УДК 004.056.5:343.326

Харченко В.П., д-р техн. наук
Чеботаренко Ю.Б.
Корченко А.Г., д-р техн. наук
Пацира Е.В., канд. техн. наук
Гнатюк С.А.

КИБЕРТЕРРОРИЗМ НА АВИАЦИОННОМ ТРАНСПОРТЕ

Национальный авиационный университет

Проведен анализ кибертерроризма, выделены основные черты, характеризующие кибертерроризм в гражданской авиации. Выполнена систематизация и классификация кибератак, что позволит осуществлять формализацию возможностей систем противодействия для повышения эффективности их выбора и формировании требований при их разработке

Вступление

Окружающий нас мир был, есть и будет сложным и противоречивым. Все большее число происходящих в нем процессов приобретает глобальный характер. Соблазн найти быстрое и однозначное решение сложных политических, социальных или экономических проблем силовыми противоправными методами привел к возникновению такого опасного явления как терроризм. Не обошло стороной это явление и гражданскую авиацию. К сожалению, новейшие достижения в области компьютерных наук, информационных технологий, средств коммуникации, способствовали не только техническому прогрессу в авиации, но и породили новые виды преступлений. К числу последних относится кибертерроризм.

Целью статьи является качественный анализ явления кибертерроризма на авиационном транспорте, выделение основных его черт, систематизация и классификация кибератак.

Основные определения и понятия

На основе анализа [1 - 3] дадим определения базовым терминам, используемым для освещения понятия кибертерроризма на воздушном транспорте.

Информационная авиационная система (ИАС) – это совокупность взаимосвязанных компонентов (например, систем), представляющих собой информационные, кадровые и материальные ресурсы, процессы и технологии, которые обеспечивают сбор, обработку, преобразование, хранение и передачу информации в авиационной отрасли.

Глобальная навигационная спутниковая система (ГНСС) – это ресурс ИАС, который представляет собой информационную спутниковую систему, позволяющую определять координаты, скорость и направление движения объектов в любой точке земного шара в любое время суток при любой погоде с помощью специальных приемников.

ATN – это ресурс ИАС, который представляет собой сеть авиационной электросвязи (межсетевая структура), которая позволяет обеспечить взаимодействие наземной подсети передачи данных «воздух-земля» и подсети передачи данных бортового оборудования.

GES – это ресурс ИАС, который представляет собой наземную земную станцию фиксированной спутниковой службы, которая расположенная в определенном фиксированном пункте на суше и предназначается для обеспечения фидерной линии в авиационной подвижной спутниковой службе.

Акт незаконного вмешательства (АНВ) – это акты или попытки совершения актов, создающих угрозу безопасности гражданской авиации (ГА) и воздушного транспорта.

Угроза безопасности – потенциально возможное событие, которое может

привести к нежелательному воздействию на характеристики безопасности ресурса ИАС.

Конфиденциальность – базовая характеристика безопасности ресурса ИАС, которая отображает его свойство нераскрытости и доступности без соответствующих полномочий.

Целостность – базовая характеристика безопасности ресурса ИАС, отображающая его свойство противостоять несанкционированной модификации.

Доступность – базовая характеристика безопасности ресурса ИАС, которая отображает его свойство, состоящее в возможности использования соответствующих ресурсов в заданный момент времени согласно установленным полномочиям.

Уязвимость – слабое место в ИАС (ее неспособность противостоять угрозам), которое может быть использовано для реализации угрозы.

Перехват – несанкционированное получение информации незаконным подключением к каналам связи ИАС, визуально или с помощью радиотехнических средств.

Активный перехват – перехват, во время которого у противника есть возможность не только перехватывать информацию, но и влиять на нее, например, задерживать или удалять сигналы, которые передаются каналами связи аэронавигационных систем.

Пассивный перехват – получение информации с возможностью только наблюдать за ее обменом в ИАС и не оказывать на нее никакого влияния.

Прямой перехват – перехват информации путем непосредственного подключения (например, дополнительного терминала) к линии связи ИАС.

Косвенный перехват – перехват информации (например, индуктивных волн) без использования непосредственного подключения к линии связи.

Доступ – это взаимодействие между ресурсами ИАС, которое обеспечивает передачу информации между ними, а в процессе доступа к информации в частности реализуется ее копирование, модификация, уничтожение, инициализация и т.п.

