DOI:10.26104/NNTIK.2023.18.76.022

Арынбаев Э.К.

БИЛИМ БЕРҮҮ ТАРМАГЫНДАГЫ ИНТЕРНЕТ САБАТТУУЛУГУНУН ОРДУ

Арынбаев Э.К.

МЕСТО ИНТЕРНЕТ-ГРАМОТНОСТИ В ОБРАЗОВАНИИ

E. Arynbaev

THE PLACE OF INTERNET LITERACY IN EDUCATION

УДК: 372.8

Интернет сабаттуулугу азыркы маалыматтык коомдо маанилүү көндүм болуп саналат. Бул көндүмгө ээ болгон адамдар интернеттен алынган маалыматты издөө, талдоо, баалоо, ошондой эле максаттарына жетүү үчүн жаңы технологияны эффективдүү колдоно алышат. Интернет сабаттуулуктун билим берүүдөгү орду да абдан маанилүү. Интернет маалыматтын эң маанилүү булагы болгон азыркы дүйнөдө билим берүү мекемелери окуучуларга окуу предметтерин гана эмес, тармактан алынган маалыматты табуу, баалоо жана колдонуу менен байланышкан техникалык көндүмдөрдү да өздөштүрүүсүнө жардам бериши керек. Ошол эле учурда интернет коопсуздугу маселеси интернет сабаттуулугунун маанилүү бөлүгү болуп, билим берүү тармагында да негизги орунда туруусу керек. Бул студенттерге коопсуз жана жоопкерчиликтүү интернет колдонуучулар болууга жардам берет жана тармакты колдонуу менен байланышкан тобокелдиктерди азайтат. Макалада интернетти пайдалануу сабаттуулугунун билим берүүдөгү маселелери каралган.

Негизги сөздөр: *окуучу, интернет, интернет сабаттуулук, маалыматтык-коммуникациялык технология, коопсуздук, билим берүү, маалымат, интернет коопсуздугу.*

Интернет-грамотность является важным навыком в современном информационном обществе. Люди с этой способностью могут искать, анализировать, оценивать информацию, полученную из Интернета, и эффективно использовать новые технологии для достижения своих целей. Роль интернет-грамотности в образовании также очень важна. В современном мире, где Интернет является важнейшим источником информации, образовательные учреждения должны помогать учащимся овладевать не только учебными предметами, но и техническими навыками, связанными с поиском, оценкой и использованием информации из Интернета. В то же время безопасность в Интернете является важной частью интернет-грамотности и должна занимать важное место в образовании. Это помогает учащимся стать безопасными и ответственными пользователями Интернета и снижает риски, связанные с использованием сети. В статье рассматриваются вопросы интернет-грамотности в образовании.

Ключевые слова: *студент, Интернет, интернет-грамотность, информационно-коммуникационные технологии, безопасность, образование, информация, интернет-безопасность.*

Internet literacy is an important skill in today's information society. People with this ability can search, analyze, evaluate information obtained from the Internet and effectively use new technologies to achieve their goals. The role of Internet literacy in education is also very important. In today's world, where the Internet is the most important source of information, educational institutions must help students master not only academic subjects, but also the technical skills associated with finding, evaluating and using information from the Internet. At the same time, Internet safety is an important part of Internet literacy and should have an important place in education. This helps students become safe and responsible Internet users and reduces the risks associated with using the network. The article deals with the issues of Internet literacy in education.

Key words: *student, Internet, Internet literacy, information and communication technologies, security, education, information, Internet security.*

Жаңы маалыматтык-коммуникациялык технологиялардын өнүгүшү, анын коомдун бардык ишмердүүлүк чөйрөлөрүндө кеңири пайдаланылышы менен интернет чоң мааниге ээ болуу менен жашоо-буздун ажырагыс бир бөлүгү болуп калды. Интернеттин жардамы менен маалымат алабыз, бири бири-биз менен байланышабыз, маалымат алмашабыз, керектүү товарларды жана кызматтарды онлайн сатып алабыз, банк кызматтарын колдонобуз, көңүл ачабыз жана башка көптөгөн интернет кызматтарын пайдаланабыз. Айрыкча 2019-жылдын аягында Кытайдын чыккан инфекция жана анын дүйнөгө таралышынан пайда болгон кырдаал бүткүл адамзаттын жашоосуна көп жаңыча жашоону алып келди. Анын натыйжасында интернеттин коомдогу орду мурдагыдан да көбүрөөк мааниге ээ болуп калды [1].

