ISSN 1992-6502 (Print) Вестник УГАТУ ISSN 2225-2789 (Online)
2019. Т. 23, № 4 (86). С. 132–146 http://journal.ugatu.ac.ru

УДК 004.056

АНАЛИЗ ЗАЩИЩЕННОСТИ СИСТЕМЫ СБОРА, ХРАНЕНИЯ И ОБРАБОТКИ ТЕЛЕМЕТРИЧЕСКОЙ ИНФОРМАЦИИ О СОСТОЯНИИ БОРТОВЫХ СИСТЕМ ЛЕТАТЕЛЬНОГО АППАРАТА

М. Б. ГУЗАИРОВ[1], А. И. ФРИД[2], А. М. ВУЛЬФИН[3], В. В. БЕРХОЛЬЦ[4], А. Д. КИРИЛЛОВА[5]

[1] guzairov@ugatu.su, [2] frid46@mail.ru, [3] vulfin.alexey@gmail.com, [4] torina4@yandex.ru, [5] kirillova.andm@gmail.com

ФГБОУ ВО «Уфимский государственный авиационный технический университет» (УГАТУ)

Поступила в редакцию 24.04.2019

Аннотация. Выполнен анализ структуры и рассмотрены вопросы анализа защищенности модульной системы сбора, хранения и обработки телеметрической информации о состоянии бортовых подсистем летательного аппарата в автоматическом режиме. Система строится исходя из модульного принципа и содержит подсистемы с высокой степенью связности компонент. Выявлены основные угрозы и уязвимости рассматриваемой системы в аспекте нарушения целостности накапливаемых данных, разработаны сценарии реализации угроз внешним и внутренним злоумышленником на основе графов атак, которые позволяют учитывать взаимосвязь и свойства объектов системы на основе результатов анализа уязвимостей, модели нарушителя и данных о конфигурации сети.

Ключевые слова: системы сбора, хранения и обработки телеметрии; автоматизированная информационная система; анализ защищенности; граф атак.

ВВЕДЕНИЕ

Возникающие неисправности и предотказные состояния бортовой аппаратуры летательного аппарата (ЛА) могут быть диагностированы на основе обрабатываемой телеметрической информации (ТМИ), что позволяет специалистам наземных технических служб планировать ремонтные и профилактические мероприятия на основе оценки текущего состояния оборудования. Накапливаемая и обрабатываемая ТМИ о фактическом состоянии отдельных модулей в процессе эксплуатации и всего комплекса бортовых систем ЛА в реальном масштабе времени на предприятие-изготовитель (ПИ) узлов авиационной техники позволит повысить эффективность эксплуатации ЛА в штатном состоянии, при возникновении сбоев, а также атаках злоумышленников – при расследовании инцидентов.

Необходимость передачи ТМИ на ПИ с целью последующего анализа является одним из направлений совершенствования перспективных бортовых систем. Ввиду возможного воздействия внешних и внутренних угроз ключевым аспектом обеспечения информационной безопасности (ИБ) в таких системах является непрерывный мониторинг и обеспечение целостности ТМИ, на основе анализа которой принимаются управленческие решения по продолжению полета и разработке перспективных бортовых систем ЛА.

В настоящее время в технических заданиях на разработку некоторых цифровых систем автоматического управления (контроля) подсистем ЛА указывается необходимость разработки и внедрения в эти системы устройств, обеспечивающих передачу информации о состоянии управляемых

Работа поддержана грантом РФФИ № 17-07-00351

(контролируемых) подсистем на предприятие-изготовитель с помощью телеметрии в режиме реального времени. В частности, такое требование выдвигается к цифровым системам управления перспективными авиационными двигателями.

Одной из задач при передаче ТМИ является обеспечение защищенности информации от несанкционированных изменений, т.е. целостности. Известно множество подходов к ее решению [1–6], однако решение применительно к каналу передачи информации с борта ЛА на предприятие-изготовитель подсистем ЛА авторам не известно. В частности, не разработаны сценарии реализации угроз на основе топологического анализа защищенности системы, учитывающие взаимосвязь и свойства объектов системы на основе результатов анализа уязвимостей, модели нарушителя и данных о конфигурации сети, не разработаны графовые модели, которые являются необходимым этапом для последующей оценки рисков ИБ с помощью когнитивного моделирования.

Целью исследования является анализ защищенности системы сбора, хранения и обработки ТМИ о состоянии бортовых подсистем ЛА в аспекте обеспечения целостности ТМИ.

Для достижения поставленной цели сформулированы задачи:

– выполнить анализ структуры системы сбора, хранения и обработки ТМИ о состоянии подсистем ЛА;

– выявить основные угрозы и уязвимости рассматриваемой системы;

– разработать сценарии реализации угроз на основе графов атак.

АНАЛИЗ ПРОБЛЕМЫ ЗАЩИЩЕННОГО СБОРА, ХРАНЕНИЯ И ОБРАБОТКИ ТМИ В ТЕРРИТОРИАЛЬНО РАСПРЕДЕЛЕННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

Предлагаемая в [7–9] автоматизированная информационная система (АИС) наземных служб технического обслуживания представляет собой набор программных и аппаратных средств, необходимых для приема, хранения и обработки информации о параметрах состояния сложных технических изделий (СТИ) на борту ЛА. АИС является территориально распределенной системой, объединяющей инфраструктуру информационных систем наземных станций технического обслуживания и информационную систему ПИ посредством защищенных каналов связи. Получение ТМИ реализовано посредством считывания журнала состояния СТИ на борту ЛА при проведении технического осмотра и обслуживания на наземных станциях с помощью беспроводных и/или проводных сенсорных сетей.

Анализ основных отдельных аспектов построения защищенной системы сбора, хранения и обработки ТМИ наземными службами технического обслуживания рассмотрен в работах авторов [10–12].

СТРУКТУРА ЗАЩИЩЕННОЙ СИСТЕМЫ СБОРА, ХРАНЕНИЯ И ОБРАБОТКИ ТМИ О СОСТОЯНИИ БОРТОВЫХ ПОДСИСТЕМ ЛА

АИС решает основные задачи, связанные с приемом ТМИ о состоянии бортовых систем ЛА. Основные способы получения данных:

1) непосредственно с борта ЛА по организованному защищенному радиоканалу;

2) посредством считывания журнала состояния СТИ на протяжении всего предыдущего периода эксплуатации при проведении технического осмотра и обслуживания ЛА на наземной станции [9, 13];

3) с помощью внесения данных журнала событий оператором в базу хранимой ТМИ на ПИ в автоматизированном режиме через защищенное соединение с помощью Web-приложений [8].

Обобщенная структура территориально распределенной модульной системы сбора, хранения и обработки ТМИ, поступающей с ЛА, разработана в [9] и представлена на рис. 1. Защищенная система сбора, хранения и обработки ТМИ о состоянии бортовых подсистем ЛА строится исходя из модульного принципа и содержит достаточно крупные подсистемы с высокой степенью связности компонент внутри и достаточной степенью автономности на уровне взаимодействия самих подсистем. Каждый уровень и подсистемы строятся на основе организационных принципов, характерных для спе-

цифики решаемой задачи, и регламентируются существующими нормативными документами [14, 15].

