**НҰРАШБЕК Інжу,**

**Зоя Космодемьянская атындағы №23 мектеп-лицейінің 6«Д» сынып оқушысы.**

**Жетекшісі: ИМАНТАЕВА Асия Нерубековна.**

**Шымкент қаласы**

**КИБЕРҚЫЛМЫС**

Әрбір заманауи адам күн сайын Интернетте уақыт өткізеді. Енді Интернетте уақыт өткізетін кез-келген адам үшін ең маңызды мәселелердің бірі-компьютерлік қылмыстың даму мәселесі. Қазір отбасында барлығы дерлік компьютер, ноутбук, планшет немесе смартфон бар. Қарапайым пайдаланушының жеке деректеріне немесе ірі кәсіпорындар мен ұйымдарға зиян келтіргісі келетін адамдар көбейіп келеді. Біз үшін қауіпсіздік мәселесі бірінші орынға шығады. Киберқылмыс-бұл виртуалды кеңістіктегі (киберкеңістіктегі) кез-келген қылмыстық әрекет. Кейбір киберқылмыстарда оларды істен шығару мақсатында компьютерлерге немесе басқа құрылғыларға тікелей шабуылдар жасалады. Басқа киберқылмыстарда компьютерлерді киберқылмыскерлер зиянды бағдарламалық кодтарды тарату, заңсыз ақпарат алу, алаяқтық мақсатында жеке деректерді ұрлау үшін пайдаланады. Сонымен, киберқылмыс-бұл қылмыстың құрамдас бөлігі ретінде киберкеңістікте (Интернетті немесе басқа компьютерлік желіні қолдана отырып) жасалған қылмыстар.

**Киберқылмыстың келесі екі санатын бөлуге болады:**

* зорлық-зомбылық немесе өзге де ықтимал қауіпті (физикалық қырып-жою қаупі, киберқылмыс, балалар порнографиясы, киберэкстремизм, кибертерроризм);
* зорлық-зомбылықсыз қылмыстар (киберкеңістікте иеленуді құқыққа қарсы бұзу, киберворовство, кибер алаяқтық, Интернет желісінде жезөкшелік қызметтерін жарнамалау, интернет желісін пайдалана отырып есірткінің заңсыз айналымы, Интернет желісінде құмар ойындар, электрондық орын ауыстырудың көмегімен ақшаны жылыстату, деструктивті киберқылмыстар және басқа да киберқылмыстар).

Еуропа Кеңесінің конвенциясында киберқылмыстың түрлері бес топқа біріктірілген.

Бірінші топқа компьютерлік деректер мен жүйелерге қарсы бағытталған барлық компьютерлік қылмыстар кіреді (мысалы, заңсыз қол жеткізу, деректерге немесе тұтастай жүйелерге араласу).

Екінші топ технологияларды пайдалануға байланысты құқыққа қарсы әрекеттерден тұрады (жалғандық жасау, деректерді алу, бұғаттау немесе өзгерту, өзге тәсілдермен экономикалық пайда алу).

Үшінші топтағы құқық бұзушылықтар деректер мазмұнына немесе мазмұнға байланысты.

Авторлық және сабақтас құқықтардың бұзылуы төртінші топқа жатады.

Кибертерроризм және зорлық-зомбылық әрекеттерін жасау үшін виртуалды кеңістікті пайдалану, сондай-ақ қоғамдық қауіпсіздікке қол сұғатын басқа да әрекеттер киберқылмыстардың бесінші тобына кіреді.

**Киберқылмыскерлер қолданатын ең көп таралған төрт әдіс бар:**

* компьютерлер мен желілерді теріс пайдалануға негізделген зиянды бағдарламаларды пайдалану.
* DDoS шабуылдары: әсер ету объектісін істен шығару үшін байланыс желілік протоколдарын қолдана отырып, серверге немесе қызметке көптеген сұраныстар жасау.
* әлеуметтік инженерия мен зиянды кодтың үйлесімі: жәбірленушіні белгілі бір әрекеттерге мәжбүр етеді (электрондық поштадағы сілтемені басу, сайтқа кіру және т.б.), бұл кейіннен бірінші әдісті қолдана отырып жүйені жұқтыруға әкеледі.
* заңсыз әрекеттер: қудалау, заңсыз мазмұнды тарату, сыртқы келбет және т.б. бұл жағдайда шабуылдаушылар жасырын профильдер, шифрланған хабарламалар және басқа ұқсас технологиялар арқылы іздерін жасырады.
* Әлемнің көптеген елдерінің ережелері киберқылмыс үшін қылмыстық жауапкершілікті қарастырады, жаза айыппұлдан өлім жазасына дейін өзгереді.

