Bezbednost informacija u automobilskoj industriji – mehanizam TISAX

RADOSLAV M. RAKOVIĆ, Inženjerska akademija Srbije, Beograd

Stručni rad
UDC: 629.331:004.9
DOI: 10.5937/tehnika2403361R

Razvojem informacionih tehnologija i njihovom primenom u svim sferama delatnosti postao je aktuelan problem bezbednosti informacija. Značajan korak ka rešavanju tog problema bilo je donošenje familije standarda ISO/IEC 27000 za sistem menadžmenta bezbednošću informacija (ISMS). Praktična primena ovih standarda pokazala je da generički standard ne može da zadovolji sve specifične zahteve za bezbednošću informacija u pojedinim oblastima, pa se pristupilo donošenju sektorskih standarda u oblastima kao što su telekomunikacije, elektroprivredni sustemi, računarstvo u oblaku itd. Istovremeno, u nekim granama industrije donošeni su posebni standardi, kako bi se izrazile njihove specifičnosti. Jedna od tih oblasti je automobilska industrija, u kojoj je uspostavljen mehanizam TISAX, kako bi se obezbedilo da isporučioci poštuju zahteve za bezbednošću informacija, posebno kada je reč o informacijama vezanim za prototipove. U ovom radu dat je sažeti prikaz mehanizma TISAX, njegova struktura i sastavni elementi, kao i povezanost sa familijom standarda ISO/IEC 27000.

Ključne reči: *bezbednost informacija, Sistem menadžmenta bezbednošću informacija (ISMS), automobilska industrija, mehanizam TISAX*

1. UVOD

Buran razvoj informacionih tehnologija u poslednjih nekoliko decenija u značajnoj meri olakšao je naš svakodnevni život, kako na profesionalnom tako i na ličnom planu. Istovremeno, suočio nas je sa jednim problemom koji smo i do sada imali, ali on nije bio izražen u tolikoj meri kao što je to danas – problem bezbednosti informacija. Digitalizacija u svim sferama života učinila je informacije dostupnim, a time i ugroženim od različitih oblika zloupotrebe. Problem je prepoznat, a reakcija na njega bilo je uspostavljanje sistema menadžmenta bezbednošću informacija (engl. Information Security Management Systems – ISMS) koji je predmet serije standarda ISO/IEC 27000 ([1]-[3]) koji su zajednički izdali Međunarodna organizacija za standardizaciju (ISO) i Međunarodna elektrotehnička komisija (IEC).

Standardi serije ISO/IEC 27000 orijentisani su na uspostavljanje sistema zaštite osnovnih svojstava informacije koje se najčešće opisuje kroz trijadu CIA - poverljivosti (engl. Confidentiality), da informacija bude na raspolaganju samo onome ko na nju ima pravo integriteta (engl. Integrity), da informacija bude kompletna i tačna, i raspoloživosti (engl. Availability), da informacija bude na raspolaganju kada je potrebna, pod uslovom da pojedinac ili entitet na nju imaju pravo.

Za razliku od drugih menadžment standarda, standardi serije ISO/IEC 27000 ne odgovaraju samo na pitanje ŠTA je potrebno realizovati, već sadrže kontrole koje u priličnoj meri pomažu organizacijama da odgovore na pitanje KAKO to treba realizovati. Ipak, oni su generički standardi tj. razmatraju temu bezbednosti informacija na generalan način. S obzirom na specifičnosti nekih oblasti, izdat je set tzv. „sektorskih“ standarda, sa modifikacijama postojećih i dodavanjem novih kontrola npr. u oblastima telekomunikacija (standard ISO/IEC 27011, identičan sa preporukom ITU-T Rec-X.1051), elektroprivrednih organizacija (ISO/IEC 27019), računarsva u oblaku (ISO/IEC 27017) itd, jer se pokazalo da generički standard ne može u potpunosti da odgovori specifičnostima tih oblasti.