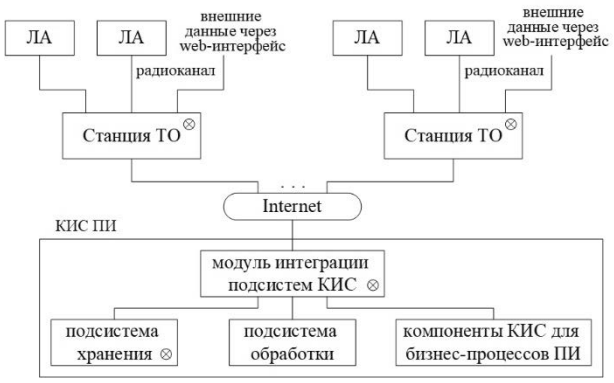


Рис. 1. Обобщенная структурная схема защищенной системы сбора, хранения и обработки ТМИ
(– зоны воздействия внешних и внутренних угроз)

Уровень сбора ТМИ систем наземных станций технического обслуживания ЛА представляет собой реализацию гетерогенной (с проводным и беспроводным сегментом) сенсорной сети первичного сбора ТМИ с выходных интерфейсов бортовых систем ЛА.

На уровне первичного накопления и подготовки ТМИ к передаче в часть сети предприятия изготовителя реализуется предварительное хранение накапливаемых данных, мониторинг и диагностика состояния системы сбора.

На уровне передачи накопленных данных реализовано создание защищенного канала через глобальные инфокоммуникационные сети и передача ТМИ в сеть АИС ПИ для последующего хранения и обработки. Система сбора, хранения и обработки ТМИ использует комплекс средств защиты информации (СЗИ), направленных на обеспечение безопасности информации ПИ. Криптошлюз «Континент» позволяет создавать VPN-канал между сетями предприятия в соответствии с криптоалгоритмом ГОСТ 28147-89 (L3 VPN-сети).

В составе корпоративной информационной сети (КИС) ПИ выделяется уровень, включающий подсистемы хранения и обработки ТМИ, а также сегмент, предназначенный для поддержки и реализации бизнес-процессов ПИ. Для обеспечения защищенности подсистем, реализующих первые два уровня предлагаемой структуры, были учтены требования нормативных документов международного и федерального стандарта. При проектировании подсистемы беспроводной сенсорной сети сбора ТМИ руководствовались требованиями стандартов [16, 17].

Физическая архитектура подсистемы сбора и хранения ТМИ на наземных станциях обслуживания ЛА построена в соответствии с NIST 800-82 [18] и ISA/IEC 62443 [19] (рис. 2).

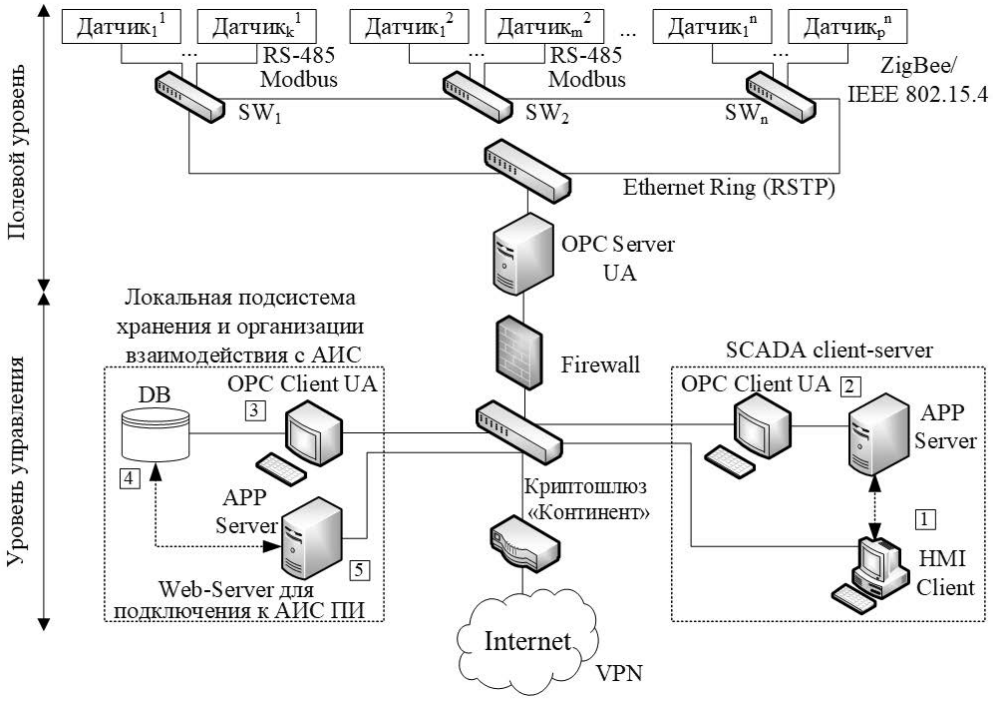
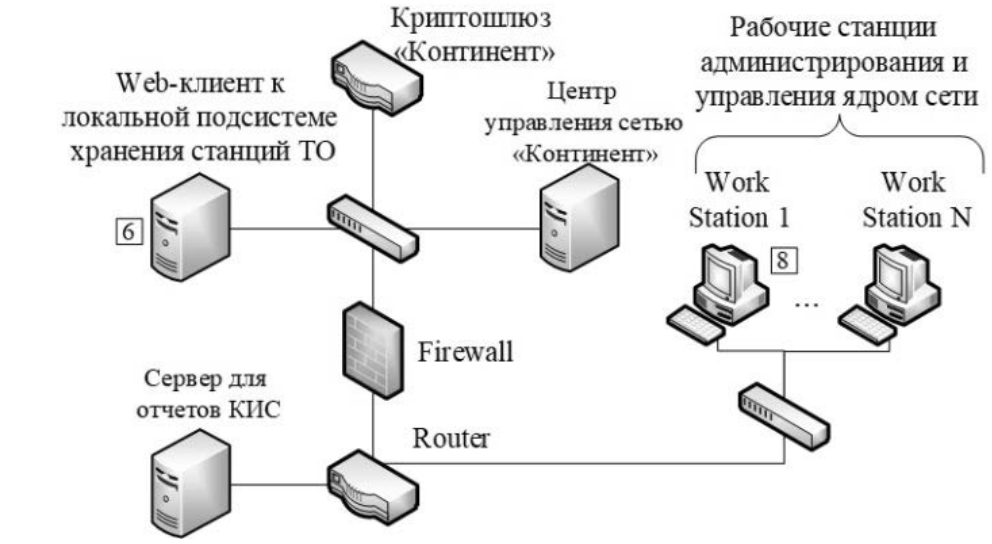


