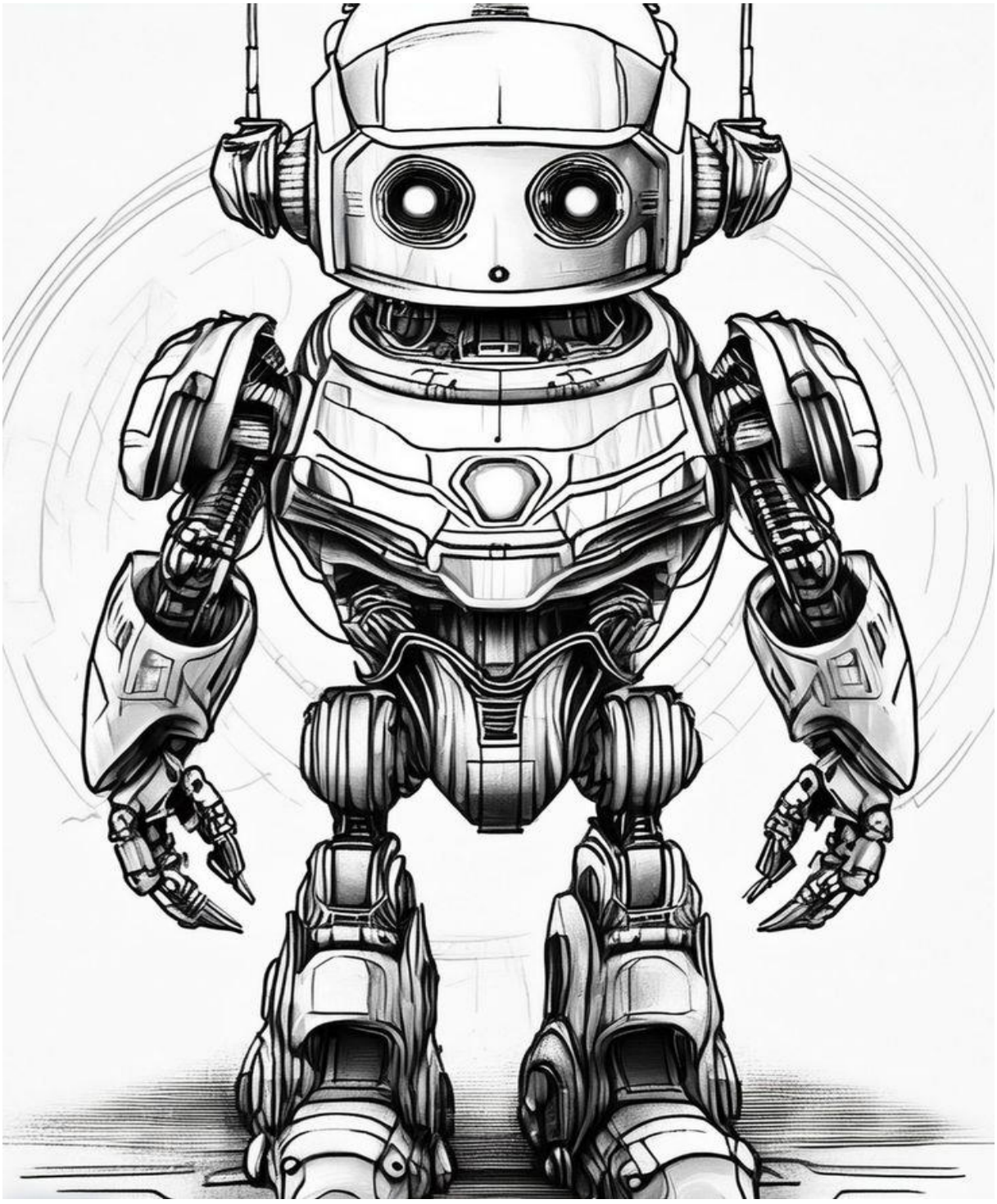
РЪКОВОДСТВО ПО ЗБУТ



Проф. д-р Емил Влайков Воденичаров, дм

2024

БЕЗОПАСНОСТ НА РАБОТНИТЕ УСЛОВИЯ В СРЕДА НА БЪРЗО-РАЗВИВАЩИТЕ СЕ МОДЕРНИ ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

2024

СЪДЪРЖАНИЕ

БЕЗОПАСНОСТ НА РАБОТНИТЕ УСЛОВИЯ В СРЕДА НА БЪРЗО-РАЗВИВАЩИТЕ СЕ МОДЕРНИ ИНФОРМАЦИОННИ ТЕХНОЛОГИИ

Въведение и обхват.

Цел: Описване на важността на стандартите за безопасност за служители, работещи с модерните технологии.

Обхват: Определяне на средите и технологиите, към които се отнасят насоките, като офиси, домашни работни места, дистанционна работа и промишлени среди с AI-управлявани машини.

Работата в офиса е разнообразна, като работните места варират от такива, които изискват високо ниво на умения и познания (например журналисти и финансови администратори), до такива, при които работникът има малък контрол върху работата си или организацията на работния си ден, като обаждане център и работа по обработка на данни. Въпреки че се считат широко за среди с нисък риск, големият (и нарастващ) дял на служителите в рамките на ЕС, които работят в офис среда, означава, че значителен брой работници са потенциално изложени на всякакви рискове за тяхното здраве, които могат да възникнат.

В съвременния офис голяма част от фокуса по отношение на рисковете за здравето са свързани с използването на компютри под някаква форма. Въпреки това е важно да се признае, че компютрите не са единственият потенциален източник на риск. Някои здравословни проблеми произтичат от основно заседналия характер на много офис-базирани работни места (независимо дали се използва компютър или не); докато документите и хартиите могат да бъдат тежки (особено в насипно състояние) и могат да доведат до рискове при ръчно боравене (особено в комбинация с продължително седене и обща липса на движение).

Много работни места в офиса стават все по-зависими от използването на компютри или не биха съществували в сегашната си форма без появата на такива компютърни системи. Компютрите са заменили почти изцяло пишещите машини за всяка работа, включваща създаване или редактиране на текст (доклади, писма и т.н.) и са трансформирали комуникационните системи чрез разработки като имейл и незабавни съобщения (SMS, Messenger apps). Освен че промени начина, по който се създават текст и други материали, това промени и работните места. Въпреки това обаче, често служителите не преминават специфични обучения за безопасност на работа. В по-нататъшното технологично развитие, появата на преносими системи като лаптопи, а през последните години смартфони и таблети, създаде допълнителни промени не само във физическия начин, по който се използват такива устройства, но и в мястото, където се използват, преместване на „компютърната работа“ от офиса в кафенето, хотела, влака, дома и много други места. Има все повече нарастващи опасения, че подобни промени водят до размиване на разликата между работа и не работа с потенциално отрицателно въздействие върху „баланса между работата и личния живот“. Дори и при по-конвенционалните компютри, технологичното развитие означава, че вече не е необходимо служителят да бъде в централизиран физически офис, а развитието на „дистанционната работа“ позволява на служителите да работят на отдалечени места (включително дома си). Дистанционната работа предоставя разнообразие от нови предизвикателства, не само по отношение на комуникацията и начина, по който тази работа е организирана, но работата далеч от централизирани, контролирани помещения прави по-трудно за работодателя да гарантира, че на дистанционния работник е осигурено безопасно и здравословно работно място, в което да работят.

Като допълнително усложнение нарастващото използване на компютърни технологии в офиса е успоредно с нарастването на

използването им у дома. Започвайки с „домашните компютри“, това сега се разшири до много от същия набор от смарт устройства, които се използват в работна среда.

Това доведе до две основни последици. Първо, това увеличи степента на „излагане“ на лицата на някои от физическите рискове, свързани с използването на тези технологии, и второ, това развитие доведе до това, че някои власти се стремят да освободят работодателите от всякакви неблагоприятни последици поради опитът им да припишат последствията от използването на технологиите като вина на самия служител, а не като липса на контрол и изпълнение на насоките по ЗБУТ и европейските нормативи.

