ՀՏԴ 338.242.2, 656.015

Ռ.Մ. ՅՈԼՉՅԱՆ, Գ.Ս. ԳՈՒԼԱԿՅԱՆ, Լ.Մ. ԳՐԻԳՈՐՅԱՆ

ԱՎՏՈՏՐԱՆՊՈՐՏԱՅԻՆ ՀՈՍՔԵՐԻ ՏԵՂԵԿԱՏՎԱԿԱՆ ԲԱՆԱԿԱՆ ՀԱՄԱԿԱՐԳԵՐԻ ԿԻՐԱՌՈՒԹՅԱՆ ՀԵՌԱՆԿԱՐՆԵՐԸ ՀՀ-ՈՒՄ

Ավտոմեքենաների շահագործման ժամանակակից պահանջները ներառում են անվտանգության միջոցներում տեղեկատվական տեխնոլոգիաների ընդլայնված կիրառություն: Վերջին տարիներին մեծացել է ՀՀ-ում շահագործվող արտասահմանյան տրանսպորտային միջոցների քանակը, որը, չնայած կիրառված անվտանգության միջոցների առկայությանը /տեսախցիկներ հանգույցներում ինքնակարգավորումներ/, առաջ է բերել անվտանգության ցուցանիշների զգալի իջեցում: Թեև այդ տրանսպորտային միջոցները հագեցած են անվտանգության տեխնիկական միջոցներով, սակայն ՀՀ-ում դրանց կիրառությունը սահմանափակ է կամ բացակայում է՝ ընդհանուր տեղեկատվական անվտանգ համակարգի ոչ լիարժեք լինելու պատճառով: Խնդրի լուծման համար անհրաժեշտ է արագ ներդնել անվտանգության ինֆորմացիոն համակարգեր, որոնք հիմնված են տեղեկատվական բանական համակարգի վրա: Նման համակարգեր հաջողությամբ շահագործվում են արտասահմանում և ապահովում բարձր ցուցանիշներ: Դա իրականացնելու համար պետք է ստեղծել տեղեկատվական տեխնիկական միջոցներից բաղկացած ցանց և պատրաստել այն սպասարկող անձնակազմ: Կարևոր են նաև տեղեկատվական անվտանգության հարցերի ապահովումը և համապատասխան բարձր որակավորմամբ մասնագետների պատրաստումը, որի համար կպահանջվի կրթական ռեսուրսների որոշակի կենտրոնացում:

Առանցքային բառեր. տեղեկատվական տեխնոլոգիա, ցանց, անվտանգություն, համակարգ, ավտոտրանսպորտ:

Ավտոմեքենաների քանակի շեշտակի աճը ՀՀ-ում վերջին տարիներին կտրուկ բարձրացրել է վտանգավորությունը և առաջացրել որոշակի բարդություններ տեխնիկական սպասարկման բնագավառում: Դա պայմանավորված է մի քանի գործոններով: Անվտանգության բարձրացման համար առավել հեռանկարային են ավտոմեքենաների միջև հաղորդակցության հաստատման մշակումներն ու արդյունավետ համակարգերի ներդրումը: ԵՄ երկրներում լիարժեք գործարկվել և իրենց արժանի կիրառությունն են գտնում ավտոմեքենաների կառավարման տարբեր տեղեկատվական բանական համակարգեր /ՏԲՀ/ և տեխնիկական միջոցներ: Այդպիսի համակարգերից են. անլար կառավարման ցանցերը, ինչպիսիք են՝ WLAN-Wireless Local Area Network, որոնցում գործում են երկու տիպի հանգույցներ՝ «ավտոմեքենա» և «ենթակառուցվածքային օբյեկտներ»