Рис. 2. Структура подсистемы сбора и хранения данных на станциях обслуживания

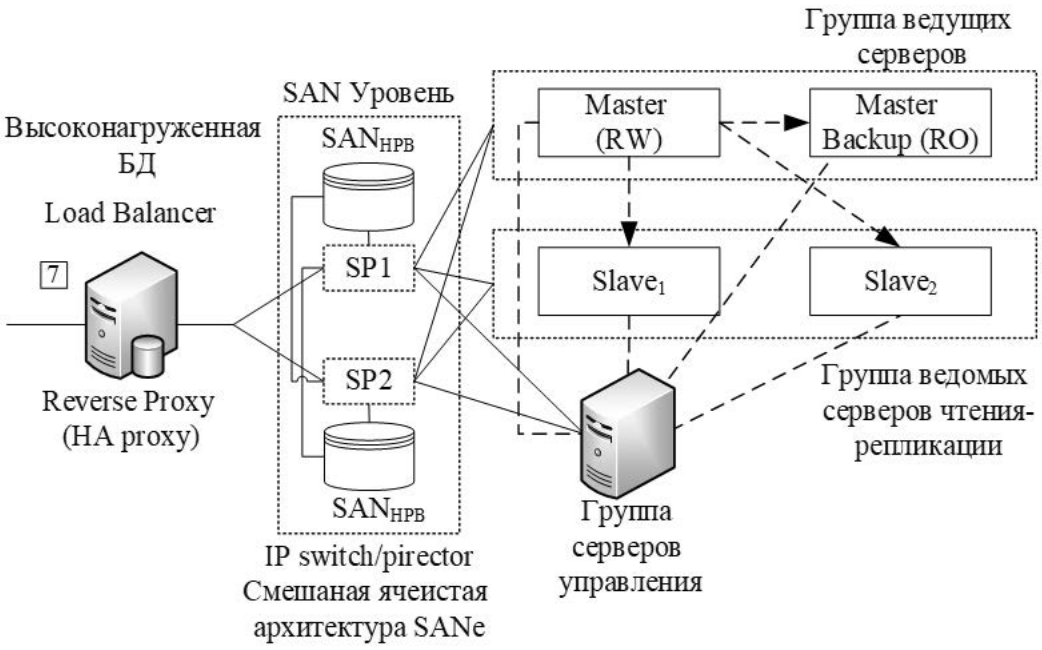
Ядро сети КИС ПИ представлено на рис. 3, *а*.

Web-client обеспечивает подключение к удаленным серверам станций обслуживания и передачу информации в хранилище ПИ. Корневой маршрутизатор реализует объединение подсистемы хранения, подсистемы обработки и КИС ПИ. Станции обслуживания WS_1-WS_N предназначены для администрирования сервисов ядра сети и основных подсистем. Сервер отчетов позволяет обращаться пользователям КИС для построения отчетов о текущем анализе параметров рассогласования модельных и натурных данных ТМИ СТИ на станциях ТО.

Для обеспечения хранения ТМИ и эффективного доступа к накапливаемым объемам данных необходимо построение отказоустойчивой системы хранения на основе использования механизмов репликации СУБД MySQL [9] (рис. 3, *б*).



а



б

Рис. 3. *а* – ядро КИС предприятия-изготовителя;
б – структура подсистемы хранения ТМИ с функциями отказоустойчивости

Состав и основные элементы подсистем описаны в табл. 1 (где C_i^j – элемент подсистемы, i – номер элемента в подсистеме, j – номер подсистемы).

Таблица 1

Элементы подсистем защищенной системы сбора, хранения и обработки ТМИ

Подсистема сбора и хранения данных на станциях обслуживания	
Firewall[1]	Межсетевой экран для организации DMZ, разграничивающей Field Network и Control Network станции обслуживания
Криптошлюз «Континент»[1]	Создание VPN-канала между сетями предприятия; Межсетевой экран для организации DMZ, разграничивающей Control Network станции обслуживания и сеть Internet Маршрутизатор для реализации опорной сети станции обслуживания
HMI $Client_1$[1]	ПК, предоставляющий возможность запуска в браузере клиентской части SCADA системы на основе Web-приложения.
APP $Server_2$[1]	Сервер приложений, предназначенный для запуска серверной части SCADA системы
OPC Client UA_3[1]	Клиент для взаимодействия с сервером OPC на основе спецификации Unified Architecture [20]
DB_4[1]	СУБД и хранилище данных для размещения оперативных данных телеметрии, накапливаемых на объекте.
APP $Server_5$[1]	Сервер приложений, предназначенный для запуска серверной части системы передачи данных в хранилище данных ПИ на основе Web-приложения
Подсистема хранения ТМИ с функциями отказоустойчивости	
Reverse Proxy (HA proxy)$_7$[2]	Узел, обеспечивающий доступ к распределенному хранилищу данных ТМИ на ПИ
Модуль интеграции подсистем КИС	
Криптошлюз «Континент»[0]	Маршрутизатор пограничный для сети ПИ и сети провайдера Межсетевой экран для организации DMZ, разграничивающей клиентский модуль для организации доступа к удаленному серверу APP $Server_5$[1] станции обслуживания и опорной сети КИС ПИ
Router[0]	Маршрутизатор опорной сети ПИ для обеспечения изоляции подсети хранения, КИС, подсети обработки информации.
Firewall[0]	Межсетевой экран для организации DMZ, разграничивающей клиентский модуль для организации доступа к удаленному серверу APP $Server_5$[1] станции обслуживания и опорной сети КИС ПИ
Web $Client_6$[0]	Клиентский модуль для организации доступа к удаленному серверу APP $Server_5$[1] станции обслуживания с целью передачи накопленных оперативных данных ТМИ в хранилище ПИ
Work $Station_8$[0]	АРМ администратора и обслуживающего персонала опорной сети КИС ПИ
Центр управления сетью «Континент»	Обеспечивает управление защищенными каналами связи с удаленными станциями ТО и ядром КИС ПИ
Сервер для отчетов КИС	Предоставляет сервис для пользователей КИС ПИ для построения отчетов о текущем анализе параметров рассогласования модельных и натурных данных ТМИ СТИ на станциях ТО.

Окончание табл. 1

АНАЛИЗ ЗАЩИЩЕННОСТИ ТМИ

Угрозы, связанные с нарушением целостности телеметрических данных, способны привести к получению ПИ неверных данных о состоянии ЛА. В [12] предлагается концепция системы мониторинга целостности ТМИ, реализующей постоянный мониторинг и моделирование параметров СТИ для выявления значимых отклонений от выделенных шаблонов режимов работы, которые, в свою очередь, будут указывать на возможные действия внешних и внутренних угроз на ТМИ.

Приведен перечень угроз несанкционированного доступа (НСД) к отдельным узлам распределенной системе сбора, передачи, хранения и обработки ТМИ с применением программных и программно-аппаратных средств, которые могут быть реализованы с целью нарушения целостности информации:

1. Угроза воздействия на программно-аппаратные узлы АИС:

– угроза воздействия на программное обеспечение с высокими привилегиями;

– угроза изменения системных и глобальных переменных;

– угроза нарушения технологии обработки информации;

– угроза некорректного использования функционала программного и аппаратного обеспечения;

– угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением;

– угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства;

– угроза несанкционированного управления синхронизацией и состоянием;

– угроза повышения привилегий;

– угроза несанкционированного воздействия на средство защиты информации;

– угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения;

– угроза перехвата управления информационной системой.

2. Угроза воздействия на узлы сетевой инфраструктуры АИС:

– угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети.

АНАЛИЗ УЯЗВИМОСТЕЙ СИСТЕМЫ СБОРА, ХРАНЕНИЯ И ОБРАБОТКИ ТМИ

Анализ объекта защиты с точки зрения наличия уязвимостей обеспечивает максимальную полноту описания возможных угроз.

Можно выделить следующие классы уязвимостей рассматриваемой системы:

– уязвимости системного и прикладного ПО;

– уязвимости аппаратного обеспечения;

– уязвимости протоколов сетевого взаимодействия.

Исходя из рассматриваемых классов уязвимостей и на основании Банка данных угроз безопасности информации ФСТЭК, построен декомпозированный список уязвимостей, потенциально имеющихся у основных программно-аппаратных узлов АИС, эксплуатация которых ведет к нарушению целостности ТМИ:

– уязвимости механизма проверки входных данных и команд API, а также мер по разграничению доступа;

– уязвимости механизма контроля доступа к разделяемой памяти, а также уязвимостями программных модулей приложений, реализующих контроль целостности внешних переменных;

– уязвимости виртуальной машины, обеспечивающей изолированность адресного пространства;

– уязвимость механизма управления синхронизацией и состоянием;

– уязвимости в средствах разграничения доступа к памяти и контроля целостности содержимого ячеек памяти;

– уязвимости программного обеспечения, выполняющего функции разграничения доступа (в алгоритме или параметрах конфигурации);

– уязвимость механизма проверки целостности обрабатываемых файлов и корректности, содержащихся в них данных;

– уязвимости программной среды управления средством защиты информации.

