С.А. Федоров, Н.А. Елисеев, О.Д. Антонов

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В СИСТЕМАХ МОНИТОРИНГА АВТОТРАНСПОРТА

(ИСТиД (филиал) СКФУ в г. Пятигорске)

Процесс мониторинга в автотранспорте возник в начале XXI века, поэтому его принято считать относительно новым направлением применения информационных технологий в области транспорта. Мониторинг в нынешнем его виде позволяет в десятки раз сократить потери, возникающие в области перевозок, осуществляемых грузовым транспортом. Данный процесс возник в Европе и США при переходе процесса пользования спутниковыми системами навигации в руки гражданских специалистов. На сегодняшний день в мире существует две основные системы спутникового мониторинга с общемировым покрытием российская ГЛОНАСС и американская GPS. Российский комплекс навигации лучше работает на высоких широтах, в тоже время американский – на средних. Для рассмотрения основных характеристик комплексов спутникового мониторинга ниже приведена таблица 1.

Таблица 1. Основные характеристики ГЛОНАСС и GPS

№ п/п	Характеристика	ГЛОНАСС	GPS
1	Количество спутников	24(3 резерв)	24(7 резерв)
2	Высота орбиты	19100-19400 км	20180 км
3	Скорость передачи информации	50 бит/с	50 бит/с
4	Период обращения	11 часов 15,7 минут	11 часов 56,7 минут
5	Способ разделения сигналов	Частотный	Кодовый
6	Рабочие частоты	1602,56-1615,5 МГц 1246,44-1256,5 МГЦ	1575,42 1227,6
7	Точность	7-10 м	5-6 м
8	Погрешность	0,997	0,95

Исходя из данных таблицы, система ГЛОНАСС несколько уступает GPS, но этот разрыв минимален и постоянно сокращается.

Декомпозиция процесса мониторинга – это представление всей схемы процессов в комплексном виде, предназначенное для понимания сути процессов, протекающих в данной системе. Декомпозиция

Применение декомпозиции для решения данной задачи обусловлено тем, что данная схема позволяет эффективно определить те области информационной системы, куда может быть проведена атака, а также позволяет представить область, в которой сконцентрированы данные, интересные злоумышленнику. Данная схема изображена на рисунке 1.

В ходе исследования процесса мониторинга были выявлены совокупности угроз, которые являются самыми опасными для системы:

—атаки на проводные и беспроводные сети передачи данных;

—атаки на системы аутентификации.

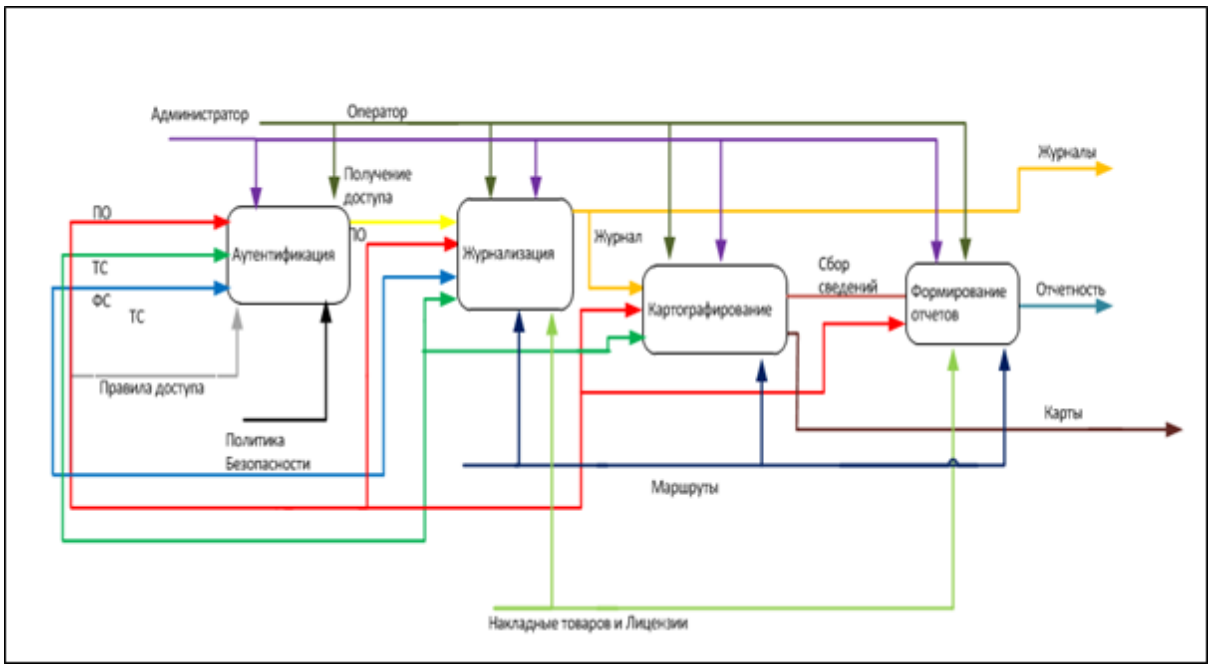

Рисунок 1 – Декомпозиция информационной системы мониторинга автотранспорта

Атаки из с этих совокупностей угроз делятся на следующие:

1) подслушивание (Сниффинг);
2) изменение данных;
3) анализ сетевого трафика;
4) подмена доверенного субъекта;
5) перехват сеанса;
6) отказ в обслуживании;
7) парольные атаки;
8) атаки на уровне приложений;
9) компьютерные вирусы;

Атаки на системы аутентификации бывают следующих видов:

1) самозванство;
2) повторная передача;
3) подмена сторону аутентификационного обмена;
4) отражение передачи;
5) вынужденная задержка;
6) атака с выборкой текста;
7) атака на основе неправильной интерпретации.