Jedna od oblasti koja ima specifične zahteve za bezbednost informacija je i automobilska industrija. Da bi se te specifičnosti zadovoljile razvijen je poseban mehanizam za ocenjivanje bezbednosti informacija kod isporučilaca i razmenu rezultata, poznat kao TISAX® (engl. Trusted Information Security Assessment Exchange). U radu je na sažet način prikazana

Adresa autora: Radoslav Raković, Inženjerska akademija Srbije, Beograd, Kneza Miloša 9
e-mail: rrakovic@ep-entel.com
Rad primljen: 20.05.2024.
Rad prihvaćen: 29.05.2024.

suština ovog mehanizma, s obzirom da je u priličnoj meri primenjen na svetskom nivou, kao de facto standard u toj grani industrije.

2. ZAŠTO TISAX?

Originalni proizvođač opreme (engl. Original Equipment Manufacturer - OEM) sarađuje sa velikim brojem kompanija, od projektovanja, preko proizvodnje i distribucije svojih vozila. Da bi se saradnja poboljšala, OEM je u situaciji da sa isporučiocima deli poverljive informacije kao što je dizajn prototipa, itd. Ako ti vredni podaci nisu zaštićeni, razmena u lancu snabdevanja može da dovede do gubitaka, manipulacija ili čak krađe poslovnih tajni, što u značajnoj meri može da utiče na poziciju OEM na tržištu, pa čak i da dovede do prestanka rada. U skladu sa tim, OEM želi da osigura da njegovi isporučioci i partneri, uključujući organizacije u segmentu marketinga i prodaje, imaju adekvatan ISMS pre nego što sklope ugovore sa njima.

U nastavku je navedeno nekoliko slučajeva incidenata vezanih za bezbednost informacija u automobilskoj industriji, raspoloživih u literaturi [4]:

- 1993: Rukovodilac prodaje General Motors-a (GM) prešao je u Volkswagen (VW) sa 10.000 dokumenata uključujući strateške planove. Šteta je bila na nivou nekoliko stotina miliona USD.
- 2010: Jedan kineski par kopirao je hiljade dokumenata GM-a o hibridnim vozilima i pokušao da ih prosledi jednom kineskom proizvođaču.
- 2011: Troje zaposlenih u Renault-u odali su informacije konkurenciji o četiri prototipa električnih vozila.
- 2018: Došlo je do curenja osetljivih informacija obima 160 Gbytes vezanih za više proizvođača (100 kompanija, uključujući VW, GM, Toyotu, Teslu) koje su imale jednu malu kanadsku kompaniju kao kooperanta.

Treba imati u vidu da se informacije o incidentima i načinu njihovog nastajanja ne objavljuju često, iz razumljivih razloga, jer to može da utiče na urušavanje reputacije proizvođača.

Prednosti TISAX sertifikacije su sledeće [5], [6]:

- Standardizuje zahteve za bezbednost informacija u automobilskoj industriji koja ima svoje specifičnosti, a posebno u zaštiti informacija u razvoju prototipa, što često može biti predmet industrijske špijunaže.
- Povećava kredibilnost sistema bezbednosti informacija u organizacijama učesnicama.
- Izbegava se često ocenjivanje kao i dupliranje ocenjivanja – rezultati ocenjivanja vrede tri godine i koriste se za sve klijente sa kojima organizacija posluje.
- Obezbeđuje se transparentnost kroz harmonizovani katalog.
- Stavlja se fokus na potrebe i očekivanja OME za koga isporučilac radi.
- Omogućuje se zajedničko prepoznavanje rezultata ocenjivanja.
- Olakšava se obnavljanje postojećih ugovora.
- Podstiče se poverenje u lancu snabdevanja.