ОПРЕДЕЛЕНИЕ ИСТОЧНИКОВ УГРОЗ ИБ СИСТЕМЫ СБОРА, ХРАНЕНИЯ И ОБРАБОТКИ ТМИ О СОСТОЯНИИ БОРТОВЫХ ПОДСИСТЕМ ЛА

В данной статье внимание уделяется разработке сценариев реализации атак, связанных со случайным или преднамеренным действием угроз на ТМИ.

В зависимости от наличия права постоянного или разового доступа в контролируемую зону, в пределах которой размещается оборудование системы, рассматриваются внешние и внутренние нарушители. Общая классификация рассматриваемых нарушителей в зависимости от предоставленных прав доступа с описанием способов реализации угроз представлена далее.

Внешний нарушитель

В качестве внешнего нарушителя ИБ рассматривается нарушитель, который не имеет непосредственного доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой

зоны в силу принятых на предприятии мероприятий по ограничению доступа посторонних лиц в контролируемую зону.

Внешний нарушитель может осуществлять следующие действия по нарушению целостности ТМИ:

1) подмену базовой и/или абонентской радиостанции – подавление сигнала базовой/абонентской радиостанции и поднятие на частоте ее радиообмена собственной радиостанции, передающей поддельную информацию;

2) отправку поддельной информации в радиоканал – создание пакета данных с поддельной телеметрической информацией и отправка его базовой/абонентской радиостанции;

3) повторную отправку ранее перехваченной в радиоканале информации – перехват легитимного сообщения, передаваемого по радиоканалу, и его повторная отправка участнику движения через некоторый период времени.

Внутренний нарушитель

Внутренний нарушитель представляет собой сотрудника организации, который обладает определенными правами доступа к техническим средствам и ресурсам системы, находящимся в пределах контролируемой зоны.

К внутренним нарушителям могут относиться:

1. Администраторы подсистем и БД:

– Администратор сегмента полевого уровня станции ТО ЛА. Решает задачи конфигурирования и управления распределенной сетевой инфраструктурой гетерогенной сети сбора ТМИ с бортовых систем ЛА, получаемых по радиоканалу, либо с помощью организации проводного подключения к бортовым системам на станции ТО. Точками потенциального воздействия на систему с целью нарушения целостности ТМИ является НСД к OPC-серверу.

– Администратор сегмента управления станции ТО ЛА. Решает задачи конфигурирования и управления сетевой инфраструктурой предварительного хранения ТМИ. Управляет параметрами взаимодействия с полевым уровнем посредством конфигурирования OPC-сервера. Поддерживает работоспособность программно-аппаратных средств клиент-серверной SCADA-системы. Управляет работой оперативного хранилища ТМИ на станции ТО ЛА. Управляет работой серверной частью Web-приложения для организации удаленного доступа к оперативному хранилищу из АИС ПИ. Точками потенциального воздействия на систему с целью нарушения целостности ТМИ является НСД к SCADA-системе, параметрам оперативного хранилища ТМИ, параметрам серверной части Web-приложения.

– Администратор подсистемы высоконагруженной системы хранения ТМИ в составе АИС ПИ (SAN). Обеспечивает конфигурирование и работу высоконагруженной БД хранения ТМИ. Точками потенциального воздействия на систему с целью нарушения целостности ТМИ является НСД к параметрам конфигурационного сервера хранилища и серверам SAN.

– Администратор подсистемы обработки данных ТМИ с помощью иерархии математических моделей СТИ (Apache Spark [21], Hadoop [22]). Управляет работой вычислительного кластера, предназначенного для обеспечения работоспособности моделей СТИ. Примененная схема виртуализации на основе построения легковесных контейнеров [23] с встроенными средствами криптозащиты не допускает необнаруживаемого несанкционированного изменения параметров самой модели.

Таким образом, администратор обладает полной информацией о системе (сети), имеет доступ ко всем техническим средствам обработки информации и данным, к средствам защиты информации и протоколирования, обладает правами конфигурирования и административной настройки, конфигурирования и распределения ключевой документации между пользователями. На него возложены задачи администрирования программно-аппаратных средств и БД системы для интеграции и обеспечения взаимодействия различных подсистем. Они потенциально могут реализовывать угрозы ИБ, используя возможности по непосредственному доступу к защищенной информации, обрабатываемой и хранимой в системе, а также к техническим и программным средствам, включая средства защиты.

2. Персонал по техническому обслуживанию, сопровождению ПО на защищаемом объекте:

– Специалист по обслуживанию полевой сетевой инфраструктуры станции ТО ЛА. Поддерживает работоспособность полевой инфраструктуры.

– Оператор АРМ сегмента управления станции ТО ЛА. Выполняет мониторинг работы технического процесса сбора данных телеметрии с бортовых систем ЛА. Точка доступа с целью нарушения целостности ТМИ является НСД к узлу, реализующему поддержку HMI SCADA-клиента.

– Специалист обслуживания высоконагруженной системы хранения ТМИ в составе АИС ПИ (SAN). Точка доступа с целью нарушения целостности ТМИ является НСД к конфигурационному серверу хранилища и серверам SAN.

– Специалист обслуживания подсистемы обработки данных ТМИ с помощью иерархии математических моделей СТИ (Apache Spark, Hadoop).

Таким образом, персонал по техническому обслуживанию и сопровождению ПО обладает возможностями внесения закладок в технические средства системы на стадии их внедрения и сопровождения Они могут обладать любыми фрагментами информации о топологии системы и технических средствах обработки и защиты информации в системе. Обладает частичной информацией об алгоритмах и программах обработки информации, протоколах, реализуемых и используемых в конкретных подсистемах и системе в целом, а также о применяемых принципах и концепциях безопасности, обладает возможностями внесения ошибок, недекларированных возможностей, программных закладок, вредоносных программ в ПО.

3. Начальник сегмента управления обладает всеми возможностями администратора системы. Располагает конфиденциальной информацией, к которой имеет доступ.

Степень информированности нарушителя зависит от многих факторов, включая реализованные в системе конкретные режимные и организационно-технические меры. Таким образом, объективно оценить объем знаний вероятного нарушителя в общем случае практически невозможно, поэтому рассматриваются категории внутренних нарушителей только с максимальными правами доступа.

РАЗРАБОТКА СЦЕНАРИЕВ РЕАЛИЗАЦИИ УГРОЗ ИБ НА ОСНОВЕ ГРАФОВ АТАК

Сценарии поведения внутреннего и внешнего нарушителя отображаются через построение графов атак.

Графы атак являются инструментом топологического анализа защищенности информационной системы и позволяют учитывать взаимосвязь и свойства объектов информационной системы на основе результатов сканирования сети, модели нарушителя и данных о конфигурации сети (правила фильтрации межсетевого экрана, маршрутизации, обнаружения атак, достижимости хостов и т.д.). Классификация представления графов атак приведена в табл. 2 [24–26].

Для формирования рассуждений в условиях неопределенности в соответствии с оценками вероятностей событий и связи между событиями удобным является построение на основе ориентированного на условия зависимостей графа сетевой модели в виде сети Байеса [25, 27].