Бирок ошол эле учурда интернеттин пайдасы менен бирге маалыматтын жана жеке жашоонун коопсуздугуна байланыштуу белгилүү бир коркунучтар да жок эмес. Демек, интернеттин актуалдуулугу анын коопсуздугун камсыз кылуу жана колдонуучулардын интернет сабаттуулугун өнүктүрүү зарылчылыгы менен да байланыштуу.

Интернет колдонуучулардын санынын өсүшү жана технологиянын өнүгүшү менен кошо эле киберкылмыштуулук кеңири таралып, анын түрлөрү көбөйүп баратат. Хаккерлер, шылуундар жана башка интернет чабуулчулар колдонуучулардын жеке маалыматтарына жетүү үчүн ар кандай ыкмаларды колдонуп жатышат [3].

Интернет коопсуздугу жеке маалыматтарды уруксатсыз пайдалануу менен эле чектелбестен бүтүндөй чоң мекемеге кээде мамлекеттик саясатка да зыян келтирген учурлар кездешет.

Интернеттеги жеке маалыматтарга зыян алып келүүчү коркунучтар ар кандай булактардан, анын ичинде киберкылмышкерлерден, хаккерлерден, компьютердик вирустардан, фишингдик чабуулдардан жана маалымат технологияларын кыянаттык менен пайдалануунун башка түрлөрүнөн келип чыгышы мүмкүн.

Киберкылмышкерлер жана хакерлер колдонуучунун жеке маалыматтарына жетүү, веб-сайттарды бузуу же компьютерлерге зыяндуу программаларды көчүрүп иштетүү үчүн ар кандай ыкмаларды пайдаланышат. Анын ичинде фишинг чабуулдары, компьютердик вирустар жана башка зыяндуу программалар да колдонуучулардын коопсуздугуна олуттуу коркунуч келтирип, зыяндуу программалар компьютерлерге орнотуп, купуя маалыматтарды чогултуп, аккаунттарды жана сыр сөздөрдү кармап, спам же башка зыяндуу программаларды таратуу үчүн колдонулат. Мындан тышкары, интернетте мамлекеттик же коммерциялык уюмдар тарабынан колдонуучулардын маалыматтарын алардын уруксатысыз же катышуусуз колдоно турган коркунуч болушу мүмкүн, бул маалыматтардын сыртка чыгып кетишине, жеке маалыматтардын купуялык укуктарынын бузулушуна жана башка олуттуу кесепеттерге алып келет. Интернетте колдонуучулардын коопсуздугуна жана алардын жеке маалыматтарына таасир этүүчү кеңири таралган онлайн коркунучтардын айрымдарына токтололу:

Зыяндуу программалык камсыздоо (вирустар, курттар (червдер), трояндар): бул колдонуучунун уруксатысыз компьютерге орнотулуп, жеке маалыматтарды көчүрүп алуучу же компьютерге зыян келтирүүчү программалар.

Фишинг: Бул расмий же ишенимдүү булактардын билдирүүлөрүн, электрондук каттарын жамынып, сырсөздөр жана кредиттик карта номерлери сыяктуу колдонуучунун купуя маалыматтарын алууга багытталат.

Жеке маалыматты уурдоо: Кол салгандар колдонуучунун жеке компьютерине, электрондук почта даректерине, телефон номерлерине жана башкаларга кирип, жеке маалыматтарын уурдашат.

