Рудный индустриалдық институтында ақпараттық қауіпсіздікті қамтамасыз ету бойынша пайдаланушының нұсқаулығы

1.Жалпы ережелер

1.1.Осы нұсқаулық Интернет желісінің ресурстарымен және сервистерімен жұмыс істеу кезінде оқытушылардың, қызметкерлердің және студенттердің іс-қимыл тәртібін белгілейді.

1.2.Нұсқаулықпен танысу және оны сақтау білім беру мекемесінің барлық оқытушылары, қызметкерлері мен студенттері, сондай-ақ интернет-ресурстармен және сервистермен жұмыс істеуге рұқсат етілген басқа адамдар үшін міндетті болып табылады.

2.Білім беру мекемесінде Интернет желісін пайдалануды ұйымдастыру.

2.1.Студенттерді оқыту мен тәрбиелеудің мақсаттары мен міндеттеріне сәйкес келмейтін ақпараттық ресурстарға қол жеткізуге тыйым салынады.

2.2.Оқытушылар, қызметкерлер және студенттер интернет желісін пайдаланған кезде мазмұны Қазақстан Республикасының заңнамасына қайшы келмейтін және білім беру процесіне тікелей қатысы бар ресурстарға ғана рұқсат беріледі.

2.3.Желі ресурстарын пайдалану кезінде зияткерлік құқықтар туралы заңнаманы және өзге де қолданыстағы заңнаманы сақтау міндетті болып табылады.

2.4.Авторизациялауды көздейтін желілік сервистерді пайдаланған кезде басқалардың есептік деректерін пайдалануға тыйым салынады.

2.5.Интернет желісіне қосылатын барлық компьютерлерде орнатылған, қолданыстағы және жаңартылатын вирусқа қарсы бағдарламалық қамтамасыз ету болуы міндетті.

3. Пайдаланушылардың құқықтары, міндеттері мен жауапкершілігі.

3.1.Интернет желісінің ресурстарын пайдалану білім беру процесі мақсатында жүзеге асырылады.

3.2.Қызметкерлер интернет желісінің жұмысын ұйымдастыруға және қолжетімділікті шектеуге жауапты адамның рұқсаты бойынша жаһандық Интернет-ресурстарға қолжетімділікті тегін пайдалана алады.

3.3.Интернет желісінде жұмыс істеуге осы нұсқаулықпен танысқан және жұмыс ережелерін сақтауға міндеттенген адамдар жіберіледі.

3.4.Пайдаланушыларға тыйым салынады:

- мазмұны мен тақырыптары кәмелетке толмағандар үшін жол берілмейтін және (немесе) Қазақстан Республикасының заңнамасын бұзатын сайттарға (порнография, эротика, зорлық-зомбылықты, терроризмді, саяси және діни экстремизмді, ұлттық, нәсілдік және т. б. алауыздықты насихаттау, ұқсас бағыттағы өзге де ресурстар) кіруге;
- вирустары немесе басқа да компьютерлік кодтары бар, кез келген компьютерлік немесе телекоммуникациялық жабдықтың немесе бағдарламаның функционалдығын бұзуға, жоюға не шектеуге арналған материалдарды, сондай-ақ коммерциялық бағдарламалық өнімдерге сериялық нөмірлерді және оларды генерациялауға арналған

бағдарламаларды, логиндерді, парольдерді және интернет желісіндегі ақылы ресурстарға рұқсатсыз қол жеткізуге арналған өзге де құралдарды жүктеуге және таратуға, сондай-ақ жоғарыда көрсетілген ақпаратқа сілтемелер орналастыру;
- вирусқа қарсы пакетте орнатылған вирустардың болуын алдын ала тексермей орындалатын немесе өзге де файлдарды жүктеу және іске қосу;
- азаматтардың ар-намысы мен қадір-қасиетіне нұқсан келтіретін ақпаратты таратуға;
- Интернет желісі арқылы кез келген мәмілелерді жүзеге асыруға;
- Интернет желісінде жұмысты ұйымдастыруға жауапты болып тағайындалған тұлғаның келісімінсіз көлемді ресурстармен (бейне, аудио, чат, фото) жұмыс істеу.
3.5.Пайдаланушылар жауапты:
- РИИ ақпараттық ресурстарымен жұмыс істеу үшін берілген парольді жария еткені үшін. Құпия сөзді ауыстырған кезде ол кемінде 6 таңбадан тұруы керек, кемінде бір бас әріп және латын тілінде бір жол болуы керек. Мүмкіндігінше құпия сөз ретінде туған жыл немесе есімі қойылмаған дұрыс;
- берілетін, қабылданатын және басып шығарылатын ақпараттың мазмұны үшін;
- жабдыққа кез келген залал келтірілмеуі (мүлікті бүлдіру, жабдықты жұмыс жағдайынан шығару) пайдаланушы заңнамаға сәйкес материалдық жауаптылықта болады;
3.6.Пайдаланушылар құқылы:
- уақыт кезеңі ішінде Интернет желісінде жұмыс істеу;
- алынған ақпаратты алынбалы дискіде сақтауға (дискета, CD, флэш-диск).
4.Штаттан тыс жағдайлардағы әрекеттер.
4.1. Интернет желісіне қосылуды жоғалтқан (оның ішінде ішінара) кезде ақаулықты анықтаған тұлға бұл туралы Интернет желісіне қосылуды ұйымдастыру үшін жауапты қызметкерге хабарлайды.
5.Компьютерлік қауіпсіздікті қамтамасыз ету мақсатында пайдаланушы:
5.1 компьютерде вирусқа қарсы бағдарламалық қамтамасыз етуді қосу. Файлдық жүйені автоматты түрде сканерлеу режимін қосады. Компьютер қосылған кезде бүкіл файлдық жүйені күнделікті автоматты түрде тексеру режимін қосады. Антивирустық базаларды күнделікті автоматты түрде жаңарту функциясын іске қосады.
5.2 күн сайын вирусқа қарсы бағдарламалық қамтамасыз етудің жай-күйін тексеру, атап айтқанда:
5.2.1. автоматты қорғау режимінің тұрақты қосылуын қамтамасыз ету;
5.2.2. вирусқа қарсы базаларды жаңарту күні ағымдағы күннен бірнеше күннен артық ерекшеленбеуі тиіс;
5.2.3. күнделікті антивирустық тексеру журналдарын қараңыз;
5.2.4 вирустар пайда болған кезде оларды жоюды бақылау.
5.2.5 кем дегенде айына бір рет http://windowsupdate.microsoft. сайтқа кіру соңғы операциялық жүйенің жаңартулары орнатылғанын тексеру.

5.2.6. Электрондық поштамен жұмыс кезінде өте сақ болыңыз. Категориялық: бейтаныс адамдардан алынған хаттарға қосылған файлдарды ашуға тыйым салынады.
5.2.7 вирусқа қарсы бағдарламалық қамтамасыз етумен жұмыс басталар алдында олардың сыртқы ақпарат тасымалдағыштарын міндетті түрде тексеруі қажет.