РЕЗЮМЕ

В статье дан анализ систем питания топливом двигателей с искровым зажиганием. Рассмотрены особенности работы системы питания карбюраторного двигателя, система центрального впрыскивания и система распределенного впрыскивания. Приведены схемы выше упомянутых систем с указанием основных узлов и деталей. Преимущества впрыскивания отына в двухтактных и четырехтактных двигателях.

RESUME

The article analyzes the fuel supply systems of spark-ignition engines. The features of the operation of the carburetor engine power system, the central injection system and the distributed injection system are considered. The diagrams of the above mentioned systems are given, indicating the main components and parts. Advantages of gasoline injection in two-stroke and four-stroke engines.

ӘОЖ 004.056

Білім алушы: Кубаева Г., студент
Ғылыми жетекші: Касымова А.Х., п.м.а.,п.ғ.к жетекші
«Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, Орал қ..

АҚПАРАТТЫҚ КЕҢІСТЕГІ КИБЕРҚАУІПСІЗДІК

АННОТАЦИЯ

Мақалада, киберқауіпсіздік түсінігің түсінігі мен олардың пайда болу жолдары жыне қоргалу әдістерінің негіздері ашылған. Киберқауіпсіздік компьютерлерге, желілерге, операциялық жүйесінің басқа да конфигурацияланатын бағдарлама құрамдастарына қоданылады. Киберқауіпсіздіктің негізгі мақсаты ақпаратты ұрлаудың немесе зиян келтірудің алдын алу болып табылады. Бұл мақсатқа жетуде қауіпсіз it инфрақұрылымының үштігі маңызды рөл атқарады-құпиялылық, тұтастық және қол жетімділік. Киберқауіпсіздік бағдарламалалардың, желілер мен мәліметтердің біртұтастығын кибер шабуылдардан қорғау технологияларының, әдістемелер мен процестердің жиынтығын білдіретін өзекті мәселелермен электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық коммуникациялық инфрақұрылымды ортасының сыртқы және ішкі қауіп-қатерлерден қорғалу білім алушыларға ақпарттық кеңістіктегі киберқауіпсіздік негіздері мәлімделенеді.

***Кілттік сөздер**: Киберқауіпсіздік, электрондық ақпарат, ақпараттық ресурстар, ақпараттық коммуникация, инфрақұрылым, мемлекеттік құпия, интернет, желі, шифрлау, технология*

Қазіргі таңда технология дамыған заманда киберқауіпсіздік бүкіл әлемде өзекті мәселе болып отыр. Киберқауіпсіздік түсінігің жан-жакты қарастыратын болсақ, ол ақпартпен жүйелер мен электрондық желілер « өнеркәсіптік және автоматика мен бақылау жүйелері» деп аталатын атауга ие. Өнеркәсіптік және автоматика мен бақылау жүйелерін қауіпсіздігі заңсыз енуді немесе қасақана араласуды,ия болмаса қорғалатын ақпаратқа қолжетімділікті болдырмауы.

Киберқауіпсіздік білім беру бағдарламасы, білім алушыларға бағдарламалық жасақтама жасау және әртүрлі масштабта қызмет ету саласында өзін көрсетуге мүмкіндік беретін бағдарламалық жасақтама негіздері пәндерін қамтиды. Оқыту нәтижелері

бойынша білім алушылар бірнеше бағдарламалау тілдерін жетік меңгереді, банктер, сақтандыру компаниялары, мемлекеттік және ұлттық ұйымдар және басқалары сияқты ірі компанияларға арналған бағдарламалық жасақтама жасай алады. Бағдарлама мобильді құрылғыларға, мәліметтер базаларына және веб-қосымшаларға қосымшалар жасау дағдыларын дамытуға көмектеседі. Киберқауіпсіздік компьютерлерге, желілерге, операциялық жүйесінің басқа да конфигурацияланатын бағдарлама құрамдастарына қоданылады. Киберқауіпсіздәк бағдарламалалардың, желілер мен мәліметтердің біртұтастығын кибер шабуылдардан қорғау технологияларының, әдістемелер мен процестердің жиынтығын білдіретін өзекті мәселе.