Социалдык инженерия: Мында чабуулчулар колдонуучуларды купуя маалыматка жетүү же компьютерлерге зыяндуу программаларды жуктуруп алуу үчүн социалдык тармактын пайдалануучуларын манипуляциялайт.

Купуялыктын бузулушу: Бул хакердик чабуулдар аркылуу жеке жактардын же мекемелердин жашыруун маалыматтары сыртка уруксатсыз чыгып, жайылтылат.

Киберкуугунтук (кибербуллинг): Бул коркутууларды, мазактоолорду жана башка колдонуучуларга карата басмырлоонун жана зомбулуктун башка түрлөрүн камтыган онлайн зомбулуктун бир түрү.

Каалабаган жарнамалар жана спамдар: Бул жарнамаларды, спам электрондук каттарды жана керексиз байланыштын башка түрлөрүн камтышы мүмкүн. Алар колдонуучуларды тажатып гана тим болбостон, зыяндуу программаларды кармап, жеке компьютердин коопсуздугуна коркунуч келтирет.

DDoS чабуулдары: Бул чабуулчулар тармакты же сайтты колдонуучуларга жеткиликсиз кылуу үчүн сайтка же тармакка ашыкча жүк келтирүү менен маалыматтын жоголушуна же Интернеттеги маанилүү ресурстарга убактылуу жете албай калууну уюштурушат.

Акча уурдоо: Бул колдонуучунун финансылык каражаттарына олуттуу зыян келтире турган онлайн сатып алууларды, каржылык алдамчылыктарды жана акча уурдоонун башка түрлөрүн камтыйт.

Автордук укукту бузуу: Бул интеллектуалдык менчик укуктарын бузууну, материалдарды авторлордун уруксатысыз көчүрүү же кайра таратууну жана автордук укуктун мыйзамдарын бузуунун башка түрлөрүн камтыйт.

Порнография жана зомбулук: Бул колдонуучулардын психикасына, ден соолугуна жана жакшы жашоо образына зыян келтириши мүмкүн болгон коомго жагымсыз, адаттын тыш маалыматтарга кирүү мүмкүнчүлүгүн жаратат.

Мыйзамдарды бузуу: Бул тыюу салынган маалыматты таратуу же мыйзамсыз товарларды сатуу сыяктуу мыйзамсыз онлайн аракеттерди камтыйт.

Жалпы интернетте пайда болгон коркунучтар билим берүү тармагына да олуттуу терс таасирин тийгизет. Акыркы жылдары онлайн билим берүүнүн өсүшү менен интернетти билим берүү максатында колдонууга байланыштуу жаңы коркунучтар пайда боло баштады. Алардын айрымдарына токтололу:

Плагиат – окуучулардын башкалардын эмгегин көчүрүп алып, аны өздүк кылып көрсөтүүсү. Плагиатты аныктай турган атайын программалар бар, бирок бул дайыма эле аны токтотууга жардам бере бербейт.

Жеке маалыматка мыйзамсыз кирүү – окуучулардын маалымат базасына же жеке маалыматына уруксатсыз кирүүнү камтыйт.

Онлайн курс шылуундары – мааниси жок жалган курстарды түзүү же курстарды аяктагандыгы тууралуу жасалма сертификаттарды сатуу.

Билим берүү мекемелеринин веб-сайттарын, порталдарын бузуу – электрондук почта даректери, сырсөздөрү жана башка купуя маалыматтары сыяктуу жеке маалыматтарын уурдоо, жеке баалоого байланышкан маалыматтарды өзгөртүү ж.б.