Кампанията „Здравословни работни места“ за периода 2023—2025 година има за цел да повиши осведомеността относно въздействието на новите цифрови технологии върху работата и работните места и свързаните с тях предизвикателства и възможности в областта на безопасността и здравето при работа (БЗР). Съгласно подхода за „Нулева смъртност“ към свързаните с работата смъртни случаи в Стратегическата рамка на ЕС за здравословни и безопасни условия на труд за периода 2021—2027 година, както и целите на европейската стратегия в областта на цифровите технологии, кампанията се стреми да включи БЗР в по-широкообхватния дебат за политиките на ЕС и взема под внимание свързаното с пола измерение, както и потребностите на специфични групи, работещи при повишен риск. Кампанията се определя от пет приоритетни области:

1) Работата през цифрови платформи
2) Усъвършенствана роботика и изкуствен интелект
3) Дистанционна работа
4) Умни цифрови системи
5) Управление на работещите чрез изкуствен интелект

Развитието на цифровите технологии намират все повече приложения в трудовата дейност. Компютрите и машинното обработване на информацията чрез програми и извършване на аритметични логически действия дават възможност не само за получаване на множество сведения, но и за вземане на бързи решения. Електронните прибори могат да заместват човека в редица области: статистически сведения, наблюдение и контрол, което позволява все по-високо ниво на автоматично функциониране. Приносът на електрониката позволява човекът да се замени с робот, което предполага наличието на информация и произтичат термините автоматизация, или информатизация, или роботизация. Според литературата на EU-OSHA базираните на AI системи са интелигентни машини, които събират и анализират данни, за да правят прогнози и решения, така че да могат да постигнат конкретни цели. Системите, базирани на AI, са много гъвкав и широко разпространен в различни сектори: здравеопазване и медицинска диагностика, образование или грижи за възрастни хора, поддръжка на клиенти (чатботове), както и маркетингови, бизнес анализи или финансови съвети. Усъвършенстваната роботика (включена в системи, базирани на AI) може да се опише като сложни системи способни да изпълняват сложни задачи самостоятелно или да работят заедно с хора. Някои примери за това са мобилни роботи, роботи за сглобяване и екзоскелетни роботи. Констатациите от проучването OSH Pulse разкриват, че използването на усъвършенствана роботика и AI на работното място все още не е много разпространена в сравнение с други технологии (т. е. персонални компютри), тъй като приблизително 5% от анкетираните съобщават, че използват машини или роботи, включващи AI, докато само 3% използват роботи, взаимодействащи с работника (коботи). Констатациите са много подобни на докладваните от Евростат проучване (Urzì Brancati, Curtarelli, Riso, & Baiocco, 2022), обаче, тъй като технологиите са се очаква да се разпространи още повече в бъдеще, също и в резултат на включването

на по-напреднали технологии в „по-старите“ (напр. AI в персонални компютри или таблети), разбирайки потенциалните рискове, които носенето е от решаващо значение. Предимствата от приемането на такива технологии в работна среда са добре известни: усъвършенствана роботика системите са в състояние да изпълняват задачи по-ефективно, с по-висока прецизност и издръжливост и предлагат хората по-безопасни условия, като поемат по-опасните задачи. AI и анализите на данни също могат да бъдат използвани за подобряване на ефективността на инспекциите за БЗР (EU-OSHA, 2019d). Въвеждането на такива обаче технологиите също могат да представляват рискове за работниците, които могат да бъдат физически, организационни и психосоциални (EU-OSHA, 2022a; EU-OSHA, 2019c). Например, въвеждането на усъвършенствани роботизирани системи може създават ергономични проблеми, ако хората и роботите споделят пространство, което не е предназначено за хора, което може следователно трябва да работят в неудобни или неудобни позиции; споделянето на пространство с робот също може увеличават риска от инциденти и сблъсъци. От организационна гледна точка въвеждането на усъвършенстваната роботика и AI могат да повлияят на комуникацията, киберсигурността и практиките за повишаване/преквалификация. И накрая, въвеждането на усъвършенствана роботика и AI системи може да доведе до редица психосоциални проблеми рискове, включително страх от загуба на работа, повишено натоварване, липса на доверие, загуба на автономност, загуба на неприкосновеност на личния живот и повишена изолация. EU-OSHA публикува три основни доклада за въздействието на съвременната роботика и изкуствената работа върху БЗР интелигентност, а именно „Усъвършенствана роботика и автоматизация: последици за безопасността и здравето при работа“ (EU-OSHA, 2022a), „Усъвършенствана роботика, изкуствен интелект и автоматизация на задачи: дефиниции, употреби, политики и стратегии и безопасност и здраве при работа“ (EU-OSHA, 2022b) и „Когнитивна

автоматизация: последици за безопасността и здравето при работа“ (EU-OSHA, 2022c). EU-OSHA също публикувани 11 кратки политики (EU-OSHA, 2022e; EU-OSHA, 2023bb; EU-OSHA, 2022d; EU-OSHA, 2023a; EU-OSHA, 2023cc; EU-OSHA, 2023ff; EU-OSHA, 2023hh; EU-OSHA, 2022w; EU-OSHA, 2022k; EUOSHA, 2022cc).

Общи принципи на безопасност. Ергономия и здраве при работа с технологии.

Рисковете, произхождащи от въздействието на ергономичните фактори на работната среда, са разпространени в сектори от различни дялове на икономиката и свързани с изпълнение на репетативни действия, скорост на работа и статично натоварване, работа с големи групи от хора, като причинители на стрес: „стоене прав или вървене”; „повтарящи се движения с ръцете;” „работа директно с хора, които не са служители на фирмата, като напр. клиенти, пътници, ученици, пациенти и др.”; „работа с кратки срокове”. Разпространението на риска от стоенето прав или вървенето почти през цялото време в икономическите сектори е далеч по-широко в сравнение с други индикатори за ергономичните фактори включващи „повдигане или придвижване на хора”; „носене/придвижване на тежки товари”. Работата в – хотелиерство и ресторантьорство, образование, строителство и преработваща промишленост в най-голяма степен включва стоене прав или вървене. За наетите в сектори преработваща промишленост и хотелиерство и ресторантьорство, както и за офисните работници работещи и попълващи големи масиви от данни може да се отчете значима стойност на влияние на фактора „повтарящи се движения с ръцете почти през цялото време”. По отношение на ергономичните фактори най-значимо отрицателно влияние има в сектор хотелиерство и ресторантьорство, преработваща промишленост, строителство. Наличието на значимо отрицателно влияние на два ергономични фактора се отчитат в добивна промишленост, образование, хуманно здравеопазване и социална

работа, държавно управление, финансови и застрахователни дейности и създаване и разпространение на информация и творчески продукти, далекосъобщения. За секторите административни и спомагателни дейности се отчита значимо влияние на един рисков фактор от групата на ергономичните фактори. В условията на роботизация и дигитализация на съвременната промишленост не малка част от теми рискови фактори ще бъдат избегнати с въвеждане на дистанционно управлявани апарати (роботи), който да извършват тежката физическа работа под контрола и супервизията на човек.

Почти независимо от това как работи един офис служител, нараства признанието за важната роля на движението за поддържане на мускулно-скелетното здраве и че оставането в по същество фиксирана поза за продължителни периоди не е благоприятно за добро здраве. Когато тази поза включва седене, тогава всяко въздействие на липсата на движение се влошава от факта, че заседналата поза е фундаментално вредна за гърба и повишава рискът от развитие на дълбока венозна тромбоза (ДВТ) от продължителни заседнали пози. Очевидно начинът, по който един служител седи и работи (включително позата, която приема при взаимодействие с компютърните си системи), може да усложни ефекта от заседналия характер на тяхната работа. Продължителните неправилни пози, особено неудобните позиции на крайниците и шията, произтичащи от недостатъчно внимание, отделено на разположението на офис оборудването, като екрани, клавиатури и други устройства за въвеждане, ще ускорят или изострят развитието на мускулно-скелетни симптоми (МСС). Симптомите включват болка, подуване, изтръпване и могат да доведат до затруднено движение или дълготрайна инвалидност, ако не се предприемат действия. Особено чести са усложненията в следствие на повтарящи се движения. Различните държави и власти използват редица различни термини, за да опишат МСС. Те включват кумулативни травми, нарушения на горните крайници и повтарящи се наранявания (RSI). Някои източници също използват

последния термин като „диагноза“ (макар и без клинична дефиниция), която прилагат към неспецифични симптоми. Без значение на термина, те обхващат състояния със специфични медицински диагнози (напр. замръзнало рамо, синдром на карпалния тунел (CTS)) и други, при които има болка без специфични симптоми. Болките във врата, горните крайници и гърба са от особено значение за офис служителите предвид повтарящия се, статичен и интензивен характер на тяхната работа.

Въпреки че няма съмнение, че работата в офиса, включваща използването на компютри, може да провокира симптоми или да изостри съществуващи МСС, има известен въпрос относно степента, в която такава работа ги причинява директно и кога има провокиране на симптоми на съществуващи разстройства (като изглежда такъв е случаят с CTS).