Киберқауіпсіздік – электрондық нысандағы ақпараттың және оның өңдеу, сақтау, беру (электрондық ақпараттық ресурстарды, ақпараттық жүйелер мен ақпараттық коммуникациялық инфрақұрылымды) ортасының сыртқы және ішкі қауіп-қатерлерден қорғалу жағдайы деп тоқталатын болсақ, білім алушыларға ақпарттық кеңістіктегі киберқауіпсіздік негіздерін мәлімдеу мақсатымыз болып табылады..

Құқық бұзушылар құпия ақпаратты заңсыз көшіріп алу немесе редакциялау мақсатымен кибершабуыл жасайды. Оны,негізінен,адамдардан қаржыны ұрлаудан немесе ұйымдағы өндірістік немесе жұмыстық процесттерді бұзу,мемлекеттік құпияларды қорлау мақсатында жүзеге асыра алады. Қазіргі таңда көптеген ұйымдар мен үкеметтәк мекемелерде жұмысқа қажетті барлық материалдарды, ақпаратты және де жеке мәліметтерін жинау,сақтау және өңдеу басты максаттардың бірі,ал олар қорғауды қажет етеді. Себебі,ақпарат құпия болуы керек.егер олар қорғалмаса кері салдарға әкеледі.

Киберқауіпсіздік тұжырмдамасы Қазақстанның әлем бойынша дамыған елдер қатарына енуіндегі «Қазақстан-2050» стратегиясының тәсілдерің ең басты мәселесі болып табылады. Ақпарттық қауіпсіздіктің класссикалық үлгісі ақпараттың қауіпсіздігі үшін маңызды үш белгіні қамтамасыз етуге негізделеді: құпиялық.тұтастық және қолжетімділік.Ақпараттың құпиялығы онымен өзінің иесі белгіленген қатаң шектелген адамдар тобымен ғана таныса алады дегенді білдіреді. Егер ақпаратқа қолжетімдііһлікті немесе құпиялықтың бұзылуына жол беріледі[1].

Ақпараттың тұтастығы- ақпараттың бұрмаланбаған түрде сакталу қабілеті. Ақпараттың заңсыз және иесі көздемеген өзгеруі тұтастықтың өзгеруі. Яғни, оператор қатесінің немесе уәкілеттілігі жоқ адамның қасақана іс-әрекетінің нәтижесі. Әсіресе аса маңызды ақпартттық-коммуникациялық инфрақұрылым обьектілерінің жұмыс істеуімен байланысты деректердің тұтастығы ерекше маңызды. Атап айтсақ, әуе қозғалысы,электрмен және энергиямен жабдықтауды басқарудың атоматтандырылған жүйелері және т.б. Ақпараттың қолжетімділігі- ақпараттық жүйенің тиісті уәкілеттіктері мен бар субъектілерге ақпаратқа дер кезінде бқгетсіз рұқсат беру қабілеті мен анықтамалары.Ақпаратты жою немесе бұғаттау қолжетімділіктің жойылуына алып келеді. Қолжетімділік – ақпараттық- коммуникациялық қызметтерді беру жолымен клиентерге қызмет көрсетуге бағытталған ақпарттық жүйе. Мысал: Теміржол және авициялық билеттерді сатудың, банк қызметтердің ақпараттық жүйелері, интернетте өнімдерді интернет ресурстарымен және электрондық тарату. Ал,уәкілетті пайдаланушы белгілі бір қызметтерге ,көбіне желілік рұқсат ала алмаған жағдайда қызмет көрсетуден бас тартады. Енді әлеументтік желілердегі қауіпсіз қарм-қатнастың ережелерін айтсақ, күн сайын контакт, whatsApp, фейсбук, инстаграм, телеграмм, твиттер т.б. әлеументтік желілерді пайдаланушылар саны күн сайын артуда. Әлеументтік желіліердің көмегіңмен адамдар бір-бірімен қарым –қатнас жасайды, фотосуреттермен мәліметтер алмасады.Мұндай ресурстар неғұрлым танылмал бола бастаған сайын,алаяқтарда оларға көбірек қызығушылық танытуда. Осыған байланысты оларды пайдалану қауіпті бола түседі. Әлеументтік желілерді пайдалану кезіндегі қауіпсіздіктер:жеке ақпаратты жария ету, қауіпті танысулар, қылмыскердің назарын аудару,жұмыс іздеу,музыка, бейне жазба.балалармен жасөспірімдердің қз өміріндегі барлық оқиғагы әлеументтік желілерге жариялау,статус пен фотосуреттер арқылы бала мен отбасының қай жерде болатындығы,

