Analiza sigurnosnih rizika prijevoza lijekova

Bibić, Martina

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

Analiza sigurnosnih rizika prijevoza lijekova

Safety Risks Analysis of Drug Transport

Mentor: doc. Dr. sc. Pero Škorput

Student: Martina Bibić

JMBAG: 0067292685

Zagreb, rujan 2024.

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 20. lipnja 2024.

Zavod: **Zavod za inteligentne transportne sustave**
Predmet: **Inteligentni transportni sustavi I**

DIPLOMSKI ZADATAK br. 7741

Pristupnik: **Martina Bibić (0067292685)**
Studij: Inteligentni transportni sustavi i logistika
Smjer: Logistika

Zadatak: **Analiza sigurnosnih rizika prijevoza lijekova**

Opis zadatka:

Svaka imovina, bila materijalna ili nematerijalna, ima određenu vrijednost, sklona je ranjivosti i prijetnjama. Ukoliko se prijetnje ostvare, logističko poduzeće trpi određene posljedice. Analiza sigurnosnih rizika nužan je preduvjet za umanjivanje rizika i smanjivanja nastanka štetnog događaja, odnosno prevencija pojava štetnog događaja tijekom prijevoza lijekova. U ovom diplomskom radu potrebno je analizirati sigurnosne rizike prijevoza lijekova te istražiti i definirati parametre rizika, odnosno parametre uzroka potencijalne ugroze sigurnosti. U diplomskom radu potrebno je opisati specifičnosti opskrbnog lanca i distribucije lijekova te opisati metodološku podlogu analize sigurnosnih rizika. Također, potrebno je analizirati sigurnosne ugroze prijevoza lijekova te mjere unaprjeđenja sigurnosti prijevoza.

Mentor:

izv. prof. dr. sc. Pero Škorput

mr. sc. Krešimir Veselko (komentor)

Predsjednik povjerenstva za diplomski ispit:

SAŽETAK

Distribucija lijekova predstavlja ključnu komponentu u lancu opskrbe zdravstvenog sektora. Zbog specifičnih zahtjeva koji se odnose na skladištenje i transport farmaceutskih proizvoda, kao i zbog stroge regulative koja prati ovu djelatnost, iznimno je važno osigurati visoku razinu sigurnosti u svim fazama transporta. Ovaj rad detaljno se bavi identifikacijom, analizom i procjenom sigurnosnih rizika koji mogu nastati tokom transporta i skladištenja lijekova s posebnim naglaskom na primjenu FMEA analize (Failure Mode and Effects Analysis) za identifikaciju mogućih grešaka i njihovih posljedica. Tri ključne analize koje se provode u radu uključuju: analizu transportnih ruta, analizu skladištenja i analizu kontrole pristupa i sigurnosti u pretovarnom skladištu. U analizi transportnih ruta, naglasak je stavljen na tehničku ispravnost vozila, održavanje temperaturnih uvjeta i utvrđivanje potencijalnih prepreka tijekom prijevoza. Analiza skladištenja se bavi uvjetima skladištenja, poput kontrole temperature i sigurnosti lijekova, dok analiza kontrole pristupa ispituje sigurnosne mjere i procedure unutar pretovarnih skladišta. Sve analize koriste FMEA metodologiju za izračun broja prioriteta rizika i omogućuju rangiranje rizika prema njihovoj ozbiljnosti. Predložene su strategije za smanjenje rizika, uključujući primjenu naprednih tehnologija kao što su GPS, RFID, IoT senzori i Geofencing, čime se omogućava precizno praćenje i upravljanje sigurnosinm rizikom. Naglašava se potreba za kontinuiranim nadzorom i prilagođavanjem sigurnosnih mjera, kako bi se osigurala kvaliteta lijekova i zaštitilo zdravlje pacijenata.

KLJUČNE RIJEČI: transport lijekova; procjena rizika; resursi; neželjeni događaj; FMEA analiza, analiza sigurnosnih rizika

SUMMARY

Medical products distribution is a key component in the healthcare supply chain. Due to the specific requirements relating to the storage and transport of pharmaceutical products, as well as the strict regulations accompanying this activity, it is extremely important to ensure a high level of safety at all stages of transport. This paper-work deals in detail with the identification, analysis and evaluation of safety risks that may arise during the transport and storage of medicinal products with special emphasis on the application of FMEA analysis (failure mode and effects analysis) for the identification of possible errors and their consequences. Three key analyses carried out in the paper-work include: transport route analysis, storage analysis and access control and security analysis in the crossdock warehouse. In the analysis of transport routes, emphasis was placed on technical roadworthiness of vehicles, maintenance of temperature conditions and identification of potential obstacles during transport. Storage analysis deals with storage conditions, such as temperature control and safety of medicines, while access control analysis examines security measures and procedures within transhipment warehouses. All analyses use the FMEA methodology to calculate the number of risk priorities and allow the ranking of risks according to their severity. Risk mitigation strategies have been proposed, including the use of advanced technologies such as GPS, RFID, IoT sensors and geofencing, allowing accurate monitoring and management of safety risk. It pointing-out the need for continuous monitoring and adaptation of safety measures to ensure the high quality of medicines and to protect patients health.

KEYWORDS: drug transport; risk assessment; resources; unwanted event; FMEA analysis, safety risk analysis

SADRŽAJ

1. UVOD

Analiza procjene rizika je osnova za upravljanje sigurnošću u čitavom lancu opskrbe farmaceutskim proizvodima. Ranije razumijevanje mjera sigurnosti i zaštite zdravlja kroz dugi niz godina temeljilo se na načelu pridržavanja zakonskih propisa. Međutim, raznolikost radnih aktivnosti, osobitost svakog radnog mjesta te poslovanja ne mogu se u potpunosti obuhvatiti i tretirati zakonskim odrednicama ma kako ih široko tumačili. Pristup koji se temelji na otkrivanju onoga što je već prošlo po zlu, ili što nije u skladu sa zakonskim odrednicama, ne može predvidjeti što se sve može dogoditi niti može spriječiti nastanak štetnog, neželjenog događaja. Analiza rizika omogućuje prepoznavanje svih opasnosti koje mogu naškoditi poslovanju, proizvodima i radnicima te uzrokovati neželjene posljedice tj događaje. Zato analiza rizika omogućuje procjenjivanje ozbiljnosti tih posljedica i pronalaženje najprikladnijih rješenja za zaštitu od njih. Prevencija je vodeće načelo analize procjene rizika.

Kroz drugo poglavlje ovog diplomskog rada opisuje se proces distribucije lijekova, od njihove proizvodnje u farmaceutskim tvornicama, preko skladištenja u centraliziranim skladištima, do njihovog transporta i dostave krajnjim korisnicima. Naglašava se važnost svakog segmenta u distribuciji i povezane sigurnosne mjere koje su ključne za očuvanje farmaceutskih proizvoda.

Kroz sljedeća tri poglavlja ovog diplomskog rada utvrđuje se pojam rizika i podjela rizika na osnovne i dopunske. Opisuje sustav upravljanja kakvoćom prijevoza lijekova za uspostavu sustava kakvoće koji uključuje načela upravljanja rizicima, kako bi se osigurala kvaliteta lijekova i cjelovitost distribucijskog lanca. Kako bi se uspostavio sustav kakvoće definiran je proces upravljanje rizicima koji smanjuju nepovoljne situacije i posljedice, a ključni koraci uključuju utvrđivanje, procjenu, postupanje i praćenje rizika.

U šestom poglavlju ovog diplomskog rada prikazan je postupak proces procjene rizika koji je ključni proces u upravljanju sigurnosnim rizicima. Proces obuhvaća devet koraka, uključujući identifikaciju resursa, prijetnji i ranjivosti, analizu postojećih kontrola, određivanje vjerojatnosti i posljedica prijetnji, preporuke za kontrolu umanjivanja rizika te izrade dokumentacije kao osiguranje da svi rezultati i preporuke budu zabilježeni i dostupni.

Kroz sedmo poglavlje diplomskog rada detaljno su opisani podaci prikupljeni iz tri ključne analize sigurnosnih rizika u logističkom lancu distribucije lijekova. To su analiza transportnih ruta, analiza skladištenja u Osijeku, te analiza kontrole pristupa i sigurnosti u pretovarnom

skladištu. Svaka od ovih analiza koristi metodologiju FMEA (Failure Mode and Effects Analysis). Rad također analizira kako se rezultati ovih analiza putem FMEA metodom mogu koristiti za unapređenje postojećih sigurnosnih procedura.

Osmo poglavlje ovog diplomskog rada pruža sveobuhvatnu diskusiju o rezultatima iz analiza iz prethodnog poglavlja. Naglašava se važnost kontinuiranog nadzora i adaptacije sigurnosnih mjera u skladu s novim izazovima i tehnologijama prikazano grafikonom koji uspoređuje ocjene rizika za analiza transportnih ruta, analiza skladištenja u Osijeku, te analiza kontrole pristupa i sigurnosti u pretovarnom skladištu.

Kroz deveto poglavlje ovog diplomskog rada opisuju se strategije za smanjenje rizika i osiguravanja proizvoda kroz sigurnosti u distribuciji i logističkim procesima. Navedene mjere su ključne za smanjenje rizika, osobito u transportu i skladištenju lijekova. Opis i definicija naprednih tehnologija poput RFID-a, IoT senzora, GPS-a i Geofencing-a prikazuje kako se može značajno poboljšati praćenje i kontrola logističkih operacija. Isto tako korištenje integriranih sustava upravljanja rizicima i KPI-ova omogućuje centralizirano praćenje i poboljšanje učinkovitosti, dok poboljšana komunikacija, obuka zaposlenika i suradnja unutar organizacije doprinose sigurnosti i operativnoj uspješnosti.

2. OPSKRBNI LANAC DISTRIBUCIJE LIJEKOVA

Distribucija lijekova u farmaceutskoj industriji ključan je proces, koji zahtijeva strogu i zakonsku regulaciju, koordinaciju i logističke strategije kako bi se osiguralo da lijekovi stignu do pacijenata u optimalnom stanju. Proces distribucije lijekova obuhvaća cijeli niz aktivnosti koje počinju nakon proizvodnje lijeka i završavaju njegovim dolaskom do krajnjeg korisnika, bilo da je to ljekarna, bolnica ili sam pacijent. Svaki korak u lancu distribucije mora biti pažljivo planiran i kontroliran kako bi se očuvala kvaliteta i sigurnost lijekova.

Proces započinje u tvornicama, gdje se lijekovi proizvode pod strogim uvjetima kako bi se osigurala njihova učinkovitost i sigurnost. Nakon proizvodnje, lijekovi prolaze kroz fazu kontrole kvalitete, gdje se provjerava jesu li ispunili sve regulatorne zahtjeve i standarde te se pohranjuju se u centralizirana skladišta. Ova skladišta su obično smještena u blizini glavnih prometnih čvorišta i opremljena su naprednim sustavima za kontrolu temperature, vlažnosti i svjetlosti kako bi se očuvala stabilnost lijekova. Skladišta moraju biti u skladu s regulativama koje propisuju optimalne uvjete skladištenja za različite vrste lijekova. Nakon što su lijekovi pohranjeni u centraliziranim skladištima, slijedi faza transporta prema regionalnim skladištima ili distributivnim centrima. Ovaj transport može uključivati različite metode, poput cestovnog, zračnog ili pomorskog prijevoza, ovisno o udaljenosti i hitnosti isporuke. Za lijekove koji su osjetljivi na promjene temperature, koristi se hladni lanac, specijalizirani sustav transporta koji osigurava da lijekovi ostanu unutar propisanog temperaturnog raspona tijekom cijelog puta.

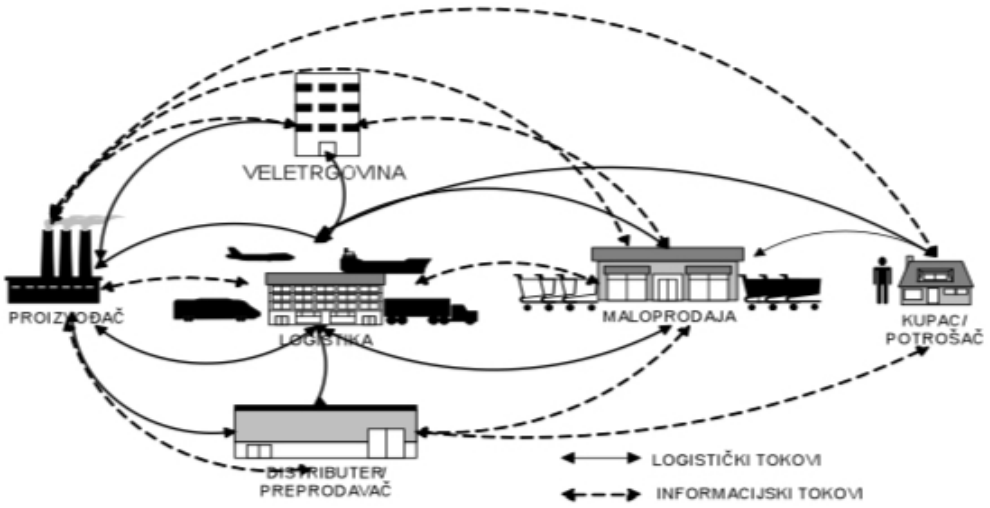
Lijekovi moraju biti transportirani na način:

- da se ne izgubi njihova kvaliteta i identifikacija,
- da se izbjegne kontaminacija
- da su poduzete odgovarajuće mjere za sprječavanje oštećenja, rasipanja, loma ili krađe
- da su zaštićeni od nepovoljnih utjecaja topline, hladnoće, svjetla, vlage i sl.,
- da su zaštićeni od mikroorganizama ili štetočina,
- da se poštuju temperaturni uvjeti koje je propisao proizvođač ili su navedeni na vanjskom pakiranju i koji se u tijeku transporta moraju pratiti umjerenom opremom.[1]

Tijekom transporta, praćenje pošiljki u stvarnom vremenu postaje ključno. Korištenje napredne tehnologije, poput RFID (radiofrekvencijska identifikacija) i GPS sustava, omogućuje

praćenje lokacije, temperature i stanja pošiljke u svakom trenutku. Ovo praćenje osigurava da se bilo kakve nepravilnosti ili problemi mogu odmah uočiti i riješiti prije nego što se pošiljka dostavi krajnjem korisniku. Kad lijekovi stignu u regionalna skladišta ili distributivne centre, oni se dalje raspodjeljuju prema lokalnim potrebama. Distributeri igraju ključnu ulogu u ovoj fazi, osiguravajući da lijekovi stignu do ljekarni i bolnica u skladu s narudžbama i regulativnim zahtjevima.