Жалпысынан алганда интернет коопсуздугу колдонуучулардын жеке маалыматтарын коргоо жана тармакты колдонуу менен байланышкан коопсуз-

дук багытындагы тобокелчиликтерди азайтуу үчүн өзгөчө көңүл бурууну талап кылган маанилүү маселе болуп саналат. Ошондуктан Интернет коркунучтары менен күрөшүү менен алектенген ар кандай уюмдар жана мамлекеттик органдар, маалыматтык коопсуздук адистери киберчабуулдардан жана интернет коркунучтарынын түрлөрүнөн коргонуунун жаңы ыкмаларын түзүү үчүн тынымсыз иштешет. Ар кандай программалардагы жана системалардагы алардын алсыз жактарын аныктоо жана аларды жоюу боюнча изилдөөлөр жүргүзүлүп, тиешелүү чаралар көрүлүүдө. Алар интернет колдонуучуларды коопсуздуктун негиздерине үйрөтүү жана жаңы коркунучтар жана алардан коргонуу жолдору тууралуу маалымат таратуу боюнча иш-чараларды өткөрүшөт. Ал үчүн маалыматтарды шифрлөөнүн жаңы ыкмаларын түзүп ишке киргизишет, зыяндуу программаларды жана вирустарды аныктоочу программаларды түзүшөт, колдонуучулардын аккаунттарын коргоо үчүн көп факторлуу аутентификацияны иштеп чыгып орнотушат, интернет колдонуучуларды коопсуздуктун негиздерине үйрөтүү боюнча иш чараларды өткөрүшөт, маалыматтык коопсуздук чөйрөсүн жөнгө салуучу мыйзамдарды жана ченемдик укуктук актыларды иштеп чыгып, тиешелүү мамлекеттик органдарга сунушташат. Бирок, интернет коркунучтары тынымсыз өзгөрүп, татаалдашып жаткандыктан, алар менен күрөшүү ыкмаларын тынымсыз өркүндөтүү жана маалыматтык коопсуздуктун жогорку деңгээлин кармап туруу чечилбеген маселе боюнча калууда [4].

Бул онлайн коркунучтарды алдын алуу үчүн билим берүү мекемелери күчтүү коопсуздук саясатын ишке ашырып, окуучуларга интернетти кантип коопсуз колдонуу керектиги боюнча билим берип, интернетте плагиат жана башка мыйзамсыз аракеттерди аныктоо үчүн атайын программалык жабдылыштарды, платформаларды пайдаланса болот. Ошондуктан бүгүнкү күндө интернетти пайдалануу сабаттуулугу абдан маанилүү. Интернетти пайдалануунун сабаттуулугу төмөнкүлөрдү камтыйт [2, 5, 6, 7]:

- Интернетте жайгашкан маалыматтын ишенимдүүлүгүн баалоо;
- Социалдык тармактарды, электрондук почтаны жана башка онлайн ресурстарды коопсуз колдонуу;
- Интернеттеги жеке маалыматтарды коргой билүү;
- Электрондук документтер жана файлдар менен иштөө;
- Ар кандай пайдалуу онлайн системаларды, платформаларды колдонуу;
- Интернетте этика эрежелерин сактоо;
- Керектүү маалыматты алуу үчүн онлайн ресурстарды издөө жана тандоо;
- Ачкыч сүйлөм боюнча издөө, чыпкаларды колдонуу ж.б. сыяктуу эффективдүү интернет издөө ыкмаларын колдонуу;
- Макалаларды, тезистерди жана башка иштерди жазууда колдонулган маалымат булактарын туура келтирүү;
- Интернетти колдонуу боюнча көйгөйлөр же суроолор боюнча жардам алуу;
- Кесепеттүү программа, фишинг, алдамчылык ж.б. сыяктуу онлайн коркунучтардын ар кандай түрлөрүн айырмалоо;
- Интернеттеги коркунучтардан коргоо үчүн антивирустук программаларды жана брандмауэрлерди орнотуу жана конфигурациялоо;
- Коопсуз сырсөздөрдү түзүү жана башкаруу ж.б.

Ошондуктан, интернетти колдонуунун коопсуздугун жана натыйжалуулугун жогорулатуу үчүн окуу программаларына интернет сабаттуулугун киргизүү менен жалпы интернеттин колдонуучуларына жайылтуу зарыл. Билим берүү тармагындагы интернет коркунучтары менен күрөшүү бир нече кадамдарды камтыйт:

1. Интернетти коопсуз колдонууга үйрөтүү: окуучуларга жана мугалимдерге интернет коопсуздугунун негизги принциптерин үйрөтүү керек, анын ичинде логин жана сыр сөздөрдү колдонуу, антивирустук программаларды туура орнотуу, жашыруун маалыматты коргоо ж.б.

