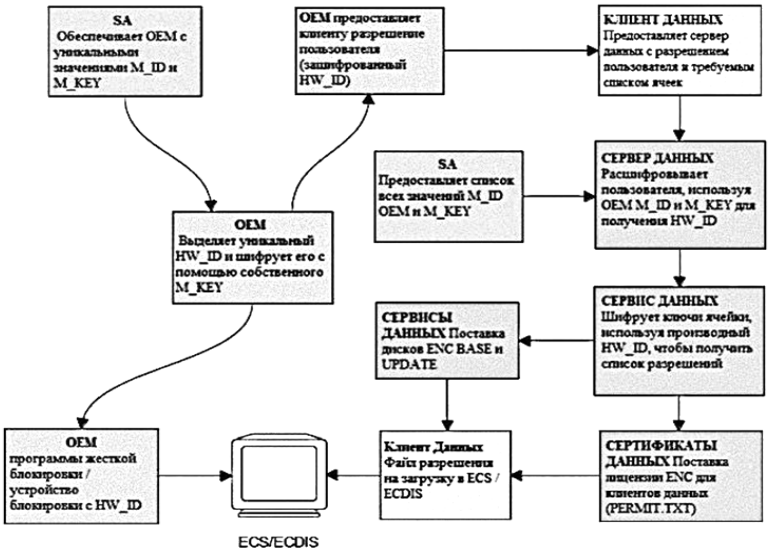

Рис.2 – Схема лицензирования ENC высокого уровня

Эти кнопочные переключатели с самовозвратом поставляются клиенту, чтобы кодировать, в файле разрешения. Чтобы сделать каждый набор, клеточные разрешения эксклюзивны, клеточные кнопочные переключатели с самовозвратом должны кодироваться, набор и комбинация, этот уникальный для каждого клиента данных. Оригинальные производители оборудования назначают уникальное имя, уникальный идентификатор (Hw_id) каждой из их установок и обеспечивают кодируемую копию в форме пользовательского разрешения, к каждому клиенту данных. Уникальный идентификатор (Hw_id), сохраненный в пользовательском разрешении кодирует оригинальных производителей оборудования, кодируют уникальный

идентификатор (Hw_id)с их собственным уникальным кнопочным переключателем изготовителя (M_key) с самовозвратом таким образом, что уникальный идентификатор (Hw_id) не может копировать другой изготовитель. Серверы данных имеют доступ к оригинальным производителям оборудования уникальным кнопочным переключателям производителя (M_keys) и могут, поэтому расшифровать уникальный идентификатор (Hw_id), сохраненный в пользовательском разрешении.

Серверы данных кодируют свои кнопочные переключатели с самовозвратом с изготовителями уникального идентификатора (Hw_id), производя набор клеточных разрешений.

3.2 Пользовательское разрешение.

Пользовательское разрешение создает оригинальное производительское оборудования и поставляется клиентам данных как часть их оборудования таким образом, что они могут получить необходимый доступ к кодируемым электронным навигационным карт (Encs) от серверов данных. Следующая секция определяет композицию и формат пользовательского разрешения. Все клиенты данных с установками, способными к пользованию данными, защищенными со схемой S- 63, должны иметь уникальную аппаратную идентификацию, уникальный идентификатор (Hw_id), что вместе определяет потребителя.

Такой уникальный программный идентификатор (Hw_id) часто реализуется как механизм защиты от несанкционированного копирования или другими средствами, гарантирующими уникальную идентификацию для каждого оборудования. Уникальный идентификатор (Hw_id) неизвестен клиенту данных, но оригинальное производительское оборудование обеспечит пользовательское разрешение, которое кодируемый вариант уникального идентификатора (Hw_id) и уникальный для данного клиента данных. Пользовательское разрешение создает взятие заданного уникального идентификатора (Hw_id) и кодируя это с кнопочным переключателем изготовителя (M_key) с самовозвратом. Циклическая проверка избыточности (CRC)32 алгоритм есть бегут на кодируемом уникальном идентификаторе (Hw_id) и результат присоединил к этому. Наконец изготовитель прилагает их заданный идентификатор изготовителя (M_id) до конца получающейся строки. Уникальный идентификационный ключ (M_key) и уникальный идентификатор (M_id) поставляет администратор схемы и они уникальны для каждого изготовителя. Клиент данных получает доступ к S-63 кодируемые электронные навигационные карт (Encs), сообщая это пользовательское разрешение серверу данных, кто может затем выдать специфику клеточных разрешений. Поскольку пользовательское разрешение содержит уникальный идентификатор (M_id), это может быть использовано серверами данных, чтобы идентифицировать уникальный идентификационный ключ (M_key), чтобы затем

использовать его для расшифровки данных. Список изготовителя уникального идентификационного ключа (M_key) и уникальный идентификатор (M_id) выпущен и обновлен администратором схемы ко всем серверам данных, подписывающимся на схему. Этот список будет обновлен периодически как новые оригинальные производительские оборудования будут присоединяться к схеме.