Sve faze distribucije lijekova podložne su strogim regulativama, koje propisuju uvjete skladištenja, transporta i rukovanja lijekovima. Nacionalne i međunarodne agencije, poput Hrvatske agencije za lijekove i medicinske proizvode (HALMED) ili Europske agencije za lijekove (EMA), redovito provode inspekcije i nadzor. Distribucija lijekova suočava se i s nizom izazova, uključujući logističke probleme poput kašnjenja u isporuci, prekida u hladnom lancu ili nepredviđenih okolnosti kao što su prirodne katastrofe. Krađe i falsifikati također predstavljaju značajan rizik, s obzirom na visoku vrijednost lijekova. Zbog toga se u distribuciji lijekova primjenjuju visoke sigurnosne mjere, poput GPS praćenja, sigurnosnih pečata i specijaliziranih transportnih ruta i sl. Kako bi se suočila s ovim izazovima, farmaceutska industrija sve više koristi tehnološka rješenja koja poboljšavaju učinkovitost i sigurnost distribucije. Automatizacija, umjetna inteligencija i napredni softverski sustavi omogućuju optimizaciju skladištenja, planiranje transportnih ruta i predviđanje potreba za zalihama, čime se smanjuje rizik od grešaka i povećava pouzdanost.



Slika 1. Logistički i informacijski tokovi; izvor [3]

3. SUSTAV UPRAVLJANJA KAKVOĆOM PRIJEVOZA LIJEKOVA

Svi sudionici u distribuciji lijekova obvezni su uspostaviti sustav kakvoće koji uključuje načela upravljanja rizicima kakvoće s jasno definiranim i u cijelosti dokumentiranim odgovornostima, postupcima i mjerama upravljanja rizicima za aktivnosti koje obavljaju, s aktivnim učešćem rukovodećeg osoblja kao i radnika pratećih službi, u cilju osiguranja kakvoće lijekova i cjelovitosti lanca u prometu lijekova.

Sustav upravljanja kakvoćom obuhvaća:

- sustav kakvoće,
- upravljanje ugovorenim radom za aktivnosti kupovine, nabave, čuvanja, opskrbe ili izvoza,
- redovite preglede i nadzor sustava kakvoće,
- upravljanje rizicima.[1]

Rizični događaj ima veličinu i vjerojatnost pojave na nekom području u određenom razdoblju te u svakoj aktivnosti suočeni smo s mogućnošću da se nađemo u ne baš poželjnoj situaciji koja se može i ne mora ostvariti, a nije ju uvijek lako prepoznati ili predvidjeti. Upravo taj efekt neizvjesnosti za određeni cilj naziva se **rizik** [2]. Termin rizik je vrlo široke upotrebe koja zavisi od osobne percepcije pojma rizika i promatranog konteksta. Najčešće pojam rizika označava vjerojatnost pogreške i nastanka štetnog događaja za određenu aktivnost, projekt ili investiciju, dok u širem smislu označava i pojam opasnosti od štetnog događaja.

Slika 2. Stop; izvor: [5]

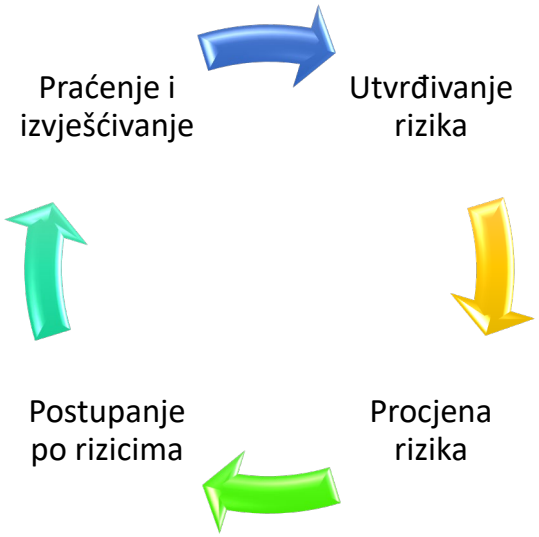
4. UPRAVLJANJE TRANSPORTNIM RIZICIMA

Upravljanje transportnim rizicima čini skup procesa koji se provode sa svrhom povećanja vjerojatnost da će se u slučaju pojave prijetnji, otkloniti ili umanjiti nepovoljne situacije i njihove posljedice. Neki od ciljeva procesa upravljanja rizikom mogu biti maksimiziranje vrijednosti tvrtke, očuvanje poslovne funkcije i egzistencije tvrtke nakon nastanka štete, usklađenost sa zakonskim propisima, minimiziranje neizvjesnosti vezanih za veće katastrofe i rizike. Svi rizici kojima je neki poslovni sustav izložen ne mogu se prepoznati niti u potpunosti otkloniti ali se pronalaženjem razumnog odnosa između različitih aspekata opasnosti, mogućih posljedica i mjera za kontrolu i smanjenje mogu svesti na prihvatljivu razinu.

Transportni rizik predstavlja sumu mogućih neželjenih događaja i šteta koji mogu nastati pri prijevozu, odnosno transportu. Opasnosti koje se mogu dogoditi na transportnom putu od mjesta polazišta do mjesta odredišta i koje mogu izazvati djelomičnu ili potpunu štetu ili neželjeni događaj. Potrebno je obratiti posebnu pažnju na transportne rizike jer roba na transportnom putu je izvan nadzora svih sudionika.

Proces upravljanja rizicima je ciklus koji sadrži korake:

- Utvrđivanje rizika,
- Procjena rizika
- Postupanje po rizicima
- Praćenje i izvještavanje o upravljanju rizicima [4]

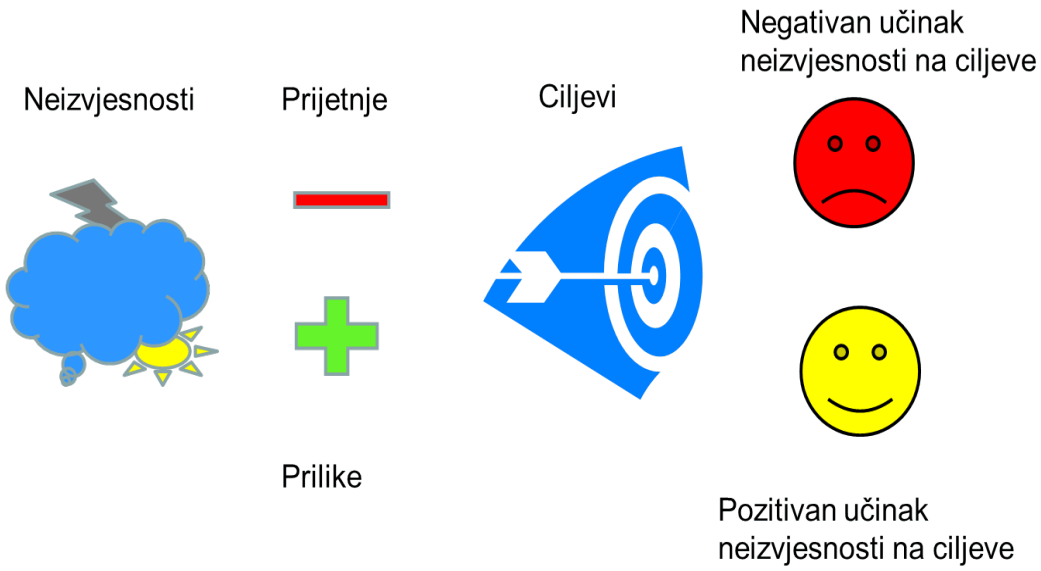


Slika 3. Ciklus upravljanja rizicima; izvor: [4]

5. UTVRĐIVANJE RIZIKA

Utvrđivanje rizika može se utvrditi na razini određenog cilja i načina ostvarenja. Jedno od osnovnih pitanja koje trebamo postaviti pri utvrđivanju rizika je: Kako možemo ostvariti zadani cilj, odnosno zašto se određeni cilj ne bi mogao ostvariti i koje bi bile prepreke za ostvarenje istog?

Rizike promatramo kao učinak, rezultat koji može imati neizvjesnost na naše ciljeve. Postoje razni događaji koji mogu negativno utjecati na naše ciljeve, ali nemaju svi jednaku važnost. Stoga je potrebno utvrditi one rizike koji su nam značajni u odnosu na zacrtane ciljeve. Potrebno je napomenuti da učinak neizvjesnosti na ciljeve može biti i pozitivan i negativan. Iako je uvriježeno sagledavati rizike u okviru negativnih učinaka (prijetnje), potrebno je razmatrati rizike i u smislu pozitivnih učinaka kao prilike koje možemo iskoristiti.



Slika 4. Pozitivan i negativ učinak na ciljeve;
izvor: [5]

Postoji više načina kategorizacije rizika a mogu biti specifični za pojedinu branšu na koju se odnose. Ponekad su kategorije određene regulatornim, zakonskim ili zahtjevima industrije, a nerijetko su prilagođene prema potrebi.

Transportni rizici mogu se podijeliti u dvije osnovne grupe:

- osnovni rizici

- dopunski rizici. [6]

5.1. OSNOVNI RIZICI

Osnovni rizici su oni rizici a koji su svojstveni prijevozu robe, a to su:

- prometne nezgode (sudar prijevoznih sredstava, prevrnuće, nasukavanje, potonuće, iskliznuće, rušenje, pad letjelica i sl.),
- elementarne nepogode (oluja, snježna lavine, poplavi, potresi i sl.),
- požar,
- eksplozija osiguranog predmeta npr. nekog opasnog tereta na brodu,
- razbojništvo (oduzimanje tuđe imovine upotrebom sile protiv neke osobe ili samo prijetnje silom, u namjeri protupravnog prisvajanja te imovine (piratstvo).

Slika 5.; izvor: [7]

5.2. DOPUNSKI RIZICI

Dopunski rizici su rizici opasnosti kojima je podložna roba za vrijeme distribucije, ali te opasnosti, za razliku od osnovnih rizika, nisu svojstvene prijevoznom pothvatu nego ovise o nizu drugih okolnosti, prije svega o svojstvima same robe.

Dopunske rizike je moguće podijeliti na:

- krađa i neisporuka,
- manipulativni rizici (rizici kojima je izložena roba za vrijeme rukovanja, s jednog prijevoznog sredstva na drugo i sl., npr. lom robe, oštećenje ambalaže).
- ostali dopunski rizici – u ove rizike ubrajaju se oni dopunski rizici kojima je zajedničko da je nastanak štete vezan za svojstvo same robe a njezin uzrok potječe izvana. Npr.: pokisnuće, dodir s drugom robom ili predmetom, hrđa, vlaga.

6. PROCJENA RIZIKA

Procjena rizika je proces upravljanja sigurnosnim rizikom a koji uključuje identifikaciju, analizu i uklanjanje rizika. Uključuje i periodičko ispitivanje te dokumentaciju. Organizacije koriste proces procjene rizika da odrede veličinu potencijalnih prijetnji i da rizik uklope u svoj sustav. Analiza svih ranjivosti i prijetnji, vjerojatnost realizacije rizika i moguće posljedice kao i analiza troškova/koristi uključeni su u ovaj proces. Rezultati provedenog postupka procjene rizika daju se na uvid menadžmentu organizacije, kao i podaci koji su neophodni za donošenje odluka vezanih uz ulaganje u sigurnosna rješenja i proizvodnje. Na temelju tih podataka organizacije odlučuje o tehnikama upravljanja rizikom.

Proces procjene rizika je vrlo složen i ključan je proces u mnogim organizacijama te kao takav može utjecati na poslovanje kao što je bolja sigurnost, manji gubici te povećana učinkovitost.

Proces procjene rizika sastoji se od devet koraka:

- ✓ Korak 1: Sustavna identifikacija i klasifikacija;
- ✓ Korak 2: Identifikacija prijetnji;
- ✓ Korak 3: Identifikacija ranjivosti;
- ✓ Korak 4: Analiza postojećih kontrola;
- ✓ Korak 5: Vjerojatnosti pojave neželjenih događaja;
- ✓ Korak 6: Analiza posljedica;
- ✓ Korak 7: Određivanje rizika;
- ✓ Korak 8: Preporuka kontrola za umanjivanje rizika;
- ✓ Korak 9: Dokumentacija. [8]

Slika 6.; izvor: [9]

6.1. IDENTIFIKACIJA RESURSA

Identifikacija resursa temeljni i prvi korak u procesu procjene rizika, posebno u složenim operacijama logističkih poduzeća. Detaljna identifikacija, procjena i klasifikacija resursa omogućuje poduzećima bolju i kvalitetniju zaštitu. Ovaj korak postavlja osnovu za daljnju analizu rizika i donošenje odluka o sigurnosnim mjerama i strategijama upravljanja rizicima. Resursi predstavljaju sve vrijednosti u organizaciji koje su ključne za njeno poslovanje. To mogu biti fizičke stvari kao što su zgrade i oprema, ili nematerijalne stvari kao što su podaci i intelektualno vlasništvo.

Za kvalitetno utvrđivanje resursa, potrebno je postaviti pitanja kao što su:

- Što je kritično za poslovanje?
- Koliki je potencijalni utjecaj gubitka?
- Stupanj prioriteta zaštite?

Identifikacija resursa u logističkim poduzećima uključuje:

- Fizičke resurse (skladišta, transportna sredstva, oprema),
- Informacijske resurse (IT sustavi, baze podataka, intelektualno vlasništvo),
- Ljudske resurse (operativno osoblje, menadžment, specijalisti),
- Financijske resurse (financijski planovi, investicije, osiguranje).

Slika 7.; izvor: [10]

Kako bi imalo što bolju analizu rizika, logističko poduzeće nakon identifikacije resursa provodi procjenu resursa, odnosno njihovu vrijednost.

Procjenu vrijednosti resursa možemo provesti kroz metode:

- Financijska procjena (tržišna vrijednosti resursa, procjena troškova zamjene ili obnove resursa),
- Poslovna kritičnost (ocjenjivanje resursa prema njihovoj važnosti za poslovne procese, identifikacija resursa čiji gubitak bi imao značajan utjecaj na poslovanje),
- Osjetljivost podataka (procjena osjetljivosti informacija, klasifikacija podataka prema povjerljivosti).