Таблица 2

Классификация графов атак

Название	*Описание*
граф перечисления состояний	вершинам соответствуют тройки (s, d, a), где s – источник атаки, d – цель атаки, a – элементарная атака; дуги обозначают переходы из одного состояния в другое
граф ориентированных на условия зависимостей	вершинам соответствуют результаты атак, а дугам – элементарные атаки, приводящие к таким результатам
граф зависимости эксплойтов	вершины соответствуют результатам атак или элементарным атакам, дуги отображают зависимости между вершинами – условия, необходимые для выполнения атаки и следствие атаки

Рассмотрим уровень сбора ТМИ систем наземных станций технического обслужива-

ния ЛА, который представляет собой реализацию сенсорной сети первичного сбора ТМИ с выходных интерфейсов бортовых систем ЛА с помощью проводных и беспроводных датчиков. На уровне первичного накопления и подготовки ТМИ к передаче в часть АИС ПИ реализуется предварительное хранение накапливаемых данных, мониторинг и диагностика состояния системы сбора.

Целью атаки являются:

– Оперативные данные ТМИ, которые могут быть модифицированы злоумышленником до внесения в БД на узлах S CADA клиент-серверного типа [28];

– БД хранения оперативных данных ТМИ, которые могут быть модифицированы злоумышленником;

– Накопленные в БД данные, передаваемые через Web-приложение в КИС ПИ.

Граф атак для подсистемы сбора и хранения ТМИ представлен на рис. 4 и позволяет проиллюстрировать уязвимости, используемые злоумышленником в ходе реализации угрозы для достижения цели атаки (конечного узла графа атак).

Описание рассмотренных выше уязвимостей с привязкой к программно-аппаратным элементам системы представлено в табл. 3.

Далее с помощью графа атак проиллюстрирована последовательность эксплуатации уязвимостей, позволяющая нарушить целостность данных в подсистеме хранения ТМИ и в подсистеме ядра КИС ПИ, осуществляющей взаимодействие со станциями ТО посредствам Web-приложения (рис. 5, табл. 4).

Целью атаки являются:

– ТМИ из оперативного хранилища станций ТО ЛА, получаемые посредством доступа по защищенному каналу к станциям обслуживания ЛА;

– ТМИ в долгосрочном хранилище.

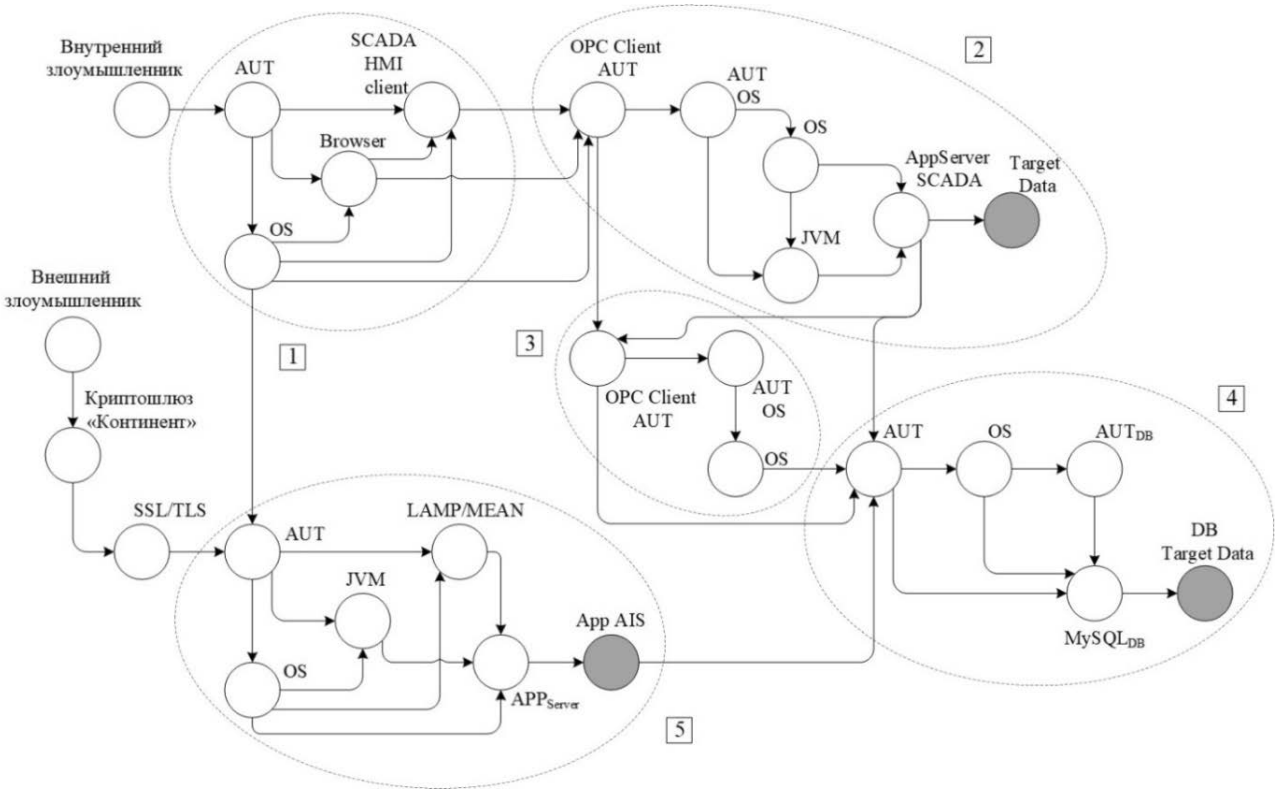


Рис. 4. Граф реализации угроз для подсистемы сбора и хранения ТМИ на наземных станциях обслуживания ЛА

Таблица 3

Уязвимости в составе графа атак для подсистемы сбора и хранения ТМИ на наземных станциях обслуживания ЛА

1. HMI Client$_1$[1]	
AUT	Эксплуатация уязвимости системы авторизации пользователя ОС (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
SCADA HMI client	Эксплуатация уязвимости прикладного ПО web-клиента SCADA HMI (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Browser	Эксплуатация уязвимости браузера ОС для запуска клиентской части SCADA HMI (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
OS	Уязвимость доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
2. APP Server$_2$[1]	
OPC Client AUT	Эксплуатация уязвимости системы авторизации клиентской части ПО OPC Client UA
AUT OS	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
JVM	Эксплуатация уязвимости виртуальной машины Java (уязвимости виртуальной машины, обеспечивающей изолированность адресного пространства)
App Server SCADA	Эксплуатация уязвимости системного ПО сервера приложений для запуска серверного Web-приложения SCADA системы (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Target Data	Оперативные данные ТМИ, которые могут быть модифицированы злоумышленником до внесения в БД на узлах SCADA client-server type
3. OPC Client UA$_3$[1]	
OPC Client AUT	Эксплуатация уязвимости системы авторизации клиентской части ПО OPC Client UA (уязвимости механизма проверки входных данных, и мер по разграничению доступа к разделяемой памяти)

Продолжение табл. 3

AUT OS	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
4. DB$_4$[1]	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
AUT $_{DB}$	Эксплуатация уязвимости системы авторизации основного пользователя СУБД (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
MySQL $_{DB}$	Эксплуатация уязвимости доступа к памяти СУБД (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
DB Target Data	БД хранения оперативных данных ТМИ, которые могут быть модифицированы злоумышленником
5. APP Server$_5$[1]	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
LAMP/ MEAN	Эксплуатация уязвимости системного ПО, реализующего работу связки сервера веб-приложений Apache, СУБД MySQL, среды исполнения PHP для поддержки интерактивных Web-страниц (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
JVM	Эксплуатация уязвимости доступа к памяти виртуальной машины Java (уязвимости виртуальной машины, обеспечивающей изолированность адресного пространства)
App Server	Эксплуатация уязвимости ПО сервера приложений (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)

