ҚАЗАҚСТАН РЕСПУБЛИКАСЫ
БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН
MINISTRY OF EDUCATION AND SCIENCE
OF THE REPUBLIC OF KAZAKHSTAN

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ
ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ
ЕВРАЗИЙСКИЙ НАЦИОНАЛЬНЫЙ
УНИВЕРСИТЕТ ИМ. Л.Н. ГУМИЛЕВА
GUMILYOV EURASIAN
NATIONAL UNIVERSITY

ЖАС ҒАЛЫМДАР КЕҢЕСІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2015» атты X Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ X Международной научной конференции студентов и молодых ученых «Наука и образование - 2015»

PROCEEDINGS of the X International Scientific Conference for students and young scholars «Science and education - 2015»

УДК 001:37.0
ББК72+74.04
Ғ 96

Ғ96
«Ғылым және білім – 2015» атты студенттер мен жас ғалымдардың X Халық. ғыл. конф. = X Межд. науч. конф. студентов и молодых ученых «Наука и образование - 2015» = The X International Scientific Conference for students and young scholars «Science and education - 2015». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie-2015/, 2015. – 7419 стр. қазақша, орысша, ағылшынша.

ISBN 978-9965-31-695-1

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 001:37.0
ББК 72+74.04

ISBN 978-9965-31-695-1

ӘӨЖ 004.5:37

КИБЕРҚЫЛМЫС КЛАССИФИКАЦИЯСЫНЫҢ ҚАТЕРЛЕРІ ХАЛЫҚАРАЛЫҚ ҚҰБЫЛЫС РЕТІНДЕ

Каирбаева Назгуль
aijuka-.94@mail.ru
Л.Н. Гумилев атындағы ЕҰУ заң факультетінің 1 курс студенті,
Астана, Қазақстан.
Ғылыми жетекшісі – Садвакасова А.К.

Көп ақпараттық технологиялар сияқты Интернет ғаламдық желісі өз эволюциясын қалыптастырып, үлкен қауіптерге мүмкіндіктер туғызады. Желі ішіндегі шабуылдар, төлем карточкаларына қатысты алаяқтық, банктік шоттардан қаражат ұрлау, корпоративтік тыңшылық – Интернет желісінде жүрген қылмыстардың тек біршамасы ғана. Мұндай құқықбұзушылық әрекеттер әлем елдеріне ғана емес, сонымен қатар өз мемлекетімізге де ұлттық қауіпсіздіктің жасаушысы – ақпараттық қауіпсіздікке қатер төнгізетін маңызды қауіп-қатерлерді құрайды.

Компьютерлік технологиялар сферасындағы қылмыс (киберқылмыс) – қазіргі заманғы компьютерлік технологияларды енгізу және дамыту деңгейіне, оларды жалпы қолдану және оларға рұқсат беруге тікелей тәуелді деңгей болып табылатын халықаралық маңызды құбылыс.Киберқылмыскердің негізгі мақсаты түрлі процесстерді басқаратын компьютерлік жүйе және онда таралатын ақпарат болып табылады. Киберқылмескерлер арсеналы – ақпараттық қару, желіге ену, бағдарламалық қамтамасыз етуді бұзу және модификациялау, ақпаратты рұқсатсыз алу және компьютерлік жүйенің жұмысын уақытша тоқтатуға қолданылатын барлық құралдар. Басқа да халықаралық маңыздағы қылмыстар секілді, киберқылмыспен күресу құралдарының маңызды бөлігі әрбір мемлекеттің өз құзыретіне кіретіндіктен, халықаралық құқық нормаларымен келістіру арқылы компьютерлік қылмыстармен күресуге бағытталған ұлттық заңнаманы параллельді дамыту керек.Мұндай жағдайда Қазақстан Республикасы демократиялық тәуелсіз мемлекет ретінде компьютерлік қылмысқа қарсы тұру мәселелерінен, сонымен қатар оның трансұлттық (трансшекаралық) формалары бөлігінде, шетте қалмауы тиіс.

Киберқылмыстармен айналысатын зерттеушілер тобы бұл қылмыстың түрлі классификацияларын ұсынады.