Identifikacija i procjena resursa je osnova za daljnju analizu rizika te kada jednom resurse identificiramo i procijenjenimo, mogu se klasificirati i prema riziku. Takva klasifikacija rizika samo je uvod u analizu rizika koja predstavlja detaljan i vrlo važan proces za bilo koje poduzeće kako bi izbjegli nepoželjne događaje. Klasifikacija resursa prema razini osjetljivosti rizika su kritični resursi, visoko osjetljivi resursi i manje osjetljivi resursi.

6.2. IDENTIFIKACIJA PRIJETNJI

Identifikacija prijetnji ključan je korak u procesu upravljanja rizicima jer omogućuje organizacijama da razumiju i predvide moguće izazove s kojima se mogu suočiti, odnosno da prepoznaju i identificiraju sve prijetnje koje bi mogle negativno utjecati na poslovanje.

U logističkim poduzećima gdje je fokus na učinkovitoj i točnoj isporuci te skladištenju robe, praćenje i prilagodba sigurnosnih mjera osiguravaju da organizacija ostane korak ispred prijetnji u poslovanju. Identifikaciju prijetnji potrebno je kontinuirano provoditi kako ne bi dolazilo do neželjenih događaja.

Prijetnje su sve potencijalne ili stvarne okolnosti ili događaji koji mogu uzrokovati štetu informacijskim sustavima, resursima ili operacijama poduzeća. Prijetnje mogu biti namjerne (npr. hakerski napadi) ili nenamjerne (npr. prirodne katastrofe). Identificiranje prijetnji definiramo na temelju određenih metoda i tehnika, a to su:

- Analiza prošlih incidenata,
- Intervjui i radionice sa zaposlenicima,
- Analiza sektora i industrije,

- SWOT (snage, slabosti, prilike, prijetnje) analiza**,**
- Scenario analiza**,**
- Praćenje medija i društvenih mreža**,**
- Suradnja s vanjskim stručnjacima**.**

Klasifikacija prijetnji može se podijeliti u nekoliko kategorija:

- Fizičke prijetnje (događaji koji fizički ugrožavaju resurse ili osoblje),
- Tehničke prijetnje (događaji povezani s tehničkim problemima ili kvarovima),
- Organizacijske prijetnje (interni faktori koji mogu utjecati na poslovanje),
- Ljudske prijetnje (čovjekove akcije koje mogu ugroziti poslovanje),
- Eksterne prijetnje (prijetnje koje dolaze izvan organizacije)

Prilikom identifikacije prijetnji, važno je procijeniti njihovu vjerojatnost i potencijalni utjecaj na organizaciju.

Procjena prijetnji možemo definirati kroz nekoliko koraka:

- Vjerojatnost - koliko je vjerojatno da će se svaka prijetnja realizirati s pomoću ranijih podataka,
- Utjecaj – koji je potencijalni utjecaj prijetnje na poslovanje, utjecaj na reputaciju, financije i drugu poslovanje,
- Prioritet – potrebno je klasificirati prijetnje prema njihovoj vjerojatnosti i utjecaju, koja prijetnja predstavlja najveći rizik,
- Izrada matrice rizika **–** koristi se matricu rizika kako bi i vizualno dobili prikaz prijetnje prema njihovoj vjerojatnosti i utjecaju.

6.3. IDENTIFIKAIJA RANJIVOSTI

Identifikacija ranjivosti je analiza slabih točaka u logističkim poduzećima. Ovaj korak uključuje prepoznavanje slabosti i nedostataka u sustavima, procesima ili strukturama koje prijetnje mogu iskoristiti. Ranjivosti su slabosti koje napadači ili negativni događaji mogu iskoristiti. One su potencijalne "rupe" u obrambenom sustavu organizacije koje mogu dovesti do kompromitacije podataka, operativnih smetnji ili gubitka resursa. Identifikacija ranjivosti je važna, jer omogućuje organizacijama da prepoznaju i adresiraju slabosti koje prijetnje mogu iskoristiti. Mogu prepoznati ranjivosti te unaprijed spriječiti neželjeni događaj te rješavanjem

ranjivosti smanjiti rizik. Identificiranjem ranjivosti može se poboljšati sigurnosne mjere i politike organizacije, logističkog poduzeća, te time se održava usklađenost s relevantnim zakonima i standardima.

Ranjivosti možemo klasificirati u nekoliko glavnih kategorija:

- Tehničke ranjivosti (ranjivosti softvera**,** mreže ili neki hardverski propust),
- Organizacijske ranjivosti (loše upravljanje, obuka zaposlenika, nedostatak resursa),
- Fizičke ranjivosti **(**sigurnosni propusti u prostorije poduzeća, nedostatak nadzora),
- Ljudske ranjivosti **(**ljudske pogreške**,** manipulacija zaposlenika za otkrivanje povjerljivih informacija),
- Operativne ranjivosti (zastoji ili prekidi, oslanjanje na vanjske dobavljače ili partnere koji mogu biti izloženi rizicima),
- Pravne ranjivosti (nepoštivanje zakona i propisa, neusklađenost s relevantnim zakonima koji mogu rezultirati kaznama ili pravnim posljedicama).

Identifikacija ranjivosti uključuje korištenje raznih metoda i tehnika kako bi se osiguralo da su sve potencijalne slabosti prepoznate. Evo nekoliko ključnih koraka u tom procesu:

- Analiza prošlih incidenata**,**
- Intervjui i radionice sa zaposlenicima**,**
- Analiza sektora i industrije**,**
- SWOT **(**snage, slabosti, prilike, prijetnje) analiza**,**
- Scenario analiza**,**
- Praćenje medija i društvenih mreža**,**
- Suradnja s vanjskim stručnjacima**.**

Jednom kada su ranjivosti identificirane, važno je procijeniti njihov potencijalni utjecaj na organizaciju. Procjena ranjivosti uključuje procjenu:

- Vjerojatnosti iskorištavanja (Kolika je vjerojatnost da će prijetnja iskoristiti ranjivost?, razmatranje povijesnih podataka i trendova može pomoći u procjeni vjerojatnosti),
- Potencijalni utjecaj (Koji je potencijalni utjecaj na poslovanje ako se ranjivost iskoristi?, Utjecaj na financije, operacije, reputaciju i druge aspekte poslovanja)

- Kritičnost ranjivosti (Klasifikacija ranjivosti prema njihovoj kritičnosti i prioritetu rješavanja, potrebno se fokusirati na ranjivosti koje predstavljaju najveći rizik za organizaciju.

6.4. ANALIZA KONTROLA

Analiza kontrola dio je procesa procjene rizika, posebno u kontekstu logističkih poduzeća. Ovaj korak uključuje identifikaciju i evaluaciju postojećih kontrola koje organizacija koristi za upravljanje rizicima i zaštitu svojih resursa i operacija. Cilj je osigurati da su kontrole učinkovite, pravovremene i odgovarajuće prilagođene specifičnim potrebama organizacije. Kroz sustavnu procjenu i optimizaciju kontrola, organizacije mogu smanjiti rizik od sigurnosnih incidenata i osigurati dugoročnu otpornost u dinamičnom poslovnom okruženju. Analiza kontrola je važna jer pomaže organizaciji da identificira praznine i slabosti, uštedi resurse, održi usklađenost s propisima i sl.

Kontrole su mjere ili postupci implementirani u organizaciji s ciljem smanjenja, eliminacije ili upravljanja rizicima. One služe za osiguravanje da prijetnje i ranjivosti ne ugrožavaju ciljeve poduzeća, te mogu biti:

- Preventivne kontrole (tehničke mjere, administrativne mjere),
- Detektivske kontrole **(**nadzor i monitoring**,** nadzorne kamere, provjere sustava i procesa),
- Korektivne kontrole (planovi za oporavak, popravci i ažuriranje),
- Kompenzacijske kontrole (alternativne metode zaštite, provedba privremenih mjera dok se ne postigne puna sigurnost

Procjena učinkovitosti kontrola ključna je za osiguranje da su implementirane mjere adekvatne za zaštitu organizacije. **Evo nekoliko metoda za procjenu učinkovitosti kontrola**:

1. Ključni pokazatelji uspjeha (KPIs**)**: definiranje specifične KPIs koji se odnose na performanse kontrola te praćenje tih pokazatelja može pružiti uvid u učinkovitost kontrola,
2. Testiranje sigurnosnih kontrola**:** provođenje simulacije i testiranje istih kako bi se procijenila otpornost kontrola na prijetnje uz redovito provjeravajte funkcionalnost sigurnosnih mjera,

3. Revizija kontrola: nezavisne revizije mogu pružiti objektivan uvid u učinkovitost kontrola uz osiguranje da su kontrole u skladu s politikama i regulativama,
4. Povratne informacije od zaposlenika,
5. Analiza incidenata**:** analiza sigurnosne incidente kako bi se razumjelo gdje su kontrole zakazale uz identificiranje obrasca i poduzimanje koraka za sprječavanje budućih incidenata.

6.5. ODREĐIVANJE VJEROJATNOSTI

Određivanje vrijednosti omogućava organizacijama u procjeni koliko je vjerojatno da će određene prijetnje utjecati na njihove resurse i operacije te da bolje razumiju što je za sustav važno i u fokus stavi svoje resurse kako bi zaštitili svoju imovinu i postigli zadane ciljeve.

Razumijevanje vjerojatnosti prijetnji omogućuje poduzećima da bolje planiraju, implementiraju odgovarajuće kontrole i alociraju resurse za smanjenje rizika. Postoji nekoliko metoda i tehnika koje organizacije mogu koristiti za procjenu vjerojatnosti prijetnji:

1. **Kvalitativne metode procjene** koje se oslanjaju na subjektivne procjene te koriste ljestvice rangiranja kako bi odredile vjerojatnost prijetnji na sljedeći način:
   - Vrlo visoka**:** prijetnja će se gotovo sigurno dogoditi.
   - Visoka**:** prijetnja je vjerojatna i može se dogoditi.
   - Srednja: prijetnja se može dogoditi, ali nije zajamčena.
   - Niska: prijetnja je malo vjerojatna.
   - Vrlo niska: prijetnja je gotovo nemoguća.
2. **Kvantitativne metode procjene** koriste numeričke podatke i statističke analize za precizniju procjenu vjerojatnosti. Analize za procjenu kvantitativne metode su:
   - Analiza povijesnih podataka: analiza prošlih incidenata i podataka o prijetnjama kako bi se odredili trendovi i učestalost prijetnji.
   - Matematički modeli: korištenje probabilističkih modela i simulacija (npr. Monte Carlo simulacija) za kvantificiranje vjerojatnosti prijetnji.
   - Bayesova analiza: primjena Bayesove teoreme za ažuriranje procjene vjerojatnosti prijetnje na temelju novih informacija.

3. **Kombinirane metode procjene** su metode kombinacija kvalitativnih i kvantitativnih metoda, koristeći prednosti obje pristupa. Kombinacija kvalitativnih i kvantitativnih pristupa, zajedno s kontinuiranim praćenjem i prilagodbom, redovitim ažuriranjem podataka i analiza uz suradnju sa stručnjacima i edukacijom zaposlenika, pomažu organizacijama da ostanu otporne u suočavanju s prijetnjama što je ključno za učinkovit proces upravljanja rizicima.

6.6. ANALIZA UČINKA

Analiza učinka ima za cilj utvrditi koliko štetan utjecaj može rezultirati iskorištavanja ranjivosti informacijskog sustava. Da bi se provela učinkovita analiza učinka, potrebno je prikupiti određene informacije, a to su: kritičnosti i osjetljivost sustava i informacija te koja je misija sustava. U analizi učinka, svaki nepovoljni utjecaj na sigurnost sustava smatra se gubitkom ili degradacijom jednog ili više od tri sigurnosna cilja: dostupnosti, integriteta i povjerljivosti. Svaki od tih ciljeva i posljedice neispunjenja su opisani u nastavku:

1. **Gubitak dostupnosti** – nastaje kada sustav, usluga ili podaci postanu nedostupni korisnicima zbog različitih razloga. Gubitak dostupnosti može imati ozbiljne posljedice na poslovanje i operacije organizacije te može rezultirati gubitkom produktivnog vremena i onemogućiti korisnicima obavljanje njihovih funkcija. Za učinkovito upravljanje rizikom od gubitka dostupnosti, organizacije bi trebale implementirati sljedeće mjere:
   - Redovito ažuriranje sustava kako bi se smanjila ranjivost na napade.
   - Izrada i testiranje planova za oporavak od katastrofa kako bi se osigurao brz povratak sustava u operativno stanje.
   - Implementacija sustava za praćenje i otkrivanje napada koji mogu pravovremeno detektirati pokušaje uskraćivanja usluge ili druge napade na dostupnost.
   - Redovno pravljenje sigurnosnih kopija podataka kako bi se osigurala njihova dostupnost čak i u slučaju gubitka primarnog sustava.
2. **Gubitak integriteta** – znači da su podaci ili sustavi neovlašteno izmijenjeni, oštećeni ili uništeni, čime se narušava njihova valjanost i vjerodostojnost. Ako dođe do namjernih ili slučajnih promjena informacija u sustavu, to može rezultirati netočnim podacima, prijevarom ili pogrešnim odlukama. Kako bi se učinkovito upravljalo rizikom od gubitka integriteta, organizacije bi trebale poduzeti sljedeće mjere:

- Primjena kontrola pristupa: Ograničavanje pristupa podacima i sustavima samo ovlaštenim osobama smanjuje rizik od neovlaštenih izmjena.
- Upotreba enkripcije: Enkripcija podataka tijekom prijenosa i pohrane pomaže u zaštiti podataka od neovlaštenih izmjena.
- Redovite provjere integriteta**:** Provođenje redovitih provjera i revizija kako bi se osiguralo da podaci nisu promijenjeni ili oštećeni.
- Kontrola verzija i backup: Čuvanje više verzija podataka i redovito pravljenje sigurnosnih kopija omogućava povratak na prethodno stanje u slučaju gubitka integriteta.
- Edukacija zaposlenika: Obuka zaposlenika o važnosti integriteta podataka i najboljim praksama za njegovu zaštitu smanjuje rizik od ljudskih pogrešaka.

3. **Gubitak povjerljivosti** – povjerljivost se odnosi na zaštitu informacija od neovlaštenog otkrivanja. Neovlašteno objavljivanje povjerljivih informacija može uzrokovati različite štete, uključujući gubitak povjerenja javnosti, štetu za pojedince ili poduzeće, ili pravne posljedice protiv poduzeća.