Окончание табл. 3

App AIS	Эксплуатация уязвимости Web-приложения для запуска модуля доступа к БД оперативного хранения ТМИ на станциях обслуживания ЛА (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Криптошлюз «Континент»	Эксплуатация уязвимости программной среды управления маршрутизатора Эксплуатация уязвимости программной среды управления средством защиты информации – межсетевого экрана
SSL/TLS	Эксплуатация уязвимости системного ПО, реализующего создание защищенного сетевого канала

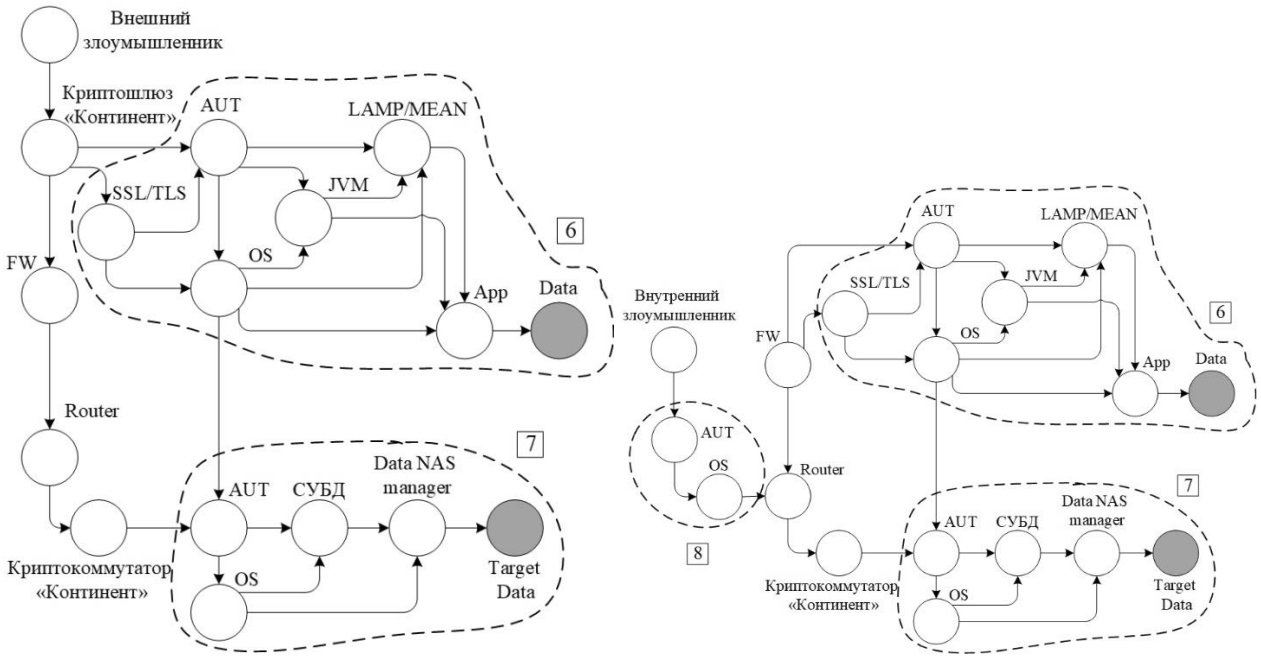
Таблица 4

Уязвимости в составе графа атак для в подсистемы хранения ТМИ и подсистемы ядра КИС ПИ

6. Web Server$_6^0$	
Криптошлюз «Континент»	Эксплуатация уязвимости программной среды управления маршрутизатора Эксплуатация уязвимости программной среды управления средством защиты информации – межсетевого экрана
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС
LAMP/ MEAN	Эксплуатация уязвимости системного ПО, реализующего работу связки сервера веб-приложений Apache, СУБД MySQL, среды исполнения PHP для поддержки интерактивных Web-страниц
SSL/TLS	Эксплуатация уязвимости системного ПО, реализующего создание защищенного сетевого канала (уязвимость сетевых протоколов)
OS	Эксплуатация уязвимости доступа к памяти ОС
JVM	Эксплуатация уязвимости доступа к памяти виртуальной машины Java

Окончание табл. 4

App	Эксплуатация уязвимости ПО сервера приложений для организации удаленного защищенного доступа к БД оперативного хранения ТМИ на станциях ТО ЛА (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Data	ТМИ из оперативного хранилища станций ТО ЛА
7. Reverse Proxy (HA proxy)$_7^2$	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС конфигурационного сервера БД (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
СУБД	Эксплуатация уязвимости доступа к памяти СУБД (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Data NAS manager	Эксплуатация уязвимости доступа к памяти конфигурационного сервера сетевого хранилища (уязвимость механизма разграничения доступа к памяти, механизма управления синхронизацией)
Target Data	ТМИ в долгосрочном хранилище
8. Work Station$_8^0$	
AUT	Эксплуатация уязвимости системы авторизации основного пользователя ОС (уязвимости механизма проверки входных данных и мер по разграничению доступа к разделяемой памяти)
OS	Эксплуатация уязвимости доступа к памяти ОС (уязвимость механизма разграничения доступа к памяти)
Router	Эксплуатация уязвимости программной среды управления маршрутизатора
FW	Эксплуатация уязвимости программной среды управления средством защиты информации – межсетевого экрана



а *б*

Рис. 5. Граф реализации угроз в подсистеме хранения ТМИ и в подсистеме ядра КИС ПИ:
а – внешний злоумышленник; б – внутренний злоумышленник

ЗАКЛЮЧЕНИЕ

В результате анализа структуры защищенной системы сбора, хранения и обработки ТМИ о состоянии подсистем ЛА выявлены основные угрозы и уязвимости, затрагивающие обеспечение целостности передаваемых и накапливаемых данных ТМИ. На основе результатов анализа разработаны сценарии реализации угроз на основе инструментов топологического анализа защищенности системы, которые позволяют учитывать взаимосвязь и свойства объектов системы на основе результатов анализа уязвимостей, модели нарушителя и данных о конфигурации сети. Разработанные графовые модели является необходимым этапом для последующей оценки рисков ИБ с помощью когнитивного моделирования.