**Жұмыстың өзектілігі**-қазіргі уақытта интернет көптеген қауіп-қатерлерге толы және оны пайдаланушылар өздерін олардан қалай қорғауды білмейді.

**Мәселе:** нашар білімге байланысты пайдаланушылар мен олардың компьютерлерінің қауіпсіздігі нашар.

**Жұмыстың мақсаты**-интернетті пайдаланатын адамдардың қауіпсіздік деңгейін арттыру үшін нұсқаулық жасау. Киберқылмыстың алдын алу және онымен күресу жолдары.

**Міндеттері:**

Ғылыми әдебиеттерді зерттеу.

Зерттеу үшін материалдар жинаңыз.

"Қауіпсіз Интернет" ойынын өткізу.

**Гипотеза:** егер адамдар Интернеттің қауіптілігі туралы көбірек білсе, компьютерлер мен олардың пайдаланушыларының қауіпсіздігі артады.

**Зерттеу нысаны:** интернеттегі қауіптерді анықтау процесі.

**Зерттеу тақырыбы**: Интернет пайдаланушыларының қауіпсіздігі.

**Әдістері:**

Интернеттен ақпарат іздеу.

Оқушыларға сауалнама жүргізу.

**Жоба мәселесі:** өзіне және жақындарына киберқылмыстан қалай қорғауды қамтамасыз ету керек?

**Жобаның қысқаша мазмұны:**

1. Киберқылмыс пен киберқылмысты қазіргі ақпараттық қоғамға ықтимал қауіп ретінде зерттеу.
2. Киберқылмыстың алдын-алу жолдары және онымен күресу жолдары қандай екенін біліңіз.
3. Киберқылмыс туралы, әлемде қандай киберқылмыстар жасалатыны, қандай күрес шаралары қабылданатыны туралы айту. Киберқылмыскерлердің іс-әрекеттерінен болатын зиянды анықтаңыз.
4. Фигуралар, фильмдер беру және, мен деген мәселе, ал барлық сонымен қатар, көрсетілгендей экранда?
5. Қарапайым адамдар киберқылмыстан қорқуы керек пе? Егер солай болса, оларды қалай қорғауға және қорғауға болады?

**Мен айтамын:**

* ақпараттық қылмыстардың қандай түрлері бар;
* хакерлік қылмыстар үшін шабуылдаушыларды қандай салдарлар күтеді
* және қалай қорғану, осылайша, алдын алу зиян.

Қазіргі уақытта киберқылмыс мәселесі ерекше өзекті болып отыр.

**Киберқылмыс**: адамзаттың жаһандық мәселесі?

Дербес компьютерлер санының қарқынды өсуі, Интернетке еркін қол жетімділік және жаңа байланыс құрылғыларының жылдам дамып келе жатқан нарығы жастарды да, аға буындағы адамдарды да виртуалды байланысқа тартады. Социологиялық сауалнамалар көрсеткендей, киберқылмыс бүгінгі таңда адамдарды алаңдататын мәселелердің бірі болып табылады.

Жоба бойынша жұмыстың басында мен мақсаттарды белгіледім: киберқылмысты зерттеу, әлемде қандай киберқылмыстар жасалуда, қандай күрес шаралары қабылдануда.

**Осы мақсаттарға жету үшін мен өзіме бірқатар міндеттер қойдым, олардың ішінде:**

* Киберқылмыс түрлерін зерттеу
* Киберқылмыскерлер кім екенін біліңіз
* Үйде хакерлерге қарсы тұру туралы ұсыныстар беріңіз

**Гипотеза:** мен киберқылмыскерлер мен киберқылмыскерлер туралы білім Қазіргі әлемдегі ақпаратпен жұмыс істеу үшін қажет деп санаймын.

**Негізгі бөлімі**

**Киберқылмыс туралы түсінік**

Киберқылмыс-бұл виртуалды кеңістіктегі қылмыс. Виртуалды кеңістікті немесе киберкеңістікті компьютердің көмегімен модельдендірілген ақпараттық кеңістік ретінде анықтауға болады, онда математикалық, символдық немесе кез-келген басқа түрде ұсынылған және жергілікті және ғаламдық компьютерлік желілер арқылы қозғалу процесінде болатын адамдар, заттар, фактілер, оқиғалар, құбылыстар мен процестер туралы ақпарат болады.немесе кез-келген нақты немесе виртуалды құрылғының, сондай-ақ басқа медианың жадында сақталған ақпарат. "Киберқылмыс" термині компьютерлік жүйе немесе желі арқылы, компьютерлік жүйе немесе желі аясында немесе компьютерлік жүйеге немесе Желіге қарсы жасалуы мүмкін кез келген қылмысты қамтиды. Бұл компьютерлердің, компьютерлік бағдарламалардың, компьютерлік желілердің жұмысына заңсыз араласу, компьютерлік деректердің рұқсатсыз модификациясы, сондай-ақ компьютерлер, Компьютерлік желілер мен бағдарламалар арқылы немесе олардың көмегімен жасалған басқа да заңсыз әлеуметтік қауіпті әрекеттер.