Основни насоки за предотвратяване на напрежение и наранявания при продължителна работа с компютри, и техника могат да се открият в съответствие със стандартите за ергономия на работния процес:

- БДС 15262-81 *„Единна система по ергономия. Работно място при извършване на работа прав. Общи ергономични изисквания“* - Стандартът се отнася за общите ергономични изисквания към работните места при извършване на работа прав, които трябва да се прилагат при проектиране на ново и модернизиране на съществуващо оборудване и производствени процеси.
- БДС 15371-81 *„Единна система по ергономия. Ергономични данни за проектиране. Максимални работни зони на ръцете в седяща поза“* - Стандартът определя максималните работни зони на ръцете на мъже и жени или само на жени в седяща работна поза, които трябва да се използват при проектиране на машини, съоръжения, работни места и др.

Двата стандарта са актуализирани към 02.04.2024 година. Тези стандарти обаче не покриват работата с преносими нефиксирани устройства, а в днешно време се изисква специално внимание към

използването на лаптопи, тъй като все по-голям брой работници използват този тип компютри през целия ден. Дизайнът на лаптопите не е съобразен с основното ергономично изискване за компютрите да имат отделна клавиатура и екран. В резултат на това, ако клавиатурата е в оптимална позиция за потребителя, екранът не е, а ако позицията на екрана е оптимална, клавиатурата не е. Използването само на лаптопи може да доведе до повишен риск от мускулно-скелетен дискомфорт, особено във врата и китките, в сравнение с нормален настолен компютър, поради позите, които обикновено се приемат.

Където е възможно да се направи това и продължителността на употреба го гарантира (кратките употреби от по-малко от 20-30 минути е малко вероятно да доведат до проблеми), препоръчително е да използвате поне отделна клавиатура, позволяваща на екрана на лаптопа да бъде повдигнати. Когато работните задачи включват интензивно използване на показалеца, тогава се препоръчва също и отделна мишка или друго посочващо устройство. Налични са много леки преносими примери на клавиатури и мишки (включително безжични модели), които могат да улеснят подобни мерки. В относително статични среди използването на докинг станция може да бъде от полза, позволявайки на периферните устройства да останат свързани. Когато такива мерки не са възможни (може би когато потребителят работи далеч от обичайното си работно място), тогава става важно да се подчертае важността на почивките и промените в дейността.

Една мярка, възприета в много съвременни офиси, е концепцията за споделеното работно бюро, при което работниците нямат лична работна станция, а споделят такава с други работници. Отново продължителността на употреба е критична, но когато дадено лице трябва да използва такава работна станция за продължителни периоди, тогава става важно характеристиките на работната станция (като екрана на дисплея, стола и

височината на бюрото) да се регулират лесно и бързо, за да отговарят на желанието на индивида да го използвате и трябва да се постави още по-силен акцент от нормалното върху информацията и обучението, за да се гарантира, че работниците са наясно с позата, която трябва да постигнат, и са достатъчно мотивирани да отделят няколко минути, за да направят необходимото корекции.

Независимо колко добра е работната позиция, продължителните статични пози не са здравословни. По този начин работната дейност трябва да позволява паузи и микропаузи, по време на които работниците могат:

• Сменят често работната си поза, като правят малки корекции на стола или облегалката;

• Изпълняване на различни задачи, като картотекиране;

• Изправяне и разходки.

Физическото разнообразие и редовните почивки от компютъра през работния ден ще помогнат за отпускане на мускулите. Изпълнението на упражнения и разтягания също ще помогне за възстановяване на тялото и ума. Такива процедури увеличават производителността и намаляват дискомфорта и оплакванията сред компютърните потребители и минимизират рисковете, свързани с използването на компютър.

Осветлението на работното място е друг водещ фактор за адекватния микроклимат и добрите условия на труд. LED светлините стават все по-популярни през последните години поради тяхната енергийна ефективност, дълъг живот и способността да произвеждат различни цветове. Въпреки това, има нарастваща загриженост относно потенциалните рискове за здравето, свързани с интензивната синя светлина, излъчвана от LED диодите използвани за осветление и вложени в редица съвременни екрани (OLED, QLED, т. н.).

В научната литература има широко разпространен консенсус, че работата с компютри не причинява никакви увреждания на очите или

зрението. Въпреки че продължителната подробна зрителна работа може да доведе до зрителен дискомфорт и преходни симптоми като тези, свързани например с изсушаване на очите(синдрома на сухата зеница), няма надеждни доказателства в подкрепа на предположението, че такава работа действително уврежда зрението. В базирано в Обединеното кралство проучване на над 1500 компютърни потребители, Melrose et al (2006) установяват, че нивото на докладваните очни симптоми не се различава от нивата, докладвани в проучвания, базирани на населението. Това предполага, че няма конкретна връзка между работата в офис и зрителните проблеми, водеща до по-висока честота на такива проблеми. Временни или преходни симптоми като главоболие и уморени, зачервени или възпалени очи могат да бъдат причинени от продължително концентриране върху екрана на дисплея, лошо позициониране на компютъра, трептене на екрани, неадекватно осветление, отблясъци и отражение или лоша четливост на хартията или екранни документи. Обобщено нарушенията могат да се разделят на:

1. Нарушени цикли на сън: Синята светлина потиска производството на мелатонин, хормон, който регулира циклите на сън и събуждане. Излагането на синя светлина преди лягане може да затрудни заспиването и запазването на съня, което води до безсъние и други нарушения, свързани със съня.

2. Синдром на компютърното зрение: Прекарването на дълги часове пред екран с интензивна синя светлина може да причини синдром на компютърното зрение, който включва симптоми като напрежение в очите, сухота, замъглено зрение и главоболие.

Начини да се предпазим от синя светлина:

1. Използваме LED светлини с ниска емисия на синя светлина: като например LED крушки с топла бяла цветова температура.

2. Очила, блокиращи синята светлина, са специално проектирани да филтрират синята светлина, което улеснява използването на екраните преди лягане и намалява риска от компютърен зрителен синдром.

3. Приложения за филтриране на синя светлина: Някои смартфони и компютри се доставят с приложение за филтриране на синя светлина, което може да се използва за намаляване на количеството синя светлина, излъчвана от екрана.

4. Почивка от екраните по правилото 20-20-20, което предполага да си прави почивка от 20 секунди на всеки 20 минути, гледайки нещо на 20 фута разстояние. Това може да помогне за намаляване на напрежението на очите и други симптоми на синдрома на компютърното зрение.

5. Използване на протектор за екран, блокиращ синя светлина: Тези протектори за екран могат да се инсталират на екрана на смартфон, таблет или компютър, за да се намали количеството синя светлина, излъчвана от екрана.

Въпреки че LED светлините имат много предимства, важно е да сме наясно с потенциалните рискове за здравето, свързани с интензивната синя светлина. Като се вземат необходимите предпазни мерки и се предпазим от синя светлина, можем да ползваме предимствата на LED осветлението, без да компрометираме здравето си.

Все по-важен рисков фактор е и завишената температура през летния период – голям брой работещи в едно помещение при липсваща или **неефективно работеща вентилационна система** в сектори като финанси, информационна поддръжка, банково дело и образование. Не са редки случаите на недостатъчна осветеност, предимно при ползване на светлинни източници с нажежаема жичка в сектори образование и култура. Липсваща или некомпетентна **поддръжка на електросъоръжения и инсталации**, особено в обществената сфера и малките и средни предприятия, водеща до завишен риск от електро поражения и пожари.

Позата при използване на смартфони/таблети:

Дефиницията на Text-neck синдром е синдром на претоварване, обикновено в резултат на прекомерно напрежение на шията от гледане надолу към всяко ръчно мобилно устройство, което може да доведе до главоболие, болки във врата, болки в раменете и ръцете, и нарушения с дишането. Текстовата поза на врата по време на използване на ръчно мобилно устройство е позицията на главата напред, докато горната част на врата се държи във флексия, а не в екстензия.

Има много данни за връзката между използването на мобилно устройство и болките във врата или симптомите, които предполагат отрицателните ефекти от Text-neck синдрома като повечето от тях показват, че доказателствата са ограничени.

Shahar и Sayers (2018) съобщават, че използването на мобилни устройства причинява развитието на изразена екзостоза, произтичаща от този ентезис при млади и възрастни. Това изследване привлече широко внимание и беше обект на значителни критики поради значителни ограничения и недостатъци, като източника, размера на извадката и възможността да се направи заключение за използването на смартфон от рентгенови доказателства.