хат алмасулар,хабарламалар жатады. Және де қосымшаларды орнату кезінде логин мен пароль жазу хакерлерге жеке ақпаратқа қолжетімді мүмкіндік береді. Бәрақ амал не? Заманауи технология осыған апарып отыр. Оны қорғау мүмкіндіктерін күшейту қажеттілі тауды.Әрбәр компьютер қолданушы баска комьютерден аккаунт ашпау керек. Өйткені ол аккаунт арқылы вирус жіберу мүмкіндігі және аккаунтты бұзу үшін әртүрлі ұсыныстармен хабарламалар жіберілуі мүмкін.Тағы бір жайды айта кетсек,ол «Парольді ұмыттыңыз ба?»деген сұрақ, осы батырманы пайдалана отырып,аккаунттарды бұзады. Парольді, электронды почтадағы мекенжайлар кітапшаларын сканерлеуге мүмкіндік бермеу керек.

Зиянды бағдарламалық жасақтама-киберқылмыскерлердің ең көп таралған құралы. Олар оны пайдаланушының компьютерін және ондағы деректерді зақымдау немесе оны өшіру үшін өздері жасайды. Зиянды бағдарлама көбінесе зиянсыз файлдар немесе пошта тіркемелері түрінде таратылады. Киберқылмыскерлер оны саяси себептермен шабуыл жасау немесе шабуыл жасау үшін пайдаланады.Зиянды бағдарлама әр түрлі болуы мүмкін, мұнда кейбір жалпы түрлер бар: *Вирустар*-файлдарды зиянды кодпен жұқтыратын бағдарламалар. Компьютер жүйесінде тарату үшін олар өздерін көшіреді. *Трояншы*– қауіптілі жасырынатын маска астында бойынша жариялыболады. Киберқылмыскерлер қолданушыларды троянды компьютерге жүктеуге мәжбүр етеді, содан кейін деректерді жинайды немесе бүлдіреді. *Жарнамалық бағдарлама*-зиянды бағдарлама таратылуы мүмкін жарнамалық бағдарламалар.*Ботнеттер*-киберқылмыскерлер өз мақсаттары үшін пайдаланатын зиянды БҚ-мен зарарланған компьютерлер желісі.*SQL инъекциясы***.**Кибершабуылдың бұл түрі мәліметтер базасынан ақпаратты ұрлау үшін қолданылады. Киберқылмыскерлер зиянды кодты дерекқорды басқару тілінде (SQL) тарату үшін деректерге негізделген қосымшаларда осалдықтарды пайдаланады.*Фишинг***.**Мақсаты пайдаланушының құпия ақпаратын алдау болып табылатын Фишинг – шабуылдар. Мысалы: банк карталарының деректері немесе парольдер. Көбінесе мұндай шабуылдар кезінде қылмыскерлер зардап шеккендерге ресми ұйым ретінде көрінетін электрондық хаттар жібереді. *Man-in-the-Middle* шабуылдары. Бұл шабуыл, оның барысында киберқылмыскер деректерді беру кезінде ұстап алады – ол тізбектегі аралық буынға айналады, ал зардап шеккендер бұл туралы Тіпті білмейді. Егер сіз, мысалы, қорғалмаған Wi-Fi желісіне қосылсаңыз, сізге осындай шабуыл жасалуы мүмкін. *DoS-шабуылдар*.