Несанкционированный доступ (НСД) – доступ к ресурсам ИАС осуществляется с нарушением правил разграничения доступа.

Терроризм – умышленные общеопасные действия, посягающие на общественную безопасность, которые направлены на создание в социальной сфере обстановки страха, беспокойства, подавленности с целью прямого или косвенного влияния на принятия любых решений (или отказа от них).

Киберпространство – это полиморфное виртуальное пространство, генерируемое ИАС как в форме сложных миров, так и в простых реализациях типа электронной почты, глобальной навигации и др.

Кибертерроризм – это применение методов терроризма в киберпространстве (например, навязывание ложных координат движущемуся объекту).

Кибератака – меры, предпринимаемые для подрыва безопасности систем или реализация угрозы характеристикам безопасности ресурсам ИАС (например, аэронавигационной) посредством использования их уязвимости.

Объект кибератаки – объекты и системы ГА, находящиеся во взаимодействии с информационной средой.

Субъект кибератаки – источник несанкционированных действий, направленных на объект кибератаки.

Понятие о терроризме

История современного терроризма уходит своими корнями далеко в глубь веков, однако вопросы, связанные с понятием терроризма и его разновидностями по сей день вызывают дискуссии в научных кругах и пока не нашли окончательного ответа. История убедительно подтверждает, что и представители власти, и криминальные элементы в борьбе за свои интересы постоянно обращались к террористическим методам. Предшественники нынешних террористов заложили основы,

начиная с которых терроризм стал принимать свой современный вид. Нельзя бороться с терроризмом, не имея даже малейшего представления о нем, условиях и причинах его возникновения, видах и современных трактовках.

Современный международный терроризм характеризуется [4 - 5]: широким размахом и отсутствием четких государственных границ; связями и взаимодействием с международными террористическими центрами и организациями; строгой организационной структурой (интегрирующую руководящую и оперативную деятельность, разведку и контрразведку, материально-техническое обеспечение, боевые группы, прикрытие и др.); жесткой конспирацией и тщательным отбором кадров; агентурной сетью, охватывающей правоохранительные и государственные органы; отличным техническим оснащением; наличием разветвленной сети конспиративных укрытий, учебных баз и полигонов.

Очевидно, что имея современные средства ведения информационной войны, международный терроризм навязывает людям свои идеи, решает мобилизационные задачи, привлекая как молодежь, так и профессиональных наемников.

Рассматривая различные подходы к классификации терроризма [5] можно сказать, что наиболее распространенными являются следующие триадные формы, основанные на различных признаках, терроризма: 1) социальный; политический; идеологический; 2) угнетенных этнических меньшинств; освободительных движений; индивидов и групп по политическим мотивам с целью изменения политической системы; 3) революционный-контрреволюционный; государственный внутренний; государственный международный; 4) внутренний; транснациональный; международный; 5) ннациональный; идеологический; геополитический [4];

Учитывая международный опыт и практическую сторону осуществления АНВ в деятельность ГА *ICAO* выделяет следующие категории угроз [6]:

– диверсии против воздушных судов (ВС) и аэропортов;

– акты незаконного захвата ВС;

– попытки незаконного захвата ВС;

– использование ВС как оружия;

– нападения на ВС в полете;

– нападения на сооружения и средства аэропорта;

– другие акты, направленные против безопасности ГА (угрозы, которые не входят в предыдущие категории).

Особенности кибертерроризма

Спектр проявлений кибертерроризма достаточно широк – от незаконного провоцирования принятия ложных решений или распространения паники и беспорядков, до проникновения в каналы и системы спутниковой связи и навигации, например, для введения ложного информационного ресурса или умышленного нарушения его целостности [7].

Кибертерроризм стал возможен вследствие возникновения и развития глобального информационного пространства. Именно глобальный характер технической базы кибертерроризма и ее доступность определили особенные черты этого вида терроризма: высокая эффективность кибератак, последствия которых могут иметь глобальный характер; пространственную неопределенность источника кибератаки; временную неопределенность и несоответствие во времени собственно кибератаки и процесса ее подготовки; возможность организации сложных кибератак одновременно на различные ИАС с различных направлений; анонимность преступления (для совершения террористического акта злоумышленнику нет необходимости пересекать границы государств и находиться непосредственно на месте преступления); снижение уровня морально-психологического давления на субъект кибератаки, связанное с пространственно-временной удаленностью от объекта кибератаки (вся борьба для субъектов кибератаки происходит в виртуальном киберпространстве); доступность

технических средств для совершения преступления (в большинстве случаев для этого необходим только компьютер с доступом в ИАС); акты кибертерроризма совершаются людьми с высоким интеллектуальным потенциалом.