Киберқылмыс — бұл сөздің тар мағынасында компьютерлік қылмысты (компьютер объект болып табылатын және ақпараттық қауіпсіздік қылмыс объектісі болып табылатын) және компьютерлер меншікке, авторлық құқыққа, қоғамдық қауіпсіздікке немесе адамгершілікке қарсы қылмыс жасау құралы немесе құралы ретінде қолданылатын басқа да шабуылдарды қамтитын қарапайым ұғым. Киберқылмыспен және оның өмір сүруіне және дамуына жағдай жасауға бағытталған басқа да әрекеттермен шектеседі (байланыс үшін электрондық поштаны пайдалану, қылмыстық идеологияны таратуға бағытталған өз сайттарын құру, сондай-ақ қылмыстық тәжірибе мен Арнайы білім алмасу).Киберқылмыскерлерді құқықтық категория және киберқылмыскерді әлеуметтік құбылыс ретінде ажырату керек сияқты, сонымен бірге олармен тығыз байланысты "қолдау" және ұйымдастырушылық қызметтің әртүрлі нысандарын қамтиды. Бұл тұрғыда қылмысты дайындаған адамдар арасында электрондық пошта алмасу, веб-сайттарға тиісті қылмыстық бағытталған ақпаратты орналастыру әлеуметтік құбылыс ретінде киберқылмысқа да қатысты.

**Киберқылмыскерлер мен киберқылмыстардың жіктелуі**

Еуропа Кеңесінің киберқылмыс туралы Конвенциясы компьютерлік қылмыстардың төрт түрін "таза түрде" дейді ,оларды компьютерлік деректер мен жүйелердің құпиялылығына, тұтастығына және қол жетімділігіне қарсы қылмыс ретінде анықтайды:

1.Заңсыз қол жеткізу — (компьютерлік жүйеге не оның бір бөлігіне құқыққа қарсы қасақана қол жеткізу);

2.Заңсыз ұстап алу - (қоғамға арналмаған компьютерлік деректерді компьютерлік жүйеге, одан не оның шегінде беруді құқыққа қарсы қасақана ұстап алу);

3.Деректерге араласу - (компьютерлік деректерді құқыққа қарсы зақымдау, жою, бұзу, өзгерту не жолын кесу);

4.Жүйеге араласу - (компьютерлік деректерді енгізу, беру, бүлдіру, жою, бұзу, өзгерту не оның жолын кесу жолымен компьютерлік жүйенің жұмыс істеуіне құқыққа қайшы елеулі кедергі жасау).

Дәл осы төрт қылмыс түрі "компьютер" болып табылады, қалғандары не компьютермен байланысты (компьютер — байланысқан), не компьютер (компьютер-facilitated) көмегімен жасалған қылмыстар. Оларға мыналар жатады:

* авторлық және сабақтас құқықтарды бұзуға байланысты қылмыстар;
* компьютерлер қылмыс құралы ретінде қолданылатын әрекеттер (электронды ұрлау, алаяқтық және т. б.);
* компьютерлер зияткерлік құралдардың рөлін атқаратын қылмыстар (мысалы, интернетте ұлттық, нәсілдік, діни араздықты тудыратын ақпаратты орналастыру және т.б.).

Сондай-ақ , хакероми деп аталатын киберқылмыскерлер туралы айту керек.

Компьютерлердің таралуымен қарапайым адамдарда жаңа ұғым пайда болды - "хакер", бұл пайдаланушыларға қызығушылықтан дүрбелең қорқынышына дейін эмоциялар тудырады. Олар туралы кітаптар мен фильмдер жазады. Хакерлер қайдан пайда болды? Хакер сөзі (бастапқыда жиһазды балтамен жасайтын адам) бірнеше анықтамаларға ие:

1. Бағдарламаланатын жүйелерден максималды мүмкіндіктерді зерттеуді және тартуды ұнататын адам, пайдаланушылардың көпшілігіне қарағанда, қажетті минимумнан терең көтерілмейді.

2. Бағдарламаланған адам бағдарламалау теориясынан гөрі даму процесіне Құмар, тіпті құмар немесе ләззат алады.

3. Құбылыстың мәнін тез түсінуге қабілетті адам.

4. Бағдарламаларды жылдам әзірлеуге қабілетті адам.