3.2.1 Определение разрешения пользователя.

Разрешение пользователя состоит из 28 символов и должно быть записано в виде текста американского стандартного кода для обмена информацией (ASCII) со следующим обязательным форматом и длиной поля:

Зашифрованный HW_ID	Проверка суммы (CRC)	Идентификатор производителя M_ID
16 символов	8 символов	4 символа

Любой алфавитный символ может быть записан в верхнем регистре.
Пример: Пользовательское разрешение
:73871727080876A07E450C043031
Первые 16 символов - Зашифрованный HW_ID
Следующие 8 символов-Проверка суммы (CRC)
Последние 4 символа-Идентификатор производителя M_ID

3.2.2 Формат HW_ID.

HW_ID - это пятизначное шестнадцатеричное число, определенное оригинальным производителем оборудования. Такой уникальный идентификатор (HW_ID) может быть реализован как ключ или другими средствами, обеспечивающими уникальную идентификацию каждой установки. Уникальный идентификатор (HW_ID) должен храниться в системе безопасным образом. Оригинальный производитель оборудования(OEM)должен назначить уникальный идентификатор (HW_ID)для каждой установки. Рекомендуется, чтобы уникальный идентификатор(HW_ID)не были последовательными. Он будет храниться в зашифрованном виде пользовательского разрешения. Уникальный идентификатор (HW_ID) зашифрован с использованием алгоритма шифрования (Blowfish) с уникальным идентификационным ключом (M_KEY) в качестве ключа, приводящего к шестнадцатеричному числу (8 байтов). Зашифрованный идентификатор (HW_ID) затем представляется в форме американского стандартного кода для обмена информацией (ASCII) в пользовательском разрешении как 16 символов. Пример HW_ID: A79AB. Пример зашифрованного HW_ID: 73871727080876A0

3.2.3. Формат суммы (CRC).

Сумма проверки - это шестнадцатеричное число извосьми символов. Оно генерируется за счет зашифрованного уникального

идентификатора (HW_ID) и преобразования его в шестнадцатеричный вид. Затем он хешируется с использованием алгоритма CRC32 и байта, преобразованного в шестнадцатеричную строку с 8-ми символами. Контрольная сумма не зашифрована и позволяет проверять целостность разрешения пользователя. Контрольная сумма в приведенном выше примере: 7E450C04

3.2.4 Формат M_ID.

M_ID - представляет собой двухсимвольный буквенно-цифровой код, выраженный как представление американского стандартного кода для обмена информацией (ASCII), предоставляемое администратором схемы. Администратор схемы предоставит всем лицензированным производителям собственную уникальную комбинацию ключей и идентификаторов производителя (M_KEY и M_ID).Изготовитель должен защитить эту информацию. Администратор схемы предоставит всем лицензированным серверам данных полный список всех заводских кодов, когда новые производители подписываются на эту схему. Эта информация используется сервером данных для определения того, какой ключ (M_KEY) используется для дешифрования уникального идентификатора (HW_ID) в пользовательском разрешении во время создания разрешений на ячейку клиента данных. Уникальный идентификатор (M_ID) в приведенном выше примере: 01 или 3031 (ASCII3).

3.2.4 Формат M_KEY.

M_KEY представляет собой пятизначное шестнадцатеричное число, предоставленное администратором схемы(SA). Оригинальный производитель оборудования использует этот ключ для шифрования назначенного идентификатора (HW_ID) при создании разрешений пользователя. Оригинальный производитель оборудования должен хранить его надежно. Этот ключ используется сервером данных для дешифрования назначенных идентификаторов (HW_ID). Пример уникального идентификационного ключа (M_KEY) - 123AB или 3132334142 (ASCII)

3.3 Разрешение ячейки.