Каждая из этих атак имеет высокий класс опасности для информационной системы.

Для решения задачи по защите информационной системы существует несколько способов, которые следует применять техническим специалистам, выполняющим функции инженеров по безопасности.

Одним из способов защиты является применение протоколов защищенных каналов связи, построенных с применением криптозащищенных туннелей или туннелей VPN.

Саму систему защиты для понимания процесса ее функционирования следует разделить на подсистемы, которые действуют на различных уровнях сетевой модели OSI.

Первый уровень сетевой модели на котором необходимо установить защиту – канальный. Здесь допустимо применять следующие протоколы:

1. ПротоколPPTP (Point – to – Point Protocol).
   Протокол, разработанный компанией «Microsoft» при поддержке других компаний для создания защищенных каналов сети. Такой протокол предназначен для создания защищенных виртуальных каналов в сети, предполагая создание криптозащищенного туннеля на канальном уровне модели OSI.
2. Протоколы L2F и L2TP– протоколы, разработанные в качестве аналога PPTP компанией CISCO.
3. Протокол PPOE– так же работает на канальном уровне Предоставляет дополнительные возможности (аутентификация, сжатие данных, шифрование). Крайне трудно данный протокол взаимодействует с межсетевыми экранами[1].

На сетевом уровне в качестве меры защиты следует применять Стек протоколов IPSec[2], который применяется в процессах аутентификации участвующих в обмене сообщениями, туннелирования трафика, шифрования пакетов протокола IP. всеобщим достоянием и возможность того что данные не были изменены. Для обеспечения процессов аутентификации, конфиденциальности и целостности, стек IPSec применяет стандартные криптографические технологии:

—обмен ключами по алгоритму Диффи – Хеллмана для распределения секретных ключей между пользователями в открытой сети;

—криптография открытых ключей, применяемая для обеспечения конкретики в обменах Диффи – Хеллмана, чтобы гарантировать подлинность двух сторон и избежать атак типа человек – посередине[3].

Наиболее высоким уровнем для организации защиты принято считать сеансовый уровень. На этом уровне работает протокол SSL – сессионный протокол безопасности, разработанный NETSCAPE Communications совместно с RSA Data Security, специально для реализации процесса защищенного обмена информацией. Криптопротолы, применяемые на этом уровне бывают следующих видов:

— Несимметричные: RSA, Диффи-Хэллмана
— Симметричные: 3-DES, AES[4].

Таким образом, на сегодняшний день уже существуют качественные системы защиты, работа которых основана на выше перечисленных протоколах. Но наука в сфере информационной безопасности не стоит на месте, поэтому в ближайшее время ожидается появление новых решений, которые увеличат сохранность информации.

Литература

1. Афанасьев А.А., Веденьев Л.Т., Воронцов А.А., Газизова Э.Р., Додохов А.Л., Крячков А.В., Кузнецов С.Б., Полянская О.Ю., Сабанов А.Г., Скида М.А., Халяпин С.Н. Аутентификация. Теория и практика / под ред. А.А. Шелупанова. М.: Горячая линия-Телеком. 2009. 552 с.
2. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети – анализ технологий и синтез решений. М.: ДМК Пресс. 2004. 510 с.
3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах. – М.: ИД «ФОРУМ» :ИНФРА – М,2010. 610 с.
4. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. – М.: ИД «ФОРУМ» :ИНФРА – М,2008. 612с.

Д.Н. Франтасов, П.А. Мельников, А.С. Климась

РАЗРАБОТКА И РЕАЛИЗАЦИЯ АЛГОРИТМА ОПРЕДЕЛЕНИЯ ВОЗМОЖНЫХ ПУТЕЙ ВЫПОЛНЕНИЯ ПРОГРАММ УПРАВЛЕНИЯ БЕСПИЛОТНЫМИ ТРАНСПОРТНЫМИ СРЕДСТВАМИ

(Самарский государственный университет путей сообщения)

В современном мире создание беспилотных транспортных средств является одним из путей повышения транспортной эффективности. Разработка таких, полностью автономных транспортных средств позволит решить ряд проблем, таких как:

- безопасность движения;
- эффективное трата энергоресурсов;
- эффективное совместное использование.

Уже давно в мире ведется разработка беспилотных транспортных средств. Со временем и развитием технологий возможность создавать беспилотные транспортные средства появилась практически у каждого человека. Однако, в процессе разработки таких транспортных средств инженеры сталкиваются со множеством проблем и одной из главных является написание программы управления движением, учитывающую возможные внешние факторы для бесперебойного движения.

Для построения программ бесперебойного движения составляются циклограммы, на которых наглядно отображены все команды, из которых состоит программа. Это позволяет оценить её качество и аналитически выявить варианты выполнения, способные привести к сбоям в работе транспортного средства. На данный момент разработан инструмент для построения циклограмм программ управления, не зависящий от аппаратной платформы и работающий с условными командами управления [1].

Существуют ветвления работы программы, возникающие в случае непредвиденных ситуаций или запланированных системных действий. Их необходимо учитывать, так как они влияют на работоспособность всей про-