2. Уруксатсыз кирүүлөрдөн корголгон тармактарды жана системаларды уюштуруу: билим берүү мекемелери өздөрүнүн компьютердик тармактарынын жана системаларынын коопсуздугун камсыз кылууга, анын ичинде брандмауэрлерди орнотууну, зыяндуу программалардан коргоону ж.б.

3. Мониторинг жана жаңыртуу: тармактар жана системалар мүмкүн болуучу коркунучтарга үзгүлтүксүз мониторинг жүргүзүү жана жаңы коркунучтардан коргоо үчүн керектүү коргоочу программаларды тынымсыз жаңыртуусу керек.

4. Маалыматтык коопсуздук боюнча эксперттер менен кызматташуу: билим берүү мекемелери интернет коопсуздугу боюнча кеңеш алуу үчүн маалыматтык коопсуздук боюнча адистешкен компаниялар же уюмдар менен өнөктөш боло алышат.

5. Социалдык инженерия боюнча тренинг: билим берүү мекемелери окуучуларды, студенттерди, мугалимдерди жана башка кызматкерлерди социалдык инженерияны таануу жана алдын алуу боюнча үйрөтүшү керек, б.а. жашыруун маалыматты алуу үчүн адамдарды манипуляциялоону болтурбоого алдын ала даяр болуу.

6. Маалыматтык коопсуздук саясатын түзүү: билим берүү мекемелеринде маалыматтардын коопсуздугун кантип камсыз кылууну жана мүмкүн болуучу коркунучтарга жооп кайтаруу жолдорун аныктаган так маалыматтык коопсуздук саясаты болушу керек.

7. Коопсуздук багытындагы билимдерди үзгүлтүксүз жаңыртуу: интернеттеги коркунучтар дайыма өзгөрүп тургандыктан, окуучуларды, студенттерди жана мугалимдерди маалыматтык коопсуздуктун жаңы ыкмаларына жана технологияларына такай окутуу зарыл.

8. Системалык коопсуздук аудити: билим берүү мекемелери системалардагы жана тармактардагы алсыз деп эсептелеген жерлерди аныктоо жана ал кемчиликтерди жоюу үчүн чараларды көрүү үчүн үзгүлтүксүз коопсуздук аудитин жүргүзө алат.

9. Байланыш үчүн коопсуз чөйрөнү түзүү: билим берүү мекемелери окуучулар жана студенттер менен мугалимдердин ортосунда баарлашуу жана маалымат алмашуу үчүн коопсуз аянтчаларды түзө алат. Мындай аянтчалар сыр сөз менен корголушу, коопсуз маалыматтарды берүү протоколуна жана башка коопсуздук чараларына ээ болушу керек.

10. Айрым сайттарга жана ресурстарга кирүү мүмкүнчүлүгүн чектөө: билим берүү мекемелери коопсуздукка коркунуч туудурган же ылайыксыз, коомго жат, адаттан тыш мазмунду камтыган айрым сайттарга жана ресурстарга кирүүнү чектеши мүмкүн.

11. Үзгүлтүксүз коркунучтарга каршы аракеттенүү: билим берүү мекемелеринде коопсуздук коркунучу менен күрөшүү боюнча пландар, ошондой эле мүмкүн болуучу коркунучтардын кесепеттерин тез жана натыйжалуу жоюуну камсыз кылуу үчүн кызматкерлер үчүн машыгуулар өткөрүлүп туруусу керек.