3. ISTORIJAT RAZVOJA TISAX I KLJUČNI POJMOVI

Nemačka asocijacija automobilske industrije – VDA (nem. Verband der Automobilindustrie) osnovana je 2000. godine, a njene članice su, između ostalih, kompanije BMW, Mercedes, Volkswagen Audi grupa, Daimler itd. Ova asocijacija uspostavila je 2017. godine svoj standard VDA – ISA (engl. Information Security Assessment), zasnovan na ISO/IEC 27001, a koji od 2018. godine moraju da ispunjavaju svi koji posluju u nemačkoj automobilskoj industriji. Dokaz za to je posedovanje TISAX sertifikata tj. oznake. U suštini, VDE ISA predstavlja odgovor na pitanje „Šta je to bezbedno rukovanje osetljivim informacijama?“, a TISAX oznaka je odgovor na pitanje „Kako možete da dokažete da bezbedno rukujete osetljivim informacijama?“, ukoliko ste isporučilac koji radi ili želi da radi sa nekim proizvođačem automobila. Asocijacija VDA je uspostavila ENX platformu (engl. European Network Exchange) da bi obezbedila podršku razmeni tih informacija. Do kraja 2020, sertifikovalo se preko 2.800 kompanija sa 5.100 lokacija. Dakle, TISAX je počeo kao nemački standard, ali se proširio na Evropu i na ceo svet.

Ključne uloge u mehanizmu TISAX su TISAX učesnici (engl. Participants) i TISAX proveravači (engl. Audit providers).

TISAX učesnik je organizacija koja je, nakon prijavljivanja na ENX platformu, uspešno obavila proces registracije [7]. Učesnici su proizvođači automobila, delova i komponenata, isporučioci sirovina, proizvođači softvera, agencije za oglašavanje, istraživački instituti i drugi učesnici u automobilskoj industriji. Učesnik može biti AKTIVAN I PASIVAN. AKTIVAN UČESNIK je proveravana strana (engl. Auditee) koja nakon uspešno završenog ocenjivanja deli sa drugim učesnicima rezultate ocenjivanja. PASIVNI UČESNIK je učesnik koji koristi rezultate ocenjivanja drugih učesnika. To je po pravilu partner tj. originalni proizvođač – OEM. Uloga učesnika i njegov odnos sa drugim učesnicima regulisani su sporazumom (engl. Participants Agreement). TISAX proveravač je organizacija koja pruža usluge ocenjivanja, akreditovana i ovlašćena od strane ENX za sprovođenje ocenjivanja [7]. U suštini, reč je o istoj ulozi koju ima sertifikaciono

telo u sistemima menadžmenta, jedina razlika je u kriterijumima za sertifikaciju.

Sve organizacije u okviru mehanizma TISAX potpisuju tzv. Ugovor o neotkrivanju (engl. Non-Disclosure Agreement – NDA) kao sporazum kojim se obezbeđuje legalna zaštita informacija organizacije, posebno kada se informacija razmenjuje van njenih granica [7]. Poseban značaj u TISAX mehanizmu ima prototip (engl. Prototype) jer se zaštiti informacija o njemu posvećuje posebna pažnja. U stvari, reč je o ranoj fazi razvoja proizvoda i/ili sistema. U automobilskoj industriji može biti vozilo, komponenta ili deo [8].

Prototip poseduje samo deo karakteristika finalnog proizvoda i/ili sistema, ali one najvažnije koje omogućavaju lakšu komunikaciju između učesnika u razvoju. Dragocen je sa stanovišta sagledavanja dosadašnjih rezultata i utvrđivanja smerova budućih aktivnosti. Zahteva veći ili manji nivo zaštite, o čemu odlučuje vlasnik intelektualne svojine.

U mehanizmu TISAX značajan pojam predstavlja i bezbednosna zona (engl. Security Zone). Odnosi se na oblasti koje su ograničene barijerama i mehanizmima pristupa, kako bi se obezbedila fizička zaštita informacione imovine [8]. Najosetljivija informaciona imovina zahteva posebne mere zaštite. Oblast se mogu odnositi na magacine, garaže, radionice, ispitne staze, istraživačke i razvojne centre, centre za obradu podataka, server sale, itd.

4. TISAX PROCES – TRI KORAKA

U skladu sa priručnikom za TISAX učesnike [9] proces se sastoji od 3 koraka – registracija, ocenjivanje (engl. Assessment) i razmena (engl. Exchange) informacija o rezultatima ocenjivanja.