Проблема кибертерроризма в гражданской авиации стала настолько очевидной и серьезной, что заставляет глубоко и всесторонне анализировать, изучать эту проблему, а затем предпринимать активные действия, направленные на предупреждение его проявлений.

Международное авиационное сообщество уделяет проблеме предупреждения кибертерроризма большое внимание. Определенные шаги в этом направлении предприняты ICAO. Так, в октябре 1998 года ассамблеей ICAO единогласно была принята резолюция, в которой особое внимание уделено некоторым правовым и техническим аспектам этой проблемы. Резолюция А32-2 призывает сотрудничающие в области гражданской авиации государства к разработке и внедрению новых эффективных средств противодействия растущей угрозы кибертерроризма. Однако, несмотря на уже предпринятые в этом направлении шаги, угроза применения актов кибертерроризма в авиации растет значительно более высокими темпами, чем методы ее предупреждения. Это хорошо видно на примере развития глобальных аэронавигационных систем.

Можно отметить, что вышеописанные триадные формы терроризма также отображаются и на кибертерроризм, а средства кибератак могут также использоваться для реализации угроз безопасности ГА категорируемые *ICAO*.

Классификация кибератак

Проблема разработки и выбора эффективных методов и средств защиты ИАС от кибератак в значительной степени зависит от ресурсов, на которые направлены атаки, внешних проявлений, возможностей нарушений характеристик безопасности и других факторов. Эффективность ее решения в первую очередь связана с определением того, на какие классы кибератак рассчитаны те или иные методы и средства противодействия. На основе проведенного анализа известных классификаций [2], методов и средств реализации атак предлагается обобщенная классификация кибератак.

С учетом того, что спектр кибератак довольно разнородный, то основным принципом по которому можно наиболее эффективно осуществить классификацию будет признаковый. Предлагается классифицировать атаки на ресурсы ИАС по следующим базовым признакам:

– автоматизации;
– взаимодействию с политикой безопасности ИАС;
– дистанционности;
– действию, порожденному НСД;
– внешнему проявлению;
– инициализационному условию;
– инструментальным средствам;
– наличию обратной связи;
– нарушению базовых характеристик безопасности;
– природе взаимодействия;
– реляционным признакам;
– специфике реализации;
– направленности результата;
– степени сложности;
– типу базового ресурса;
– семиуровневой эталонной модели.

По *автоматизации* кибератаки можно разделить на мануальные, автоматизированные и автоматические (вирусные). Мануальные кибератаки реализуются непосредственно с участием человека без использования любых специальных средств. Автоматизированные кибератаки осуществляются с постоянным участием оператора. Автоматические кибератаки реализуются без участия человека и, как правило, с использованием специализированных программных средств, функционирование которых основывается на вирусных технологиях.

По *взаимодействию с политикой безопасности* кибератаки делятся на постполитизационные и деполитизацион-

ные. Постполитизационные кибератаки основаны на использовании недостатков в уже реализованной политике безопасности ИАС. Деполитизационные кибератаки связаны с ошибками и небрежностью, которые имеют место при реализации мероприятий с обеспечением уже существующей политики безопасности ИАС.

По *дистанционности* кибератаки делятся на локальне и удаленные. Если кибератаки на ресурс ИАС осуществляются в локализованной области его расположения, то они называются локальными, а в противном случае – удаленными.

В процессе осуществления кибератак может быть реализован НСД к разным ресурсам ИАС. В этом случае *по действию, порожденному НСД* к указанным ресурсам ИАС, кибератаки с учетом делятся на интераптационные, интерсептационные, модификационные, фальсификационные и свободные. Интераптационные кибератаки реализуются путем прерывания функционирования ресурсов ИАС. Интерсептационные кибератаки осуществляются путем перехвата разнородной информации относительно ресурсов ИАС. Модификационные кибератаки в процессе доступа к ресурсам ИАС осуществляют их преобразование. Фальсификационные кибератаки основываются на внедрении в ресурсы ИАС неучтенных компонент. Свободные кибератаки не направлены на прямую реализацию НСД к ресурсам ИАС и не ориентированы на нарушение принятой политики безопасности.