Мысалы, Еуропа Одағының Конвенциясы киберқылмыстарды төрт топқа (кейін қосымша бесінші топ қосылды) бөліп, бірінші тобына компьютерлік жүйелердің тұтастығына, қолжетімділігіне қарсы жасалған «компьютерлік қылмыстар»:

- Заңсыз қол жеткізу (компьютерлік жүйеге) - 2 бап;
- Заңсыз қолға түсіру (қоғамнан тыс компьютерлік ақпаратты компьютерлік жүйеге көшіру) – 3 бап;
- Ақпаратқа қол сұғу (заңсыз зиян тигізу, өшіру, ақпаратты өзгерту) – 4 бап;
- Жүйеге қол сұғу (компьютерлік жүйе функцияларына тежегіш – өзгерту, көшіру, басқа дереккөзге жіберу, зиян тигізу) – 5 бап.[1]

Екінші топты компьютерлік жолдарды қолданумен байланыстырады (компьютерлік технологиялардағы өзгерту, өшіру, блокировка жасау сияқты экономикалық пайда түсіруді көздейтін алаяқтықтар). Үшінші топқа компьютерлік ресурстарды қолдану арқылы балалар порнографиясын тарату қылмыстары жатқызылса, төртінші топқа авторлық құқық пен сабақтас құқыққа қарсы қылмыстар енеді. 2002 ж. Конвенцияға діни, ұлттық, этникалық белгісі байланысты жасалатын дискриминациялық киберқылмыстар сияқты қосымша протокол қосылды.

Еуропа Одағының Конвенциясынан басқа, зерттеу жұмыстары арасында киберқылмыстардың екі үлкен ресми және бейресми топтары бар.

Классификациялардың бірі 1991 ж. Интерполдың Бас Секретариатының

кодификаторымен құрастырылды және 100 астам елдің ОҰБ (Орталық Ұлттық Бюро) ақпараттық жүйесіне еніп, қолжетімді. Бұл классификацияға кибертерроризм, кибераңдушылық, бала порнографиясы сияқты қылмыстар еніп, көпқатерлер қарастырылмаған. Бұл классификаторға Q әрпінен басталатын идентефикаторы бар кодтар жүйесі кіреді.

Классификатор топтарына тоқталсақ:

- QA – Санкцияланбаған қол сұғушылық;
- QD – компьютерлік мәліметтерді өзгерту;
- QUL – логикалық бомба;
- QDT – троянский конь;
- QDV – компьютерлік вирус;
- QF – компьютерлік алаяқтық;
- QFF – компьютелік подделка;
- QR – заңсыз көшірме жасау;
- QRG – компьютерлік ойындар;
- QRS – басқа да программалық жсақтамалар;
- QS – компьютерлік саботаж;
- QZE – коммерциялық құпиясы бар ақпаратты ұрлау;
- QZS – конфиденциалды ақпаратты басқа ресурстарға жіберу;
- QZZ – басқа компьютерлік қылмыстар.[1]

Американдық зерттеуші Д.Л. Шиндлер ұсынуымен «киберге» қатысты ауқымдырақ классификация ұсынылған. Негізінен шетел зерттеушілері тек «computer crimes», «computer related crimes», «computer facilitated crimes» классификацияларымен шектеледі.

Соның негізінде келесі классификация ұсынылады:

1. Адам өмірі мен денсаулығына қауіп төндіретін зорлық белгісі бар, потенциалды қауіпті киберқылмыстар;
2. Компьютерлік жүйелерге қол жеткізу арқылы конфиденциалды ақпаратқа қатысты киберқылмыстар;
3. Деструктивті киберқылмыстар;
4. Меншік құқығына, авторлық құқыққа, ақпаратқа қатысты меншік құқығына байланысты киберқылмыстар;
5. Қоғамдық қауіпсіздікке зиян тигізетін киберқылмыстар.[2]

1) Адам өмірі мен денсаулығына қауіп төндіретін зорлық белгісі бар, потенциалды қауіпті киберқылмыстар келесі категорияларды қатарына қосады:

- Физикалық жаза, жәбірлеумен қоқан-лоқы жасау – электронды почта арқылы адам психикасына әсер ететін қоқан-лоқылық белгісі бар хабарламалар жіберу. Мақсаты – жәбірленушіге өз өмірі үшін, жақын адамдардың өмірі үшін үрей туғызу;
- Кибераңдушылық – қоқан-лоқылық белгісі бар, қауіпті жағдайдың төніп жатқаның ескертетін электронды аңдушылық;

2) Компьютерлік жүйелерге қол жеткізу арқылы конфиденциалды ақпаратқа қатысты киберқылмыстардың ақпаратқа зардап тигізбей әрі алдағы уақытта қолданылмайтын сипаты бар. Мысалы, жас хакер компьютерлік жүйенің шекарасын бұзу арқылы өзіне әрі өз жастағыларға икемін дәлелдеп көрсетеді.