6.7. ODREĐIVANJE SIGURNOSNOG RIZIKA

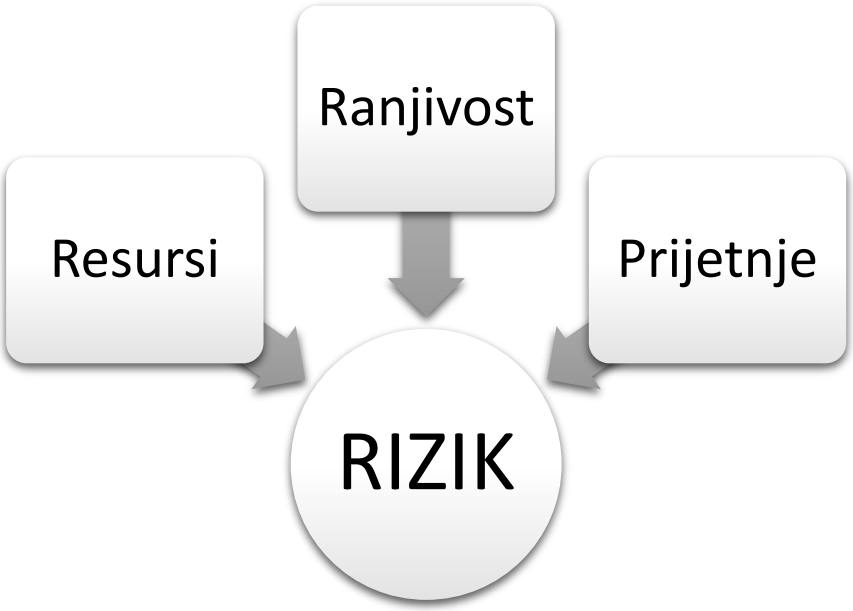
Rizik je mjera opasnosti odnosno mogućnost nastajanja neželjenog događaja, gubitka ili oštećenja svih resursa neke organizacije. Zato određivanje sigurnosnog rizika je dinamičan i iterativan proces koji zahtijeva pažljivo promišljanje i analizu. Kroz identifikaciju imovine, prijetnji, ranjivosti, te procjenu vjerojatnosti i utjecaja donosi se odluka o tome kako najbolje zaštititi svoje resurse i osigurati kontinuitet poslovanja.

Što je sustav više izložen prijetnjama, što je veći broj ranjivosti i što je resurs značajniji za organizaciju, to je i sigurnost rizika veći. Naravno, rizik neće se nikad uklanjati umanjivanjem vrijednosti resursa, već implementacijom odgovarajućih sigurnosnih kontrola koje će utjecati na parametre ranjivosti i prijetnji

S obzirom na kvantifikaciju rizika, rizici se zatim rangiraju po važnosti kako bi pomoglo u usmjeravanju resursa i napora na ublažavanje najznačajnijih rizika. Sam rizik se može promatrati kao funkcija tri parametra:

- Prijetnja
- Ranjivost i
- Vrijednost resursa;

RIZIK = f (prijetnja, ranjivost, vrijednost resursa) [11]



Slika 8. Funkcija parametra rizika

Za određivanje i analizu sigurnosnog rizika poželjno je kreirati matricu sigurnosnog rizika. Razine sigurnosnog rizika moguće je odrediti na temelju vjerojatnosti realizacije i potencijalnih gubitaka. Na temelju tih podataka moguće je kreirati matricu rizika koja će opisivati različite razine sigurnosnog rizika. [8]

Vjerojatnost realizacije	Posljedice (gubitak)		
	Niski (10)	Srednji (50)	Visoki (100)
Visoka (1)	**Nizak 10 x 1.0 = 10**	**Srednji 50 x 1.0 = 50**	**Visok 100 x 1.0 = 100**
Srednja (0,5)	**Nizak 10 x 0,5 = 5**	**Srednji 50 x 0.5 = 25**	**Visok 100 x 0.5 = 50**
Niska (0,1)	**Nizak 10 x 0.1 = 1**	**Srednji 50 x 0,1 = 5**	**Visok 100 x 0.1 = 10**

Tablica 1. Matrica rizika

Matrica prikazana na prethodnoj tablici prikazuje razine rizika te kolika je vjerojatnost ostvarenja prijetnje. Kod visoke razina rizika – potrebne snažne korektivne mjere, srednja razina rizika – potrebno izvršiti korektivne mjere u razumnom vremenskom periodu te niska razina rizika – vlasnik utvrđuje jesu li potrebne korektivne mjere ili ne. Ukoliko postoji potreba,

moguće je izraditi precizniju podjelu, što će u konačnici rezultirati i većim brojem razina sigurnosnog rizika. Tada govorimo o razinama kao što su vrlo niski, niski, srednji, visok te iznimno visok. Bitno je napomenuti da, iznimno visok rizik, može ukazati na situaciju koja zahtijeva hitnu reakciju pa čak i isključivanje sustava, prekid proizvodnje pa čak i prekid poslovanja dok se rizik ne sanira.

Nakon napravljene matrica za izračun rizika, može se odrediti vjerojatnost ostvarenja prijetnje tako da pomnožimo vjerojatnost ostvarivanja prijetnje s utjecajem na imovinu kao što je prikazano u tablici. [8]

Skala sigurnosnog rizika	
Visoki rizik	**50 - 100**
Srednji rizik	**10 -50**
Nizak rizik	**1 - 10**

Tablica 2. Vjerorajtnost prijetnje

6.8. PREPORUKA KONTROLA ZA UMANJIVANJE RIZIKA

Preporuka kontrola kao predzadnji korak u procjeni rizika odnosi se na kontrolu sigurnosti koje su osmišljene kako bi smanjile ili eliminirale rizike identificirane u procesu procjene rizika. Kontrole se primjenjuju kako bi se smanjila vjerojatnost da će se rizik ostvariti, njegov potencijalni utjecaj, ili oboje.

Glavni cilj ovih preporuka je smanjiti rizik sustava i njegovih podataka na prihvatljivu razinu. Pri razvoju preporuka za kontrole i alternativne metode za upravljanje rizicima, važno je uzeti u obzir nekoliko ključnih čimbenika:

- Politika organizacije: politike i smjernice koje organizacija prati.
- Pravni zahtjevi: relevantni zakoni i propisi koji se odnose na sigurnost informacija.
- Učinkovitost kontrola: koliko su preporučene kontrole usklađene s informacijskim sustavom.
- Sigurnost i pouzdanost: efikasnost i pouzdanost preporučenih mjera.

- Operativni utjecaj: kako će primjena kontrola utjecati na svakodnevne poslovne aktivnosti.

Preporuke za kontrole koje proizlaze iz procjene rizika služe kao osnovica za sljedeći korak – proces ublažavanja rizika. U ovo fazi, preporučene kontrole (bilo proceduralne ili tehničke) bit će procijenjene, rangirane po važnosti i implementirane. Treba imati na umu da možda neće biti moguće implementirati sve preporučene kontrole u cijelosti. Stoga je ključno provesti analizu troškova i koristi (Cost-benefit analysis) za svaku preporučenu kontrolu kako bi se osiguralo da su troškovi provedbe opravdani smanjenjem rizika za organizaciju i njezin informacijski sustav. Osim analize troškova i koristi, važno je također pažljivo razmotriti izvedivost (korisnik i tehnički zahtjevi) te operativni utjecaj (kako će primjena kontrola utjecati na performanse sustava) prilikom implementacije preporučenih mjera.

6.9. IZRADA DOKUMENTACIJE

Posljednji korak u procesu procjene rizika je izrada dokumentacije, koja je ključna za osiguranje da svi rezultati i preporuke budu pravilno zabilježeni i dostupni svim relevantnim stranama. Ovaj korak uključuje izradu službenog izvješća koje sadrži sve ključne informacije prikupljene tijekom procesa procjene rizika. Dokumentacija treba sadržavati detaljan popis svih identificiranih prijetnji i ranjivosti koje su analizirane tijekom procjene. U izvješću treba jasno navesti vjerojatnost da će se svaki identificirani rizik ostvariti, kao i procijenjeni učinak ako se rizik realizira. Detaljno opisati sve preporučene kontrole koje bi trebale biti implementirane kako bi se smanjila ili eliminirala procijenjena razina rizika. Ovo uključuje tehničke, proceduralne i organizacijske kontrole, kao i razloge za njihovu preporuku.

Neki od ključnih elemenata koji nam govore zašto je izrada dokumentacije važna, to su:

- **Transparentnost i praćenje: s**lužbeno izvješće pruža jasnu i sveobuhvatnu sliku svih aktivnosti izvedenih u okviru procjene rizika, što omogućava transparentnost i omogućuje praćenje napretka u upravljanju rizicima.
- **Komunikacija:** dokumentacija služi kao sredstvo komunikacije između timova, menadžmenta i drugih zainteresiranih strana. Omogućuje svima uključenim stranama da razumiju identificirane rizike, planirane kontrole i potrebu za daljnjim akcijama.
- **Osnova za buduće procjene:** temeljito dokumentiran proces procjene rizika pruža korisne informacije za buduće procjene i revizije, pomažući u unapređenju metoda i pristupa u upravljanju rizicima.

- **Regulatorni zahtjevi:** u mnogim industrijama i sektorima, dokumentacija procjene rizika može biti zahtjev za usklađenost s regulatornim standardima i zakonodavstvom, osiguravajući da organizacija zadovoljava sve relevantne zahtjeve.

Primjer: Izvještaja o procjeni rizika prikazan je u tablici 3. [8]

IZVJEŠĆE O PROCJENI RIZIKA
UVOD • Svrha • Opseg ove procjene rizika - Opišite sve komponente informacijskog sustava, elemente, korisnike i sve ostale pojedinosti o sustavu koje bi trebalo uzeti u obzir pri procjeni rizika.
PRISTUP PROCJENI RIZIKA Ukratko opišite pristup koji se koristio za provođenje procjene rizika kao na primjer: • Sudionici (članovi tima za procjenu rizika) • Tehnike prikupljanja informacija (koji su alati korišteni za prikupljanje informacija o sustavu, koji su upitnici korišteni i sl.) • Razvoj i opis ljestvice rizika (matrice razine rizika 3x3, 4x4 ili 5x5).
KARAKTERIZACIJA SUSTAVA Opišite sustav, uključujući hardware (server, ruter i sl.), software (aplikacije, operacijski sustav, protokole i sl.), sučelja sustava (komunikacijska veza), informacije i korisnike. Dostavite dijagram povezivanja ili dijagram toka ulaza i izlaza sustava kako bi se procijenio opseg napora za procjenu rizika za određeni sustav.
IZJAVA O PRIJETNJI Potrebno je sastaviti i navesti sve moguće izvore prijetnji u informacijskom sustavu i sve povezane prijetnje koje se primjenjuju na informacijski sustav koji se procjenjuje
REZULTAT PROCJENE RIZIKA Navedite opažanja, koji su parovi ranjivosti-prijetnje. Svako zapažanje mora uključivati: • Broj promatranja i kratak opis promatranja (npr. Opažanje 1.: Zaporke informacijskog sustava mogu se pogoditi ili razbiti) • Raspravu o paru ranjivost-prijetnja • Identifikacija postojećih ublažavajućih sigurnosnih kontrola • Rasprava i procjena vjerojatnosti (velika, srednja ili niska) • Rasprava i evaluacija analize učinka • Ocjena rizika na temelju matrice razine rizika (visoka, srednja ili niska) • Preporučene kontrole ili alternativne mogućnosti za smanjenje rizika.
SAŽETAK Ukupan broj opažanja. Opažanja se trebaju sažeti, moraju se povezati razine rizika, definirati preporuke i sve komentare u obliku tablice kako bi se olakšala provedba preporučenih kontrola tijekom procesa ublažavanja rizika za promatrani sustav.

Tablica 3. Izvješće o procjeni rizika,
izvor: [8]

7. ANALIZA SIGURNOSNIH UGROZA PRIJEVOZA LIJEKOVA

Distribucija lijekova predstavlja jedan od najsloženijih i najkritičnijih segmenata u logističkom lancu, gdje su sigurnost i kvaliteta proizvoda od najveće važnosti. U ovom sektoru, svaki potencijalni rizik može imati ozbiljne posljedice, ne samo za poslovanje, već i za zdravlje krajnjih korisnika – pacijenata. Lijekovi, kao osjetljivi proizvodi, zahtijevaju posebne uvjete transporta i skladištenja, a svaka greška u tim procesima može rezultirati gubitkom učinkovitosti lijeka, što može ugroziti zdravlje ili život pacijenata.

Zbog toga je analiza sigurnosnih rizika neophodna za identifikaciju i minimiziranje potencijalnih prijetnji koje mogu nastati tijekom distribucije lijekova. Ova analiza omogućava logističkim tvrtkama da proaktivno identificiraju slabosti u svojim procesima i implementiraju mjere za smanjenje ili eliminaciju tih rizika. Kroz sustavnu analizu, organizacije mogu unaprijediti pouzdanost svojih operacija, osigurati poštivanje regulatornih zahtjeva i, što je najvažnije, zaštititi zdravlje i sigurnost pacijenata.

U ovom poglavlju detaljno su opisani podaci prikupljeni iz tri ključne analize sigurnosnih rizika u logističkom lancu distribucije lijekova: ***analiza transportnih ruta***, ***analiza skladištenja u Osijeku***, te ***analiza kontrole pristupa i sigurnosti u pretovarnom skladištu***.

Svaka od ovih analiza koristi **metodologiju FMEA** (Failure Mode and Effects Analysis) za analizu sigurnosnih rizika povezanih s transportom i skladištenjem lijekova. FMEA je strukturirani pristup koji omogućava detaljnu analizu potencijalnih načina kvara u sustavu ili procesu, zajedno s njihovim posljedicama, vjerojatnošću pojavljivanja i mogućnošću otkrivanja prije nego što prouzrokuju štetu. Ova metodologija pomaže u određivanju prioriteta rizika, identificiranju ključnih područja koja zahtijevaju poboljšanje, te uvođenju odgovarajućih korektivnih mjera.

Konkretno, FMEA u ovom radu koristi ocjene ozbiljnosti (S), vjerojatnosti pojavljivanja (P), i mogućnosti otkrivanja (D) za izračunavanje broja prioriteta rizika (RPN), koji omogućava rangiranje rizika po njihovoj važnosti. Na taj način, FMEA omogućava donošenje informiranih odluka o tome gdje i kako implementirati preventivne mjere koje će najbolje zaštititi integritet i sigurnost lijekova tijekom njihovog puta od proizvođača do krajnjih korisnika. Dobivene ocjene koriste se za izračunavanje RPN (Risk Priority Number), što omogućava identifikaciju najkritičnijih rizika koji zahtijevaju hitnu pažnju i intervenciju.