През 2023 г. докладите изчисляват, че общият брой на потребителите на смартфони в световен мащаб ще достигне 6,8 милиарда. Като се има предвид, че световното население ще достигне малко над 8 милиарда, 8 от 10 души ще бъдат оборудвани със смартфон (85%). Сред възрастните на възраст 18-34 години, 92% и 95% съобщават, че притежават смартфон съответно в САЩ и Австралия.

Разглеждайки литературата за връзката между изпращането на текстови съобщения и болката във врата, отговорът е наистина объркан, тъй като проучванията, които са направени по темата, са противоречиви. Научните изследвания не се появяват във вакуум; те са част от нарастващ

набор от доказателства. Необходими са допълнителни опити и лонгитудинални проучвания, за да се установи връзката между изпращането на текстови съобщения и болката във врата и насоките за употреба [17].

Основната роля на шийния отдел на гръбначния стълб е да поддържа и насърчава движението на главата и шията. Накланянето на главата напред при използване на мобилни устройства драстично увеличава тежестта и върху гръбначния стълб. Средният ъгъл на цервикалния гръбначен стълб при флексия при изпращане на текстови съобщения е 37 до 47 градуса. Проучване показва, че теглото на главата се увеличава до 18,14 kg при 30 градуса и 22,23 kg при 45 градуса и това може да доведе до възпаление на връзките, мускулите и нервите на врата, което води до трайно артритно увреждане с повишена кривина на гръбначния стълб.

Стрес на работното място.

Друг основен проблем на работата е стресът на работното място - често срещан в цяла Европа. Европейска агенция за безопасност и здраве при работа докладва, че средното разпространението на стреса в Европейските държави-членки (ЕС) през 2005 г. е по-нисък в ЕС (20%), отколкото в две присъединяващите се тогава страни (България и Румъния, 31%). Наблюдавани са обаче и значителни разлики сред страните от ЕС. Най-високи нива на стрес са отчетени в Гърция (55%) и в Словения (38%), Швеция (38%) и Латвия (37%) и най-ниските нива отбелязани в Обединеното кралство (12%), Германия, Ирландия и Холандия (16%), както и в Чехия (17%), Франция и България (18%) (https://osha.europa.eu/en). Приблизително половината европейски служители смятат стреса за обичайно явление на своето работно място, на което обаче се дължи почти половината от всички загубени работни дни. Подобно на много други проблеми, засягащи психичното здраве, стресът често пъти е неправилно разбиран или заклеймяван. Ако се разгледат обаче като организационен проблем, а не като личен недостатък, психосоциалните рискове и стресът

могат да бъдат управлявани като всеки друг риск на безопасността и здравето при работа. Управлението на стреса е не само морално задължение и добра инвестиция за работодателите, но и законово изискване, заложено в Рамкова директива 89/391/ЕЕС и подкрепено от рамковите споразумения на социалните партньори относно стреса, тормоза и насилието на работното място.

Освен това Европейският пакт за психично здраве и благополучие признава променящите се изисквания и нарастващото напрежение на работното място, а работодателите се насърчават да прилагат допълнителни, доброволни мерки в подкрепа на психичното благополучие.

Адресиране на психическото напрежение от постоянна свързаност и прекомерна употреба на технологии. Препоръки за управление на времето пред екрана, уведомленията и баланса между работа и личен живот.

Интензитетът и темпото на работа са фактори, силно влияещи върху физическото и психическото здраве на наетите. Работата с висок интензитет е един от основните фактори, предизвикващи стрес на работното място. Работещите на висока скорост и чието темпо на работа е зависимо от машини са изложени в по-голяма степен на физически рискове. Интензитетът на работа е анализиран чрез индикаторите: „време, през което се работи с голяма скорост" и „работа с кратки срокове". Анализът на факторите, които определят темпото на работа, се основава на композитен индикатор. Той е съставен от индикаторите, определящи степента на зависимост в трудовата дейност от „работа, свършена от колеги", „преки искания от клиенти, пътници, ученици, пациенти", „голям брой производствени или представителни цели" и „автоматична скорост на машина или движение на продукт". Анализът на данните за връзката между степента на образование и интензитета на работа показва тенденцията работещите с по-високо образование по-често да работят с висока скорост и с кратки срокове. Мъжете работят с кратки срокове и с висока скорост

в по-голяма степен от жените, но разликата не е особено значима. Няма съществени различия между възрастовите групи по отношение на времето, през което работят с кратки срокове и с висока скорост, като изключение прави групата на младежите до 26 години, които по-рядко работят при тези условия. По отношение на зависимостта на темпото на работа от външни фактори няма значима разлика между мъжете и жените. С увеличаването на възрастта намалява и зависимостта на темпото на работа от влиянието на външни фактори за наетия. Рисковете от организацията на работата са специфични за отделните сектори.

Работа от разстояние.

Съгласно Чл. 107з., ал. 1 от Кодекса на труда: "Работата от разстояние е форма за организиране на работа, изнесена извън помещения на работодателя, извършвана по трудово правоотношение чрез използването на информационни технологии, която преди изнасянето й е била или би могла да бъде извършвана в помещенията на работодателя." На практика това е работа, която се извършва чрез използването на компютър чрез e-mail, фирмени мрежи и Интернет. Рисковете за работещите са както за физическото, така и за психическото им здраве. Когато се работи от разстояние, работникът от една страна е поставен в социална изолация, което влияе негативно върху психическото му здраве. От друга по-трудно може да се откъсне от домашните ангажименти, за да изпълнява своите служебни, изправян е сам пред някои проблеми без подкрепата на колегите или ръководството, което се асоциира с допълнителен стрес. Развитие на мускулно-скелетни нарушения, ако ергономичните аспекти не са менажирани добре. Важно е работниците и служителите да имат обособено работно място, както и да планират работния си ден, за да не се налага да използват от личното време за изпълнение на задачи. Работещите трябва да спазват определеното работно време в трудовия договор и да го отчитат, съгласно определените форми.

Използване на AI и усъвършенствана роботика. Безопасност, свързана с AI.

Цифровизацията бързо променя света на труда и изисква нови и актуални решения за здравословните и безопасни условия на труд (ЗБУТ). Появата на технологии като изкуствения интелект (ИИ), големите информационни масиви, сътрудничещите роботи, интернет, алгоритмите, цифровите трудови платформи и същевременното значително увеличаване на броя на хората, работещи от разстояние, създава възможности за работниците и работодателите, но също и нови предизвикателства и рискове за ЗБУТ. Справянето с тези предизвикателства и рискове зависят от начина на прилагане на технологиите, тяхното управление и нормативно регулиране в контекста на социалните, политическите и икономическите тенденции.

Основаните на изкуствения интелект системи и усъвършенстваните роботи променят начина, по който се планира и извършва човешкият труд. Този вид системи, които могат да бъдат вградени (напр. роботика) или невградени (напр. умни приложения), са с възможности да извършват действия, с известна степен на автономност за изпълнение на физически или когнитивни задачи и за постигане на конкретни цели. Това има значителни положителни последствия не само по отношение на производителността на предприятията, но и по отношение на ЗБУТ. Работните места в опасна среда и за изпълнение на тежки задачи могат да отпаднат, а работното натоварване може да бъде оптимизирано. Този вид системи могат да изпълняват високорискови или нетворчески повтарящи се задачи, свързани с редица традиционни и нововъзникващи рискове за ЗБУТ като за работниците ще останат нискорисковите задачи и продуктивното и по-творческо съдържание на работните места. Въпреки това съществуват и трябва да бъдат търсени решения на редица предизвикателства за ЗБУТ във връзка с използването на тези основани на изкуствения интелект системи на работното място, които произтичат главно от взаимодействието им с работниците, като неочаквани

сблъсъци, прекомерна зависимост и т. н., но и във връзка с психосоциалните и организационните аспекти.

Изкуственият интелект и цифровите технологии се появиха нови форми на управление на работниците. За разлика от предишните форми на управление, които до голяма степен се основават на контрол, осъществяван от хора, управлението на работниците чрез изкуствения интелект се отнася до нови системи и инструменти за управление, които събират данни в реално време за поведението на работниците от различни източници с цел информиране на ръководството и подпомагане на автоматизирани или полуавтоматизирани решения, основани на алгоритми или по-усъвършенствани форми на изкуствения интелект. Възможностите, предоставяни от тези нови системи за управление, основани на изкуствения интелект могат да подпомагат вземането на решения, насочени към подобряване на ЗБУТ на работното място, когато са изградени и прилагани по прозрачен начин, а работниците получават информация и участват в консултации. Правните, регулаторните, етичните и свързаните с неприкосновеността на личния живот предизвикателства и рискове и опасенията във връзка със ЗБУТ, особено по отношение на психосоциалните рискови фактори, до които водят тези нови форми на наблюдение и управление на работниците.