Киберқылмыскерлер шабуыл объектісінің желілері мен серверлеріне артық жүктеме жасайды, соның салдарынан жүйе қалыпты жұмысын тоқтатады және оны пайдалану мүмкін болмайды. Мәселен, шабуылдаушылар, мысалы, инфрақұрылымның маңызды компоненттерін зақымдауы және ұйымның қызметін доғаруы мүмкін. Инфрақұрылым объектілері ауыр аварияларға мен апаттардың көзі бола алады, сондықтан мұндай аумақтар үшін ықтимал қатерлерді кешенді талдау негізінде ғана жаңа құрылыс туралы немесе оларды одан әрі жаңғырту жөніндегі мүмкіндіктер туралы шешімдер қабылданады. Элементтер арасындағы күшті байланыстардың болуы оларды көптеген инфрақұрылым объектілерін қамтитын апаттардың каскадты сценарийлеріне бейім етеді, ал апаттың барысы элементтер арасындағы байланыс құрылымымен анықталады[2].

Wi-Fi желілерін қауіпсіз пайдалану кез келген жерде интернетке қол жетімді тегін қоғамдық нуктелері бар.Ол өркениеттің бқл игілінің арқасында желіде тқрақты қалуға ,керекті жұмысты орындауға,жаңалықтар мен оқиғаларды білуге тиімді. Wi-Fi нүктелерімен жұмыс жасау онлайн қауіpсіздікке әкеледі.Мұндай қауіпсіздіктен өту үшін мынандай негізгі іс-әрекет шараларын сақтау қажет: Wi-Fi желәсән пайдалану туралы келісіммен танысу,стандартты тіркеуден өткізу.берқауіпсіздік түрлері: *Шифрлау***.**Оны дұрыс қолданған кезде шифрлау (және бопсалау бағдарламаларының бөлігі емес) сіздің қауіпсіздігіңізді қамтамасыз етудің тамаша тәсілі болып табылады. Шифрлауды қолданатын бағдарлама немесе қызмет сіздің хабарламаларыңызды немесе файлдарыңызды қабылдайды және оларды бастапқы ақпаратты оқуға мүмкіндік бермейтін

кодқа айналдырады. Бұл дегеніміз, шабуылдаушы сіздің байланысыңызға араласса да, ол ештеңе көрмейді [3].

Шифрлау-бұл файлдарды жіберу үшін кез-келген қызметті пайдалану кезінде назар аудару керек деректерді қорғаудың сенімді әдісі. *VPN.VPN* әртүрлі мақсаттарда қолданылады, мысалы, желіге қашықтан қол жеткізуді қамтамасыз ету үшін, сонымен қатар кибершабуылдардан жақсы қорғайды. VPN қызметтері сіздің IP-мекен-жайыңызды, яғни желідегі бірегей идентификатор ретінде қызмет ететін және сіздің үй мекен-жайыңызға ұқсас мекенжайды жасырады. Егер сіз оны жасырсаңыз, алаяқтар сіздің орналасқан жеріңізді немесе желіңізді таба алмайды. Мысалы, Сіз VPN IP-мекен-жайыңызды мекен-жайға жасыра аласыз. *Аутентификация***.** Бұл қарапайым технология. Аутентификация сіз өзіңіз берген адам екеніңізді тексеруге мүмкіндік береді, сондықтан шабуылдаушылар сіздің есептік жазбаңызға кіре алмайды. Әдетте тексеру үшін тек пароль қолданылады, бірақ қазір көптеген қызметтер екі сатылы тексеруді талап етеді және бұл туралы толық келісу керек. Екі сатылы аутентификация қосымша қорғауды қамтамасыз етеді, және бұл көбінесе кіру үшін сізге электрондық пошта немесе телефон арқылы жіберілген кодты енгізу керек дегенді білдіреді, хакердің барлық осы арналарға кіруі екіталай. Қорғаудың бұл әдісі жалпы файлдар немесе кіріс хаттар сияқты онлайн режимінде деректерді сақтау үшін қолданылады. Аутентификацияның тағы бір шешімі-SSO немесе бірыңғай кіру технологиясы. Бұл шешім бір рет кіруге және бірнеше қосымшаларға қол жеткізуге мүмкіндік береді. Бұл әдіс бірнеше есептік жазбаны алаяқтықтың ең қысқа жолы болып көрінуі мүмкін, бірақ олай емес. Егер сіз бірыңғай кіру технологиясын қолдансаңыз, сізге бірегей логин және әр есептік жазба үшін өте күрделі пароль қажет емес. Сондықтанда, құпия деректердің саны және оларды ұрлау ықтималдығы азаяды[4].

