ТАҚЫРЫП: Ақпараттық кеңістіктегі киберқауіпсіздік негіздері

1. Сабақтың мақсаты: Білімгерлерге ақпараттық кеңістіктегі киберқауіпсіздік негіздері туралы мәліметтер беру.

2. Сабақтың барысы:

а) Ұйымдастыру кезеңі:

Взвод командирі білімгерлерді сапқа тұрғызады, оқытушыға рапорт береді, амандасу, түгендеу, білімгерлердің сырт көрінісін тексеру.

ә) Өтілген тақырыпты сұрау кезеңі:

1. Терроризм, террорлық акт, терроризм актісі деген не?
2. ҚР-да террорлық қауіптің қандай деңгейлері тағайындалған?
3. Жарылғыш құрылғыға ұқсас зат табылған кезде адам өзін қалай ұстау керек?
4. Террорист көлік құралдарын басып алған жағдайда және онымен сөйлескенде өзіңді қалай ұстауың керек?
5. Террористер кепілге алған жағдайда қандай шаралар қабылдау керек?
6. Террорлық әрекетке қарсы қандай ақпараттық технологиялар қолданылады ?

б) Негізгі бөлім:

Бүгінде технология қарыштап дамыған заманда киберқауіпсіздік бүкіл әлемде өзекті мәселеге айналып отыр. Киберқауіпсіздік түсінігін жан-жақты қарастыралық.

Киберқауіпсіздік түсінігі. Ақпараттық жүйелер мен электрондық желілер «өнеркәсіптік автоматика және бақылау жүйелері» деген жалпы атауға ие. Өнеркәсіптік автоматика мен бақылау жүйелерінің қауіпсіздігі деп штаттық және жоспарланған жұмысқа заңсыз енуді немесе қасақана араласуды, не болмаса қорғалатын ақпаратқа қолжетімділікті болдырмауды айтады. Киберқауіпсіздік компьютерлерге, желілерге, операциялық жүйелерге. қосымшаларға және өнеркәсіптік автоматика мен бақылау жүйесінің басқа да конфигурацияланатын бағдарлама құрамдастарына қолданылады .

Киберқауіпсіздік *бағдарламалардың, желлер мен мәліметтердің біртұтастығын кибер шабуылдардан (цифрлық шабуылдардан) қорғау технологияларының, әдістемелер мен процестердің жиынтығын білдіреді.*

Ақпараттық қауіпсіздік

Құқық бұзушылар құпия ақпаратты заңсыз көшіріп алу немесе редакциялау (жою немесе түрін өзгерту) мақсатымен (рұқсат етілмеген) кибершабуыл жасайды. Оны, негізінен, адамдардан (ақпараттық жүйелерді пайдаланушылардан) қаржыны ұрлау немесе ұйымдағы өндірістік немесе жұмыстық процестерді бұзу, тіпті мемлекеттік құпияларды ұрлау мақсатында жүзеге асырады.

Қазіргі кезде көптеген ұйымдар мен үкіметтік мекемелерде жұмысқа қажетті барлық ақпаратты, сондай-ақ қызметкерлердің, пайдаланушылардың және т.б. жеке мәліметтерін жинау, сақтау және өңдеу жолға қойылған. Ал бұл ақпаратты қорғауды талап етеді, өйткені ақпарат құпия болуы керек. Осы ақпараттардың жоғалуы немесе ұрлануы адамдар, ұйымдар және тіпті мемлекет үшін де кері салдарға әкелуі мүмкін.

Киберқауіпсіздік тұжырымдамасы («Қазақстанның киберқалқаны») Қазақстанның әлемнің ең дамыған 30 мемлекетінің қатарына ену бойынша «Қазақстан – 2050» стратегиясының тәсілдерін ескере отырып, Қазақстан Республикасы Президентінің «Қазақстанның үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» атты Жолдауына сәйкес әзірленді.

Тұжырымдама мемлекеттік органдардың жеке және заңды тұлғалардың ақпараттық қауіпсіздікті қамтамасыз ету мониторингіне, сондай-ақ ақпараттық қауіпсіздік инциденттерін, оның ішінде әлеуметтік, табиғи және техногендік сипаттағы төтенше жағдайлар, төтенше немесе соғыс жағдайларын енгізу жағдайларында алдын алу және жедел ден қою тетіктерін жасау тәсілдерінің бірлігін қамтамасыз етуге арналған.

Осы тұжырымдаманың орындалуы қазақстандық қоғамды одан әрі жаңғыртуға қызмет етеді және Қазақстанның БҰҰ-ның Киберқауіпсіздіктің жаһандық бағдарламасын іске асыруға қосқан үлесі болады.