Освен за облекчаване на работата на много работни места въвеждат нови форми на базирано на изкуствен интелект наблюдение на работниците могат също така да осигурят възможност за подобряване на наблюдението на безопасността и здравето на работниците (БЗР), чрез намаляване на излагането на различни рискови фактори, включително тормоз и насилие, и предоставяне на ранни предупреждения за стрес, здравословни проблеми и умора.

Съветите в реално време, съобразени с индивида, могат да повлияят на поведението на работниците и да подобрят безопасността и здравето.

Мониторингът, базиран на изкуствен интелект, би могъл да подкрепи превенция, основана на доказателства; усъвършенствана оценка на риска на работното място и по-ефективни базирани на риска, целеви инспекции по БЗР. Информацията може да се използва от организациите за идентифициране на проблемите на БЗР, включително психосоциални рискове, и когато се изискват интервенции на организационно ниво.

Но са необходими етични решения и ефективни стратегии и системи за работа с голямото количество чувствителни лични данни, които могат да бъдат генерирани. Адекватни законови разпоредби, даващи на националните инспекции по труда достъп до анонимизирани данни, биха могли, предоставят възможност за основана на доказателства превенция и създаване на политики. Необходимостта от събиране на данни за работниците трябва да бъде балансирана спрямо правата на работниците на личен живот и тяхната безопасност и здраве. Важно е да се осигури прозрачност при събирането
и използването на такива данни, а работниците и техните представители следва да бъдат овластени чрез същия достъп до информация.

От 2016 г. насам Европейската агенция за безопасност и здраве при работа (EU-OSHA) предприема обширни прогнозни изследвания относно цифровизацията и БЗР. От 2020 г. EU-OSHA „Общ преглед на БЗР“ се основава на тази прогнозна работа, за да предостави допълнителни информация за политика, превенция и практика относно предизвикателствата и възможностите за БЗР в резултат на цифровизацията. Общоевропейската кампания за здравословни работни места, която стартира през 2023 г., също е посветена на цифровизацията и БЗР. Множество практически ресурси са публикувани на уебсайта на EU-OSHA като част от тази кампания.

Киберсигурност и защита на данните.

Безопасните условия на труд включват не само физическата защита на работещите, но и сигурността на техните данни и дигиталната среда, в която те функционират. В съвременния свят цифровата сигурност е съществена част от защитата на служителите и представлява ключов елемент от цялостната стратегия за безопасност на труда. Дигиталната сигурност защитава не само личната и корпоративната информация, но също така създава безопасна работна среда, която позволява на служителите да се съсредоточат върху своите задължения без страх от киберзаплахи като хакерски атаки, кражба на данни и зловреден софтуер.

Едно от основните предимства на цифровата сигурност е защитата на личните данни на служителите. С нарастващата честота на кибератаки и течове на информация, осигуряването на стабилна защита срещу неправомерен достъп до лична и чувствителна информация е от критична важност. Това включва защитата на данни като лични идентификационни номера, банкови сметки, здравна информация и друга лична документация, която се съхранява или обработва от работодателя. Когато тези данни са добре защитени чрез криптиране и контрол на достъпа, служителите могат да бъдат спокойни, че тяхната поверителност е уважена и защитена.

Цифровата сигурност също така предотвратява риска от злонамерен софтуер и фишинг атаки, които могат да засегнат личните устройства на служителите и корпоративните системи, нарушавайки както работния процес, така и сигурността на данните. Осигуряването на обучения и ресурси за разпознаване и предотвратяване на тези заплахи е от първостепенна важност. Когато служителите са добре информирани как да избегнат подозрителни имейли, фалшиви уебсайтове или приложения, те са по-малко уязвими на манипулации и потенциални кибератаки, които биха

могли да компрометират не само личната информация, но и важни корпоративни данни.

Освен това, защитата на данните е свързана и с поддържането на доверие и спокойствие сред служителите, особено в условия на дистанционна работа. Сигурността на корпоративните системи и процеси, особено когато служителите се свързват от различни локации и устройства, изисква по-строги мерки за достъп и защита. Прилагането на инструменти за многократна автентикация, виртуални частни мрежи (VPN) и защитни стени допринася за осигуряване на безопасни условия на труд и защита на данните, независимо от това дали служителите работят в офиса или от вкъщи.

Накрая, когато организацията инвестира в цифрова сигурност, тя гарантира и продължителността на безопасните условия на труд в дългосрочен план. Поддържането на сигурни мрежи и внедряването на системи за ранно откриване на киберзаплахи намалява риска от оперативни прекъсвания, причинени от киберинциденти. Това не само намалява стреса и несигурността на служителите, но също така гарантира непрекъснатост на работата и намалява вероятността от изтичане на данни или други критични инциденти, които биха могли да застрашат работната среда и да причинят загуби за организацията.

В обобщение, цифровата сигурност е неизменна част от съвременните стандарти за безопасни условия на труд. Тя защитава служителите, като ги предпазва от киберзаплахи и същевременно осигурява сигурността на личните и корпоративни данни. Когато служителите разполагат с адекватна защита и подкрепа за справяне с цифровите рискове, те могат да работят уверено, ефективно и без излишен риск, което допринася за по-добри резултати и за по-здравословна и стабилна работна среда. Следващите

няколко параграфа са посветени на насоките за осигуряване на киберсигурност на работното място.

Кибератаките са не само все по-сложни, но и изключително креативни, като често се насочват директно към човешкия фактор. Един добре обучен служител може да бъде първата линия на защита срещу множество кибер рискове. Ето насоки за изграждането на ефективна програма за обучение, фокусирана върху превенцията на тези заплахи.

1. Въведение в киберзаплахите и значимостта на обучението

Първата стъпка от обучението трябва да бъде запознаването на служителите с видовете киберзаплахи, които могат да засегнат работното място. Тук е важно да се подчертае значимостта на персоналната отговорност и осведоменост в рамките на цялостната сигурност на организацията. Служителите трябва да разбират, че действията им могат да предотвратят сериозни инциденти, включително загуба на данни, финансови щети и увреждане на репутацията на организацията. Програмата трябва да представи основните видове киберзаплахи, които включват фишинг, зловреден софтуер (като вируси, троянски коне и рансъмуер), социално инженерство и техники за злоупотреба с уязвимости в софтуера.

2. Разпознаване на фишинг атаки

Фишинг атаките са един от най-честите методи за измама, при които атакуващите се представят като доверени източници, за да подмамят потребителите да споделят конфиденциална информация или да инсталират зловреден софтуер. Обучението трябва да обяснява основните признаци на фишинг имейли, които включват:

Неочаквани искания за лична информация или чувствителни данни: Служителите трябва да бъдат инструктирани да не разкриват пароли, номера на банкови сметки и друга лична информация чрез имейл. Правописни и граматически грешки: Много фишинг имейли съдържат правописни или граматически грешки, както и некоректни формати на дата

или час.

Подозрителни линкове и прикачени файлове: Служителите трябва да се научат да проверяват дали линковете водят към легитимни сайтове, като се внимава особено с прикачени файлове, които могат да съдържат зловреден софтуер.
Необичайни или неадресирани поздрави: Фишинг имейлите често използват общи поздрави като „Уважаеми клиент“ вместо персонализирани обръщения.

Осведоменост за зловреден софтуер

Зловредният софтуер може да попадне на устройствата чрез сваляне на заразени файлове, кликане на зловредни линкове или прикачени файлове в имейли. Зловредният софтуер може да причини значителни щети, като криптиране на файлове (рансъмуер), събиране на чувствителни данни или нарушаване на нормалната работа на системите. Служителите трябва да бъдат информирани как да разпознават и избягват зловреден софтуер, като:

- Избягват сваляне на софтуер и файлове от ненадеждни източници: Служителите трябва да се придържат само към утвърдени и лицензирани източници.
- Никога не отварят подозрителни прикачени файлове или линкове: Дори когато изпращачът изглежда познат, препоръчително е да се свържат с него, за да потвърдят, че съобщението е автентично.
- Внимават с USB устройства и външни медии: Много кибератаки се извършват чрез заразени USB устройства, затова е важно служителите да използват само проверени и одобрени външни устройства.