Registracija se sprovodi „on-line“ sa svrhom da se prikupe informacije o kompaniji učesnici i šta treba da bude predmet ocenjivanja. U toku ovog koraka prikupljaju se kontakt podaci, isporučilac se upoznaje sa TISAX pojmovima i uslovima (engl. Terms and Conditions [7]) i prihvata ih, što je predmet ugovora sa ENX. Pored toga, definiše se obuhvat - cilj ocenjivanja bezbednosti informacija za isporučioca što određuje primenjive zahteve koje ISMS mora da ispuni.

Cilj ocenjivanja zasniva se na tipu podataka kojima organizacija isporučilac rukuje u ime svog partnera. Te ciljeve po pravilu definiše partner za koga se ocenjivanje sprovodi, ili sama organizacija ukoliko ocenjivanje sprovodi sa ciljem da se pred potencijalnim klijentima deklariše kao kredibilan partner. Za sada postoji 8 TISAX ciljeva ocenjivanja, tabela 1 - prva dva su mapirana sa VDA ISA katalogom „bezbednost informacija“ [8], zatim 4 sa katalogom „zaštita prototipa“, a poslednja 2 sa katalogom „zaštita podataka“.

Tabela 1. Ciljevi ocenjivanja

RB	CILJ OCENJIVANJA	SKRAĆENICA
1	Rukovanje informacijama sa visokim zahtevima za zaštitu	IH – Info High
2	Rukovanje informacijama sa veoma visokim zahtevima za zaštitu	IVH – Info Very High
3	Zaštita prototipa, delova i komponenata	PP – Proto Parts
4	Zaštita prototipa vozila	PV – Proto Vehicles
5	Rukovanje probnim vozilima	TV – Test Vehicles
6	Zaštita prototipa tokom događaja i pravljenja filmova i fotografija	PE – Proto Event
7	Zaštita podataka u skladu sa Art. 28 GDPR	D - Data
8	Zaštita podataka iz kategorije posebnih podataka o ličnosti, Art. 9 i 28 GDPR	SD – Special Data

Tabela 2. Nivoi ocenjivanja

Metod ocenjivanja	Nivo AL-1	Nivo AL-2	Nivo AL-3
Samo-ocenjivanje	DA	DA	DA
Dokaz	NE	Provera verodo-stojnosti	Kroz verifikaciju
Intervjui	NE	Web konfe-rencija	Lično, na licu mesta
Inspekcija na licu mesta	NE	Po zahtevu	DA

Na ciljeve ocenjivanja iz tabele 1 primenjuju se nivoi ocenjivanja (engl. *Assessment Level* - AL), Tabela 2, i to AL.2 za ciljeve 1 i 7, a AL.3 za ciljeve 2-6 i 8. Nivoi ocenjivanja imaju sledeće značenje:

- AL.1 je za interne svrhe u pravom smislu reči samoocenjivanja. Proveravač proverava da li je samoocenjivanje sprovedeno, ali se ne bavi njegovim sadržajem. Ovaj nivo nema visok stepen povreenja i ne primenjuje se u mehanizmu TISAX.
- AL.2 proveravač sprovodi proveru verodostojnosti samoocenjivanja za sve lokacije unutar obuhvata ocenjivanja i to podržava dokazima i sprovođenjem intervjua sa osobom koja je zadužena za bezbednost informacija. Obično se intervju radi preko web konferencije, a po zahtevu može i lično. Ako se sprovodi puna provera daljinski to dobija nivo AL.2.5.
- AL.3 proveravač bazira pripremu za ocenjivanje na samoocenjivanju i podnetoj dokumentaciji. On pregleda dokumente i dokaze, vodi intervjue sa vlasnicima procesa, posmatra lokalne uslove i

izvršenje procesa, sprovodi neplanirane intervjue sa učesnicima procesa u pripremi za ocenjivanje.