/լուսացույց, երթևեկության կառավարման կենտրոն/: Ավտոմեքենաների միջև հաղորդակցության համակարգը բանական տարանսպորտային համակարգի բաղկացուցիչ մասն է: Ավտոմեքենաների անլար մատչելիությամբ համակարգերը (WAVE-Wireless Access in Vehicular Environments) գործում են սովորաբար միջազգային IEEE 802.11 ստանդարտով: Մոտիկ կապի միջոցներից առավել տարածված են՝ DSRC, Dedicated Short Range Communications, որոնք գործում են 2002թ-ից առայսօր: Այդ համակարգերի աշխատանքային ցուցանիշներն են. աշխատանքային հաճախականությունը՝ 5,9*ԳՀց*, ակտիվ գործելու տիրույթը՝ մինչև 1000 *մ*, տրանսպորտային միջոցի արագությունը՝ մինչև 100 *կմ/ժ*: Դա մեզ բոլորիս հայտնի Wi-Fi կապն է ավտոմեքենայի համար: Ավտոմեքենաների միջև հաղորդակցության համակարգն ունի մի քանի անվանումներ. ԵՄ-ում դա Car-to-Car (Car2Car, C2C), ԱՄՆ-ում՝ Vehicle-to-Vehicle (V2V): Ավտոմեքենայի և ենթակառուցվածքային օբյեկտի հետ կապի ձևերից են Car-to-Infrastructure (C2I), Vehicle-to-Roadside (V2R), կամ, ինչպես վերջերս են առավել հաճախ օգտագործում, Car-to-X (C2X) /«X» ասելով հասկանում են ենթակառուցվածք/: Այս համակարգերը անընդհատ կատարելագործվում են, և այդ աշխատանքներին ընդգրկված են ԱՄՆ, ԵՄ կրթական տիրույթը և մասնավոր ընկերություններ, ինչպիսիք են՝ Audi, BMW, Daimler, General Motors, Ford, Honda, Mercedes-Benz, Nissan, Opel, PSA, Toyota, Volkswagen, Volvo, էլեկտրոնիկայի հայտնի բրենդային ընկերություններ, ինչպիսիք են՝ Bosch, Continental, Siemens:

Հաղորդակցության նման համակարգերը մեքենայում տեղադրվում են WLAN մոդուլի տեսքով, որը ներառում է՝ անտենա, ընդունիչ+հաղորդիչ, կառավարման բլոկ: Այդպիսի մոդուլ կարող է ծառայել սովորական սմարթֆոնը, որում ներդրված և մեքենայի հետ համակցված է ծրագրային կառավարման համապատասխան հավելված-ծրագիր: Կառավարման ազդանշանները անտենայի միջոցով ստացվում կամ հաղորդվում են ցանցում գտնվող մեքենաներին և բացի ինֆորմացիոն էկրանին հայտնվելուց, կարող են որոշակի արտակարգ իրավիճակում կատարել կառավարող գործողություններ և ազդել «հարևան» մեքենայի ղեկավարման վրա՝ կանխելով վթարը: Բացի դա, ներկայիս ավտոմեքենաների միջև հաղորդակցության համակարգերը նախատեսվում է օգագործել նաև երթեկության կառավարման, էլեկտրոնային վճարումների, ավտոմեքենայի երթևեկության ավտոմատացման և ընթացքի հսկողության, մեծ տեղեկատվական բազաների մատչելիություն ապահովելու համար:

Ներկայումս ՀՀ-ում շահագործվող արտասահմանյան արտադրության ավտոմեքենաները էապես չեն կարող իրականացնել վերոհիշյալ գործառույթների

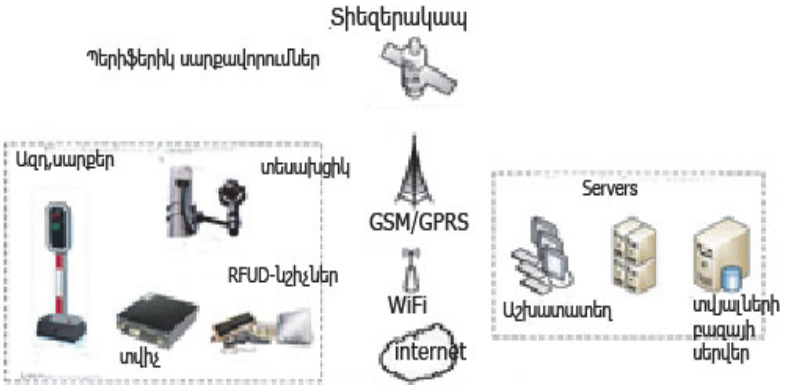
մեծ մասը՝ ինֆորմացիոն, կառավարման ցանցի բացակայության պատճառով: Անշուշտ, նման կարողությունների առկայությունը կբարձրացներ մեր երկրում անվտանգությունը, սպասարկման մշակույթը և արդյունավետությունը: GPS-GLONASS կապի միջոցների առկայությունը մեծապես կարող է լավ նախադրյալներ ստեղծել նման համակարգի մշակման և արագ ներդրման համար: Դրա համար վերլուծենք այն տեխնիկական և կազմակերպչական անհրաժեշտ բաղադրիչները և խնդիրները, որոնց լուծումները անհրաժեշտ կլինեին նման համակարգ ներդնելու և շահագործելու համար:

Անվտանգությունն ապահովվում է հնարավոր վտանգի հայտնաբերման և ահազանգման, ինչպես նաև վարորդի գործողությունների և ավտոմեքենայի շարժման գնահատման միջոցով: Համապատասխան տվիչները որոշում են շարժման ուղղության կտրուկ փոփոխությունը, առանձին անիվների պտտման արագությունը, կտրուկ արգելակումները և այլն: Այս դեպքում հաղորդակցույան միջոցները կզգուշացնեն. խաչմերուկով անցնելիս, ձախ շրջադարձի ժամանակ հանդիպակաց մեքենայի հայտնվելը, ավտոմայրուղի մտնելիս ճանապարհին հայտնված խոչընդոտի առկայությունը՝ հանկարծակի արգելակելիս թիկունքից հարվածի դեպքում, ինչպես նաև կիրականացնեն ճանապարհային նշանների մասին հատուկ զգուշացում: Չնայած ներկայումս այս խնդիրների մի մասը ՀՀ-ում ևս բավարար հաջողությամբ լուծվում են ռադարների, տեսախցիկների լայնորեն կիրառման միջոցով, այնուամենայնիվ, Car-to-Car համակարգի հնարավորությունն ավելի լայն են: Անլար կարգավորման ձևաչափում տեխնոլոգիաները օպտիմալ ուղու ընտրության հարցերում կողմնորոշվում են՝ ելնելով տրանսպորտային հոսքի կարգավորման, լուսացույցների կառավարման, տրանսպորտային հանգույցներում խցանումների կարգավորման, հատուկ ծառայությունների մեքենաների անարգել տեղաշարժման և տարբեր չափանիշներից /վարձավճար, ժամանակ, տարածություն և այլն/:

Սակայն ՀՀ-ում շահագործվող ավտոմեքենաներում նախատեսված կարևորագույն հնարավորությունների որոշ մասը դեռևս իրենց պատշաճ կիրառությունը չեն գտել: Ինչպես, օրինակ՝ հնարավորություն, որը թույլ է տալիս մեքենաներին՝ մեկը մյուսին հսկելու և փոխարինելու /գոնե որոշակի չափով/ ոստիկանության, անվտանգության ծառայություններին: Անլար ինֆորմացիոն կապով ինֆորմացիայի փոխանակումը տեղեկատվական դաշտում և ավտոմեքենայի կառավարման ավտոմատացումը դեռևս բացակայում են ՀՀ ավտոմեքենաների շահագործման ժամանակ: Միաժամանակ, նման հնարավորությունների ներդրումը առաջ կբերի որոշակի խնդիրներ՝ կապված տեղեկատվական անվտանգության

և ավտոմատ կառավարման համակարգի դեռևս ոչ բավարար հուսալի աշխատանքի հետ, ինչպես նաև ՏԲՀ ներդրումը կբարձրացնի ավտոմեքենայի գինը /ոչ պակաս 15%/: Թերևս առավել ծախսատար տեխնիկական հարցը՝ կապված ավտոմեքենայի տեղորոշման հետ, կարող ենք համարել հիմնականում լուծված: Դրանում ՀՀ-ում մեծ դեր է խաղացել դեռ 2018թ դեկտեմբերին Բյուրականում ԳԼՈՆԱՍՍ տիեզերական կապի միջոցների սերվերային կենտրոնի բացումը, որով հնարավոր եղավ ստեղծել Հայաստանի մանրակրկիտ քարտեզը, և մեծ հեռանկար բացվեց տիեզերական նավիգացիոն տեխնոլոգիաների զարգացման գործում: Սա մեծ խթան է՝ արագորեն ներդնելու և զարգացնելու միջազգային բոլոր չափանիշներին համապատասխան տրանսպորտային միջոցների անվտանգ երթևեկությունն ապահովող ավտոմատ բանական համակարգ: Բացի դա, Երևանում անցկացված /2019 թ. հունիսի 24 – 28/ «Ինժեներական շաբաթ» միջազգային ֆորումում ներկայացված Հարավային Կորեայում արդեն ներդրված 5G կապի նորագույն հետազոտական համակարգերի մշակումները ցույց տվեցին, որ ՀՀ ունի այն կիրառելու մեծ հեռանկարներ /առաջին հաջող տեխնիկական լուծումները ֆորումում ներկայացրել էր նաև ՀԱՊՀ/: Անկասկած, կապի միջոցների նոր և յուրահատուկ միջոցները կարող են լայն հեռանկարներ և հնարավորություններ ստեղծել ավտոմոբիլային տնտեսության շահագործման ու սպասարկման գործընթացներում:

Ներկայացնենք հիմնական տեխնիկական խնդիրները, որոնք անհրաժեշտ են նշված համակարգերի ներդրման համար: GPS-ГЛОНАСС համակարգերի տեխնիկական հնավորությունները կարող են ապահովել տեղաշարժերի, տրանսպորտային միջոցների, բեռների լիակատար հսկողություն, կառավարարում և գործընթացների կարգավորման մեծ արդյունավետություն (նկ.1):

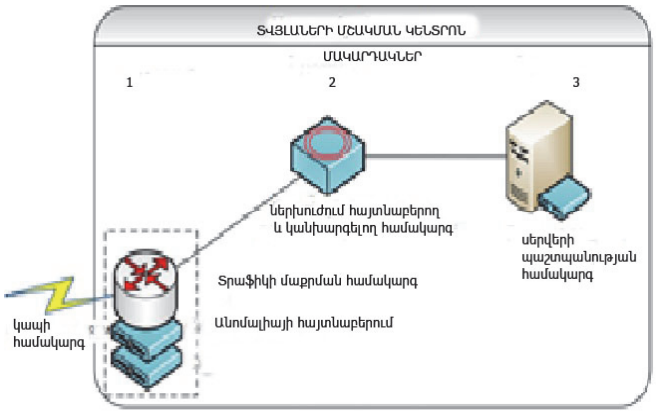


Նկ. 1. Տեղակատվական բանական համակարգի ապարատային բազան

Տեխնիկական խնդրի լուծումն իր հերթին հանգեցնում է ՏԲՀ-ում կարևորագույն խնդիրների լուծմանը: Թերևս դրանց լուծելու հաջողությամբ է պայմանավորված ՏՀԲ կիրառման արդյունավետությունը: Նման խնդիրներից են. չթույլատրված ներխուժում ակտիվ և պերիֆերիկ սարքավորումների կառավարման տիրույթ, բարձր մակարդակի տեղեկատվական անվտանգություն և ինքնավերականգնվելու մեծ ռեսուրսներ:

Դրանք ապահովելու համար շահագործվող տեխնիկական միջոցները պետք է անցած լինեն միջազգային սերտիֆիկացում, ունենան ստացիոնար տարածական խիտ ցանց և պարբերաբար իրականացնելն մոնիտորինգ՝ կանխելու հնարավոր կիբեռ-հարձակումները, ինֆորմացիայի մշակման կենտրոններում և ՏԲՀ-ում օգտագործվող միջցանցային տեղեկատվական տիրույթներում ապահովելու տվյալների անձեռմխելիություն և պաշտպանություն, հակավիրուսային ծրագրային ապահովություն: ՏՀԲ-ի կարևորագույն խնդիրներից է հատկապես ներխուժումների /նամանավանդ՝ համակարգային և ցանցային տիրույթում/ հայտնաբերման և կանխարգելման համակարգերի արդյունավետ աշխատանքի ապահովումը /հատկապես ներխուժումներից/:

Վերջին ժամանակներս առավել տարածված DDoS (Distributed Denial of Service, DdoS «սպասարկման բաշխված մերժում») (նկ.2) հարձակումների վերլուծությունը՝ ինֆոթրաֆիկի անընդհատ վերլուծության և շեղումների գնահատման միջոցով, զգալիորեն նվազեցրել է հարձակումների իրավական ազդեցությունը:



Նկ. 2. DdoS հարձակումներից պաշտպանության կազմակերպումը

Այս հարձակումների հիմնական թիրախը սերվերային և ցանցային տիրույթն է, որի արդյունքում հնարավոր է ամբողջ ցանցի խափանում, և այն մնում է առավել տարածվածը կիբեռ-հարձակումների ցանկում: Ներխոսժումներից

պաշտպանական համալիրում օգտագործվել է ցանցի բազմաշերտ պաշտպանության սկզբունքը: Կանխարգելիչ գործողությունները հիմնված են «հայտնաբերել, որոշել աղբյուրը և կանխել ներխուժումը» մեխանիզմների վրա: Համալիր պաշտպանական միջոցառումներ են պահանջվում հակավիրուսային և կապի միջոցների ինֆորմացիոն անվտանգության գործընթացներում: Դրանք առնչվում են «համացանց-GSM/GPRS ցանց– տիեզերակապ» տիրույթներին, որտեղ առավել խոցելի են մուտքերի ինքնաճանաչման ցանցային արձանագրությունները /օրինակ՝ TCP/IP արձանագրությունը/ ՝ ոչ լիարժեք նախագծման արդյունքում: Յուրահատուկ տեղ է հատկացվում անլար ցանցերի պաշտպանությանը, քանի որ ՏԲՀ հիմնական գործընթացները այս տիրույթում են իրականացվում: Այն իրականացվում է սովորաբար ցանցային մատչելիությունը ստուգող միջազգային IEEE 802.1x կամ VLAN ստանդարտների միջոցով, որը ստուգում է ընդունիչ թափանցած ազդանշանի իրավասությունը և «համոզվում» նրա իսկության մեջ: Ցանցի որևէ տեղամասում թափանցման մերժումը առաջ է բերում նմանատիպ մերժում ցանցի ամբողջ տիրությում՝ այդպիսով պաշտպանելով ցանցային միջավայրը անթույլատրելի մուտքերից:

Տեղեկատվության արտահոսքը ՏԲՀ-ի ամենաարդիական և ամենատարածված խնդիրն է: Առաջացած սպառնալիքներն այս դեպքում կարող են հանգեցնել բացասական լուրջ հետևանքների, ինչպես, օրինակ՝ հսկող և գործավար կազմակերպությունների կողմից պատժամիջոցների և լրջագույն տուգանքների, որոնք ունեն պատասխանատվության քրեական տարրեր՝ կապված անձնական տեղեկատվության անթույլատրելի հասանելիության տրամադրման հետ: Այսպիսի վտանգները բացառելու կամ նվազագույնի հասցնելու համար պետք է հսկվեն. անձնական և գաղտնապահական տեղեկատվության տեղաշարժերը համացանցում, էլեկտրոնային փոստի շահագործումը, անձնական կամ պաշտոնական տեղեկատվության պատճենումը կրիչների վրա /flash-հիշողություն, օպտիկական սկավառակներ, շարժական կապ և այլն/: Նման նախազգուշական միջոցառումներն ապահովում են զգալի պաշտպանություն՝ անթույլատրելի և քիչ հսկվող ամենահաճախ կատարվող գործողություններից:

Այսպիսով, ժամանակակից տրասնպորտային ցանցը պահանջում է կառավարման կազմակերպչական, տեխնիկական և իրավական արդիական լուծումներ, որոնք ապահովելու համար առավել ինտենսիվ ներդրվում և կիրառվում են բանական տեղեկատվական կառվարման համակարգերը: Դրանց կիրառության ապահովման համար անհրաժեշտ են ժամանակակից հաղորդակցության տեխնիկական միջոցներ: Դա ենթադրում է զգալի ֆինանսական ներդրումներ: Սա-