Ақпараттық қауіпсіздіктің классикалық үлгісі ақпараттың қауіпсіздігі үшін маңызды үш белгіні қамтамасыз етуге негізделеді: *құпиялылық, тұтастық* және *қолжетімділік.* Ақпараттың құпиялығы онымен өзінің иесі белгілеген катаң шектелген адамдар тобы ғана таныса алады дегенді білдіреді. Егер ақпаратқа қолжетімділікті уәкілеттілігі жоқ адам алатын болса, рұқсат етілмеген қолжетімділікке немесе құпиялықтың бұзылуына жол беріледі.

Заң немесе иесі қорғайтын ақпараттың кейбір түрлері үшін құпиялық ең маңызды белгілерінің (қызметтік акпарат, заңмен қорғалатын құпиялар түрлері, қолжетімділігі шектеулі жеке деректер, мысалы, банктің клиенттері, кредиторлары туралы мәліметтер, салықтық деректер, медицина мекемелеріндегі емделушілердің денсаулық жағдайы туралы мәліметтері және т.б.) бірі болып табылады.

Ақпараттың тұтастығы – ақпараттың (деректердің) бұрмаланбаған түрде сақталу қабілеті. Ақпараттың заңсыз және иесі көздемеген өзгеруі (оператор қатесінің немесе уәкілеттілігі жоқ адамның қасақана іс-әрекетінің нәтижесінде) тұтастықтың бұзылуына алып келеді.

Әсіресе аса маңызды ақпараттық-коммуникациялық инфрақұрылым объектілерінің жұмыс істеуімен байланысты деректердің тұтастығы ерекше маңызды (мысалы: әуе қозғалысын, электрмен және энергиямен жабдықтауды басқарудың автоматтандырылған жүйелері және т.б.) .

Ақпараттың қолжетімділігі – ақпараттық жүйенің тиісті уәкілеттіктері бар субъектілерге ақпаратқа дер кезінде бөгетсіз рұқсат беру қабілеті мен анықталады.

Ақпаратты жою немесе бұғаттау (қателіктің немесе қасақана іс-әрекеттің нәтижесінде) қолжетімділіктің жойылуына алып келеді.

Қолжетімділік – ақпараттық-коммуникациялық қызметтерді беру (теміржол және авиациялық билеттерді сатудың, банктік қызметтердің ақпараттық жүйелері, интернетте енімдерді интернет-ресурстармен және электрондық БАҚ-пен тарату) жолымен клиенттерге қызмет көрсетуге бағытталған ақпараттық жүйе.

Уәкілетті пайдаланушы белгілі бір қызметтерге (көбінесе желілік) рұқсат ала алмайтын жағдайды қызмет көрсетуден бас тарту деп атайды.

Әлеуметтік желілердегі қауіпсіз қарым-қатынастың ережелері. Бүгінде қоғам мүшелері әлеуметтік желілерсіз өз өмірін елестете алмайды. Күн өткен сайын Вконтакте, Одноклассники, Фэйсбук, Твиттер т.б. сияқты әлеуметтік желілерді пайдаланушылар саны артып келеді. Әлеуметтік желілердің көмегімен адамдар бір- бірімен қарым-қатынас жасайды, мәліметтер, фотосуреттер және т.б. алмасады. Мұндай ресурстар неғұрлым танымал бола бастаған сайын, алаяқтар да соғұрлым оларға көбірек қызығушылық танытуда. Осыған байланысты оларды пайдалану қауіпті бола түседі.

Әлеуметтік желілер өлемі сан алуан

Әлеуметтік желілерді пайдалану кезіндегі қауіптіліктер:

1. Жеке ақпаратты (оның ішінде, басқа адамдарға тиістілерін де) жария ету. Бұған тіпті мәліметтердің одан әрі таралуына себепші болатын дос-жаранға жіберген хабарламалар да жатады. Жеке ақпаратты қорғау саласындағы құқықбұзушылықтар тізбегі осылай құрылады.

2. Қауіпті танысулар. Кейбіреулер кәмелетке толмағандармен хат алмасу арқылы азғыруды жүзеге асырса, кейбіреулер жеке кездесуге алдап көндіреді.

3. Қылмыскерлердің назарын аудару. Балалар мен жасөспірімдердің өз өміріндегі барлық оқиғаны әлеуметтік желілерде жария етуі. Тек бір ғана статус пен фотосуреттер бойынша бала мен оның отбасы мүшелерінің қай жерде болатынын, баланың қашан жалғыз қалатынын, қай кезде пәтердің қараусыз қалатынын білуге болады.

4. Жұмыс іздеу, музыка, бейнежазба және т.б. мәліметтерді көшіріп алуға мүмкіндік береді-мыс дейтін қосымшалардың қауіпсіздігіне сенімді болмасаң, оларды орнатудың қажеті жоқ. Көбіне олар орнату кезінде жеке акаунттан логин мен пароль сұратады. Бұл хакерлерге жеке ақпаратқа қолжетімділікті алу мүмкіндігін береді.