Ocenjivanje se sprovodi u četiri podkoraka:

- Priprema za ocenjivanje – zavisi od nivoa zrelosti ISMS organizacije. Priprema za zasniva na VDA ISA katalogu [8], a sprovodi se kroz samoocenjivanje.
- Izbor TISAX proveravača, sa liste ovlašćenih organizacija.
- TISAX proveravač sprovodi ocenjivanje u skladu sa zahtevima klijenta, u jednom ili više koraka, zavisno od rezultata. Provera može biti inicijalna, provera plana korektivnih mera ili provera njegovog sprovođenja (engl. Follow Up).
- Rezultati ocenjivanja – formira se izveštaj kad kompanija ispuni sve zahteve, koji je osnov za dobijanje TISAX znaka.

Sam izveštaj ima standardnu strukturu [9] - deo A: Informacije vezane za ocenjivanje, deo B: Sumarni rezultati, deo C: Rezultati po glavama i kriterijumima, deo D: Nivo zrelosti za svaki od zahteva i deo E: Detaljni rezultati ocenjivanja.

U koraku razmene, informacije o rezultatu ocenjivanja dele se sa partnerom. Pošto se izveštaj formira u više nivoa, organizacija sama odlučuje koji nivo će podeliti sa drugima. Rezultat vredi 3 godine, a onda se proces u tri koraka ponavlja.

U slučaju generalne razmene opcije su da se rezultat ne objavljuje, da se objavi samo Deo A, Deo A sa TISAX oznakom ili sa TISAX oznakom i Delom B. Kada je u pitanju poseban učesnik, postoje još tri opcije – zajedničko im je objavljivanje Dela A, TISAX oznake i delova B i C, a tome se mogu dodati i deo D, odnosno delovi D i E.

Treba naglasiti da postoji i poseban dodatak priručniku za učesnike [10] koji se odnosi na situaciju kada učesnik ima veliki broj lokacija sa centralizovanim ISMS. Ta situacija poznata je kao SGA (engl. Simplified Group Assessment) tj. „uprošćeno grupno ocenjivanje“. U tom slučaju, provera se može sprovoditi po principu uzorka S-SGA (engl. Sample-based SGA) ili na principu rotiranja lokacija pri raznim koracima u ocenjivanju R-SGA (engl. Rotation-Schedule-based SGA).

5. VDA ISA KATALOG

Kriterijumi ocenjivanja sadržani su u posebnom dokumentu – VDA ISA katalogu. Aktuelna verzija je verzija 6.0.0 koja je doneta u novembru 2023. godine a primenjuje se od 1.04.2024. godine. Sadrži tri kataloga [8] – katalog „bezbednost informacija“ sa 45 kontrola, koji je zasnovan na kontrolama iz Annexa A standarda ISO/IEC 27001, katalog „zaštita prototipa“ sa 22 kontrole, specifične za prototip i katalog „zaštita podataka“ sa 12 kontrola, baziranih na evropskoj regulativi EU 2016/679, poznatijoj kao GDPR [11].

Prikaz kontrola vezanih za segment zaštite prototipa dat je u tabeli 3.

Tabela 3. Kontrole u katalogu za zaštitu prototipa [8]