7.1. ANALIZA TRANSPORTNIH RUTA

Transportne rute predstavljaju bitnu komponentu u distribuciji lijekova, jer se tijekom transporta mogu pojaviti različiti rizici koji mogu utjecati na sigurnost i kvalitetu lijekova. U ovoj analizi prikupljeni su podaci koji se odnose na moguće načine kvara tijekom transporta, kao i njihove posljedice, vjerojatnost pojavljivanja, te mogućnost otkrivanja.

Promatrane rute utemeljene su na podacima preuzetim iz validacije transporta, podacima kvalifikacije opreme i povijesnim podacima nadzora temperaturnih uvjeta odnosno evaluacijama odstupanja. Ciljani produkt provođenja analize transportnih ruta je stavljanje rizika tijekom ruta pod kontrolu, odnosno njihovo smanjivanje do prihvatljive mjere. Najkritičniji efekti rizika ruta su narušavanje kvalitete proizvoda odnosno uništenje proizvoda zbog izostanka zadovoljavanja temperaturnih uvjeta transporta te kašnjenje ili izostanak isporuke robe kupcima.

Analiza se provodi korištenjem podataka na razini jedne poslovne godine kako bi rezultati bili što relevantniji. Prikupljanje povijesnih podataka provodi se korištenjem validiranog GPS sustava (fleet management aplikacije) Smartivo, koju Društvo koristi za temperaturni nadzor i praćenje dostavnih vozila, usporedno s pregledom podataka s tovarnih listova određenih ruta.

Slijedom navedenoga definirani su sljedeći zahtjevi:

- Za svaku rutu definirati otklanjanje prepoznatih preostalih rizika,
- Prepoznati eventualne potrebne dorade na unapređenju poslovnih procesa,
- Osvijestiti i prihvatiti rizike koje nije moguće potpuno otkloniti ili kontrolirati.

Podaci u tablici br. 4. su strukturirani na sljedeći način:

- Ozbiljnost greške (S): Ozbiljnost posljedica svakog načina kvara tijekom transporta ocijenjena je na skali od 1 do 10, pri čemu viša ocjena označava ozbiljniji utjecaj na sigurnost ili kvalitetu lijekova. Na primjer, kvar hlađenja u transportnom vozilu može biti ocijenjen s visokom ocjenom ozbiljnosti zbog mogućnosti oštećenja osjetljivih lijekova.
- Vjerojatnost pojavljivanja greške (P): Ovaj parametar ocjenjuje koliko je vjerojatno da će se određeni kvar pojaviti tijekom transporta, također na skali od 1 do 10. Vjerojatnost može ovisiti o različitim faktorima kao što su tehničko stanje vozila, vremenski uvjeti, ili složenost rute.
- Vjerojatnost otkrivanja greške (D): Ova ocjena procjenjuje koliko je vjerojatno da će se kvar otkriti prije nego što prouzrokuje štetu. Niska ocjena detekcije ukazuje na potrebu za poboljšanjem sustava praćenja i kontrole tijekom transporta.

Tablica 4. Analiza rizika na transportnim rutama									
S= ozbiljnost greške (1= vrlo mala; 2= mala; 3= srednja; 4= velika; 5= vrlo velika)									
P= vjerojatnost pojavljivanja greške (1= vrlo mala; 2= mala 3= srednja; 4= velika; 5= vrlo velika)									
D= vjerojatnost otkrivanja (1= vrlo vjerovatno; 2= vjerovatno; 3= mala vjerojatnost; 4= gotovo nevjetojatno; 5= nevjerojatno)									
RPN (ocjena rizika) = SxPxD, Ako je RPN veći od 20 moraju se poduzeti mjere									
Br.	**Područje/ procesni koraci**	**Zahtjevi/ Postojeće mjere kontrole**	**Moguća greška / rizik/ neispravnost**	**Moguće posljedice**	**(S) ozbiljnost greške**	**(P) vjerojatnost pojavljivanja**	**(D) vjerojatnost otkrivanja**	**RPN**	**KAPA STATUS (završeno/u postupku) RPN= (SxPxD)**
1.	Kvalifikacija dostavnog vozila	Opremanje i homologacija, mapiranje vozila, Umjeravanje mjernih osjetnika, nadzor nad uvođenjem novih vozila, redoviti nadzor nad Izvještajima mapiranja i Planovima umjeravanja.	Temperaturno odstupanje tijekom transporta	Uništenje robe zbog utjecaja nesukladne temperature. Nemogućnost isporuke robe kupcu.	5	1	3	**15**	/
2.	Tehnička ispravnost dostavnog vozila	Nabavka novih vozila svake 4 godine. Redovito obavljanje redovnih servisa vozila. Izbjegavanje kretanja na rutu sa vozilom za koje se sumnja u moguću neispravnost. Edukacije i zahtjevi odgovornosti vozača	Kvar vozila tijekom rute	Uništenje robe zbog utjecaja nesukladne temperature. Kašnjenje s isporukom ili nemogućnost isporuke robe kupcu.	5	2	3	**30**	Za svaku pojedinu rutu odrediti najudaljeniju točku te procijeniti vrijeme reakcije slanja zamjenskog vozila iz OPh. Uzeti u obzir validacijska svojstva održavanja temperatura vozila i hladnjaka. Procijeniti da li je moguće zatražiti pomoć na terenu (ljekarne Društva, drugi vozač na susjednom terenu)

3.	Periferna ispravnost vozila (pneumatici, brisači i sl.)	Pregled pneumatika i brisača od strane vozača i voditelja TD. Pregled i mjerenje guma od strane stručnog osoblja pri sezonskoj zamijeni. Pravovremena periodička zamjena pneumatika. Rezervna guma i alat u vozilu. Osposobljenost vozača za pregled i zamjenu. Izbjegavanje makadama.	Pucanje, bušenje pneumatika tijekom rute.	Izazivanje havarije (fizičko uništenje robe ili temperaturno odstupanje) Kašnjenje s isporukom robe kupcu.	5	1	3	**15**	/
4.	Ispravnost uređaja za hlađenje / grijanje	Nabavka novih uređaja svake 4 godine. Redovito obavljanje redovnih servisa uređaja. Izbjegavanje kretanja na rutu ukoliko postoji sumnja u moguću neispravnost uređaja. Edukacije i zahtjevi odgovornosti vozača. Osiguranje robe u vozilu.	Kvar uređaja za hlađenje / grijanje tijekom rute	Uništenje robe zbog utjecaja nesukladne temperature	5	2	3	**30**	Za svaku pojedinu rutu odrediti najudaljeniju točku te procijeniti vrijeme reakcije slanja zamjenskog vozila iz OPh. Uzeti u obzir validacijska svojstva održavanja temperatura vozila i hladnjaka. Procijeniti da li je moguće zatražiti pomoć na terenu (ljekarne , drugi vozac na susjednom terenu Društva, drugi vozač na susjednom terenu.

5.	Ispravnost uređaja (sustava) za temperaturni nadzor	Redoviti uvid u ispravnost uređaja. Validirani sustav i pružatelj usluge GPS nadzora. Korištenje kvalificiranih transportnih kutija te kontroliranih i validiranih procesa, kao temelja za temperaturnu konzistentnost. U slučaju kvara, korištenje zamjenskog Data Loggera Osiguranje	Kvar uređaja tijekom rute nekontroliranom broju osoba	Nemogućnost izdavanja temp. zapisa rute odnosno dokazivanja održanih temp. zahtjeva transporta	4	3	3	**36**	Opremanje vozila sa dodatnim Data Loggerom (EBI 300)
6.	Izvanredni uvjeti na cesti	Opremljenost vozila adekvatnim pneumaticima (zima / ljeto). Vozila opremljena lancima. Educirani i opremljeni vozači	Zastoj zbog snježnih oborina	Kašnjenje s isporukom robe kupcu ili nemogućnost isporuke robe kupcu	4	3	3	**36**	Uračunavanje dodatnog vremena trajanja rute u zimskim mjesecima.
7.	Izvanredni uvjeti na cesti	Informiranje o radovima na cesti i alternativnim pravcima (HAK	Zastoj zbog radova na cesti	Kašnjenje s isporukom robe kupcu ili nemogućnost isporuke robe kupcu	3	3	2	**18**	/

8.	Izvanredni uvjeti na cesti	Informiranje o vremenskim uvjetima i prohodnosti te alternativnim pravcima. Vršenje dostava manjim vozilima (kombi ili pick up) ukoliko je moguće. Vraćanje robe u skladišne prostore Društva ili odgoda rute do povoljnijih uvjeta.	Zatvaranje mosta ili dijela ceste zbog udara vjetra	Kašnjenje s isporukom robe kupcu ili nemogućnost isporuke robe kupcu	3	3	2	**18**	/
9.	Izvanredni događaj na cesti	Održavanje vozila. Opremljenost vozila adekvatnim pneumaticima. Kontrola brzina i vožnje vozača od strane voditelja. Edukacije i odgovornosti vozača. Poštivanje radnog vremena vozača i potrebnog odmora. Osi. robe u vozilu.	Havarija, sudar, izlijetanje vozila	Fizičko uništenje robe. Temp. odstupanje. Kašnjenje s isporukom robe kupcu ili nemogućnost isporuke robe kupcu.	5	2	5	**25**	Procedura o postupanju vozača i voditelja transporta (kontakt, slanje zamjenskog vozila, slanje vučne službe) Za svaku pojedinu rutu odrediti najudaljeniju točku te procijeniti vrijeme reakcije slanja zamjenskog vozila.
10.	Specifičnost rute	Poznavanje alternativnih pravaca. Poznavanje rasporeda vožnje trajekata (kod zatvora roba se vraća u OPh, a dostava vrši slijedeći put prema rasporedu). Poznavanje vremena dizanja spuštanja mostova. Poznavanje radnih vremena i adresa kupaca (napomena na otpremnici)	Ne vozi trajekt, dignut most, kupca nema na adresi	Kašnjenje s isporukom robe kupcu ili nemogućnost isporuke robe kupcu	4	2	2	**16**	/

7.2. ANALIZA RIZIKA SKLADIŠTENJA

Skladište u Osijeku predstavlja jednu od važnih točaka u logističkom lancu, gdje su lijekovi pohranjeni prije daljnje distribucije. U ovoj analizi fokus je stavljen na identifikaciju rizika unutar skladišta, uključujući sve faktore koji mogu utjecati na sigurnost i kvalitetu skladištenih lijekova.

Podaci u tablici 5. su strukturirani na sljedeći način:

- Ozbiljnost greške (S): Ocjene ozbiljnosti posljedica potencijalnih kvarova u skladištu ocjenjuju se na skali od 1 do 10. Ozbiljniji kvarovi, poput kvara klimatizacijskog sustava, mogu imati značajan utjecaj na lijekove, posebno one koji zahtijevaju posebne uvjete skladištenja.
- Vjerojatnost pojavljivanja greške (P)**:** Vjerojatnost pojavljivanja grešaka, kao što su tehnički kvarovi opreme ili ljudske pogreške, ocijenjena je na skali od 1 do 10. U ovoj analizi uzimaju se u obzir specifični uvjeti skladišta, poput starosti opreme ili učestalosti održavanja.
- Vjerojatnost otkrivanja greške (D): Ovaj parametar ocjenjuje mogućnost pravovremenog otkrivanja greške prije nego što dođe do štetnih posljedica. U skladišnom okruženju, sustavi poput alarma ili senzora igraju ključnu ulogu u detekciji.
- Kao i u prethodnom slučaju, podaci su strukturirani u tablici koja uključuje sve relevantne načine kvara, ocjene za S, P i D, te odgovarajući RPN.

Tablica 5. Analiza rizika za skladišnu lokaciju Osijek									
S= ozbiljnost greške (1= vrlo mala; 2= mala; 3= srednja; 4= velika; 5= vrlo velika)									
P= vjerojatnost pojavljivanja greške (1= vrlo mala; 2= mala 3= srednja; 4= velika; 5= vrlo velika)									
D= vjerojatnost otkrivanja (1= vrlo vjerojatno; 2= vjerojatno; 3= mala vjerojatnost; 4= gotovo nevjerojatno; 5= nevjerojatno)									
RPN (ocjena rizika) = SxPxD, Ako je RPN veći od 20 moraju se poduzeti mjere									
Br.	**Područje/ procesni koraci**	**Zahtjevi/ Postojeće mjere kontrole**	**Moguća greška / rizik/ neispravnost**	**Moguće posljedice**	**(S) ozbiljnost**	**(P) vjerojatnost**	**(D) vjerojatnost**	**RPN**	**STATUS (završeno/u postupku) RPN= (SxPxD)**
1.	Skladištenje proizvoda	Proizvodi se skladište u čistim i zatvorenim prostorijama	Neadekvatni uvjeti čuvanja lijekova	Ugrožena ispravnost lijekova	5	1	1	**5**	Prostorije skladišta su zatvorene, redovito se čiste te se redovito provode DDD mjere
2.	Skladištenje proizvoda	Proizvodi se skladište pod odgovarajućim temperaturnim uvjetima uključujući i osjetljive proizvode koji se skladište u hladnom lancu	Neadekvatni uvjeti čuvanja lijekova	Ugrožena ispravnost lijekova	5	1	2	**10**	Prostor u kojem se skladište lijekovi uključujući i hladnjak u kojemu se skladišti hladni lanac su termomapirani te se temperature nadziru 24 h dnevno sustavima nadzora sa umjerenim mjernim osjetnicima

3.	Skladištenje proizvoda	Kontinuirana opskrba električnom energijom	Prekid opskrbe el.energijom može dovesti do poremećaja temperaturnih uvjeta	Ugrožena ispravnost lijekova	5	1	1	**5**	U skladišnim prostorima je dostupan je agregat koji se pali u slučaju nestanka el.energije
4.	Osoblje	Dostupnost odgovorne osobe za promet na veliko lijekovima	Neispunjavanje svih zadataka odgovorne osobe u prometu na veliko lijekovima	Ugrožena ispravnost lijekova	5	3	2	**30**	Organizacijom rada nije predviđeno da Odgovorna osoba za promet lijekova na veliko bude smještena u Osijeku, obzirom da se ne radi o klasičnom veleprodajnom skladištu nego o pretovarnom skladištu. Odgovorna osoba u tom smislu ne bi bila pod dovoljnim radnim opterećenjem da bi se zaposlila na lokaciji pa se poslovi odgovorne osobe odrađuju iz Zagreba. Odrada poslova odgovorne osobe provodi se putem delegiranja određenih zadataka na lokalne zaposlenike, svakodnevnom komunikacijom i redovitim kvartalnim samoinspekcijama.
5.	Osoblje	Dovoljan broj stručnog osoblja za neometano obavljanje potrebnih poslova	pogreške u radu	Ugrožena ispravnost lijekova	5	1	1	**5**	U skladištu u Osijeku zaposlen je dovoljan broj stručnog osoblja koje se redovito educira po potrebi
6.	Sustav upravljanja kakvoćom	Osigurati provođenje i održavanje sustava upravljanja kakvoćom	Nema nadzora stručne osobe nad sustavom kakvoće	Distribuiraju se neadekavatni proizvodi prema kupcima	5	3	2	**30**	Sustav kakvoće vodi se centralno iz Zagreba. Dokumentacija se distribura od strane Kvalitete te se redovito provode edukacije. Svakodnevno se komunicira s voditeljem skladišta. Temperature se osim dnevno kontroliraju na tjednoj bazi od strane odgovorne osobe u Zagrebu. Dodatno će se provoditi redovite samoinspekcije skladišta Osijek sa kvartalnom učestalošću te po potrebi i češće ukoliko se kroz rad uoči potreba.