Чтобы расшифровать ячейку электронной навигационной карты, клиент данных должен иметь доступ к ключу шифрования, используемого для его шифрования. Поскольку ключи шифрования известны только серверу данных, должно быть средство доставки этой информации клиентам данных защищенным образом. Эта информация предоставляется сервером данных, например, региональный координационный центр электронной навигационной карты (RENC) клиенту данных в зашифрованном виде, известном как разрешение ячейки. Для доставки разрешения ячейки предоставляется один файл и называется PERMIT.TXT. Этот файл может содержать несколько

разрешений ячеек на основе покрытия электронной навигационной карты (ENC), требуемого клиентом данных. Файл PERMIT.TXT будет доставлен либо на жестком носителе, либо с использованием онлайн-сервисов в соответствии с рабочими процедурами сервера данных. Эти процедуры будут доступны клиентам данных при покупке лицензии. Каждая запись разрешения ячейки также содержит дополнительные поля, которые предоставляются, чтобы помочь оригинальным производителям оборудования- системам управлять лицензией клиента данных и разрешать файлы с нескольких серверов данных. Клиенты данных могут получить лицензию на доступ к электронной навигационной карте (ENC), предоставив серверу данных свой уникальный пользовательский доступ. Затем серверы данных могут извлекать уникальный идентификатор (HW_ID) из пользовательского разрешения, используя уникальный идентификационный ключ (M_KEY) клиента данных и создавать разрешения для конкретных клиентов на основе этого значения. Поскольку разрешения на ячейки выдаются для определенного уникального идентификатора (HW_ID), онине могут быть переданы между установками (системами клиента данных). Этот способ связывания разрешения с установкой поддерживает создание зашифрованных компакт-дисков, которые распространены среди всех клиентов данных, подписываемых на услугу. Система клиента данных расшифровывает разрешение ячейки, используя назначенный уникальный идентификатор (HW_ID), надежно хранимый с помощью аппаратных или программных средств. Затем расшифрованные ключи ячеек могут использоваться системой для дешифрования ячейки электронной навигационной карты. Т.к. несколько серверов данных создают файлы разрешений для электронной навигационной карты в своей службе, ответственность за управление файлами разрешений от нескольких серверов данных лежит на системе клиента данных.

3.3.1.Файл разрешений (PERMIT.TXT).

Разрешающая способность ячеек всегда предоставляется в файле PERMIT.TXT, имя файла всегда указывается в верхнем регистре (UPPERCASE), равно как и любые алфавитные символы, содержащиеся в файле. Файл полностью закодирован в стандартном коде для (ASCII):

Раздел	**Описание**
:Заголовок	Сюда относится дата создания файла и версия формата.
: Разрешения ENC	ENC (официальные) с сервера данных перечислены в этом разделе.
: Разрешения ECS	ECS (неофициальные) с сервера данных могут быть перечислены в этом разделе.

Сервер данных предоставляет информацию о том, как файлы разрешений будут доступны, будь то на жестких носителях или онлайн-сервисах.

3.3.2 Форматы файлов разрешений – заголовков.

В следующей таблице определяется содержимое, и формат каждого заголовка раздела в файле разрешения.

Раздел	Имя поля	Значение
Дата и время	:Дата	Имя поля, дата и время разделяются символом пробела (SP <h20>). Дата будет указана как YYYYMMDD и время как HH: MM с использованием 24-часовых часов. Пример:: ДАТА 20050809 11:11
Версия мета-разрешения	:Версия	Целое число в диапазоне от 1 до 99. Оно будет увеличено на 1 для каждой новой версии спецификации формата файла разрешения. S-63 Edition 1.1 определяет значение как «2».то есть: ВЕРСИЯ 2
Тип разрешения сотовой ячейки	:ENC	Поле содержит определение разрешений, доступных в лицензии на распространение ENC с сервера данных. В верхнем регистре поле обозначается следующим знаком: ENC
Тип разрешения сотовой ячейки	:ENS	Поле содержит определение мета-разрешений, доступных в лицензии на распространение ECS от DataServer. Поле обозначается следующим ярлыком в верхнем регистре: ECS

Пример:

: DATE 20080809 11:11

: ВЕРСИЯ 2

: ENC [Список разрешенных разрешений ячеек для официальных ENC]

: ECS [Список разрешений для разрешенных ячеек для других векторных продуктов]

3.3.3. Разрешенные поля записи.

Запись разрешения сотовой ячейки состоит из разделенных запятыми полей:

Поле	Значение
Сотовая ячейка	Определено в разделах 4.3.4 и 4.3.5
Индикатор уровня обслуживания	0 для разрешения на подписку 1 для разрешения на покупку
Номер издания [необязательно]	Номер выпуска DSID-EDTN ячейки ENC (только для серверов данных)
Идентификатор сервера данных	Это двухзначный буквенно-цифровой номер, выданный SA
Комментарий	Свободное текстовое поле для комментариев по разрешению ячейки и т.д.