Принципи на защита срещу социално инженерство

Социалното инженерство е манипулативна техника, чрез която кибер престъпниците се опитват да подведат служителите да разкрият конфиденциална информация. Това може да се случи по телефона, чрез

чатове или дори при директен контакт. За да намали риска от социално инженерство, обучението трябва да включва насоки като:

- Избягване на разкриването на конфиденциална информация без подходяща идентификация: Служителите трябва да знаят как да проверяват самоличността на човека, с когото комуникират.
- Повишена подозрителност към неочаквани запитвания или странни искания: Престъпниците често използват спешни ситуации, за да подмамят служителите да разкрият информация.
- Не се доверявайте на прекалено приятелски или настоятелни лица: Манипулацията често се осъществява чрез изграждане на доверие и симпатия.

Използване на технологии и добри практики за защита

За ефективно обучение е важно да се включат и технологични мерки, които служителите могат да използват, за да се защитят:

- Използване на силни и уникални пароли: Служителите трябва да бъдат информирани за значението на сложните пароли и за ползването на мениджъри на пароли;
- Активация на многофакторна автентикация (MFA): Многофакторната автентикация добавя допълнителен слой защита, като изисква вторично потвърждение при достъп до важни системи;
- Редовно актуализиране на софтуера и операционните системи: Обновленията често включват защити срещу нови заплахи, затова е важно служителите да поддържат софтуера актуален;
- Използване на VPN за достъп до корпоративните ресурси извън офиса: Виртуалните частни мрежи осигуряват сигурен канал за връзка и предпазват от неоторизиран достъп.

Провеждане на симулации и тестване

След теоретичното обучение, организацията трябва да провежда симулации на фишинг атаки и други киберинциденти, за да провери

степента на готовност на служителите и да ги тренира за бързо и адекватно реагиране. Тези симулации дават реален опит и помагат за засилване на вниманието към сигурността.

Редовно актуализиране на обучението

Киберзаплахите постоянно се променят, затова програмата за обучение трябва редовно да се актуализира, като отразява новите тенденции в киберсигурността. Препоръчва се провеждането на опреснителни курсове и предоставяне на актуални насоки на служителите.

Една ефективна програма за обучение ще осигури на служителите нужната осведоменост и умения за предотвратяване на кибератаки, като по този начин ще създаде култура на сигурност в организацията. С такъв подход, служителите ще са подготвени и уверени в разпознаването и избягването на фишинг атаки, зловреден софтуер и други киберзаплахи

Обработка на данни с AI.

Работата през цифрови платформи е всеки вид платена работа, извършвана през, посредством или с посредничеството на онлайн платформа, т. е. онлайн пазар, функциониращ на базата на цифрови технологии, който улеснява връзките при търсенето и предлагането на работна ръка. Работата, извършвана през платформи, може да бъде много разнообразна: тя може да включва сложни или прости задачи, когнитивни или ръчни задачи, и може да се предоставя онлайн и да бъде изцяло във виртуалното пространство или извършвана лично на място. Работата през цифрови платформи предоставя възможности за заетост на работещите в географски райони, в които липсват такива възможности, или на маргинализирани групи работници, но също така води до редица предизвикателства и рискове за ЗБУТ на работниците, за които трябва да се търсят решения. Качествено нова фаза на масовата информатизация е създаването и развитието на световната информационна система (интернет). Оформя се концепция за работа от разстояние чрез телекомуникациите,

което поставя и въпроса и за работата от дома. Разработват се нови системи за наблюдение на безопасността и здравето на работниците като приложения за смартфони, преносими устройства, мобилни камери за наблюдение или безпилотни летателни апарати, интелигентни очила, приложения, основани на ИКТ, и интелигентни лични предпазни средства. Те могат да се използват с цел наблюдение на физиологичното или психичното състояние на работниците, равнищата на стрес, умора, бдителност и сърдечната честота, както и позата и движенията на тялото, за наблюдение на местоположението на работниците в опасни зони, за даване на указания на работниците или изпращане на предупредителни сигнали към ръководителите или дори към службите за спешна помощ. Съществуват и опасения във връзка с неприкосновеността на личните данни и собствеността върху данните, ефикасността и стандартизацията.

Изследователската програма на Европейска агенция за безопасност и здраве при работа (EU-OSHA) има за цел да осигури за създателите на политики, изследователите и работните места надеждна информация относно потенциалните въздействия на цифровизацията върху ЗБУТ, така че да могат да се предприемат навременни и ефективни действия за гарантиране на безопасността и здравето на работещите.

Обучение и поддържане на осведоменост.

Техническа грамотност и AI.

С разширяването на новите технологии, изкуствения интелект (AI) и дистанционната работа, редовните обучения за безопасност и киберсигурност са от съществено значение за създаване на информирани и защитени работни среди. Въвеждането на нови технологии създава възможности за по-голяма продуктивност и иновации, но също така въвежда нови рискове, свързани с безопасността на служителите и сигурността на информацията. Обучението по безопасност и киберсигурност помага на служителите да използват тези технологии отговорно и компетентно като по

този начин се намалява рискът от злоупотреби, технически грешки и киберзаплахи.

Първостепенна цел на обученията за безопасност при новите технологии и AI системи е да изградят знания и умения, които позволяват на служителите да разпознават и предотвратяват потенциални рискове. При използването на AI системи например, служителите трябва да знаят как да работят с тези технологии по начин, който минимизира вероятността от грешки като неправилни входни данни или неточни изходи. Това включва инструкции за разпознаване на случаи на "bias" в AI моделите и умения за правилна настройка и проверка на данните, които захранват системите. Също така, те трябва да бъдат обучени да разбират етичните и правните последствия от използването на AI, особено в деликатни процеси като обработка на лични данни.

Киберсигурността е друг критичен аспект на обученията. В днешната дигитална среда служителите са изложени на различни киберзаплахи, като фишинг атаки, зловреден софтуер и атаки за изнудване, които могат да компрометират сигурността на цялата организация. Обученията по киберсигурност трябва да включват инструкции за разпознаване на подозрителни имейли, основни принципи за защита на пароли и сигурно споделяне на информация. Специално внимание трябва да се обръща на практиките за сигурност при работа от вкъщи, като използване на сигурни интернет връзки, редовни обновявания на софтуера и избягване на публични мрежи при достъп до корпоративна информация.

Организацията на тези обучения трябва да бъде систематична и редовна, тъй като технологиите се променят бързо и новите заплахи за сигурността възникват постоянно. Ефективните обучения трябва да включват практическа част, в която служителите могат да упражнят наученото, като се сблъскат с реалистични сценарии на потенциални проблеми или кибератаки. Освен това, чрез провеждане на уебинари, онлайн

курсове или специални интерактивни сесии, обученията могат лесно да достигнат до всички служители, включително тези, които работят от вкъщи.

Една добра практика е също да се провеждат тестове и упражнения за оценка на знанията на служителите след всяко обучение, като по този начин се проверява тяхната готовност и се идентифицират области, в които е необходимо допълнително обучение или съдействие. Периодичните актуализации и напомняния, включително съобщения с новини и съвети за сигурност, могат да поддържат информираността на служителите и да ги подсещат за важността на безопасната работа с технологии.

Систематичните и редовни обучения за безопасност и киберсигурност не само защитават организацията от потенциални заплахи, но и създават култура на осведоменост и отговорност сред служителите. Когато служителите са добре обучени и информирани, те се чувстват по-уверени в работата си и могат да използват новите технологии максимално ефективно, без да компрометират сигурността и ефективността на организацията. Това е от ключово значение за успешното внедряване на иновации и поддържането на конкурентоспособността в една динамична бизнес среда.
Включване на обучение за това как да се реагира в случай на технически аварии, като сривове на системата, прекъсване на захранването или неизправност на AI.

Мониторинг на работния процес.

Редовни одити на работните места.

Периодичните проверки на работните места играят ключова роля в поддържането на съответствие с насоките за ергономия, сигурност и безопасност, което е основен аспект за здравето и продуктивността на служителите. Тези проверки служат за идентифициране и елиминиране на потенциални рискове, свързани с неправилна работна поза, недостатъчна осветеност, шум или опасни условия, които биха могли да доведат до злополуки или хронични здравословни проблеми. Като част от регулярната

политика на организацията, проверките могат да включват оценка на ергономичните аспекти на работното място, състоянието на използваното оборудване, както и ефективността на мерките за безопасност и защита.

При извършване на проверките се оценява съответствието на работната среда с определените стандарти за ергономия, които включват фактори като позицията на компютърния екран, височината на стола, поддръжката на гърба и китките, както и регулирането на осветеността и температурата. Неправилната ергономия може да доведе до умора и натоварвания, които с времето да прераснат в мускулно-скелетни заболявания и да намалят продуктивността на служителите. Затова е важно редовно да се прави оценка на тези фактори, като се използват утвърдени стандарти за ергономия и здравословни условия на труд.