7.	Dokumentacija	Vođenje aktivnosti za koje veleprodaja ima dozvolu te osigurano kvalitetno vođenje zapisa	Provođenje aktivnosti koje nisu u skladu s dozvolom i neodgovarajući zapisi	Skladištenje i transport krivotvorene i oštećene robe, zapisi ne postoje ili su neadekvatni	5	1	1	**5**	Sva roba koja ulazi u skladište puštena je u promet u veleprodaji Zagreb od strane odgovorne osobe (iste osobe kao i za Osijek), roba koja ulazi u skladište je već zapakirana za svakog kupca i ne otvara se, zapisi se šalju na pregled odgovornoj osobi u Zagreb.
8.	Edukacija	Osigurano je da se izrađuju i provode programi početne i kontinuirane edukacije za osoblje uključeno u poslove obuhvaćene prometom lijekova te krivotvorina	Osoblje nije educirano te postoji mogućnost da se uništi ili distribuira neodgovarajuća roba na neodgovarajući način	Skladištenje i transport krivotvorene i oštećene robe, zapisi ne postoje ili su neadekvatni	5	1	1	**5**	Osoblje je educirano u skladu s Planom edukacije kompanije za tekuću godinu i po potrebi tijekom godine prema SOP-ovima koji se revidiraju a za novozaposlene postoji Plan edukacije za osnovne i stručne procese, npr. GDP

9.	Obustava i povlačenje serije lijeka iz prometa	Koordiniraju se i provode hitne radnje prilikom obustave stavljanja lijeka u promet i povlačenja lijeka iz prometa	Distribuiraju se neadekvatni i povučeni lijekovi	Neadekvatni i povučeni lijekovi dolaze do kupaca	5	1	1	**5**	Obustave i povlačenja vode se od strane odgovorne osobe iz Zagreba, koja je ista i za Osijek. Osoblje je educirano prema SOP-ovima za navedene aktivnosti
10.	Reklamacije	Osigurano je učinkovito rješavanje reklamacija	Reklamirani proizvodi se ne distribuiraju, reklamacije se ne proslijeđuju odgovornoj osobi	Distribuiraju se neadekvatni i oštećeni proizvodi prema kupcima	5	1	1	**5**	Reklamacije se rješavaju od strane odgovorne osobe u Zagrebu o čemu su educirani djelatnici u Osijeku; da svaku takvu reklamaciju proslijede kao i reklamirani preoizvod prema Zagrebu.
11.	Procjena dobavljača i kupaca	Osigurano provođenje procjene i odobravanja dobavljača i kupaca - odobreni ugovori između davatelja i primatelja ugovora koji određuju njihove obaveze u odnosu na promet ili prijevoz lijekova	Nabavlja se roba od neprovjerenih dobavljača, transportira se na neadekvatan način	Distribuira se neprovjerena roba na neadekvatan način koja takva dolazi do kupaca	5	1	1	**5**	Provođenje procjene i odobravanja dobavljača provodi se od strane djelatnika Nabave i Kvalitete, a pod nadzorom odgovorne osobe na lokaciji Zagreb (ista odgovorna osoba kao i za Osijek). Sa dobavljačima roba i usluga potpisuju se ugovori o kvaliteti u kojima su definirane sve obaveze jedne i druge strane.

12.	Samoinspekcije	Osigurano je da se samoinspekcije obavljaju u odgovarajućim redovitim razdobljima, prema unaprijed donesenom pisanom planu i da postoje predviđene potrebne korektivne mjere	Prostor ne zadovoljava kriterije GDP-a, djelatnici nisu adekvatno educirani, ne poštuje se propisano SOP-ovima	Neadekvatni, oštećeni, krivotvoreni proizvodi distribuiraju se prema kupcima	5	1	1	**5**	Samoinspekcije se obavljaju redovito prema planom zadanim frekvencijama i nadziru od strane odgovorne osobe, propisuju se korektivne mjere u slučaju bilo kakvih odstupanja. Za lokaciju Osijek predviđeno je kvartalno provjeriti sustav kvalitete od strane Odgovone osobe.
13.	Delegiranje dužnosti	Vode se odgovarajući zapisi o svim delegiranim dužnostima	Aktivnosti provode needucirani djelatnici na neadekvatan način	Distribiraju se neadekvatni, oštećeni, neprovjereni proizvodi neutvrđenog porijekla	5	2	1	**10**	Sve delegirane dužnosti propisane su i odobrene od strane Odgovornih osoba o čemu postoje zapisi, a djelatnici su nadzirani od strane odgovorne osobe.

14	Vraćeni/odbijeni povućeni ili krivotvoreni lijekovi	Donose se odluke o stavljanju u karantenu ili postupanju s vraćenim, odbijenim, povučenim ili krivotvorenim lijekovima	Distribuiraju se neadekvatni, krivotvoreni i povućeni lijekovi	Neadekvatni proizvodi dolaze do kupaca	5	1	1	**5**	U skladu s propisanim procedurama u SOP-ovima odgovorna osoba donosi odluku o stavljanju u karantenu neadekvatnih vraćenih, odbijenih, povućenih ili krivotvorenih proizvoda. Odluke se donose u Zagrebu.
15.	Povrat proizvoda	Odobravanje povrata vraćenih lijekova u zalihe pogodne za prodaju	Neodobreni proizvodi vraćenih lijekova nalaze se u distribuciji	Neadekvatni proizvodi dolaze do kupaca	5	1	1	**5**	Povrat se odobrava i pregledava na lokaciji u Zagrebu od strane Odgovorne osobe u sladu s propisanim procedurama u SOP-u (ista odgovorna osoba kao i za lokaciju Osijek).
16.	Transport proizvoda	Adekvatna distribucija proizvoda do proizvođača	Transport pod neadekvatnim temperaturnim uvjetima	Ugrožena kvaliteta lijekova	5	1	1	**5**	Transport proizvoda do krajnjeg kupca provodi se u temperaturno kontroliranim vozilima, a hladni lanac u aktivnim hladnjacima. Temperature se prate cijelo vrijeme transporta te se iste redovito pregledavaju. U slučaju neadekvatne temperatre otvaraju se nesukladnosti. Transportne rute su validirane. Eventualna odstupanja obrađuju se prema SOP OK 048 od strane odgovorne osobe u Zagrebu.

7.3. ANALIZA KONTROLE PRISTUPA I SIGURNOSTI U PRETOVARNOM SKLADIŠTU

Pretovarna skladišta često su mjesta gdje se odvijaju kritični procesi premještanja robe, što ih čini podložnim specifičnim sigurnosnim rizicima. Analiza kontrola pristupa i sigurnosti u pretovarnom skladištu fokusira se na rizike povezane s pristupom neovlaštenih osoba, mogućim krađama, ili neadekvatnim rukovanjem robom.

Analiza je provedena sagledavanjem uzroka koji bi mogli doprinijeti neovlaštenom pristupu skladištu i potencijalnom otuđenju skladištenih proizvoda. Detektirani rizici su podijeljeni u grupe prema izvoru rizika:

- Rizici geolokacijskog položaja skladišta
- Rizici građevinske i tehničke izvedbe skladišta
- Procesni rizici

Razradom grupa rizika detektirani su parametri rizika po detektiranim grupama prikazani tablicom 6. u nastavku.

Parametri rizika geolokacijskog položaja skladišta	**Parametri rizika građevinske i tehničke izvedbe skladišta**	**Parametri procesnih rizika skladišta**
Smještaj objekta na izoliranom području ili osami	Čvrstoća izvedbe ulaznih vrata	Dostupnost ključeva, dostupnost alarmnih šifri
Smještaj objekta na području bez javne rasvjete	Sigurnost i izvedba brave, Alarmni sustav	Edukacija osoblja zaposlenog u skladištu
Smještaj objekta na pustom području bez dinamike slučajnih prolaznika	Dodatna vrata pod ključem (pretprostor), vanjska rasvjeta objekta	Vrijeme zadržavanja robe u skladištu
	Dodatni otvori na građevini (prozori, prolazi, veze sa susjednim skladištima)	Periodi u kojima je skladište bez nadzora

Tablica 6.; Parametri prepoznatih grupa rizika za sigurnost robe u skladištu od neovlaštenog pristupa odnosno otuđenja

Nakon definiranja svih parametara rizika odnosno parametara uzroka potencijalne ugroze sigurnosti skladišta i skladištene robe od neovlaštenog pristupa trećih osoba i otuđenja, poduzete su korektivne i preventivne radnje. Korektivne i preventivne radnje uključivale su provjeru svih navedenih parametara, potpisivanje ugovora o zaštiti, ugradnju alarmnog sustava, ugradnju senzora pokreta, ugradnju dodatne rasvjete, organizaciju radnog procesa i edukaciju djelatnika. Po izvršenju korektivnih i preventivnih radnji načinjena je završna analiza preostalih vezanih rizika u formi FMEA analize, tablica 6. te je procijenjeno da je preostali rizik iskontroliran i prihvatljiv.

Podaci u tablici 7. niže strukturirani su na sljedeći način:

- Ozbiljnost greške (S): Ocjena ozbiljnosti potencijalnih sigurnosnih prijetnji, poput krađe lijekova, koja može imati ozbiljne posljedice za poslovanje i javno zdravlje. Ocjene se kreću na skali od 1 do 10.
- Vjerojatnost pojavljivanja greške (P): Ovaj parametar ocjenjuje koliko je vjerojatno da će se sigurnosni incidenti dogoditi, uzimajući u obzir čimbenike kao što su broj neovlaštenih pristupa, učinkovitost sigurnosnih sustava, i povijest incidenata.
- Vjerojatnost otkrivanja greške (D): Ovdje se procjenjuje koliko je vjerojatno da će sigurnosni sustavi ili osoblje otkriti prijetnju prije nego što se dogodi šteta. Ocjene se temelje na učinkovitosti trenutnih sustava kontrole pristupa i nadzora.
- Podaci iz ove analize također su organizirani u tablicu koja sadrži sve relevantne načine kvara, njihove ocjene S, P i D, te odgovarajući RPN.

Tablica 7. Analiza rizika kontrole pristupa i sigurnosti robe od otuđenja za pretovarno skladište Osijek									
S= ozbiljnost greške (1= vrlo mala; 2= mala; 3= srednja; 4= velika; 5= vrlo velika)									
P= vjerojatnost pojavljivanja greške (1= vrlo mala; 2= mala 3= srednja; 4= velika; 5= vrlo velika)									
D= vjerojatnost otkrivanja (1= vrlo vjerovatno; 2= vjerovatno; 3= mala vjerojatnost; 4= gotovo nevjetojatno; 5= nevjerojatno)									
RPN (ocjena rizika) = SxPxD, Ako je RPN veći od 20 moraju se poduzeti mjere									
Br.	**Područje/ procesni koraci**	**Zahtjevi/ Postojeće mjere kontrole**	**Moguća greška / rizik/ neispravnost**	**Moguće posljedice**	**(S) ozbiljnost greške**	**(P) vjerojatnost pojavljivanja**	**(D) vjerojatnost otkrivanja**	**RPN**	**KAPA STATUS (završeno/u postupku) RPN= (SxPxD)**
1.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Izolirano okruženje omogućuje nesmetan prilaz i pokušaj provale u skladište od trećih osoba	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Prilaz skladištu nalazi se uz glavnu prometnicu i javnu rasvjetu te se slijedom navedenoga ne smatra rizičnim zbog izoliranoga okruženja.
2.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Mračno okruženje omogućuje nesmetan prilaz i pokušaj provale u skladište od trećih osoba	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Ispred vanjskog ulaza u skladište postavljena je rasvjeta opremljena senzorom pokreta što isključuje rizik od provala potaknutih mračnim okruženjem.
3.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Vanjska ulazna vrata su trošna i imaju bravu jednostavnu za obijanje	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Vanjska ulazna vrata su nova rolo vrata opremljena elektronskom bravom.