Антивирус және брандмауэр**.** Бұл қарапайым қорғаныс құралдарын өзіңіз орната аласыз және олар барлық ноутбуктер мен мобильді құрылғылар үшін қажет. Брандмауэрден қорғау және антивирустар зиянды бағдарламаларды тоқтатуға көмектеседі, тіпті егер сіз "жүктеу" түймесін бассаңыз да; киберқауіпсіздік қауіптерін анықтап, оларды дереу алып тастаңыз немесе қауіпсіз қалтаға жылжытыңыз.*SIEM***.** Ақпараттық қауіпсіздік және қауіпсіздік оқиғаларын басқару жүйесі (SIEM) — бұл нақты уақыт режимінде жұмыс істейтін қорғаныс құралы. SIEM шешімдері бағдарламалық жасақтама немесе қызметтер түрінде қол жетімді. Компанияның қызметін бақылау арқылы олар кез-келген бұзушылықтар туралы бірден ескертеді және проблемалардың алдын алады. Пайдаланылған бағдарламаға немесе қызметке байланысты SIEM сәйкестік туралы есептер шығаруға көмектеседі және апаттан кейін ақпараттық жүйенің жұмысын қалпына келтіруге көмектеседі[5]. Киберқауіпсіздік - бұл ұғым біздің өмірімізге енгелі қашан. Жеке мәліметту қорғау қажеттілігі қоғамның диджиталдануымен бірге артып келеді. Егер бұрын тек электронды поштаның құпиясөздерін және копьютерді вирустардан қорғау керек болса, бүгінгде әлеуметтік желілердегі аккаундтардың қауіпсіздігін қамтамасыз етуіміз қажет. Сондай-ақ виртуалды мұрағаттар мен сервистерді, қосымшалардағы жеке мәліметтерді, криптовалюталық әмияндарды және тағы да басқаларын қорғауымыз тиіс.

"Киберқауіпсіздік" және "ақпараттық қауіпсіздік" ұғымдары синоним ретінде жиі қолданылады. Алайда, іс жүзінде бұл терминдер әр түрлі және бір-бірін алмастырмайды. Киберқауіпсіздік дегеніміз **—** киберкеңістіктегі шабуылдардан қорғау, ал ақпараттық қауіпсіздік дегеніміз-деректерді аналогтық немесе цифрлық болсын, кез-келген қауіп-қатерден қорғау.

Киберқауіпсіздік тәжірибелерін өнеркәсіптік кәсіпорындардан бастап қарапайым пайдаланушылардың мобильді құрылғыларына дейін әртүрлі салаларда қолдануға болады:

Сындарлы инфрақұрылымның қауіпсіздігі-компьютерлік жүйелерді, сындарлы ақпараттық инфрақұрылым объектілерінің желілерін қорғау шаралары. КИИ объектілеріне электр желілері, көлік желісі, автоматтандырылған басқару жүйелері және

ақпараттық-коммуникациялық жүйелер және елдің қауіпсіздігі мен азаматтардың әл-ауқаты үшін қорғалуы өмірлік маңызы бар көптеген басқа жүйелер жатады.