Сигурността на работното място е също толкова важна, тъй като неправилното разположение на предмети и оборудване, несъобразените изходи за аварийни ситуации или недостатъчната пожарна безопасност могат да създадат сериозни рискове. Периодичните проверки обикновено включват преглед на безопасността на всички съоръжения и системи за спешна помощ, като пожарогасители, евакуационни пътища, осветление в аварийни случаи и знаци за ориентация. Тези проверки трябва да гарантират, че служителите разполагат с подходящи средства за защита, че има адекватен достъп до аварийни изходи и че всички елементи от плана за сигурност са в добро състояние и леснодостъпни при нужда.

Периодичният мониторинг за безопасност включва и мерки за предотвратяване на инциденти чрез редовни инспекции на техническото оборудване, особено на уреди с висока натовареност, като компютри, машини и мебели. Преглеждат се тяхното състояние, възможните дефекти или признаци на износване, които биха могли да представляват заплаха за здравето на служителите. При наличие на идентифицирани рискове, се

препоръчва незабавна намеса чрез ремонт или подмяна на съответните компоненти, за да се предотвратят бъдещи инциденти.

Редовното извършване на тези проверки не само допринася за повишаване на безопасността на работното място, но също така създава култура на отговорност и ангажираност към благосъстоянието на служителите. Служителите също се поощряват да съобщават за нередности или да предлагат подобрения, когато видят проблеми, което увеличава тяхната осведоменост и съпричастност към политиката на организацията. Освен това, събраните данни от редовните инспекции могат да бъдат използвани за подобряване на политиките и насоките за безопасност и ергономия, така че те да отразяват най-новите тенденции и нужди на работната сила.

Обратна връзка и непрекъснато подобрение.

Създаването на ефективни канали за докладване на проблеми или предлагане на подобрения е съществена част от всяка успешна стратегия за управление. Такива канали позволяват на служителите да участват активно в подобряването на работната среда и процедурите, като същевременно укрепват връзката между тях и ръководството. Един от най-важните аспекти в този процес е да се изградят леснодостъпни и сигурни механизми, чрез които служителите могат да съобщават за възникнали проблеми или да споделят идеи за оптимизация на насоките. Важно е тези канали да бъдат разработени така, че да осигуряват анонимност и конфиденциалност, когато това е необходимо, както и да стимулират откритост и доверие.

Първата стъпка към създаването на ефективни комуникационни канали е установяването на ясни и лесни за разбиране насоки, които обясняват как служителите могат да подадат сигнал или да предложат подобрения. Тази информация трябва да бъде видима и достъпна за всички служители – например в корпоративния интранет или на информационни табла в офиса. Ясно трябва да се комуникират и условията за поверителност,

като по този начин се гарантира на служителите, че техните сигнали ще бъдат разгледани обективно и че няма да се сблъскат с негативни последици заради докладван проблем или предложена идея.

Технологичните решения също играят ключова роля при изграждането на тези канали. Внедряването на онлайн портали или специални софтуерни приложения, където служителите могат да докладват директно проблеми или да оставят предложения, значително улеснява процеса. Тези платформи могат да включват различни функционалности като например възможност за проследяване на статуса на подадените сигнали и предоставяне на обратна връзка от страна на ръководството. По този начин се изгражда по-голяма прозрачност в комуникацията и същевременно служителите са информирани за резултатите от техните предложения или сигнали.

Редовното организиране на срещи и обсъждания, където служителите могат да изразяват мнението си, също може да бъде ефективен канал за комуникация. Такива форуми дават възможност за обсъждане на различни гледни точки и директна обратна връзка. Ръководството може да използва тези срещи, за да обясни решенията и промени в насоките, както и да подчертае, че идеите на служителите имат реално въздействие върху взетите решения. Това ангажиране на служителите в процеса на вземане на решения не само създава усещане за съпричастност, но и повишава тяхната мотивация и удовлетворение от работата.

Не на последно място, регулярната обратна връзка към служителите е критично важна за успеха на тези канали. Когато служител подаде сигнал или предложение, е добре да получи потвърждение, че то е прието и разгледано. По този начин се изгражда доверие и се показва на служителите, че техният принос е ценен. В случаите, когато дадена идея не може да бъде осъществена, е препоръчително ръководството да обясни причините и да

изрази благодарност за направеното предложение. Това показва уважение към мнението на служителите и поощрява бъдещото им участие в процеса на подобрение.

Създаването на ефективни канали за докладване и предлагане на подобрения изгражда култура на отворена комуникация и взаимно доверие. Когато служителите се чувстват свободни да изразят мнението си и знаят, че ръководството е ангажирано с тяхното удовлетворение и безопасност, се повишава цялостната ефективност на организацията и се създават условия за устойчиво подобрение на работните процеси.

Съответствие с правните норми.

Процедурата за спазване на стандартите на КТ и ЗБУТ е предназначена да гарантира, че всички насоки и политики в организацията отговарят на изискванията за безопасност и здраве при работа, като същевременно се придържат към най-високите стандарти за ергономия и безопасна работа с техника. Процесът започва с внимателен преглед и съпоставка на съществуващите изисквания, свързани с КТ и ЗБУТ, за да се идентифицират ключовите аспекти, които трябва да бъдат включени и съобразени в работната среда.

Основен елемент на тази процедура е осигуряването на ергономичност на работните места, което включва детайлно проучване и адаптиране на условията, за да се минимизира рискът от физически дискомфорт или дългосрочни увреждания сред служителите. Това може да обхваща всичко от височината на работните бюра и удобството на столовете до подходящото осветление и минимизиране на отблясъци по екраните. Целта е да се създаде работна среда, която да подкрепя естественото положение на тялото, като по този начин се намалява напрежението и се увеличава комфорта на служителите.

При работата с компютри и други екрани процедурата предвижда следене и прилагане на правила за правилна употреба на мониторите. Според стандартите на ЗБУТ се изисква монитори и екрани да бъдат разположени на правилното разстояние от очите на служителите, като същевременно се избягва прекомерното използване на синя светлина, което може да натовари зрението. Служителите трябва да бъдат информирани за оптималното време на работа пред екраните, както и за важността на редовните почивки, които да предотвратяват умора и напрежение.

Безопасната работа с техника е друг ключов аспект на тази процедура. Според изискванията на КТ и ЗБУТ, организацията е отговорна да осигури оборудване, което е сертифицирано и безопасно за употреба, както и да гарантира, че служителите са обучени и знаят как да използват техническите средства правилно. Това включва също така и наличието на инструкции за безопасност при работа с всяко специфично оборудване, редовно проверяване и поддръжка на техниката, както и своевременно докладване и разрешаване на всякакви неизправности.

За да се гарантира, че тези процедури се прилагат ефективно и в съответствие със стандартите на КТ и ЗБУТ, организацията трябва редовно да провежда вътрешни одити и прегледи на работната среда и работните практики. Чрез тези проверки се установява доколко насоките са адекватно приложени и се идентифицират потенциални зони за подобрение. В случай на отклонения от стандартите, се предприемат необходимите корекции и се изготвят препоръки за бъдещо подобрение на работните условия, за да се гарантира постоянното спазване на нормативните изисквания.

Друг съществен момент от дейността по въвеждане на нови технологии е имплементирането на нормативни документи за защита на данните в организационна среда изисква внимателно съобразяване с различни местни, национални и международни регулации като например Общия регламент за защита на данните (GDPR) в Европейския съюз.

Спазването на тези закони е особено важно, когато в работните процеси се използва изкуствен интелект (AI) и се събират, обработват или съхраняват данни. Процесът по имплементация започва с пълен анализ на текущите потоци на данни в организацията като се идентифицират видовете данни, които се обработват, техните източници, както и тяхното предназначение.

Основен компонент на спазването на регламентите за защита на данните е установяването на прозрачност и яснота при обработката на данните. Това означава, че всяка организация, която работи с лична информация, трябва ясно да информира клиентите, служителите и всички засегнати лица какви данни се събират, с каква цел и за какъв период ще се съхраняват. Също така е необходимо да се осигурят механизми, чрез които потребителите да могат да упражнят своите права, предвидени от GDPR, като правото на достъп, корекция, изтриване и ограничаване на обработката на данните.

При работата с изкуствен интелект и автоматизирани системи за обработка на данни е важно да се гарантира, че данните се използват само за съответната цел и че се прилагат мерки за минимизиране на събраната информация. Това включва практики като анонимизация и псевдонимизация на данните, които помагат за защита на личната информация, особено когато данните се използват за обучение на AI модели. Допълнително, AI системите трябва да бъдат проектирани така, че да осигуряват защитен и сигурен достъп до данните, предотвратявайки нежелано разпространение или достъп от неоторизирани лица.