По *внешнему проявлению* кибератаки делятся на пассивные и активные. В результате своего действия пассивные кибератаки не осуществляют непосредственное влияние на ресурсы ИАС и могут не нарушить их характеристики безопасности. В результате активных кибератак на ресурсы ИАС осуществляется непосредственное влияние и нарушаются их характеристики безопасности.

По *инициализационному условию* кибератаки делятся на условные и безусловные. Условные кибератаки инициализируются в случае возникновения определенного события. Момент инициализации безусловных кибератак не сопровождается определенным изменением состояния ресурсов ИАС и определяется источником кибератаки.

По используемым *инструментальным средствам* кибератаки делятся на программные, аппаратные и нетипичные. Программные кибератаки основываются на специальных микрокодированных или макрокодированных средствах, которые функционируют в пределах ИАС для реализации своих функций. Аппаратные кибератаки основываются на разнообразных механических, электрических, электромеханических, электронных, электронно-механических и других устройствах, которые используются автономно или совместно с другой аппаратурой для выполнения соответствующих функций. Нетипичные кибератаки реализуются на основе таких средств, которые не относятся к аппаратным или программным.

По *наличию обратной связи* с атакованным ресурсом ИАС, кибератаки бывают с обратной связью и без обратной связи. В процессе реализации кибератаки с обратной связью осуществляется получение от атакованного ресурса ответа на определенные действия, которые необходимы, например, для дальнейшего продолжения указанного процесса на более эффективном уровне, который достигается благодаря анализу реакций объекта кибератаки на определенные изменения. Кибератака без обратной связи реализует свои действия независимо от реакции атакованного ресурса ИАС.

При реализации кибератак осуществляется нарушение основных характеристик безопасности ресурсов ИАС. В этом контексте по типу *нарушения базовых характеристик безопасности* кибератаки бывают К-действия (нарушение конфиденциальности ресурсов), Ц-действия (нарушение целостности ресурсов) и Д-действия (нарушение доступности ресурсов). Если в процессе кибератаки нарушаются разные характеристики безопас-

ности, то результирующий тип будет комбинирован с основных, например, КЦД-действия – кибератака, которая нарушает конфиденциальность, целостность и доступность ресурсов ИАС.

По *природе взаимодействия* с ресурсами ИАС кибератаки делятся на физические и логические. Для первых характерна физическая форма взаимодействия, которая проявляется в виде разного рода прямых блокировок, повреждений, проникновений, краж и т.п. Для вторых не присуще прямое физическое взаимодействие с ресурсами и они (в основном) связаны с логикой событий, например, анализом протоколов, перегрузкой, подбором паролей, захватом сеансов и др.

По *реляционным признакам* источника кибератаки и атакованного ресурса ИАС кибератаки делятся на: мономономные, полимономные, монополичные и полиполичные. Мономономные атаки реализуются из одного источника на один конкретный ресурс ИАС. Полимономные кибератаки осуществляются одновременно с нескольких источников (два и большее) на один ресурс ИАС и нацелены на достижение одной конкретной цели. Монополичные кибератаки реализуются из одного источника одновременно на множество ресурсов ИАС (два и больше) и направлены на достижение конкретной цели. Полиполичные кибератаки объединяют в себе полимономные и монополичные технологии по которым множество источников осуществляет кибератаки на множество ресурсов ИАС с целью достижения поставленной цели.

По *специфике реализации* кибератаки делятся на фрагментированные, без умолчаний, скрытые, пигибекинговые, маскарадные, непрямые, социотехнические, криптоаналитические и неспецифические. Фрагментованые кибератаки базируются на принципе декомпозиции и поэтапной реализации. Кибератаки, которые реализуются без использования значений по умолчанию, ориентированы на преодоление систем обнаружения кибератак, которые основываются на сигнатурных (шаблонных) технологиях. Скрытые кибератаки используют разнообразные средства, которые позволяют оставаться необнаруженными в локализованной области атакованного ресурса ИАС. Пигибекинговые кибератаки основаны на несанкционированном получении доступа к временно неконтролируемому ресурсу ИАС, например, после некорректного завершения сеанса работы легального пользователя ИАС. Маскарадные кибератаки основаны на формировании такого поведения нарушителя, которое разрешает ему выдать себя за легальный источник. Косвенные кибератаки основаны на том, что нападение осуществляется через третье лицо (посредника), а истинный источник нападение остается неизвестным. Социотехнические (социальный инжиниринг) кибератаки связаны с получением данных от атакованных людей в процессе информационного обмена. Криптоаналитические кибератаки основаны на использовании широкого спектра криптоаналитических методов и средств для взлома ресурсов ИАС, защищенных разными криптографическими средствами. К неспецифичным категориям кибератак относятся те, которые не имеют вышеупомянутых особенностей реализации, при этом следует учитывать, что технологии кибератак постоянно развиваются и данный признак может быть расширен.