3) Деструктивті киберқылмыстар ақпарат пен мәліметтерге зақым келтіруді ғана қарастырады. Түрлері:

- Желіні бұзып, ақпарат немесе программаны өшіру;
- Web-серверді бұзып, Web-парақшаларды жою;
- Компьютер немесе желі ішіне вирустарды, құрттарды, қауіпті программаларды енгізу.

Бұл кез келген түрі қолданушыны бұл желіні қолдану мүмкіндігін шектейді. Бұл қылмыстар хакерлердің «қызық» көріп, жасауы да мүмкін немесе бір топ қылмыскерлердің

компьютерлік саботажы жасауы мүмкін. Бұл «хактивизм» құбылысы мен түрлі вирустар Интернетке жолы бар барлық компьютер қожайындары үшін үлкен проблемаға айналған.

4) Меншік құқығына, авторлық құқыққа, ақпаратқа қатысты меншік құқығына байланысты киберқылмыстар екі үлкен топ кибер ұрлық пен кибер алаяқтық боп бөлінеді.Д.Л. Шиндлер кибер ұрлықты келесі түрлерге бөледі:

- Иемденіп алу және шығындау. Мысалы, қызметкердің компьютерлік жүйеде төлеу тізімдемесіне заңды қолжетімділігі болып, ол өз шотына қосымша қаражатты түсіру үшін мәліметтерлі өзгертеді немесе компьютер көмегімен банктағы шоттан фонд қаражатын өз шотына аударады.
- Заңсыз ассигнациялау. Қылмыскердің жүйеге кіру мүмкіндігі болып, ол құжаттарды өзгерте отырып, өзіне тиісті емес мүлікті иеленіп алады.
- Бірлескен шпионаж. Қылмыскерлер компьютер мен желі арқылы коммерциялық құпияны ұрлаумен айналысады. Сонымен қоса қаражаттық ақпарат, конфиденциалды клиенттер тізімі, бизнестегі маркетингтік стратегиялар ұрланады.
- Плагиат – басқа авторлық материалдарды өз атынан шығару.
- Пираттық қарақшылық - авторлық құқыпен қорғалған программалық жасақтамаларды, музыка, кино, кітап сияқты өнер туындыларын авторға шығын келтіру арқылы заңсыз көшіру.[3]

Кибералаяқтықты Еуропа Одағының Конвенциясы киберкеңістіктегі басқа тұлғаны мүлкінен компьютерлік жүйедегі ақпаратты өшіру, өзгерту, блокадалау арқылы айырып, бұл өзі әрі үшінші тұлғалар үшін экономикалық пайда табу ниетімен жасалады. Қылмыскерлер желідегі қаржылық пирамида, тегін қоңырау шалулар сияқты ескі нұсқадағы алдаушылықтарын әлі де қоланады. Интернет тек бұл қылмескерлердің шеңберің кеңейтіп, оларды қолға түсіру мүмкіндігін азайтады. Киберкеңістіктегі алаяқтықтың таралған түрі, мысалы, АҚШ-та құнды қағаздар «алаяқтығы». АҚШ-тың құнды қағаз бен биржа Комиссияның (SEC)деректері бойынша, 1999 ж. құнды қағаздармен жасалған шарттардың 16 % -ы Интернет арқылы жасалған, соның негізінде 110 алаяқтық сипатындағы кибер әрекеттер тіркелді.[4]

5) Қоғамдық қауіпсіздікке зиян тигізетін киберқылмыстар қатарына кибертерроризм мен киберкеңістікті террористік мақсатта пайдалану түрлері жатады.