5. Басқа компьютерлерден, тіпті ол досыңның компьютері болса да, әлеуметтік желілердегі жеке аккаунттарды ашпау. Өйткені онда сенің аккаунтың туралы мәліметтерді жіберетін вирус болуы мүмкін.

6. Достардан жіберілген тәрізді көрінетін хабарламалар жиі кездеседі, бірақ оларды достарыңның аккаунттарын бұза алған алдаяқтардың жіберуі мүмкін. Егер хабарлама күмәнді болып көрінсе, досыңмен тікелей немесе телефон арқылы жеке байланысып, бұл хабарламаның шынымен досыңнан келгендігіне көз жеткізу қажет.

7. Әлеуметтік желілерге өзің туралы ақпаратты орналастыру кезінде абай болған жөн. Алаяқтар көбіне құпия сұраққа жауап беруді өтінетін «Парольді ұмыттыңыз ба?» батырмасын пайдалана отырып, аккаунттарды бұзады.

8. Әлеуметтік желіге кіру кезінде тек браузердің мекенжай жолын немесе қосымшасын пайдалану керек. Интернеттегі күмәнді сілтеме бойынша әлеуметтік желіге өту жағдайында жеке мәліметтерді ұрлау үшін пайдаланылатын сайтқа түсу тәуекелі туындайды.

9. Өз достарыңның мекенжайларын құпияда ұстау үшін әлеуметтік желілерге электрондық поштадағы мекенжайлар кітапшасының сканерленуіне мүмкіндік бермеу керек.

10. Достарыңа кімдерді қосу керек екендігін қадағалап отыру қажет. Алаяқтар көбіне осындай жолмен қарым-қатынастың тар шеңбері үшін қолжетімді мәліметтерді білуге тырысады.

11. Өз жұмыс орнында әлеуметтік желілерді пайдаланбауға тырысу. Әлеуметтік желі вирустарды немесе тыңшылық бағдарламаларды таратудың көзіне айналуы, олар құпия мәліметтердің жоғалуына әкелуі мүмкін.

Wi - Fi желілерін қауіпсіз пайдалану ережелері. Қазіргі кезде кез келген жерде (қала, ауыл немесе жай ғана көше, қоғамдық орын, мекеме, вокзал) интернетке қолжетімді тегін қоғамдық Wi-Fi нүктелері бар. Өркениеттің бұл игілігінің арқасында желіде тұрақты қалуға, керекті жұмысты орындауға, әлеуметтік медиа-империяны басқаруға, жаңалықтар мен оқиғалардан хабардар болып отыруға болады. Алайда жоғарыда айтылғандай, жалпыға ортақ қолжетімді Wi-Fi нүктелерімен жұмыс істеу онлайн қауіпсіздікке айтарлықтай қатер төндіруі мүмкін. Мұндай қатерден қауіпсіз өту ушін мынадай негізгі іс - шараларды қабылдау қажет:

«Wi-Fi желісін пайдалану туралы келісімді» мұқият оқып шығу, стандартты тіркеуден өту. Бұл келісімде нақ кандай мәліметтердің ұсынылуы тиіс екендігі, бұл меліметтердің қандай пайдаланылатыны және қай жерде сақталатыны туралы мәліметтер

Веб-сайттар мен қосымшалар үшін қорғалған жалғастыруларды пайдалану. Бұл хакерлердің құпия ақпаратты ұрлауынан қорғайды.

Бейресми дүкендерден қандай да бір косымшаны жүктемеу және орнатпау, сондай-ақ антивирустық бағдарламалық қамсыздандыруды қосқанда, жүйелік бағдарламалық қамтымның жаңартылғандығына көз жеткізу.

Жалпыға қолжетімді желілердің үйлердегі немесе жұмыс орындарындағы желілерге қарағанда, қаскүнемдердің ықпалына көбірек ұшырайтынын есте сақтаған жөн.

Банкілік ақпаратты енгізу немесе өте маңызды веб сервиске жедел кіру қажет болған жағдайда қауіпсіздеу балу үшін, балама ретінде қоғамдық «Wi-Fi» нүктесін емес, ұтқыр интернетті пайдаланған дұрыс.

в) Қорытынды бөлім:

Сұрақтар:

1. Киберқауіпсіздік термині нені білдіреді?
2. ҚР да әзірленген киберқауіпсіздік тұжырымдамасының («Қазақстанның киберқалқаны») мені неде?
3. Әлеуметтік желілерді пайдаланудың қандай қауіптілігі бар?
4. Әлеуметтік желілерді пайдалану кезінде алдын ала сақтанудың қандай іс-шараларын қабылдау керек?
5. Оқу орындарына Wi-Fi керек пе? Оны қолдану қауіпсіз бе? Оның зиянды сәулелерінен қалай қорғануға болады?
6. Wi-Fi желілерін қауіпсіз пайдалану ережелері туралы әңгімелеңдер.