Oznaka	Naziv poglavlja u katalogu / Kontrolno pitanje
8.1	Fizička i bezednost okruženja
8.1.1	U kom obimu je raspoloživ koncept bezbednosti koji opisuje minimalne zahteve koji se odnose na fizičku i bezbednost okruženja za zaštitu prototipa?
8.1.2	U kom obimu je prisutna bezbednost perimetra koja sprečava neautorizovani pristup zaštićenim objektima?
8.1.3	U kom obimu je spoljni omotač zaštićene zgrade konstruisan tako da spreči uklanjanje ili otvaranje komponenata spoljnog omotača korišćenjem standardnih alata?
8.1.4	U kom obimu su definisane bezbedne oblasti osigurane od vizuelnog pogleda spolja?
8.1.5	U kom obimu se zaštita od neautorizovanog ulaska reguliše u formi kontrole pristupa?
8.1.6	U kom obimu su prostorije obezbeđene nadzorom protiv upada?
8.1.7	U kom obimu se upravlja pristupom posetilaca?
8.1.8	U kom obimu postoji razdvajanje klijenata u zajedničkom prostoru?
8.2	Organizacioni zahtevi
8.2.1	U kom obimu postoje sporazumi/obaveze o neotkrivanju u skladu sa važećom regulativom?
8.2.2	U kom obimu su zahtevi za podugovarače poznati i koliko su ispunjeni?
8.2.3	U kom obimu zaposleni i članovi tima stvarno učestvuju u obukama i merama za jačanje svesti u vezi sa rukovanjem prototipom?
8.2.4	U kom obimu su bezbednosna klasifikacija projekta i mere koje je prate poznati?
8.2.5	U kom obimu je definisan proces odobravanja pristupa bezbednim oblastima?
8.2.6	U kom obimu postoje regulative pravljenje snimaka (fotografija, filmova) i rukovanje sa njima?
8.2.7	U kom obimu je definisan i uspostavljen postupak unošenja i korišćenja mobilnih uređaja za snimanje u bezbednosnim oblastima?
8.3	Rukovanje vozilima, komponentama i delovima
8.3.1	U kom obimu se transport vozila, komponenata i delova klasifikuje i sprovodi u skladu sa bezbednosnim zahtevima naručioca?

Oznaka	Naziv poglavlja u katalogu / Kontrolno pitanje
8.3.2	U kom obimu je osigurano da se vozila parkiraju / komponente i delovi čuvaju u skladu sa bezbednosnim zahtevima naručioca?
8.4	Zahtevi za probna vozila
8.4.1	U kom obimu su prethodno definisani zahtevi za kamufliranje implementirani od strane članova tima?
8.4.2	U kom obimu su mere za zaštitu odobrenih testova i probnog terena prepoznate i sprovedene?
8.4.3	U kom obimu su zaštitne mere za odobrene testove i probna vozila na javnim putevima prepoznate i sprovedene?
8.5	Zahtevi za događaje i snimanje
8.5.1	U kom obimu su poznati bezbednosni zahtevi za prezentacije i događaje koji uključuju vozila, komponente ili delove?
8.5.2	U kom obimu su poznate zaštitne mere za snimanje filmova ili fotografisanje koje uključuje vozila, komponente ili delove?

Za svaku kontrolu postoje obavezujući („must have“) i opcioni („should have“) zahtevi, zahtevi za normalan nivo + eventualno dodatni zahtevi za visok (high) + veoma visok (very high) nivo zaštite, a definiše se nivo zrelosti (engl. Maturity Levels) na 6-stepenoj skali (0-5), koji se vizuelno prikazuje o obliku SPIDER dijagrama. Nivoi zrelosti imaju sledeće osnovne karakteristike [8]:

0- Nekompletan (engl. Incomplete): Proces ne postoji, ne prati se ili nije pogodan za dostizanje ciljeva. Nema dokaza ili ih je veoma malo.

1- Sproveden (engl. Performed): Proces se prati, ali uopšte nije ili nije dovoljno dokumentovan („neformalan proces“). Osnovne prakse implementirane su na proverljiv način.

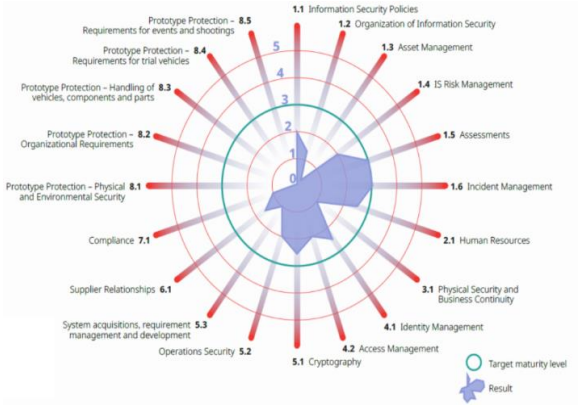
2- Upravljan (engl. Managed): Proces dostizanja ciljeva se prati. Raspoloživa je dokumentacija o procesu i dokazi o njegovoj implementaciji. Upravlja se procesom i proizvodima rada.