По *направленности результата* кибератаки делятся на расширяющие, искривляющие, распространяющие, раскрадывающие, перегрузочные, информационные, удерживающие и уничтожающие. Расширяющие кибератаки ориентированы на получение больших полномочий на права доступа к ресурсу ИАС. Искривляющие кибератаки связаны с осуществлением любых прямых изменений в целевом ресурсе ИАС. Распространяющие кибератаки направлены на получение доступа к ресурсу ИАС и его раскрытие без соответствующих на это полномочий. Раскрадывающие кибератаки направлены на несанкционированное использование

ресурса без нанесения прямого убытка. Перегрузочные кибератаки направлены на загрузку ресурса до такого уровня, что он теряет свои функциональные свойства относительно его использования. Информационные кибератаки связаны с собиранием необходимых данных и не предусматривают осуществления прямого НСД к ресурсу ИАС. Удерживающие кибератаки предназначены для временной задержки ресурса ИАС с целью снижения его актуальности. Уничтожающие кибератаки ориентированы на безвозвратную ликвидацию ресурса ИАС.

По *степени сложности* кибератаки можно разделить на простые, сложные и системные. Простые кибератаки представляют собой несложные в реализации последовательности действий, направленные на выполнение отдельных процедур. Сложные кибератаки являются комбинацией простых, предназначенных для реализации ряда необходимых функций. Системные кибератаки строятся на основе сформированного системного подхода с многошаговой комбинацией действий и использованием простых кибератак для эффективной реализации специально направленного комплекса функций.

По *типу базового ресурса*, на который ориентированы кибератаки, последние делятся на: УВС-ресурсные (кибератаки на узлы вычислительной сети), ЛВС-ресурсные (кибератаки на локальные вычислительные сети), ИН-ресурсные (кибератаки на информационные носители), ОС-ресурсные (кибератаки на операционные системы), ПВ-ресурсные (кибератаки на протоколы взаимодействия), ПИАС-ресурсные (кибератаки на персонал ИАС), РП-ресурсные (кибератаки на рабочие приложения), СА-ресурсные (кибератаки на сценарии автоматизации), ФД-ресурсные (атаки на файлы данных) и др. Если атаки ориентированы на другие типы ресурсов, то при их классификации вводится соответствующее дополнительное сокращение, а в случае множественного действия тип определяется комбинацией базовых ресурсов, например, РП-ФД-ресурсные – атаки на рабочие приложения и файлы данных.

Международная организация стандартизации (*ISO*) предложила семиуровневую эталонную модель с целью разграничения функций различных протоколов в процессе передачи информации от одного абонента другому. Таких классов функций выделено семь. Они получили название уровней, каждый из которых выполняет определенные задачи в процессе передачи блока информации, причем соответствующий уровень со стороны-приемника производит преобразования, обратные тем, которые произведены на том же уровне на передающей стороне (источнике). В этой связи атаки по *семиуровневой эталонной модели* на ресурсы ИАС можно определить на уровне: физическом, кодируемым параметром $K0_{(2)}=2^0$, канальном, кодируемым параметром $K1_{(2)}=2^1$, сетевом, кодируемым параметром $K2_{(2)}=\ ^2$, транспортном, кодируемым параметром $K3_{(2)}=2^3$, сеансовом, кодируемым параметром $K4_{(2)}=2^4$, представления данных, кодируемым параметром $K5_{(2)}=2^5$, прикладном, кодируемым параметром $K6_{(2)}=2^6$.

Кибератаки, которые классифицируются по признаковому принципу, могут в каждом конкретном случае при определении общего класса содержать не только одну, но и больше компонент любого из признаков.