Желілік қауіпсіздік-негізгі желілік инфрақұрылымды рұқсатсыз кіруден және дұрыс пайдаланбаудан, сондай-ақ ақпаратты ұрлаудан қорғау. Технология құрылғыларға, қолданбаларға және пайдаланушыларға қауіпсіз инфрақұрылым құруды қамтиды.

Қолданба қауіпсіздігі-қолданба деңгейінде қолданылатын және Қолданба деректерінің немесе кодының ұрлануын, бұзылуын болдырмауға бағытталған қауіпсіздік шаралары. Әдістер қосымшаларды әзірлеу, жобалау, орналастыру және пайдалану кезінде туындайтын қауіпсіздік мәселелерін қамтиды.

Бұлттық қауіпсіздік-бұлтты есептеу жүйелерін киберқауіптерден қорғау саясаттарының, басқару элементтерінің және құралдарының өзара байланысты жиынтығы. Бұлттық қауіпсіздік шаралары деректердің, онлайн инфрақұрылымның, сондай-ақ қолданбалар мен платформалардың қауіпсіздігін қамтамасыз етуге бағытталған. Бұлттық қауіпсіздік дәстүрлі киберқауіпсіздікпен бірқатар ортақ тұжырымдамаларға ие, бірақ бұл салада өзінің озық тәжірибелері мен бірегей технологиялары бар.

Қорыта айтқанда. Қазіргі әлемде ұйымдар коммерциялық, қаржылық, медициналық, өңдеу және энергетика саласы, соның ішінде барлық мемлекеттік құрылымдар - жинақ, сақтау жәнетбарлық қажетті ақпаратты, сондай-ақ қызметкерлердің жеке дербес деректерін өңдеу , пайдаланушылар, тапсырыс берушілер және келушілер. Негізінен, барлық осы ақпарат қорғауды қажет етеді, өйткені құпия және оның ағып кетуі, жоғалуы немесе ұрлануын алдын-ала болжауға болмайды,олар адамдар мен ұйымдардың (мемлекеттік) өзіне нашар салдары төндіреді. Бүкіл қалалардың, елдердің және тұтастай алғанда әлемдік қоғамдастықтың инфрақұрылымын тікелей қамтамасыз ететін ұйымдар жан-жақты кешенді кибершабуылға ұшырауы ықтимал. Мұндай ұйымдар немесе құрылымдар Сыни инфрақұрылым . Сыни инфрақұрылымдар күрделі, кеңістік-бөлінген, көп компонентті жүйелер болып табылады, олардың тұрақты жұмысы экономиканың жұмыс істеуі және адамдардың өмірі үшін өте маңызды. Кибершабуылдар экономикалық зиян шектіреді, онлайнқызметтерге қоғамдық сенімді кетіреді және азаматтарға, олардың меншіктері мен құпиялығына залал келтіреді. Киберқауіпсіздік нені білдіреді? IT мамандарынын жауапты басты мәлесі болып отыр, әлеументтік желілерді пайдаланудың қандай қауіпсіздіктері бар екенің, Wi-Fi қолдану қауіпсіздіктерін мен қатарВеб-сайттар мен қосымшалар үшін арналған жалғастыруларды пайдалану қажеттілі туындайды. Қандайда бір қосымшаны жүктемей тұрып антивирустық бағдарламалық қамтамасыздандыруды қосқанда, жүйелік бағдарламалық қамтыиның жаңартылғанына көз жеткізуі. Жалпы қауіпсіздік үшін ұтқыр интернетті пайдаланған дұрыс.

ПАЙДАЛАНЫЛҒАН ӘДЕБИЕТТЕР ТІЗІМІ

1. «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы.

