4. Дещо зміненим має бути механізм розсекречування носіїв, які засекречені згідно зі ЗВДТ та мають відповідні, встановлені Законом "Про державну таємницю", реквізити: гриф, дату та строк засекречування, посилання на відповідну статтю ЗВДТ та інше.

За умови, якщо розсекречування носія інформації можливе тільки при внесенні змін в ЗВДТ, тобто виключення відповідної статті, чи зміни її змісту, це вирішується тільки через розгляд цих носіїв державними експертами з питань таємниць в порядку, визначеному "Положенням про державного експерта з питань таємниць", "Методичними рекомендаціями держекспертам" та "Рекомендаціями з організації діяльності експертних комісій при держекспертах".

У тому випадку, коли розсекречування носіїв секретної інформації не потребує внесення змін до ЗВДТ чи Розгорнутого відомчого переліку відомостей, що становлять державну таємницю, розсекречування проводиться керівником підприємства, організації, де носій було засекречено, з урахуванням висновку комісії спеціалістів підприємства, без проходження носіїв секретної інформації через держексперта.

Взагалі, для всіх приведених вище варіантів розсекречування носіїв секретної інформації може бути доцільним, з метою виключення безпідставного, необгрунтованого, передчасного розсекречування, розробити перелік типових, найбільш важливих та принципових носіїв секретної інформації, розсекречування яких обов′язково має проводитись через державних експертів з питань таємниць з урахуванням строків давності цих носіїв. Можливо продумати ще якісь конкретні умови диференційованого підходу до визначення, які носії можуть розсекречуватися без узгодження з держекспертом з питань таємниць.

Висновки

Звичайно ж викладене вище не в змозі в повному обсязі вирішити проблему розсекречування та в деталізованому вигляді викласти механізм розсекречування, який би врахував усі можливі ситуації. Такий гнучкий деталізований механізм розсекречування можливо розробити тільки шляхом системного підходу та координації зусиль різних відомств України, Служби безпеки в першу чергу, Міністерства оборони, Держстандарту, Міністерства промислової політики та інших. Результатом такої роботи має бути або окремий нормативний документ у вигляді інструкції чи положення про порядок розсекречування носіїв секретної інформації, або ж окремий розділ нової загальної інструкції з забезпечення режиму секретності на підприємствах, відомствах та в організаціях України. Не розробивши такий документ в найближчий час:

по-перше, не можливо буде, як і дотепер, оптимізувати процес захисту державної таємниці, тобто зосередити всі зусилля на захисті тільки тієї інформації, яка має найбільшу цінність для держави;

по-друге, не вирішиться сама по собі проблема розсекречування носіїв секретної інформації колишнього СРСР, навіть, з урахуванням започаткованої сьогодні СБУ роботи з цього питання, яка носить, на мій погляд, досить загальний характер, а саме інвентаризація носіїв, запити до Росії, узагальнення і подача пропозицій міністерствам.

Література: 1. Закон України "Про державну таємницю" від 26. 01. 1994 р. із змінами і доповненнями від 21. 09. 1999 р. 2. Положення "Про державного експерта з питань таємниць". Збірка № 2 Держкомсекретів. – К. 1998 р. 3. Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні: Матеріали ювілейної науково-технічної конференції. – К. 1998. 4. Інструкція по забезпеченню режиму секретності № 0126 – 1987 р.

УДК 342; 343

К ОПРЕДЕЛЕНИЮ ВИДА И РАЗМЕРА НАКАЗАНИЯ ЗА КОМПЬЮТЕРНЫЕ ПРЕСТУПЛЕНИЯ В СООТВЕТСТВИИ С УГОЛОВНЫМ КОДЕКСОМ УКРАИНЫ

Павел Орлов, Елена Громыко*, Виталий Носов, Владимир Голубев**, Наталья Филипенко, Евгений Оспищев

Национальный университет внутренних дел, г. Харьков,

**Харьковская облгосадминистрация,*

***Центр исследования проблем компьютерной преступности, г. Запорожье*

Аннотация: **Обоснована необходимость внесения изменений в раздел XVI нового Уголовного**