Примечание:

Поле «Номер издания» больше не является обязательным требованием в S-63, версия 1.1. OEM-производители, реализующие

версию 1.1, больше не должны создавать зависимости в своих системах, которая проверяет взаимосвязь между номером издания ENC и ключом ячейки, используемым для его шифрования. Клиенты данных должны проверять, есть ли в строке разрешения действительный ключ ячейки. Серверы продолжают поддерживать файлы версии PERMIT.TXT версии 1.0 до тех пор, пока не будет определено, что он больше не требуется.

3.3.4 Определение разрешения ячейки.

В таблице указаны поля, содержащиеся в разрешении сотовой ячейки, с определением цели каждого из них.

Поле	**Цель**
Имя ячейки	имя ячейки позволяет системам базы данных связывать правильный ключ шифрования с соответствующим зашифрованным файлом ячейки ENC.
Дата истечения срока действия	это срок, когда истекает срок действия лицензии базы данных. Системы должны предотвращать установку новых элементов ENC, новых выпусков или обновлений, созданных после этой даты.
Зашифрованный ключ ячейки 1 (ECK1)	ECK1 содержит ключ дешифрования для текущей версии ячейки ENC.
Зашифрованный ключ ячейки 2 (ECK2)	ECK2 содержит ключ дешифрования, который будет использоваться, когда следующий ключ ячейки будет повторен. Будущий ключ содержится в разрешении соты, чтобы позволить серверам данных периодически изменять Ключ соты без одновременного выдачи новых разрешений ячеек всем Клиентам данных.

3.3.5 Формат разрешений ячеек

Разрешение ячеек должно быть записано в виде текста ASCII со следующим обязательным форматом и длиной поля:

Поле	**Символы**	**Формат**
Имя ячейки	8	Буквенно-цифровую строку, следующую за соглашением, определенным в S-57 Раздел 3.1 Приложение B, раздел 5.6 для имен ячеек, исключая расширение имени файла. Пример: NO4D0613
Срок годности	8	Числовая строка, которая содержит дату истечения срока действия лицензии для каждой ENC в формате YYYYMMDD. Пример: 20000830 (30 августа 2000 г.)
ECK1 и ECK2	16	Ключи ячейки - это 5 байтовых случайных чисел - их шестнадцатеричные представления шифруются с помощью Blowfish, а затем выражаются в шестнадцатеричном виде в разрешении. Примечание. Алгоритм шифрования blowfish приведет к тому, что зашифрованные данные будут дополнены длиной до 8 байтов. Это означает, что зашифрованные сотовые ключи на самом деле имеют длину 8 байтов, хотя они незашифрованы, они всего 5 байтов (10 шестнадцатеричных символов). Пример: ECK1: BEB9BFE3C7C6CE68 ECK2: B16411FD09F96982

Контрольная сумма разрешения ENC	16	Содержит зашифрованную контрольную сумму для Разрешения сотовой ячейки. Он зашифрован с использованием алгоритма Blowfish с конкретным HW_ID клиента данных и является 8-байтным числом. Эта контрольная сумма зашифровывается в отличие от незашифрованной контрольной суммы разрешения пользователя.например Контрольная сумма ENC в приведенном ниже примере: 795C77B204F54D48

ВЫВОДЫ.

Описываемая структура взаимодействия участников МГО позволит существенно повысить уровень информационной безопасности конфиденциальных данных участников и обеспечить защиту информации в электронных картографических навигационных системах.

СПИСОК ЛИТЕРАТУРЫ

[1] Издание S57 3.1: Стандарт передачи IHO для цифровых гидрографических данных.Международное гидрогра-ское бюро. – 114 с.
[2] Стандарт цифровой подписи (DSS), Публикация федеральных стандартов обработки информации (FIPSPub) 186. – 130 с.
[3] Информационные технологии. Взаимосвязь открытых систем. Каталог. Аутентификация. X.509 версия 3 – Международный союз электросвязи. – 64 с.

INFORMATION PROTECTION STRUCTURE IN THE INTERNATIONAL HYDROGRAPHIC ORGANIZATION

Mikhailov S., Shevtsov Yu.

The publication "S-63 IHO Data Protection Scheme", later referred to as "the scheme", describes the recommended standard for the protection of ENC information. It defines security constructs and operating procedures that must be followed to ensure that the data protection scheme is operated correctly and to provide specifications that allow participants to build S-63 compliant systems and distribute data in a secure and commercially viable manner.

The Standard was adopted as the official IHO standard, by the IHO member states in December 2002 (IHO CL 66, 2002). It defines the roles and responsibilities for protecting ENC data produced by National Hydrographic Offices and distributed to customers with ECS / ECDIS systems.

Keywords. Information Security Standard, electronic navigation chart, hydrographic service