կայն կապիտալի ներգրավման համար մեծ խթան կարող է հանդիսանալ ՀՀ-ում ներկայիս ներդրումային բարենպաստ իրավիճակը, որի հիմնական գրավականը կլինեն մրցակցության հավասար և ազատ պայմանները: ՏԲՀ տեխնոլոգիաների ներդրումն ապահովելուց առավել կարևոր խնդիրներ են տեղեկատվական անվտանգության ապահովումը և հատկապես որակյալ կադրերի բավարար քանակությամբ ներգրավումը: Անշուշտ, սա պահանջում է որոշակի ժամանակ և մասնագիտական պատրաստման փարձառու միջավայրի ներգրավում: Հաշվի առնելով, որ այս հարցը պետք է լինի շարունակական, ուստի առավել կկարևորվի տեղում նման բարդ ու պատասխանատու գործընթացի մեկնարկը՝ տեղեկատվական անվտանգության կենտրոնի տեսքով: Վերոհիշյալ կադրային և կրթական խնդիրների լուծման համար ՀՀ-ում կան բավարար կրթական և ուսումնական ռեսուրսներ, և խնդրի լուծման դեպքում անհրաժեշտություն կլինի նրանց համախմբումը մեկ ընդհանուր գաղափարի շուրջ: Ավելորդ չէ նշել, որ նման նախապատրաստական ծրագրերն ունեն ներդրումներ ներգրավելու շատ մեծ գրավչություն, իսկ խնդրի իրատեսական արդյունքը կախված կլինի հմուտ մենեջմենտից և հետևողական ու բաց ներդրումային քաղաքականությունից:

ԳՐԱԿԱՆՈՒԹՅԱՆ ՑԱՆԿ

1. **Kabashkin I**. Transport Telematics. - Riga: RAU, 1999. - 342 p.
2. Intelligent Transport Systems (ITS): an area to be strengthened in the Transport sector. http://www.unece.org/trans/theme_its.html
3. Интеллектуальные транспортные системы. Схема построения архитектуры интеллектуальных транспортных систем. Часть 1. Сервисные домены в области интеллектуальных транспортных систем, сервисные группы и сервисы. Государственный стандарт, Российская Федерация, от 01 августа 2011 года № ГОСТ Р ИСО 14813-1-2011.
4. http://systemsauto.ru/another/monitoring-and-reporting-road-quality.html
5. http://systemsauto.ru/another/vehicle_tracking_system.html
6. http://systemsauto.ru/active/car-to-car.html?fbclid=IwAR0kbGAA5knwPM1dRx6OgcRb54LaIO3y38k4nfVLRCREQv9F9j7rZl_oYtU
7. https://3dnews.ru/900329

Р.М. ЕЛЧЯН, Г.В. ГУЛАКЯН, Л.М. ГРИГОРЯН

ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ АВТОТРАНСПОРТНЫХ СЕТЕЙ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В РА

Одним из основных требований при эксплуатации автомашин для системы безопасности является применение информационных технологий. В последние годы резко увеличилось количество автомашин в РА, и, несмотря на предпринятые меры по усилению безопасности автотранспорта (видеокамеры, дополнительные меры транспортных развязок), это привело к снижению показателей безопасности автотранспорта. Современные средства автотранспорта оснащены современными техническими системами коммуникаций и обеспечения безопасности движения, однако в действующих условиях РА круг решаемых задач безопасности остается низким или ограниченным (несмотря на то, что за границей подобные средства уже полностью решают сложные задачи безопасности автотранспорта). Для решения этой проблемы необходимо быстрое внедрение сетей информационных интеллектуальных систем, обеспечивающих функциональное расширение в системе управления безопасностью транспортного движения. Поэтому подготовка специалистов сервиса информационной сети и информационной безопасности является актуальной. Для решения к данной проблемы необходимо определённая концентрация учебно-подготовительных ресурсов страны.

Ключевые слова: информационные технологии, сеть, безопасность, система, автотранспорт.

R.M. YOLCHYAN, G.S. GOULAKYAN, L.M. GRIGORYAN

PERSPECTIVES OF APPLYING AUTOMOBILE TRANSPORTATION INTELLECTUAL INFORMATION SYSTEMS IN RA

One of the requirements to the operation of vehicles for the security system is the application of information technologies. In recent years, the number of cars in RA has sharply increased, and despite the measures taken to strengthen the safety of vehicles (video cameras, additional measures for road interchanges), this has led to a decrease in vehicle safety indicators. Modern vehicles are equipped with modern technical means of communication and traffic safety, however, under the current conditions in Republic of Armenia, the range of security tasks to be solved remains low or limited (despite the fact that abroad such vehicles completely solve the complex problems of vehicle safety). To solve this problem, it is necessary to implement networks of information intelligent systems quickly, providing functional extensions to the traffic safety management system. Therefore, the training of specialists of the information network service and information security is urgent, the solution of which requires a certain concentration of educational resources of the country**.**

Keywords: information technology, network, security, system, automobile transportation.