СПИСОК ЛИТЕРАТУРЫ

1. **On SCADA** control system command and response injection and intrusion detection / W. Gao, et. al. // Proceedings of the 5th Annual Anti-Phishing Working Group eCrime Researchers Summit. IEEE, 2010. Pp. 1-9. **[** W. Gao, et. al., “On SCADA control system command and response injection and intrusion detection”, in *Proceedings of the 5th Annual Anti-Phishing Working Group eCrime Researchers Summit*. IEEE, 2010, pp. 1-9. **]**

2. **Bigham J., Gamez D., Lu N.** Safeguarding SCADA systems with anomaly detection // International Workshop on Mathematical Methods, Models, and Architectures for Computer Network Security. Springer, Berlin, Heidelberg, 2003. Pp. 171-182. **[** J. Bigham, D. Gamez, N. Lu, “Safeguarding SCADA systems with anomaly detection”, in *International Workshop on Mathematical Methods, Models, and Architectures. Computer Network Security*, pp. 171-182, 2003. **]**

3. **He Q., Blum R. S.** Smart grid monitoring for intrusion and fault detection with new locally optimum testing procedures // Proceedings of the International Conference on Acoustics, Speech and Signal Processing. Prague, Czech Republic, 2011. Pp. 3852-3855. **[** Q. He, R. S. Blum, “Smart grid monitoring for intrusion and fault detection with new locally optimum testing procedures”, in *Proceedings of the International Conference on Acoustics, Speech and Signal Processing*, pp. 3852-3855, 2011. **]**

4. **Фазлиахметов Т. И., Фрид А. И.** Модель для оценки эффективности обеспечения целостности метрологических данных в производственных системах нефтегазового комплекса // Вопросы защиты информации. 2011. №. 2. С. 31–36. **[** T. I. Fazliahmetov, A. I. Frid, “A model for evaluating the effectiveness of ensuring the integrity of metrological data in the production systems of the oil and gas complex”, (in Russian), in *Voprosy zashhity informacii*, no. 2, pp. 31-36, 2011. **]**

5. **Дубровин А. С., Душкин А. В., Губин И. А.** Описание сервиса контроля целостности автоматизированной системы обработки данных // Вестник Воронежского института ФСИН России. 2013. №. 2. С. 45–48. **[** A. S. Dubrovin, A. V. Dushkin, I. A. Gubin, “Description of the integrity control service of an automated data processing system”, (in Russian), in *Vestnik Voronezhskogo instituta FSIN Rossii*, no. 2, pp. 45-48, 2013. **]**

6. **Горбачевская Е. Н.** Исследование механизмов защиты данных в корпоративных информационных системах // Вестник волжского университета им. В. Н. Татищева. 2012. №. 4 (20). С. 18–23. **[** E. N. Gorbachevskaja, “Study of data

protection mechanisms in corporate information systems", (in Russian), in *Vestnik volzhskogo universiteta im. V. N. Tatishheva,* no. 4 (20), pp. 18-23, 2012. **]**

7. **Architecture** of the security access system for information on the state of automatic control systems of aircraft / A. I. Frid, et. al. // Proceedings of the 19th International Workshop on Computer Science and Information Technologies CSIT'2017, (Germany, Baden-Baden, October 8-10, 2017). Vol. 2. Pp. 21-27. **[** A. I. Frid, et. al., "Architecture of the security access system for information on the state of automatic control systems of aircraft", in *Proceedings of the 19th International Workshop on Computer Science and Information Technologies*, (CSIT'2017), vol. 2, pp. 21-27, 2017. **]**

8. **The architecture** of the web application for protected access to the informational system of processing critically important information / A. I. Frid, et. al. // Proceedings of the 19th International Workshop on Computer Science and Information Technologies CSIT'2017, (Germany, Baden-Baden, October 8-10,2017). **[** A. I. Frid, et. al., "The architecture of the web application for protected access to the informational system of processing critically important information". in *Proceedings of the 19th International Workshop on Computer Science and Information Technologies,* (CSIT'2017), 2017. **]**

9. **Защищенный** доступ к базе данных о состоянии систем автоматического управления (САУ) авиационными ГТД через веб-приложение / М. Б. Гузаиров и др. //Информация и безопасность. 2017. Т. 20, № 3. С. 410–413. **[** M. B. Guzairov, et al., "Secure access to the database of the status of automatic control systems (ACS) by aircraft GTE through a web application", (in Russian), in *Informacija i bezopasnost*, vol. 20, no. 3, pp. 410-413, 2017. **]**

10. **Simulation** modelling of the transmission system of the telemetric information on the status of the on-board aircraft status / M. B. Guzairov, et. al. // Data Science. IV International Conference on Information Technology and Nanotechnology. 2018. Pp. 105-111. **[** M. B. Guzairov, et. al., "Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status", in *Data Science. IV International Conference on Information Technology and Nanotechnology,* pp. 105-111, 2018. **]**

11. **The structure** of secure system for collection, storage and processing of telemetric information on the state of aircraft subsystems / V. V. Berkholts, et. al. // Industrial 4.0. 2018. Issue 4/2018. Pp. 209-212. **[** V. V. Berkholts , et. al., "The structure of secure system for collection, storage and processing of telemetric information on the state of aircraft subsystems", in *Industrial 4.0.*, Issue 4/2018, pp. 209-212, 2018. **]**

12. **Simulation** modelling of the transmission system of the telemetric information on the status of the on-board aircraft status / M. B. Guzairov, et. al. // Информационные технологии и нанотехнологии. 2018. С. 2275–2281. **[** M. B. Guzairov, et al., "Simulation modelling of the transmission system of the telemetric information on the status of the on-board aircraft status", in *Informacionnye tehnologii i nanotehnologii*, pp. 2275-2281, 2018. **]**

13. **Protected** access to the data-base on the status of automatic control systems (ACS) by aviation GTE via the web application / M. B. Guzairov, et. al. // Information and Security. 2017. Vol. 20, No. 3 (4). Pp. 410-413. **[** M. B. Guzairov, et al., "Protected access to the data-base on the status of automatic control systems (ACS) by aviation GTE via the web application", in *Information and Security*, vol. 20, no. 3 (4), pp. 410-413, 2017. **]**

14. **Приказ ФСТЭК России от 14 марта 2014 г. № 31** «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и окружающей среды» / [Электронный ресурс]. URL: https://fstec.ru/ normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 26.03.2019). **[** *"On approval of requirements to protection of information security in automated systems of production and technological processes control at critically important objects, potentially dangerous objects, and the objects representing higher danger to the human life and health and environment*", (in Russian), Order FSTEC of Russia № 31 dated of 14.03.2014 (2019, March 26). [Online], Available: https://fstec.ru/ normotvorcheskaya/akty/53-prikazy/868-prikaz -fstek-rossii-ot **]**

15**. Приказ ФСТЭК России от 23 марта 2017 г. № 49** «О внесении изменений в состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные приказом федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21, и в требования к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды, утвержденные приказом федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31» / [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/110-prikazy/1419-prikaz-fstek-rossii-ot-23-marta-2017-g-n-49 (дата обращения 26.03.2019). **[** "*On Amending the Composition and Content of Organizational and Technical Measures to Ensure the Safety of Personal Data when Processing in Personal Information Systems approved by the Order of the Federal Service for Technical and Export Control of February 18, 2013 No. 21, Requirements to ensure the protection of information in automated control systems of production and technological processes in critical facilities, potentially hazardous facilities, as well as objects posing an increased risk to life and health of people and the environment, approved by the order of the Federal Service for Technical and Export Control March 14, 2014 No. 31"*, (in Russian), Order FSTEC of Russia № 49 dated of 23.03.2017 (2019, March 26). [Online], Available: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/ 110-prikazy/1419-prikaz-fstek-rossii-ot-23-marta-2017-g-n-49 **]**

16. **ГОСТ Р ИСО/МЭК 27033-1-2011.** Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 1. Обзор и концепции. М.: Стандартинформ, 2012. 66 с. **[** *Information technology (IT) Methods and means of ensuring safety. Network security. Part 1. Overview and concepts*, (in Russian), Federal standart R ISO/IEC 27033-1-2011, Moscow, Standartinform, 2012. **]**

17. **ГОСТ Р ИСО/МЭК 27033-3-2014.** Информационная технология (ИТ). Методы и средства обеспечения безопасности. Безопасность сетей. Часть 3. Эталонные сетевые сценарии. Угрозы, методы проектирования и вопросы управления. М.: Стандартинформ, 2014. 40 с. **[** *Information*

technology (IT) Methods and means of ensuring safety. Network security. Part 3. Reference network scenarios. Threats, design methods and management issues, (in Russian), Federal standart R ISO/IEC 27033-3-2014, Moscow, Standartinform, 2014. **]**