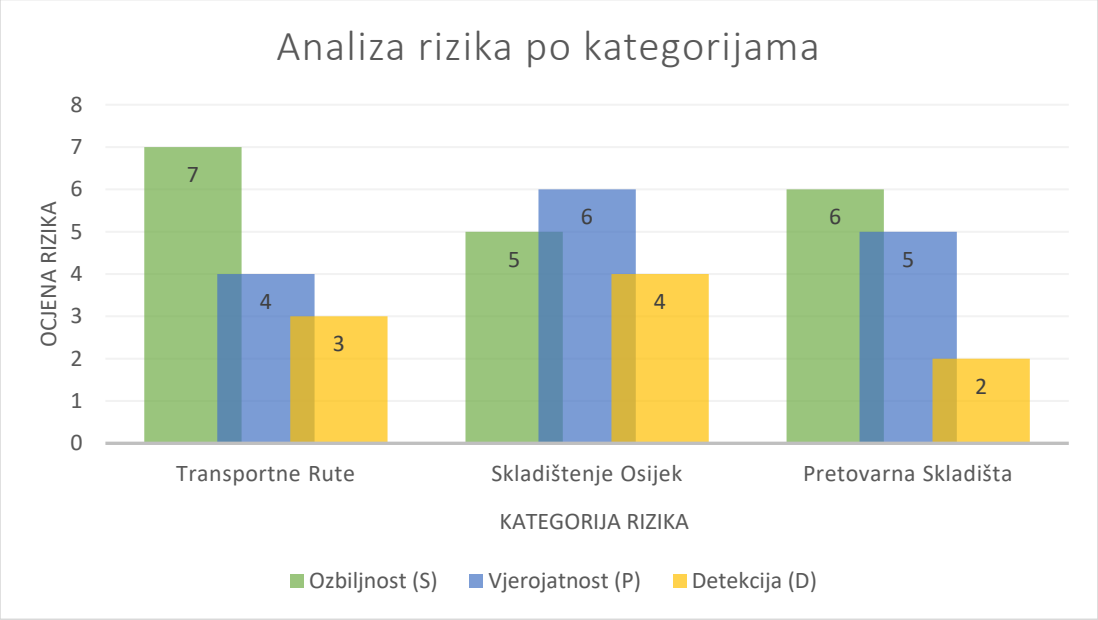
4.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Dodatni ulaz/otvor omogućava nesmetan prilaz i pokušaj provale u skladište od trećih osoba	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Skladište nema dodatnih ulaza niti prozora koji bi generirali dodatni rizik neovlaštenog ulaska trećih osoba.
5.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Ključ ili pristupna šifra elektronske brave lako su dobavljivi i dostupni nekontroliranom broju osoba	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Pristupne šifre elekronske brave zadužuje mali broj strogo definiranih korisnika. Svaki korisnik zadužuje kontroliranu jedinstvenu šifru preuzetu pod materijalnom i krivičnom odgovornošću.
6.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Skladište nije pod nadzorom djelatnika u dužem vremenskom razdoblju	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Djelatnici u skladište dolaze svakih nekoliko sati (4 do 5 sati) u razdobljima kada u skladištu postoji veća količina skladištene robe. Kada su frekvencije dolaska manje, vikendom i praznicima u skladištu boravi tek nekoliko proizvoda odnosno povrata.
7.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Obijena vanjska vrata omogućuju nesmetan ulaz u skladište	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Senzor pokreta na ulazu nakon 30 sekundi pali alarm. Ovlašteni korisnik unutar 30 sekundi po ulasku može isključiti pokretanje alarma. Osim zvučnog signala, dojavu o neovlaštenom pristupu zaprima i AKD zaštita, koja odmah zove korisnike odnosno izlazi na teren i dojavljuje policiji.

8.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Roba u skladištu stoji dugo i u velikim količinama	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Roba u skladištu stoji do nekoliko sati u velikim količinama, a ostatak dana u malim količinama (povrati, karantetne). U skladištu nema zaliha.
9.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Obijena vanjska vrata i isključen alarm omogućuju nesmetan ulaz u skladište i pristup pošiljkama / proizvodima	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Roba nije smještena odmah iza vanjskih vrata, već je unutar tog prostora smještena komora sa metalnim vratima pod ključem. Ključ se nalazi kod koordinatora.
10.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Prolaz ili prozor iz skladišta susjednih poslovnih subjekata omoghučavaju nesmetan ulazak u skladište trećim osobama	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Skladište nema dodatnih prolaza niti prozora prema susjednim poslovnim subjektima, koji bi generirali dodatni rizik neovlaštenog ulaska trećih osoba.
11.	Fizička i tehnička zaštita robe u skladištu Osijek	Pošiljke sigurne od otuđenja ili uništenja od strane trećih osoba	Djelatnici nisu educirani o načinu rada koji podrazumijeva odrade radnih aktivnosti sukladno procesima osiguranja skladišta kroz sve navedene sustave zaštite	Otuđenje ili uništenje pošiljki / proizvoda	5	2	1	**10**	Djelatnici su educirani o zahtjevanom načinu rada

8. ANALIZA RIZKA PO KATEGORIJAMA

Podaci prikupljeni iz ovih triju analiza pružaju sveobuhvatan uvid u različite aspekte sigurnosnih rizika unutar logističkog lanca distribucije lijekova za vodeću nacionalnu veledrogeriju u Hrvatskoj, Oktal Pharma d.o.o.. Oktal Pharma d.o.o. prisutna je na cijelom teritoriju Republike Hrvatske putem četiri centra koji se nalaze u Zagrebu, Osijeku, Rijeci i Dugopolju (Splitu), od čega su dva, ona u Zagrebu i Dugopolju, distribucijski skladišni centri. Kvalitetnom mrežom dostavnih ruta i optimalnim brojem dostavnih vozila osigurana je pokrivenost cijelog teritorija Hrvatske. Regionalnu pokrivenost u distribuciji Oktal Pharma osigurava internim transportnim kapacitetima i ugovornim partnerima s ukupno više od 70 vozila. Sva vozila opremljena su prema najvišim standardima izolacijom i sustavima grijanja i hlađenja, a za potrebe održavanja uvjeta transporta sukladnim onima za skladištenje. Kako bi se osiguralo kontinuirano praćenje kvalitete transporta, sva vozila opremljena su sustavima nadzora pozicije vozila i temperaturnih uvjeta u tovarnom prostoru putem GSM/GPS sustava. Optimalnim rasporedom voznog parka u više od 70 dostavnih ruta obuhvaćeno je više od 2800 dostavnih mjesta diljem Hrvatske s više isporuka unutar jednoga dana u većim gradovima.

Svaka analiza rizika doprinosi boljem razumijevanju specifičnih rizika u transportu, skladištenju i pretovarnim operacijama, omogućujući donošenje informiranih odluka o prioritetima i potrebnim korektivnim mjerama. Kroz analizu tih podataka, FMEA metodologija pruža temelj za kontinuirano unapređenje sigurnosti i pouzdanosti logističkih operacija.



Slika 9. Analiza rizika po ocjeni i kategoriji

Prikazan je grafikon koji uspoređuje ocjene rizika (ozbiljnost, vjerojatnost i detekcija) za tri ključne kategorije: transportne rute, skladištenje u Osijeku, i pretovarna skladišta. Grafikon vizualno prikazuje kako se različiti rizici ocjenjuju unutar svake od ovih kategorija, što može pomoći u identificiranju područja koja zahtijevaju najveću pažnju i implementaciju sigurnosnih mjera.

Transportne rute imaju najvišu ocjenu ozbiljnosti rizika, što znači da su incidenti na ovim rutama najopasniji. S obzirom na relativno nisku mogućnost otkrivanja problema (ocjena 3), potrebno je uložiti u napredne tehnologije praćenja i praćenje u stvarnom vremenu kako bi se smanjili potencijalni rizici.

Skladištenje u Osijeku pokazuje visoku vjerojatnost rizika (ocjena 6), što sugerira potrebu za poboljšanjem operativnih postupaka i sigurnosnih mjera unutar skladišta. Iako je ozbiljnost rizika manja nego kod transporta, činjenica da su incidenti češći zahtijeva dodatne preventivne mjere.

Pretovarna skladišta imaju nisku mogućnost detekcije (ocjena 2), što je zabrinjavajuće jer to znači da bi problemi mogli proći neopaženo sve dok ne prouzrokuju štetu. Poboljšanje nadzora i implementacija automatiziranih sustava detekcije ključni su za smanjenje ovih rizika.

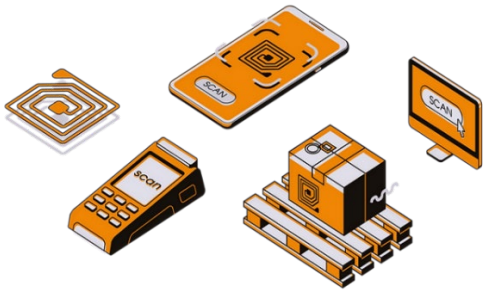
9. MJERE UNAPRJEĐENJA SIGURNOSTI PRIJEVOZA I LOGISTIČKIH PROCESA

Poboljšanje detekcije problema u logističkim procesima, posebno u kontekstu transporta i skladištenja lijekova, ključno je za smanjenje rizika i osiguranje sigurnosti proizvoda. U radu je navedeno nekoliko strategija koje se mogu primijeniti za poboljšanje detekcije problema uvođenje naprednih tehnologija praćenja i senzora, automatskih sustava za detekciju, poboljšanja procesa kontrole i održavanja.

9.1. RFID (Radio-Frequency Identification)

RFID (Radio Frequency Identification) je bežična i beskontaktna tehnologija koja koristi radiovalove za čitanje i razmjenjivanje informacija pohranjenih na oznaci ili naljepnici pričvršćenoj na predmetu. Oprema koja se koristi u svrhu označavanja i praćenja proizvoda mora biti prilagođena proizvodima i poslovanju te ne smije ometati redovni radni proces. Podaci mogu biti od serijskog broja do detaljnih podataka o proizvodu. Te se informacije bežično prenose u središnju bazu podataka gdje im se može lako pristupiti i upravljati. Praćenje proizvoda u stvarnom vremenu ključno je za učinkovito upravljanje opskrbnim lancem, s obzirom na to da pruža točan pregled stanja proizvoda time omogućuje donošenje boljih odluka u vezi s poslovanjem ili automatski upozoriti na potencijalne probleme.
Korištenjem RFID oznaka za praćenje pristupa osjetljivim područjima, može se osigurati visoka razina sigurnosti i kontrolu pristupa. Brza automatizirana evidencija i identifikacija osoblja i posjetitelja pomaže u prevenciji neautoriziranog pristupa. U kombinaciji s drugima sigurnosnim sustavima, RFID nudi slojevitu obranu koja znatno smanjuje rizike sa sigurnošću fizičkog i intelektualnog vlasništva.

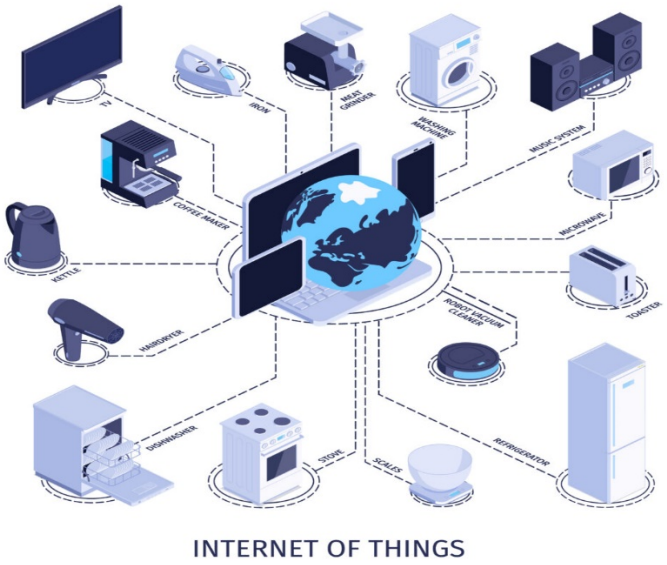
Glavne prednosti korištenja RFID tehnologije su to da ih možemo beskontaktno pročitati (čak i u slučajevima kada nisu izravno vidljivi), zaštita podataka (RFID karticu je nemoguće duplicirati), otpornost na ostale vanjske utjecaje te možemo upisivati informacije.



Slika 10. RFID tehnologija; Izvor: [12]

9.2. IoT SENZORI

IoT Senzor (Internet of Things) je uređaj koji prima i prati podražaj te odgovara električnim signalom. Podražaji mogu biti različiti parametri kao što su temperatura, vlažnost, vibracije, tlak unutar transportnih vozila i skladišta, svojstvo ili stanje koje se prima i pretvara u električni signal. Ako senzori otkriju anomalije koje bi mogle ugroziti sigurnost lijekova, automatski će poslati upozorenje upravljačkim sustavima.



Slika 11. IoT; Izvor: [13]

Kao i svi ostali aspekti tehnologije, tako i IoT ima svoje prednosti i nedostatke. Jedna od prednosti je svakako brzo i jednostavno prikupljanje informacija bez obzira na geografsku udaljenost s pomoću komunikacije preko mreže međusobno povezanih uređaja. IoT olakšava komunikaciju između uređaja i čini ju bržom, uz uštedu vremena i novca. Pored toga, automatiziranje zadataka koje uređaji moraju izvršiti, pomaže u poslovanju povećati kvalitete usluga i smanjenju razine ljudske intervencije.

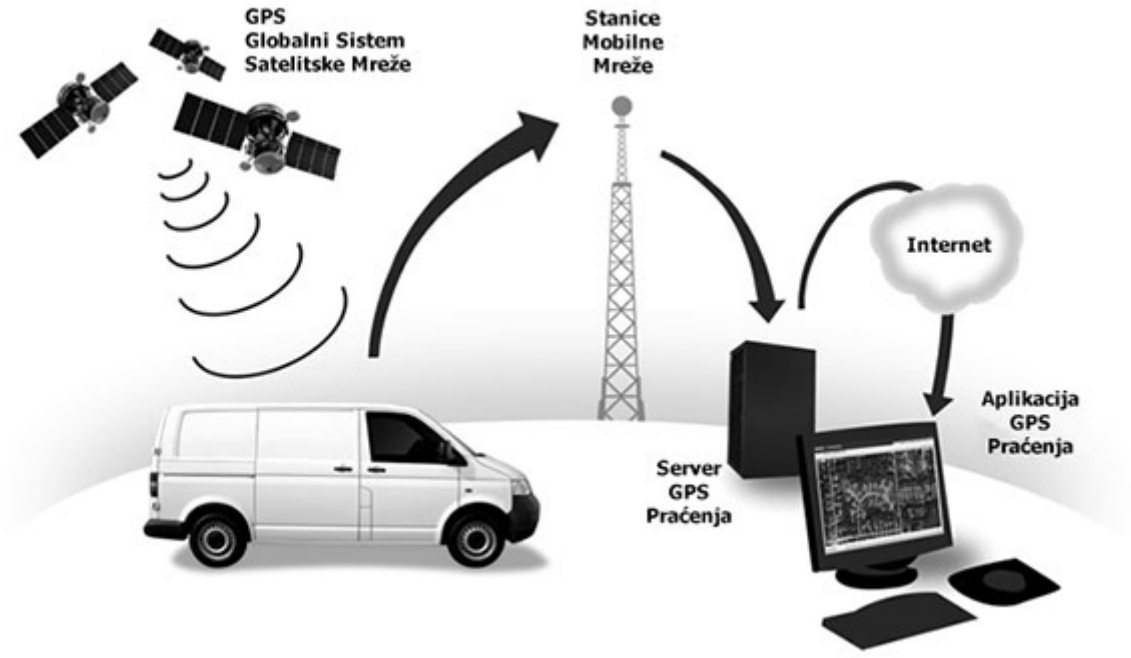
Danas se velika pažnja pridaje zaštiti privatnosti i "obrani" od hakerski napada. U kontekstu toga, IoT-u se može pronaći jedna povelika zamjerka. Budući da su uređaji spojeni na internet, postoji veliki rizik od "curenja" informacija koje bi mogle biti od velike važnosti. Odnosno, povjerljive informacije možda neće biti zaštićene i lako bi ih se moglo hakirati te u konačnici i zloupotrijebiti. Drugi veći nedostatak odnosi se na pitanje radnih mjesta. Automatizacija svakog zadataka sa sobom povlači i osjetan pad potrebe za ljudskim resursima što može imati i izravnog negativnog utjecaja na zapošljavanje ljudi.