кодекса Украины "Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей", который регламентирует определение вида и степени наказания за действия, предусмотренные статьями этого раздела, а также рассмотрена целесообразность создания специализированных пенитенциарных учреждений.
Summary: **The necessity of change of a sort and degree of punishments in the section XVI of the new criminal code of Ukraine "Crimes in an orb of use of computers, systems and computer webs", and also necessity of making of the specialized penitantiary establishments is justified.**
Ключевые слова: **Защита информации, компьютерное преступление, вид наказания, степень наказания, пенитенциарное специализированное учреждение.**

I Введение

Стремительное развитие технического прогресса наряду с созданием новых благ привело к появлению новых видов преступлений, выражающихся в противоправных действиях, выделенных законодателем в Раздел XVI "ПРЕСТУПЛЕНИЯ В СФЕРЕ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННО-ВЫЧИСЛИТЕЛЬНЫХ МАШИН (КОМПЬЮТЕРОВ), СИСТЕМ И КОМПЬЮТЕРНЫХ СЕТЕЙ". Далее по тексту такого рода преступления назовем "компьютерными преступлениями".

Тенденция роста количества совершенных преступлений и, соответственно, понесенных убытков в этой сфере были (и есть) объектами статистических исследований разных международных организаций.

Калифорнийский университет Сан-Диего (США) опубликовал результаты исследования, проведенного в сети Internet по вопросу об атаках на интернет-серверы типа DOS. За три недели, которые проходило исследование, ученые зарегистрировали 12 805 DOS-атак, направленных против 5 тыс. серверов. В течение недели исследователи установили, что ежечасно 150 IP-адресов становятся жертвами DOS-атак. Среди двух тысяч пострадавших организаций – в основном компании, занимающиеся электронной торговлей.

Так по официальной статистике Computer Security Institute, в 2000 году в США экономические убытки от компьютерных преступлений составили 265,6 млн. долл. Потери банков Франции в этой сфере достигают 1 млрд. франков в год, это при том, что количество таких преступлений ежегодно увеличивается на 30 – 40%. “Компьютерная мафия” Германии похищает за год около 4 млрд. марок. А в Великобритании лишь ассоциация страховых компаний несет ежегодные убытки на сумму свыше 1 млрд. фунтов стерлингов [1].

Приведенные цифры позволяют говорить о необходимости создания четкой системы по борьбе с компьютерной преступностью и установление эффективной системы наказаний за соответствующие преступления.

Следует отметить, что суровость наказания за совершение компьютерных преступлений в таких странах как Великобритания и Китай привела к уменьшению числа последних, заставляя правонарушителей, которые специализируются на осуществлении компьютерных преступлений, выискивать страны, в которых наказания за эти противоправные действия менее суровые или эти действия не являются противоправными.

В США преступления в сфере компьютерных технологий в ближайшее время могут быть отнесены в особый разряд "федеральных преступлений, расценивающихся как террористические". Такие преступления будут караться пожизненным тюремным заключением, если Акт по борьбе с терроризмом, предложенный министром юстиции США Джоном Эшкрофтом (John Ashcroft), будет принят в его нынешнем виде [2].

Понятно, что соответствующая “сфера деятельности” предполагает наличие у преступника профессиональных специальных знаний и навыков, то есть, требует от него соответствующего интеллектуального уровня. Люди такого уровня, как правило, способны контролировать соотношения между потенциальной целью преступных действий и размером наказания за них.

Субъект компьютерного преступления характеризуется:

- высокой профессиональной квалификацией;
- наличием доступа к компьютерному оборудованию, которое может становиться: орудием преступления, соответствующим местом совершения преступления, средством для совершения преступления или местом повышения квалификации преступника.

Новым Уголовным кодексом Украины предусмотрен раздел XVI "Преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей". Статьями раздела приводится перечень соответствующих преступлений, за совершение которых установлены такие виды наказаний: штраф, лишение права занимать определенные должности, лишение права заниматься определенной деятельностью, исправительные работы, ограничение свободы и лишение свободы на определенный срок [3].

Исходя из определения цели наказание выступает карой за совершенное деяние и имеет целью исправление осужденных, а также предупреждение совершения новых преступлений как осужденными, так и другими лицами [3]. Рассмотрим как виды и размер наказаний, предусмотренные разделом XVI УК Украины, соответствуют цели наказания.