18. **NIST** Special Publication 800-82 Revision 2. Guide to Industrial Control Systems (ICS) Security ISA/IEC 62443 “Industrial Automation and Control Systems Security”

19. **Mahnke W., Leitner S. H., Damm M.** OPC unified architecture // Springer Science & Business Media, 2009. **[** W. Mahnke, S. H. Leitner, M. Damm, *OPC unified architecture*. Springer Science & Business Media, 2009. **]**

20. **Mllib**: Machine learning in apache spark / X. Meng, et. al. // The Journal of M-chine Learning Research. 2016. Vol. 17. № 1. Pp. 1235-1241. **[** X. Meng, et. al., “Mllib: Machine learning in apache spark”, in *The Journal of Machine Learning Research*, vol. 17, no. 1, pp. 1235-1241, 2016. **]**

21. **The hadoop** distributed file system / K. Shvachko, et. al. // MSST. 2010. Vol. 10. Pp. 1-10. **[** K. Shvachko, et. al., “The hadoop distributed file system”, in *MSST*, vol. 10, pp. 1-10, 2010. **]**

22. **Anderson C.** Docker [software engineering] // IEEE Software. 2015. Vol. 32, No. 3. Pp. 102–c3. **[** C. Anderson, “Docker [software engineering]”, in *IEEE Software*, vol. 32, no. 3, pp. 102-c3, 2015. **]**

23. **Алексеев Д. М., Иваненко К. Н., Убирайло В. Н.** Построение графа атак для анализа защищенности компьютерных сетей // Символ науки. 2016. № 7-2. С. 31–34. **[** D. M. Alekseev, K. N. Ivanenko, V. N. Ubirajlo, “Building an attack graph to analyze the security of computer networks”, (in Russian), in *Simvol nauki*, no. 7-2, pp. 31-34, 2016. **]**

24. **Mell P., Harang R.** Minimizing Attack Graph Data Structures // In the Tenth International Conference on Software Engineering Advances, (Barcelona, Spain). 2015. Pp. 376-385. **[** P. Mell, R. Harang, “Minimizing Attack Graph Data Structures”, in *the Tenth International Conference on Software Engineering Advances,* pp. 376-385, 2015. **]**

25. **Friedman N., Geiger D., Goldszmidt M.** Bayesian network classifiers // Machine learning. 1997. Vol. 29, No. 2-3. Pp. 131-163. **[** N. Friedman, D. Geiger, M. Goldszmidt, “Bayesian network classifiers”, in *Machine learning*, vol. 29, no. 2-3, pp. 131-163, 1997. **]**

26. **Development** of a cyber security risk model using Bayesian networks / J. Shin, et al. // Reliability Engineering & System Safety. 2015. Vol. 134. Pp. 208-217. **[** J. Shin, et al., “Development of a cyber security risk model using Bayesian networks”, in *Reliability Engineering & System Safety,* vol. 134, pp. 208-217, 2015. **]**

27**. Lahti J. P., Shamsuzzoha A., Kankaanpää T.** Web-based technologies in power plant automation and SCADA systems: A review and evaluation // 2011 IEEE International Conference on Control System, Computing and Engineering. IEEE, 2011. Pp. 279-284. **[** J. P. Lahti, A. Shamsuzzoha, T. Kankaanpää, “Web-based technologies in power plant automation and SCADA systems: A review and evaluation”, in *2011 IEEE International Conference on Control System, Computing and Engineering*. IEEE, pp. 279-284, 2011. **]**

ОБ АВТОРАХ

ГУЗАИРОВ Мурат Бакеевич, проф. каф. ВТиЗИ УГАТУ. Дипл. инж.-электромех. (УАИ, 1973). Д-р техн. наук поупр. в соц. и экон. системах. Иссл. в обл. сист. анализа, упр. в соц. и экон. системах.

ФРИД Аркадий Исаакович, проф. каф. ВТиЗИ УГАТУ. Дипл. инж.-электром. (УАИ, 1968). Д-р техн. наук по управ. в техн. системах (УГАТУ,2000). Иссл. в обл. управ. сложн. сист. в условиях неопределенности.

ВУЛЬФИН Алексей Михайлович, доцент каф. ВТиЗИ УГАТУ. Дипл. инженера-программиста (УГНТУ, 2008). Канд. техн. наук по системному анализу, управлению и обработке информации (УГАТУ, 2012). Иссл. в обл. интеллектуального анализа данных и моделирования сложных технических систем.

БЕРХОЛЬЦ Виктория Викторовна, асп. каф. ВТиЗИ УГАТУ. Дипл. инженера по специальности: вычислительные машины, комплексы, системы и сети (УГАТУ, 2015). Иссл. в обл. обеспечения информационной безопасности.

КИРИЛЛОВА Анастасия Дмитриевна, асп. каф. ВТиЗИ УГАТУ. Дипл. магистра по направлению: информатика и вычислительная техника (УГАТУ, 2017). Иссл. в обл. обеспечения информационной безопасности.

METADATA

Title: Analysis of the protection of the system of the collection, storage and processing of telemetric information on the condition of airplane systems.

Authors: M. B. Guzairov [1], A. I. Frid [2], A. M. Vulfin[3], V. V. Berkholts[4], A. D. Kirillova[5]

Affiliation:

Ufa State Aviation Technical University (USATU), Russia.

Email: [1] guzairov@ugatu.su, [2] frid46@mail.ru, [3] vulfin.alexey@gmail.com, [4] torina4@yandex.ru, [5] kirillova.andm@gmail.com

Language: Russian.

Source: Vestnik UGATU (scientific journal of Ufa State Aviation Technical University), vol. 23, no. 4 (86), pp. 132-146, 2019. ISSN 2225-2789 (Online), ISSN 1992-6502 (Print).

Abstract: The analysis of the security of the modular system for collecting, storing and processing telemetric information on the state of the onboard subsystems of the aircraft in automatic mode is considered. The main threats and vulnerabilities of the system under consideration in terms of the integrity of the accumulated data are identified, scenarios for the realization of threats by an external and internal attacker based on attack graphs are developed.

Key words: telemetry collection; storage and processing systems; automated information system; intruder model; attack graph.

About authors:

GUZAIROV, Murat Bakeevich, Prof., Dept. of Computer Engineering and Information Security. Dipl. Engineer of Electromechanical (USATU, 1973), Dr. of Tech. Sci. of manag. in social and econ. systems. Research in the field of system analysis, manag. in social and econ. systems.

FRID, Arkadij Isaakovich, Prof., Dept. of Computer Engineering and Information Security. Dipl. Engineer of Electromechanical (USATU, 1968), Dr. of Tech. Sci. of manag. in techn. systems (USATU, 2000). Research in the manag. of complex systems under uncertainty.

VULFIN, Alexey Mikhailovich, Ass.-prof., Dept. of computing equipment and information protection, software engineer dipl. (UGNTU, 2008). Cand. of tech. sci., systems analyst, councils recommend measure and information processing (USATU, 2012).

BERKHOLTS, Victoria Victorovna, Postgrad. Student, Dept. of Computer Engineering and Information Security. An engineering degree in computers, complexes, systems and networks (UGATU, 2017). Research in the area of information security.

KIRILLOVA, Anastasia Dmitriyevna, Postgrad. Student, Dept. of Computer Engineering and Information Security. Master's Degree of Informatics and Computing (UGATU, 2017). Research in the area of information security.