9.3. GPS I GEOFENCING PRAĆENJE

Globalni sustav za pozicioniranje (GPS - **G**lobal **P**ositioning **S**ystem) satelitski je navigacijski sustav koji omogućuje praćenje točne lokacije transportnih vozila u realnom vremenu. GPS nam omogućuje optimizaciju ruta a da nije samo skraćivanje udaljenosti već radi se o pametnom planiranju kako bi se maksimalno iskoristili resursi, smanjili troškovi i povećala brzina dostave.

Geofencing (geografsko ograničenje) je tehnologija koja omogućuje kreiranje virtualnih granica na geografskim kartama, a koristi se za praćenje ulaska ili izlaska vozila iz određenih zona. Ova funkcija se primjenjuje u različitim industrijama, od logistike do graditeljstva, gdje se može koristiti za osiguranje da vozila i oprema ne napuštaju definiranu rutu. Implementacijom geofencinga, poduzeća mogu automatski primiti obavijesti kada vozilo napusti predodređeno područje, što može pomoći u prevenciji krađe ili neautorizirane uporabe vozila. Također, geofencing može pomoći u optimizaciji logističkih operacija ograničavanjem ruta koje vozači mogu koristiti, što dovodi do smanjenja troškova goriva i povećanja sigurnosti.

Kombinacija GPS-a i geofencinga je odlično rješenje za pregled čitave flote vozila te vozače. Može automatski upozoriti na neovlašteno skretanje s rute ili duže zadržavanje.



Slika 12. GPS sustav; Izvor: [14]

9.4. AUTOMATIZIRANI SUSTAVI ZA OTKRIVANJE KVAROVA

Automatizirani sustavi za otkrivanje kvarova (FDD - Fault Detection and Diagnosis) su sustavi koji se koristi za otkrivanje i dijagnosticiranje grešaka u sistemima ili procesima. Koriste algoritme za analizu podataka iz različitih senzora i mogu automatski otkriti nepravilnosti u operacijama. Sustav identificira uzrok nepravilnosti, te predlaže korake za njihovo otklanjanje.

Ako sustav detektira anomaliju, on može pokrenuti automatske postupke korektivnih mjera ili obavijestiti nadležnog operatera korištenjem različitih tehnologija i metoda za poboljšanje efikasnosti, sigurnosti, i pouzdanosti operacija. Sustav obuhvaća dva osnovna koraka:

1. **Otkrivanje greške**: Ovo je proces identifikacije da se u sistemu nešto ne odvija kako treba, tj. da postoji neka greška ili nepravilnost u radu. Ovaj korak se zasniva na praćenju izlaznih signala, stanja sistema ili performansi, te usporedba s očekivanim ili nominalnim vrijednostima.
2. **Dijagnosticiranje greške**: Nakon što se greška otkrije, potrebno je identificirati njen uzrok. To uključuje analiziranje podataka i upotrebu metoda kako bi se utvrdilo gdje je točno došlo do problema i što ga je izazvalo.

9.5. POBOLJŠANJE PROCESA KONTROLE, ODRŽAVANJA TE OBUKE DJELATNIKA

Poboljšanje procesa kontrole, održavanja i obuke djelatnika je ključno za osiguranje efikasnosti, pouzdanosti i sigurnosti u organizacijama. Sve komponente međusobno su povezane i njihovo unapređenje može dovesti do značajnih ušteda, smanjenja zastoja, poboljšanja kvaliteta i povećanja zadovoljstva zaposlenih. Proces kontrole kroz redovite i standardizirane inspekcije transportnih vozila i skladišta omogućuje kontinuirani nadzor, brže otkrivanje odstupanja i pravovremenu intervenciju. Ove kontrole mogu uključivati provjere stanja opreme, ispravnost senzora i integritet sigurnosnih sustava. Preventivno održavanje se temelji na praćenju stanja opreme kako bi se izbjegli neočekivani kvarovi, odnosno omogućuje pravovremene popravke, čime se smanjuje rizik od neočekivanih problema. To uključuje redovite preglede i zamjenu kritičnih dijelova prije nego što se pojave neželjeni događaji koristeći podatke iz IoT senzora i algoritama. Također, redovita edukacija i razvoj zaposlenika o korištenju novih tehnologija i automatiziranih sustava, pomažu pri učinkovitom otkrivanje problema te simulacije i vježbe kriznih situacija kako bi zaposlenici bili spremni prepoznati i reagirati na probleme što je brže moguće. To može uključivati redovne

seminare, radionice te tečajeve radi kontinuiranog učenja unutar organizacije gdje se to znanje i vještine smatraju ključnim za profesionalni razvoj. Povezivanje kontrole, održavanja i obuke kroz sustav upravljanja omogućava organizaciji da holistički pristupi poboljšanju poslovanja. Kao primjer, podaci iz sustava za kontrolu mogu ukazivati na područja koja zahtijevaju dodatnu obuku zaposlenika, dok redovito održavanje može smanjiti potrebu za hitnim intervencijama i smanjiti pritisak na zaposlenike.

9.6. IMPLEMENTACIJA SUSTAVA ZA UPRAVLJANJE RIZICIMA

Implementacija integriranog sustava za upravljanje rizicima koji prikuplja podatke iz različitih izvora (senzori, praćenje, povratne informacije od zaposlenika i dr.) može pomoći u centralizaciji i analizi podataka, čime se poboljšava identifikacija i prioritizacija rizika.

Definiranje ključnih pokazatelja performansi KPI (Key Performance Indicators) koji su specifični za detekciju problema. Pratit ove indikatore redovito kako bi se identificirale potencijalne slabosti u detekciji. Ključni pokazatelji uspješnosti (Key Performance Indicators-KPI) pomažu organizaciji definirati i mjeriti napredak prema postavljenim organizacijskim ciljevima. Za učinkovito mjerenje ključnih pokazatelja uspješnosti neophodno je postavljanje poslovnih ciljeva. Ciljevi poslovanja moraju biti specifični, mjerljivi, ostvarivi, svrsishodni i vremenski određeni. Kada su ciljevi postavljeni na navedeni način moguće je pratiti uspješnost njihovog postizanja.

Integrirani sustavi upravljanja rizicima predstavljaju pristup kojim se kombiniraju različiti sustavi unutar organizacije u jedan sveobuhvatan sustav. Ovaj pristup omogućuje organizacijama da ujedine svoje procese, politike i prakse upravljanja rizicima kako bi poboljšali svoje poslovanje na različitim područjima te izbjegli neželjenje događaje. Glavni cilj integriranih sustava upravljanja je stvaranje učinkovitijeg, ujednačenijeg i sveobuhvatnijeg pristupa vođenju organizacije.

Prednosti integriranih sustava upravljanja uključuju:

1. Smanjenje dupliranja: Integracija različitih sustava upravljanja omogućuje eliminiranje duplih aktivnosti i procesa, što smanjuje troškove i olakšava rad.
2. Povećana učinkovitost: Integracija omogućuje organizaciji da ujedini svoje procese, resurse i prakse, što dovodi do povećane učinkovitosti i produktivnosti.
3. Smanjenje kompleksnosti: Umjesto da se suočava s više različitih sustava upravljanja, organizacija ima jedan sveobuhvatan sustav koji olakšava vođenje i upravljanje.

4. Bolje upravljanje rizicima: Integrirani sustavi omogućuju organizacijama bolje upravljanje rizicima na različitim područjima poslovanja, kao što su kvaliteta, okoliš, sigurnost, itd.
5. Povećana transparentnost: Integrirani sustavi olakšavaju praćenje i izvještavanje o performansama organizacije na različitim područjima, što povećava transparentnost i odgovornost.

U konačnici, integrirani sustavi upravljanja pružaju organizacijama mogućnost da postignu sveobuhvatno vođenje poslovanja, poboljšaju svoju konkurentnost i osiguraju usklađenost s regulatornim zahtjevima i standardima.

9.7. POBOŠANJE KOMUNIKACIJE I SURADNJE UZ UPOTREBU SOFTVERSKIH PLATFORMI

U suvremenom poslovnom okruženju, organizacije se suočavaju s izazovima koji zahtijevaju učinkovito upravljanje, usklađivanje i suradnju među zaposlenicima i odjelima. Ključ za postizanje ovih ciljeva leži u kvalitetnoj komunikaciji unutar organizacije putem raznih komunikacijskih kanala.

Korištenje platforme za suradnju kroz komunikacijske kanale je neizostavni temelj organizacijske dinamike, jer omogućuje razmjenu informacija, ideja i ciljeva te stvara sinergiju među članovima tima i automatski dijeljenje informacija o mogućnosti i identifikaciji rizika.

Poslovna komunikacija svoj temelj ima u informacijama, no potrebno je napomenuti da informacije ne predstavljaju sinonim za podatke. Naime, podaci su činjenice i brojke, a podatke prikupljamo putem svih komunikacijskih alata s kojima organizacija komunicira i prikuplja podatke.

Zato usklađivanjem komunikacijskih kanala postiže se da svi dijelovi lanca opskrbe, uključujući transportne operatere i skladišne radnike, koriste standardizirane komunikacijske alate i protokole za prijavu problema.

10. ZAKLJUČAK

Sigurna distribucija farmaceutskih proizvoda od presudne je važnosti za očuvanje njihovih kvaliteta i efikasnosti, te posljedično, za osiguranje zdravlja pacijenata. Distribucija predstavlja jednu od najkritičnijih faza u farmaceutskom lancu opskrbe, s obzirom na specifične zahtjeve koji se odnose na sigurnost i kvalitetu proizvoda. Farmaceutska industrija podliježe strogim regulativama, a najmanji propust u transportu može dovesti do ozbiljnih posljedica, uključujući degradaciju lijekova i ugrožavanje zdravlja pacijenata. Upravo zbog toga, analiza sigurnosnih rizika u prijevozu lijekova predstavlja ključno područje istraživanja koje može značajno doprinijeti poboljšanju prakse u industriji.

Kroz ovaj diplomski rad, obavljena je sveobuhvatna analiza sigurnosnih rizika u distribuciji lijekova, s posebnim fokusom na identifikaciju i evaluaciju ključnih prijetnji. Analize su pokazale da su temperaturne varijacije, kašnjenja u isporuci i nepravilno rukovanje lijekovima najveći rizici u transportnom procesu. Upravljanje rizicima, kroz primjenu naprednih analitičkih metoda i integraciju sustava kvalitete, pokazalo se ključnim za osiguranje sigurnog i efikasnog transporta.

Zaključci ovog rada ukazuju na potrebu za daljnjim unapređenjem sigurnosnih protokola, posebno u smislu uvođenja novih tehnologija za nadzor i automatizaciju. Preporučuju se redovito unapređenje sigurnosnih protokola i praćenja u realnom vremenu, kao i poboljšanja u edukaciji osoblja koje je uključeno u lanac opskrbe. Primjena predloženih mjera može značajno doprinijeti smanjenju rizika i osigurati veću sigurnost u cijelom lancu opskrbe.

Ovaj rad doprinosi boljem razumijevanju kompleksnosti sigurnosnih rizika u transportu lijekova i nudi smjernice za njihovo efikasno upravljanje. Implementacija predloženih mjera mogla bi značajno smanjiti rizik od ugrožavanja kvalitete lijekova tijekom transporta i osigurati sigurniju isporuku zdravstvenih proizvoda krajnjim korisnicima.

11. LITERATURA

1. Andrijanić, I.; Gregurek, M.; Merkaš, Z.(2016.) Upravljanje poslovnim rizicima. Zagreb; [2]

2. Drago Pavić (2012). Pomorsko osiguranje pravo i praksa s osnovama kopnenog i zračnog transportnog osiguranja. Split; [6]

3. Mesarić, J, Dujak, D (2009.), SCM u trgovini na malo – poslovni pocesi i ICT rješenja [3]

4. Ministarstvo financija Republike Hrvatske (2017.) Smjernice za upravljanje rizicima u poslovanju institucija javnog. Zagreb; [4]

5. Ministarstvo zdravlja (2013.) Pravilnik o dobroj praksi u prometu lijekova, davanju dozvola za promet na veliko lijekovima, davanju dozvola za posredovanje lijekovima i davanju potvrde o dobroj praksi u prometu lijekovima na veliko; [1]

6. Škorput P., (2021.) Računalna sigurnost, Fakultet prometnih znanosti, Aurorizirana predavanja. Zagreb; [8]

7. Danijela Miloš Sporčić, Julija Puškar; Ivana Zec (2019.) Primjena modela integriranog upravljanja rizicima – Zbirka poslovnih slučajeva (Ekonomski fakultet – Zagreb);

8. Zoran Vučinić (2019.) Procjena rizika. Veleučilište u Karlovcu;

9. Josip Kereta (2021.) Upravljanje rizicima: priručnik za studente. Baltazar – Zaprešić;

10. Škola za cestovni promet, Zagreb, Program za obrazovanja odraslih [7]

11. CARNet (2003.) Upravljanje sigurnosnim rizicima; [11]

12.https://www.poslovnaucinkovitost.hr/kolumne/poslovanje/djelotvorno-upravljanje-rizicima (06.02.2023.) [5]

13. www.pempal.org (21.07.2024.) [9]

14.https://copymate.app/hr/blog/multi/planiranje-resursa-poduzeca-najbolje-prakse-upravljanja-resursima/ (21.07.2024) [10]

15. https://www.tagnology.com/was-ist-rfid?lang=hr (01.09.2024.) [12]

16.https://rolify.com/vjestine-buducnosti/digitalne-vjestine-i-tehnologija/sta-je-iot-internet-of-things-ili-internet-stvari/ (01.09.2024.) [13]

17. https://hr.europetracking.com/HR/hr/sel/gps/tracking (01.09.2024.) [14]

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad
(*vrsta rada*)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom **Analiza sigurnosnih rizika prijevoza lijekova** , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 17.09.2024.

Martina Bibić, Martina Bibić
(ime i prezime, *potpis*)