Информационная защита аэронавигационных систем

Концепция построения аэронавигационной системы, способной удовлетворить потребности гражданской авиации в новом столетии была рассмотрена и одобрена на конференции [8]. Концепция *FANS*, охватывающая системы связи, навигации, наблюдения/организации воздушного движения (*CNS/ATM*), базируется на применении технических средств, ориентированных на широкое использование спутников и компьютерных систем. Концепция *CNS/ATM* представляет разработанную ICAO стратегию решения назревших и перспективных проблем меж-

дународного воздушного транспорта. Однако высокая информационная насыщенность новых ИАС повышает требуемый уровень их защиты.

Переход к запланированному *ICAO* окончательному варианту новой информационной среды связан с разработкой и внедрением новых технологий во все сферы организации воздушного движения. Такой переход, скорее всего, будет иметь несколько этапов, характер и длительность которых будут обусловлены экономическими и техническими возможностями каждого из государств. Разные темпы развития национальных систем объективно определят время перехода от них к единой глобальной международной системе аэронавигационного обслуживания. На каждом этапе этого процесса должна быть обеспечена полная преемственность и совместимость предыдущих и последующих систем аэронавигационного обслуживания. Примером такого перехода служит переход от наземной сети авиационной фиксированной электросвязи *AFTN* к сети авиационной электросвязи *ATN* [9]. В аэронавигационном контуре (рис. 1) происходит формирование, передача, прием и обработка аэронавигационных данных. Их достоверность обеспечивает безопасность и экономичность полетов. Поэтому информационные каналы этого контура требуют особой защиты от кибератак. Угроза таких атак существует для речевого канала, каналов передачи данных и подсистем обработки данных ИАС.