12. Психологиялык бейпилдикти колдоо: билим берүү мекемелери интернет коркунучунун курмандыгы болгон окуучуларга, студенттерге жана мугалимдерге колдоо көрсөтүшү керек. Бул психикалык саламаттыкты сактоо адистери менен кеңешүүнү, ошондой эле ушул сыяктуу жагдайларга туш болгондор үчүн колдоо коомун түзүүнү камтышы мүмкүн.

13. Окуучуларга, студенттерге интернет пайдалануда коопсуз онлайн жүрүм-турумуна үйрөтүү: билим берүү мекемелери студенттерди онлайн режиминде коопсуз жүрүм-турумга үйрөтүшү керек. Бул сайттын аутентификациясы, фишинг аракеттерин аныктоо, жеке маалыматтарды сактоо ж.б. сыяктуу көндүмдөрдү камтышы мүмкүн.

14. Программалык камсыздоону үзгүлтүксүз жаңыртуу: билим берүү мекемелери компьютерлерде жана башка түзүлүштөрдө колдонулган программалык камсыздоону үзгүлтүксүз жаңыртып турушу керек. Бул алсыздыктарды жоюуга жана системаларды жаңы коркунучтардан коргоого жардам берет.

15. Маалыматтын резервдик көчүрмөсү: билим берүү мекемелери потенциалдуу киберчабуулдардан жана башка коркунучтардан коргоо үчүн өз маалыматтарынын резервдик көчүрмөсүн үзгүлтүксүз түрдө сактоого тийиш. Мындай резервдик көчүрмөнү сактоо керектүү маалыматтар жоголгон же система бузулган учурда маалыматтарды тез калыбына келтирүүгө мүмкүндүк берет.

16. Зыяндуу программаларды үзгүлтүксүз текшерүү: билим берүү мекемелери компьютерлерди жана башка аппараттарды вирустар, трояндар жана шпиондук программалар сыяктуу зыяндуу программаларга дайыма текшерип турушу керек. Бул коркунучтарды аныктоого жана аларды жоюу үчүн чараларды көрүүгө жардам берет.

17. Тармактык байланыштардын коопсуздугун текшерүү: билим берүү мекемелери өздөрүнүн тармактык байланыштарынын коопсуздугун дайыма текшерип туруулары керек. Буга Wi-Fi тармактарынын коопсуздугун текшерүү, тармакка алыстан кирүү үчүн VPN туташууларын колдонуу ж.б.у.с. кирет.

Бул кадамдардын баары билим берүү мекемелериндеги коопсуздуктун жогорку деңгээлин камсыз кылууга жана онлайн коркунучтарды азайтып, алдын алууга жардам берет.

Адабияттар:

1. Арынбаев Э.К., Көлбаева З.И. Экстремалдык кырдаалда аралыктан окутуунун көйгөйлөрү. / Наука, новые технологии и инновации Кыргызстана. 2021. № 5.
2. Бороненко Т.А., Кайсина А.В., Федотова В.С. Развитие цифровой грамотности школьников в условиях создания цифровой образовательной среды. Перспективы Науки и Образования. Международный электронный научный журнал. 2019.
3. Губин М.С. Преступления в сети Интернет. Учебное пособие. - Литрес. 2020-2.
4. Денисов Д.В. Безопасность в Интернете: защита от внешних угроз. - Литрес. 2016.
5. Калдыбаев С.К., Орозбаева А.А. Санариптик сабаттуулукту калыптандыруунун принциптери. Alatoo Academic Studies. 2022. № 2.
6. Калдыбаев С.К., Орозбаева А.А. Санариптик сабаттуулуктун ролу жана мааниси. Alatoo Academic Studies. 2020. №2.
7. Лавров В.С. Цифровая грамотность. Секреты успешного поиска и обработки информации. - Литрес. 2018.
8. https://msk.tele2.ru/journal/article/20-rules-for-safety-internet
9. https://www.ucheba.ru/project/websafety
10. Арынбаев Э.К., Колбаева З.И. Проблемы дистанционного обучения в экстремальных условиях. // Наука, новые технологии и инновации Кыргызстана. 2021. №. 5. С. 105-111.