II Анализ соответствия предусмотренных видов и степеней наказания совершенному правонарушению

Штрафы

Статья 361 предполагает за незаконное вмешательство в работу ЭВМ, систем или компьютерных сетей наказание в виде штрафа в размере семидесяти необлагаемых минимумов доходов граждан, то есть за преступление, которое может привести к последствиям на минимальном уровне (порядка десятков тысяч долларов [6]), виновный должен заплатить 1190 гривен.

Статья 362 предполагает штраф за "Похищение, присвоение, вымогательство компьютерной информации или завладение ею путем мошенничества или злоупотребления служебным положением" (преступление, по последствиям превышающее ущерб свыше нескольких десятков тысяч и до миллионов долл. США) в размере от 850 до 3400 гривен, а при других обстоятельствах от 1700 до 6800 гривен.

Статья 363 предполагает за "Нарушение правил эксплуатации автоматизированных электронно-вычислительных систем" (при тех же последствиях для потерпевшей стороны) штраф в размере до 850 гривен, а при других обстоятельствах до 1700 гривен.

Все эти статьи предусматривают усиление наказания, если эти же действия причинили существенный вред.

Какой же количественный порог установлен для определения суммы "существенного вреда" для потерпевшей стороны? Одна и та же сумма ущерба для разных категорий потерпевших может определяться как существенный, так и несущественный вред. Такая неоднозначность в трактовке понятия "существенный вред" может привести к ошибочной квалификации совершенного преступления.

Так, например, в США федеральный закон “О компьютерном мошенничестве и злоупотреблении” (Computer Fraud and Abuse Act of 1986) [4] предусматривает наступление уголовной ответственности, если изменение и уничтожение компьютерной информации причинило убытки, сумма которых превышает 1000 долл. США. Согласно этому же закону Федеральный суд может применять к преступникам штраф в размере до 250000 долл. США и заключение на срок до пяти лет.

В США уголовное законодательство некоторых штатов связывает уголовную ответственность с размерами убытков в денежном выражении (Юта, Техас, Коннектикут и т. п.). В других штатах уголовная ответственность наступает даже при отсутствии материального ущерба, в частности, в случаях несанкционированного доступа к:

- конфиденциальной информации (Невада, Вирджиния, Нью-Йорк);
- результатам медицинского обследования (Нью-Йорк, Вирджиния);
- данным о трудовой деятельности, заработной плате, предоставленных кредитах и частных делах (Вирджиния).

В штате Небраска любой несанкционированный доступ является преступлением.

Наказания за эти преступления отличаются в разных штатах. В частности, в штате Джорджия нарушение права доступа в некоторых случаях может повлечь заключение сроком до 15 лет.

По законодательству штата Юта, одним из наиболее эффективных критериев определения наказания за совершенное правонарушение является размер причиненного ущерба (или такого, который мог быть причинен). Критерии позволяют разграничить случаи наступления (используя терминологию отечественного права) гражданско-правовой, административной и уголовной ответственности. В таком случае введение четкой квалификации действия в зависимости от размера ущерба позволит избавиться от субъективизма при определении наказания.

В статьях 361 – 363 УК Украины наблюдается явное несоответствие трёх материально-финансовых последствий преступления:

1. Расходов для потерпевшей стороны;
2. Доходов, полученных правонарушителем;
3. Суммы штрафов.

Указанными статьями при определении сумм штрафов не учтены затраты правонарушителя по получению специальных ("компьютерных") знаний, дорогостоящего компьютерного оборудования и оплаты подключения к Internet (либо использования служебного положения). Ведь в настоящее время высокопроизводительная компьютерная техника является достаточно дорогостоящей для среднестатистического гражданина Украины. Несложный подсчет позволяет определить среднюю стоимость «рабочего места» украинского компьютерного правонарушителя – около 600...1500 долл. США. Если же правонарушитель использует служебное положение для совершения преступления, т. е. «рабочее место» на службе, в ВУЗе и т. п., то такие обстоятельства при совершении преступления должны влиять на наказание.

Лишение права занимать определенные должности или лишение права заниматься определенной деятельностью

Данный пункт наказания в большей мере касается работников государственных бюджетных организаций. При этом оклады подавляющего большинства госслужащих в сотни и тысячи раз ниже предполагаемой выгоды, которую получает "компьютерный" правонарушитель. Таким образом, "лишение права занимать определённые должности или заниматься определённой деятельностью на срок до трёх лет (36 месяцев)"[3] при соблазне получения "незаконной выгоды" в крупных размерах требует дополнительного исследования и возможной коррекции.