5. Белгілі бір жүйе бойынша сарапшы, әдетте, оны жиі қолданады.

6. Сарапшы немесе кез-келген энтузиаст.

7. Шығармашылық жеңуден немесе шектеулерді айналып өтуден интеллектуалды ләззат алатын адам.

8. Қажетті ақпаратты табуға тырысатын шабуылдаушы

Қазіргі заманғы "Хакер" ұғымы барлық желілік хакерлер мен компьютерлік вирустарды жасаушыларды сипаттайды.

Сондай-ақ, хакерлерді қылмыстық әрекеттерінің сипатына қарай бөлуге болады.

**Кракер**-қолданбалы бағдарламалық жасақтаманы бұзумен айналысады, әдетте shareware-бағдарламалардан (негізінен пайдаланушыға толық нұсқасын көрсетуге арналған шектеулі функционалды бағдарламалар) толық коммерциялық нұсқаларды алу үшін. Кракер-өте жоғары деңгейдегі бағдарламашы.

**Фрикер-**тегін қоңырау шалу мүмкіндігін табу үшін телефон желілерін зерттейді. Тарихи тұрғыдан алғанда, фрикеризм-ХХ ғасырдың 60-70-ші жылдары пайда болған хакерлік қызметтің алғашқы түрі. Соңғы жылдары фрикерлер ұялы телефон желілерін зерттеумен де айналыса бастады.

**Кардер**-несие карталарының нөмірлерін және олардың иелері туралы ақпаратты заңсыз алумен айналысады. Көбінесе бұл қызмет хакермен біріктіріледі. Кардеризм ең ауыр қылмыс болып саналады, сондықтан хакерлік әрекеттің ең қауіпті түрі болып табылады.

Вирус жазғыш-вирустардың емлесі хакерлік әрекетке жататындығы туралы факт өте қайшылықты. Бірақ, соған қарамастан, соңғы уақытта тек Outlook пошта бағдарламасындағы қателіктер арқылы таратылатын пошта вирустары кеңінен таралуда және мұндай қателерді іздеуді хакерлік қызмет деп санауға болады.

**Қорытынды**

Компьютерлік шабуыл мемлекеттің ақпараттық инфрақұрылымын толығымен парализдеуге және әлеуметтік, қаржылық немесе экологиялық апатқа әкелуі мүмкін. Кибершабуыл үшін жаза қатаң болады: миллион тг айыппұл немесе 5-10 жылға бас бостандығынан айыру соңғы жылдардағы киберқылмыскерлер 2015 жылдың 15 ақпанында Касперский зертханасы, Европол және Интерпол киберқылмыс операциясын ашты, онда хакерлер 1 миллиард доллар ұрлады.тонау екі жылға созылды және бүкіл әлем бойынша 100-ге жуық қаржы ұйымдарына әсер етті. Ресей, Украина, Қытай және бірқатар Еуропа елдерінің Халықаралық қылмыстық тобы қылмысқа күдікті.

2016 жылғы 5 ақпанда хакерлер Бангладештің Орталық Банкінің АҚШ-тың ФРЖ-дағы шотынан 101 миллион доллар ұрлады. Ірі біржолғы ұрлықтардың бірінің сомасы одан да көп болуы мүмкін (950 миллион доллардан астам), бірақ хакерлер аударым жасаған кезде қате жіберді, бұл қылмыстық схеманы ашты.

2016 жылдың 14 ақпанында хакерлер Голливудтағы Пресвитериан медициналық орталығының компьютерлерін бақылауға алды. Ақпараттық жүйелерге кіруді қайтару үшін қылмыскерлер 17 мың биткоин (3,6 миллион доллар) сатып алуды талап етті. Төрт күннен кейін клиника бұл соманы төледі. 2016 жылдың 14 қарашасында PCWorld журналы американдық FriendFinder Network компаниясының сайттарын пайдаланушылардың 412 млн аккаунтын бұзғанын хабарлады. Ақпараттың көп бөлігі танысу сайтынан ұрланған. Хакерлер электрондық пошта мекенжайлары мен құпия сөздерді ұрлады.

Осылайша, қойылған мақсаттарға қол жеткізілді деп болжауға болады. Біз көптеген жаңа, қызықты және пайдалы нәрселерді білдік. Алынған білім өмірде бәрімізге пайдалы болады.

Қоғам өмірінің компьютерлік жүйелерге тәуелділігі неғұрлым күшті болса, ҚР мен басқа елдердің киберқылмыскерлердің барлық түрлеріне осалдығы соғұрлым қауіпті болады. Қауіпсіздік туралы бүгін ойлану керек, ертең кеш болуы мүмкін.