2.Киберқауіпсіздік – http://protect.htmlweb.ru

3.Киберқауіпсіздік - http://wikipedia.org

4.Үшінші әлемдік, кибернетикалық, 5 қазан 2015- http://lenta.ru/articles/2015/10/05/cyberwar

5. Cyberwellness profle Republic of Kazakhstan, Last updated on 5th March 2015 – https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_ Profles/Kazakhstan.pd

РЕЗЮМЕ

В статье раскрыты основы понятия кибербезопасности и способы их возникновения. Кибербезопасность распространяется на Компьютеры, Сети, другие настраиваемые программные компоненты операционной системы. Основная цель кибербезопасности-предотвратить кражу или повреждение информации. Триада безопасной ИТ-инфраструктуры играет важную роль в достижении этой цели-конфиденциальность,

целостность и доступность. Кибербезопасность актуальными вопросами, представляющими собой совокупность технологий, методик и процессов защиты единства программ, сетей и данных от кибератак, обучающимся заявляются основы кибербезопасности в информационном пространстве для защиты электронных информационных ресурсов, информационных систем и информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

RESUME

The article reveals the basics of the concept of cybersecurity and the ways of their occurrence and methods of protection. Cybersecurity applies to computers, networks, and other configurable software components of the operating system. The main purpose of cybersecurity is to prevent information theft or damage. An important role in achieving this goal is played by the trinity of secure IT infrastructure-privacy, integrity and accessibility. Cybersecurity protection of Electronic Information Resources, Information Systems and information communication infrastructure from external and internal threats to the environment with current problems representing a set of technologies, methods and processes for protecting the integrity of programs, networks and data from cyber attacks students are told the basics of cybersecurity in the information space.

ӘОЖ 614.8.067

Білім алушы: Каршгиев А.О., магистрант
Ғылыми жетекші: Ибраев А.С., ғылыми жетекші, техника ғылымдарының кандидаты, доктор Ph,
«Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, Орал қ..

ҰЙЫМ ҚЫЗМЕТКЕРЛЕРІНІҢ ЕҢБЕК ҚАУІПСІЗДІГІ МЕН ДЕНСАУЛЫҒЫН ЖҮЙЕЛЕУ

АННОТАЦИЯ

Ұйымның қауіпсіздігін қамтамасыз етудің мақсаты оның меншігі мен қызметкерлерін сыртқы және ішкі қауіп - қатерлерден, кездейсоқ кез-келген қасақана әрекеттердің салдарынан оларға материалдық, моральдық және физикалық зиян келтіруден қорғау болып табылады. Кәсіпорындағы еңбекті қорғау және қауіпсіздік техникасы – бұл жұмыс беруші жүктеген міндеттерді жүзеге асыру кезінде жұмысшыларды сақтау үшін маңызды шаралар кешені. Еңбек жағдайларын түбегейлі жақсартуға, егер олардың қалыптасуы жұмыс процесінің тікелей жүзеге асырылуынан бұрын басталса, яғни техника мен технологияны жобалау сатысында қол жеткізуге болады. Еңбек жағдайларын жақсарту адамдардың әл-ауқатына, олардың еңбек өнімділігіне немесе оған деген көзқарасына теріс әсер етуі мүмкін қолайсыз факторлардың әсерін жоюға немесе шектеуге бағытталған. Еңбек жағдайларын жетілдірудің әлеуметтік қорытындысы еңбек жағдайлары санитариялық-өнеркәсіптік нормативтерден ауытқулары бар адамдар санын қысқарту.

Кілт сөздер: *еңбек қауіпсіздігі, кәсіпорындағы қауіпсіздік техникасы, жауапкершілік, нысан, электр жабдығы, объект.*

Ұйымның қызметін оның қауіпсіздігін және қызметкерлердің денсаулығын әртүрлі қауіптерден (тәуекелдерден) сенімді қорғаныс көмегімен қамтамасыз етпей елестету мүмкін емес.