Друг съществен елемент в имплементацията на законите за защита на данните е установяването на процедури за реакция при нарушения. Това включва определяне на екип по защита на данните, който да отговаря за мониторинг на процесите и за реакция при евентуално нарушение на сигурността. В случай на изтичане или неоторизиран достъп до лични данни, организацията е задължена да уведоми засегнатите лица и

съответните надзорни органи в срок като предостави подробна информация за нарушението и мерките, които са предприети за ограничаване на последиците.

Необходимо е също така редовно да се провеждат обучения и да се предоставят указания на всички служители относно техните задължения и отговорности, свързани със защитата на данните. Това включва познания за основните принципи на GDPR и осъзнаване на рисковете от нарушения на данните. Когато в даден процес е включен изкуствен интелект, служителите трябва да бъдат информирани за правилата за етична обработка на данни и за евентуалните последици от некоректно използване на информация.

За да бъде имплементацията успешна и устойчива, организацията трябва редовно да оценява и актуализира своите политики и практики за защита на данните. Това включва вътрешни одити и прегледи на съответствието с GDPR и други приложими закони, както и прилагане на корективни мерки при необходимост. Само чрез постоянно подобрение и мониторинг на процесите организацията може да гарантира пълното съответствие със законите за защита на данните и да осигури доверие и сигурност за всички, чиито данни обработва.

Планиране на аварийни ситуации и непредвидени обстоятелства

Установяването на ефективни протоколи за реакция при инциденти, свързани с изкуствения интелект (AI) и технологиите на работното място, е от изключителна важност за защита както на служителите, така и на целостта на работните процеси. Първата стъпка в разработването на тези протоколи е да се идентифицират възможните рискове, свързани с използването на AI системи и технологии. Такива рискове могат да включват нежелани изходни данни или решения, автоматизирани процеси, които предизвикват физически или психически дискомфорт за служителите, и

случаи, в които самите технологии могат да бъдат манипулирани или компрометирани, което застрашава сигурността на работното място.

За предотвратяване на инциденти е важно служителите да бъдат информирани и обучени да разпознават предупредителни сигнали и да знаят как да реагират, ако забележат нередност. Протоколите трябва да включват редовни проверки и актуализации на AI системите, за да се гарантира, че те функционират правилно и в съответствие с поставените цели. В случай на възникнал инцидент с технология или AI, трябва да се приложат ясни стъпки за незабавно уведомяване на екипа по сигурността и мениджърите. Това дава възможност за бърза оценка на ситуацията и за решаване на проблема, преди той да ескалира.

Комуникацията е основен компонент на тези протоколи – служителите трябва да имат ясно разбиране за това кого и как да уведомяват при инцидент, включително и когато инцидентът засяга тяхното здраве и безопасност. При такива случаи екипът по сигурността трябва да работи в тясно сътрудничество със специалисти по безопасност и здраве, за да се вземат навременни мерки и да се гарантира, че няма риск за служителите.

Допълнително, трябва да се осигури механизъм за обратна връзка, чрез който служителите да споделят информация за потенциални рискове или недостатъци на AI системите. Това ще спомогне за непрекъснато подобрение на протоколите за сигурност и ще позволи на организацията да се адаптира към променящите се технологии и новите предизвикателства в областта на изкуствения интелект и технологиите.

Протоколи за реагиране при кибератаки.

За създаване на ефективни процедури за реакция при нарушения на сигурността на данните и кибератаки е необходимо да се започне с подготовка и превенция. На първо място е важно да се идентифицират критичните системи и данни, които са от ключово значение за бизнеса и които изискват приоритетна защита. Следващата стъпка е изготвянето на

план за обучение на служителите, който обхваща основни аспекти на киберсигурността, включително разпознаване на фишинг атаки и правилата за работа с чувствителни данни.

Инсталирането на защитни механизми също е от съществено значение. Това включва антивирусен софтуер, защитни стени и криптографски защити, които трябва да бъдат регулярно актуализирани, за да са ефективни срещу новите заплахи. Освен това е важно да се осигури редовно архивиране на критичните данни, така че при кибератака или загуба на данни те да могат да бъдат възстановени.

При евентуално нарушение на сигурността е необходимо системите за мониторинг да са в състояние да засичат заплахите своевременно. Когато се открие потенциална заплаха или нарушение, първата стъпка е бързата оценка на инцидента. Тази оценка включва определяне на обхвата на нарушението, вида на засегнатите данни и потенциалното въздействие върху бизнеса.

След оценката следва бърза реакция, която включва изолиране на засегнатите системи и уведомяване на екипа по сигурността. Необходимо е да има ясни процедури за комуникация, които да включват вътрешните екипи и, при необходимост, външни експерти, за да се извърши задълбочено разследване и смекчаване на последствията.

Регулаторни и специфични за индустрията съображения.

Всяко предприятие или компания, независимо от индустрията, трябва да разработи и добави специфични раздели в своите вътрешни политики и процедури, които отговарят на изискванията и особеностите на конкретния сектор. Тези раздели са ключови за осигуряване на безопасна и ефективна

работна среда, като същевременно помагат да се спазват законите и стандартите за безопасност и етика, които важат за съответната индустрия.

Здравеопазване.

В здравеопазването имплементирането на изкуствен интелект за диагностика и лечение изисква специфични мерки за безопасност и защита на личните данни. Тези раздели трябва да обхващат отговорностите на медицинските екипи и AI специалистите за коректното използване на AI инструменти при диагностициране на пациенти. AI системите трябва да бъдат обучени и настроени така, че да предоставят точни и надеждни резултати, като същевременно се осигурява прозрачност и проследимост на данните, с които работят. Освен това е от съществено значение да се въведат процедури за редовна оценка на алгоритмите, за да се минимизират потенциални грешки и пристрастия. Когато AI е използван в процеси като сканиране на изображения, медицинските професионалисти трябва да бъдат информирани за съществуващите рискове и ограничения, както и за това какво трябва да бъде тяхното взаимодействие със системите, за да се избегнат възможни неправилни интерпретации или погрешни диагнози. Регулярните обучения на персонала и стриктната защита на данните на пациентите също са неотменни части от тези процедури.

Производство.

В производствените компании, където се използват роботи и автоматизирани машини, е важно да се гарантира безопасността на служителите около роботизираните системи. Разделът за безопасност трябва да описва конкретни протоколи за работа с роботизирани ръце, включително предпазни мерки за избягване на злополуки при работа с машини, които имат физически компонент и взаимодействат с хората в производствената среда. Това включва инсталирането на сензори за движение и защитни бариери, които да предотвратят навлизането на служители в опасната зона

по време на работата на роботите. В случай на неизправност на машината, процедурите трябва да предвиждат незабавни мерки за безопасност, като бързо спиране на робота и известяване на екипите по поддръжка. Редовната инспекция на роботизираните системи и обучението на персонала за разпознаване на потенциални рискове също са важни аспекти от тези раздели.

Финанси.

Във финансовата индустрия, където AI се използва широко за алгоритмична търговия и анализ на големи обеми от данни, е наложително да се въведат раздели за етично и сигурно използване на AI системите. Алгоритмичната търговия включва автоматични транзакции на финансовите пазари, които трябва да бъдат не само прецизни, но и етични, за да се избегнат финансови злоупотреби или сривове на пазара. Разделите за финанси трябва да определят правила за мониторинг и контрол на AI алгоритмите, включително лимити за техните действия и ясни протоколи за отстраняване на технически проблеми в реално време. Финансовите AI системи трябва също така да бъдат преглеждани и одобрявани от екипи по етика и законодателство, за да се гарантира, че действията им отговарят на изискванията за прозрачност и законност в индустрията. Освен това е от съществено значение тези системи да бъдат проектирани с мерки за защита на финансовите данни и алгоритми, които да предотвратяват манипулации на пазара и неоторизиран достъп.

Добавянето на тези индустриално-специфични раздели към политиките на компанията не само осигурява спазване на най-добрите практики за безопасност и етика, но и укрепва доверието към организацията от страна на служителите, клиентите и регулаторните органи. Тези политики трябва да бъдат редовно актуализирани в съответствие с последните технологични разработки и законови изисквания, като същевременно

включват обучения и ръководства за служителите, за да могат да разбират и изпълняват тези изисквания по време на ежедневната си работа.

проф. д-р Емил Воденичаров, дм