3- Uspostavljen (engl. Established): Standardni proces je definisan, integrisan u celinu sistema, prati se i razvija. Zavisnost od drugih procesa je dokumentovana i kreirani su interfejsi. Postoje dokazi da je proces održiv u dužem vremenskom period.

4- Predvidljiv (engl. Predictable): Uspostavljeni proces se prati. Efektivnost procesa se kontinuirano prati prikupljanjem ključnih podataka – merenjem. Definisane su granične vrednosti izvan kojih proces postaje nedovoljno efektivan i zatheva podešavanja (KPI- Key Performance Indicators – ključni inidikatori performansi). Procesom se upravlja na osnovu prikupljenih podataka o njegovom funkcionisanju

5- Optimiziran (engl. Optimizing): Prati se predvidljiv proces sa stalnim poboljšanjima kao glavnim ciljem. Poboljšanja sa aktivno unapređuju pomoću dodeljenih resursa. Proces se stalno inovira i optimizuje.

Primer SPIDER dijagrama po poglavljima VDA ISA kataloga i dostignutim nivoima zrelosti prikazan je na slici 1.



Slika 1 - Primer SPIDER dijagrama po poglavljima VDA ISA kataloga [5]

Treba naglasiti da sertifikacija u sklopu mehanizma TISAX ni na koji način ne obavezuje organizaciju da prethodno sertifikuje svoj ISMS u skladu sa standardom ISO/IEC 27001. Međutim, za organizacije može biti veoma korisno ukoliko su sertifikovale svoj ISMS po navedenom standardu, jer time formiraju dragocenu osnovu koja se onda nadgrađuje u skladu sa zahtevima prema VDA ISA katalogu. Orijentacije radi, implementiran i sertifikovan proces prema ISO/IEC 27001 odgovara nivou zrelosti 4.

6. RAZLIKE ISO/IEC 27001 I TISAX

Iz svega iznetog jasno je da između standarda ISO/IEC 27001 i mehanizma TISAX postoje mnoge sličnosti, ali i neke veoma bitne razlike. Razlike su sumirane u Tabeli 4.

Tabela 4. Razlike ISO/IEC 27001 i TISAX

ISO/IEC 27001	TISAX
Zahtevi su prezentovani na generalan način, omogućuju implementaciju ISMS u svim organizacijama, postoji 10 glava standarda (po Annex SL)	Zahtevi su prezentovani u formi kataloga pitanja sa tri domena – bezbenost informacija (45), zaštita prototipa (22) i zaštita podataka (12)
Sastavni deo standarda je Annex A sa kontrolama ali taj katalog nije zatvoren, organizacija može da implementira i dodatne kontrole u skladu sa ocenjivanjem rizika, ako proceni da bi to doprinelo efektivnosti ISMS	Bavi se zaštitom prototipa što nije obuhvaćeno standardom ISO/IEC 27001 (fizička i bezbednost okruženja, vozilo, komponente i delovi, zahtevi za testiranje vozila)

ISO/IEC 27001	TISAX
Ocena usaglašenosti sprovodi se kroz izjavu „usaglašeno / nije usaglašeno“, bez utvrđivanja nivoa usaglašenosti ili stepena efektivnosti sistema BI	Usklađenost i efektivnost definisana je 6-stepenom skalom zrelosti, od 0 (najniži) do 5 (najviši)
Informacije se klasifikuju u skladu sa zakonskim zahtevima, vrednošću, kritičnošću i osetljivošću na neautorizovano otkrivanje ili modifikovanje	Klasifikacija informacija sprovodi se prema definisanim kriterijumima tj. vrednošću, zakonskim zahtevima, poverljivošću, integritetom i raspoloživošću
Mora se razviti set procedura za označavanje i rukovanje informacijama i implementirati ih u skladu sa šemom klasifikacije koju je usvojila organizacija	Uspostavljena je i sprovedena konzistentna šema za klasifikovanje dokumenata / informacija

Glavne razlike ISO/IEC 27001 i TISAX su [5]:

- Provera se u slučaju standarda ISO/IEC 27001 obavlja svake godine, u trogodišnjim ciklusima sa po dve godišnje nadzorne provere (engl. Surveillance Audits). U slučaju mehanizma TISAX ocenjivanje se sprovodi svake 3 godine.
- U slučaju standarda ISO/IEC 27001 dokaz je sertifikat, a kod TISAX mehanizma dokaz je elektronska oznaka na ENX platfomi.
- Standard ISO/IEC 27001 je međunarodno priznat, a mehanizam TISAX važi samo u automobilskoj industriji.
- U slučaju standarda ISO/IEC 27001 moraju se otkloniti velike neusaglašenosti pre izdavanja sertifikata, a provera postupanja po malim neusaglašenostima po pravilu se obavlja kroz nadzorne provere. U mehanizmu TISAX moraju se otkloniti i velike i male neusaglašenosti pre izdavanja oznake, što TISAX proveravač proveri kroz proveru plana korektivnih mera i njegovog sprovođenja. U tom smislu, deluje da je mehanizam TISAX restriktivniji od sertifikacionog procesa u slučaju standarda ISO/IEC 27001.

7. ZAKLJUČAK

U radu je napravljen sažeti prikaz mehanizma TISAX kao specifičnog standarda za obezbeđivanje zaštite informacija u automobilskoj industriji kako bi informacije koje proizvođač razmenjuje sa isporučiocima bile adekvatno zaštićene. Ukazano je da ovaj mehanizam nije u suprotnosti sa zahtevima standarda ISO/IEC 27001, da se dobrim delom na njega oslanja, ali da posebnu pažnju poklanja zaštiti informacija vezanim za prototip, s obzirom da narušavanje bezbednosti informacija u tom segmentu može imati nesagledive posledice po proizvođača i njegovu poziciju na tržištu.

LITERATURA

[1] ISO 27000:2018 Information technology - Security techniques - Information security management systems - Overview and vocabulary (ISO, 2018)

[2] ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements (ISO, 2022)

[3] ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls (ISO, 2022)

[4] Krolikowski T, Ubowska A, TISAX – optimization of IOT risk management in the automotive industry, *25th International Conference on Knowledge-based and Intelligent Information & Engineering Systems*, 2021 – Procedia Computer Science 192, 4259-4268, 2021.

[5] TISAX Assessment Technical Guide (DEKRA, 2022)

[6] Introducing TISAX (BSI, 2022)

[7] TISAX Participation General Terms and Conditions - GTC, Ver. 3-.0.1, jul 2018

[8] VDA ISA Catalogue, Ver. 6.0.0 (November 2023) https://www.dekra.com/en/vda-information-security-assessment-isa-catalog-version-6/

[9] TISAX Participant Handbook, ver 2.5.1 (mart 2023) https://www.enx.com/handbook/tisax-participant-handbook.html

[10] TISAX Simplified Group Assessment – An addendum to teh TISAX Participant Handbook fot TISAX particiants with many locations and a centralised and highly developed ISMS, 1.1 (ENX-TISAX, 2023)

[11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data - General Data Protection Regulation, OJEU, L 119/1 to 88, 2016.

SUMMARY

INFORMATION SECURITY IN AUTOMOTIVE INDUSTRY – MECHANISM TISAX

With the development of information technologies and their application in all spheres of activity, information security has become an actual problem. A significant step towards solving that problem was the adoption of the ISO/IEC 27000 family of standards for information security management systems (ISMS). The practical application of these standards showed that the generic standard cannot satisfy all specific requirements for information security in certain areas, so the adoption of sector standards in areas such as telecommunications, electric power systems, cloud computing, etc. At the same time, in some branches of industry, special standards were adopted to express their specificities. One of those areas is the automotive industry, where the TISAX mechanism has been established to ensure that suppliers comply with information security requirements, especially when it comes to information related to prototypes. This paper provides a summary of the TISAX mechanism, its structure and constituent elements, as well as its relationship with the ISO/IEC 27000 family of standards.

Key Words: *Information Security, Information security management system (ISMS), Automotive Industry, Mechanism TISAX*