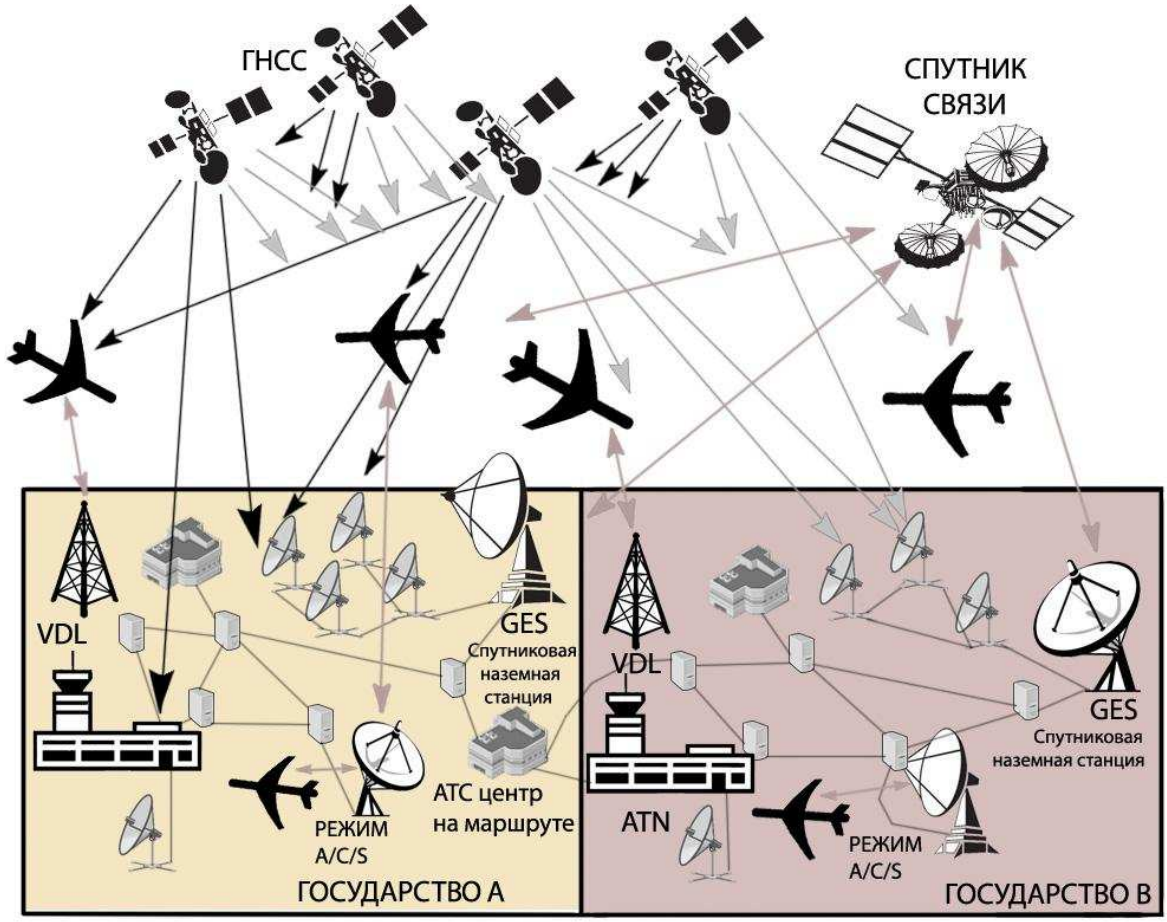

Рис. 1. Аэронавигационный контур

Переход к глобальной аэронавигации диктует необходимость разработки не только новых принципов организации потоков аэронавигационной информации, но и необходимость разработки современной минимально уязвимой много-

уровневой системы защиты информации с учетом межгосударственного характера ее циркуляции, технических и технологических особенностей ИАС.

Межсетевая структура авиационной электросвязи может состоять из отдельных подсетей общего пользования (или специальных). Это существенно усложняет проблему защиты информации от НСД доступа к ресурсам аэронавигационных систем. Согласно рекомендации *ICAO* (циркуляр 261-AN/155) желательно, чтобы в подсистемах ИАС обнаружение несанкционированной связи происходило в точке входа ИАС [10]. Несанкционированное использование ресурсов ИАС можно предотвратить за счет:

– формализации процедур представления новых пользователей;

– контроля над доступом пользователей к соответствующим ресурсам ИАС;

– ужесточения процедур проверки подлинности и паролей.

Выводы

В работе проведен качественный анализ кибертерроризма, выделены основные черты кибертерроризма на авиационном транспорте, приведены базовые понятия, которые позволяют определить явления кибертерроризма и кибератак. Сделана систематизация и классификация кибератак. С помощью данной классификации можно осуществлять формализацию возможностей систем противодействия для повышения эффективности их выбора и формировании требований при их разработке.

Рассмотренными примерами не ограничивается круг проблем, связанных с кибертерроризмом. Дальнейшего изучения и анализа требуют вопросы, связанные с классификацией ресурсов ИАС и их угроз, методами противодействия атакам, организационными мероприятиями, подготовкой кадров и т.д.

Список литературы

1. *Бабак В.П.* Інформаційна безпека та сучасні мережеві технології: Англо-український-російський словник термінів / *В.П. Бабак, О.Г. Корченко.* – К.: НАУ, 2003. – 670 с.

2. *Корченко А.Г.* Построение систем защиты информации на нечетких множествах. Теория и практические решения / *Корченко А.Г.* – К.: НАУ, 2005. – 336 с.

3. Словарь по международной гражданской авиации. Ч.1. – ICAO, 2001. – 128 с.

4. Терроризм и международные отношения в первой половине XX века [Електронний ресурс]. – Режим доступу: http://anthropology.ru/ru/texts/yachlov/terror.html.

5. *Ольшанский Д.* Психология терроризма / *Д. Ольшанский.* – СПб.: Питер, 2002. – 288 с.

6. Безпека авіації / [*В.П. Бабак, В.П. Харченко, В.О. Максимов та ін.*]; За ред. В.П. Бабака. – К.: Техніка, 2004. – 584 с.

7. *Голубев В.А.* Информационная безопасность: проблемы борьбы с киберпреступлениями: монография / *Голубев В. А.* – Запорожье: ГУ "ЗИГМУ", 2003. – 336 с.

8. Eleventh Air Navigation Conference (ANConf/11), ICAO, Montreal [Електронний ресурс]. – Режим доступу: http://www.icao.int/icao/en/anb/meetings/anconf11/index.html.

9. Руководство по техническим положениям для сети авиационной электросвязи (ATN) DOC. 9705 AN/956. – Монреаль: ICAO, 1999. – 72 с.

10. *Корченко А.Г.* Авиационная безопасность: Международные конвенции. Приложение 17 / *А.Г. Корченко, С.В. Карпенко, Е.В. Пацира.* – К.: НАУ, 2004. – 116 с.