Статистикабойынша:

- Хакерлермен шабуылданатын компьютерлердің 86% – үйдегі;
- 2006 ж.фишингтік хаттамалардың саны (желілік қиянаткерлікпен байланысты) 81% құрады;
- зияндывирустардыңзарарсыздандырутүрлерінің 18% - жаңа;
- 4,2 млн. сайттар – порнографиялық;
- блоггерлердің 55% өздерінің Интернет-күнделіктеріншынөмірдегікелеңсізоқиғаларданқауіптеніпжалғанатпен жазады.[3]

Жеке компьютерлерге зақым келтіретін 217 мың бағдарлама құрылғаннан кейін ұйымдастырылған қылмыс әлемі киберкеңістіктегі операциялардан едәуір қаражат табатынын ұғып, енді пайдаланушылардың жеке мәліметтерін ұрлауға тырысуға жұмылдырылды делінеді «МакАфи» сарапшыларымен дайындалған «2007 жылғы қауіпсіздіктің он негізгі қаупі» баяндамасында.

Компьютерлік қылмысқа қарсы тұру мәселесі – бұл кешендік мәселе. Бүгін заңдар технологиялар дамуының қазіргі заманғы деңгейіне сәйкес талаптарға сай болуы қажет. Осы мақсатпен телекоммуникациялық желілерде ақпаратты таратуды реттейтін заңнаманы жетілдіру бойынша мақсатты бағытталған жұмыс өткізілуі тиіс. Құқыққорғаушы органдардың, арнайы қызметтердің, соттық жүйенің күштерінің өзара әрекеттесуін және шоғырландыруды, оларды қажетті материалды-техникалық базамен қамтамасыз ету алдыңғы қатарлы бағыттардың бірі болып табылады.

Қолданылғын әдебиет:

1. Тропина Т.Л. Киберпреступность:понятие, состояние, уголовно-правовые меры. – Владивосток,2007. 35-40 бб.
2. Ляпунов Ю. Ответственность за компьютерные преступления. – Москва: «Законность», 1997. 8-15 бб.
3. Матвеева А. Компьютерные преступления. – Москва: «Человек и закон» , 2002. 44-47 бб.
4. Роговский Е.А. Кибербезопасность и кибертерроризм. – Москва, 2003. С.23-26

УДК 378.147

КОНВЕРГЕНЦИЯ В ОБРАЗОВАНИИ

Каиргельдин Серикболсын Баймаганбетулы
serikbolsyn_91@mail.ru
Магистрант 1 курса группы «Информатика в образовании»
ЕНУ им. Л.Н.Гумилева, г.Астана, Казахстан.
Научный руководитель – Мубараков А.М.

Аннотация

Обсуждается концепция междисциплинарного подхода к системе организации науки и образования. В качестве примера рассмотрена программа обучения конвергентным нано-, био-, информационным и когнитивным технологиям.

В Послании Президента Н.А.Назарбаева народу Казахстана «Казахстанский путь-2050: Единая цель, единые интересы, единое будущее» особое внимание уделяет повышению качества образования. Особое значение имеет призыв Главы государства к модернизации системы образования и выводу его на международный уровень развития. По словам Президента, важно восстановить логическую взаимосвязь всех видов «возрастного» образования как целостного лифта: дошкольного, начального, среднего, профессионального, высшего и пост-вузовского. Система образования должна оставаться общенациональной.

Все эти изменения возможно только при наличии детально проработанной стратегии, учитывающей как реальную ситуацию, сложившуюся в сфере образования, нарастающие тенденции и действующие отношения, так и возможные пути будущего развития общества и государства. Такая стратегия должна стать основой для разработки гибкой тактической программы действий, постоянно адаптируемой к быстро изменяющимся реальным условиям. В качестве такой гибкой тактической программы действий может выступить конвергентная технология, суть которой излагается ниже.

Известно, что до сих пор с помощью новой технологии всегда создавался новый материал, каждая вновь появившаяся технология приводила к появлению ещё одной специальности. Теперь же впервые появились технологии-интеграторы. Информатика изменяет информационное пространство, а нанотехнологии изменяют материалы. На место деления и селекции приходит интеграция.

Нужны принципиальные изменения в системе организации и финансирования науки. Сегодняшняя система и в нашей стране, и во всем мире не приспособлена к проведению междисциплинарных исследований. Очевидно, изменения нужны и в системе образования. При этом надо понимать, что система образования — самая консервативная сфера. Консервативнее, чем наука.

В науке, точнее, в её организации, многое можно изменить административно, потому что изменения коснутся ограниченного числа людей (хотя и это крайне сложныепроцессы). А в образовании задействовано почти все общество — даже если вы не учитесьсами, то вы участвуете в образовании своих детей и внуков. Образование — на порядокболее сложная,