Исправительные работы

Наказание в виде исправительных работ устанавливается на срок от шести месяцев до двух лет и происходит по месту работы осужденного. Из суммы заработка осужденного к исправительным работам ведется отчисление в доход государства в размере, установленном приговором суда, от десяти до двадцати процентов.

Практически все "компьютерные" правонарушители являются профессиональными программистами, т. е. связаны с работой в корпоративной или глобальной компьютерной сети по роду службы, и если даже они не совершили преступления на служебном месте, то все равно имеют потенциальную возможность совершать преступные деяния, используя служебное положение. Поэтому наказание в виде исправительных работ по месту работы осужденного без ограничения его свободы и тщательного контроля за его деятельностью не может в полной мере достичь основной цели – кары за содеянное и предотвратить новые правонарушения.

Ограничение свободы

Наказание в виде ограничения свободы состоит в содержании осужденного в уголовно-исполнительных учреждениях открытого типа без изоляции от общества в условиях осуществления за ним надзора с обязательным привлечением осужденного к работе.

Ограничение свободы является наиболее оптимальной заменой исправительных работ, поскольку позволит надзирать за профессиональной деятельностью осужденного и определить для него наиболее полезную для специализированных государственных учреждений работу с учетом его высокой квалификации в области компьютерных технологий и программирования.

Лишение свободы на определенный срок

Изоляция и помещение "компьютерного" правонарушителя на определённый срок в уголовно-исполнительное учреждение может иметь как позитивное, так и негативное значение не только для личного будущего осуждённого, но и для государства. Такое утверждение основано на анализе профессиональных качеств этой категории правонарушителей и информации, которая периодически появляется в зарубежных источниках. Например: «14 летний подросток из Торонто, взломав электронную защиту серверов, требовал 5000 долларов за восстановление нормальной работы аппаратуры», «15-летний подросток из Сингапура осуждён за взлом электронной защиты двух серверов», «Отсидев в тюрьме штата Калифорния, компьютерный хакер Кевин Митник был приглашен (на работу) в Сенат США для консультации по вопросам безопасности правительственных сетей и путей повышения степени их защищённости», «Президент США на операцию по борьбе с кибербандитизмом просит выделить 2 миллиарда долларов», и т. д. [5, 6]. Т. е. десятки специалистов самого высокого уровня разрабатывают программное обеспечение для компьютерных систем и сетей, а "компьютерный" правонарушитель на основании анализа этих программ определяет их уязвимые места и создаёт программные продукты, способные нанести ущерб пользователям этих компьютерных систем и сетей. Назовем такого "компьютерного" правонарушителя устоявшимся термином – хакер [7].

Хакер знает больше, с раннего юношества обучается знать больше и думать оригинальнее. Круг его реальных, физических друзей (друзей в обычном человеческом понимании слова «друг») крайне ограничен. Зато круг его «виртуальных» друзей разбросан по всему миру. Он может сутками не выходить из дома, ограничив зону своего существования несколькими квадратными метрами помещения, хаотичным скудным питанием. Радуется этот человек победам, которые большинство из окружающих не способны оценить. Это человек – фанатик.

С одной стороны, отбытие наказания такого правонарушителя в одной среде с осужденными по другим статьям УК – это достойное наказание для преступника, который нанес огромные материальные ущербы обществу.

Однако, с другой стороны, в странах СНГ общепринятое лишение свободы для такого рода осужденных **можно и нужно** изменить. Используя опыт развитых стран мира (Англия, Израиль) можно утверждать, что такие правонарушители должны отбывать срок криминального наказания в специальных пенитенциарных учреждениях, которые условно можно назвать "пенитенциарными центрами". Они позволят использовать научный потенциал осужденных хакеров с пользой для государства и наверстать некоторое отставание Украины в развитии компьютерных технологий. Для плодотворной работы таких преступников, на наш взгляд, целесообразно создать единый компьютерный центр закрытого типа, или использовать уже существующие специализированные учреждения СБУ, МВД, Генеральной прокуратуры.

Естественно, процесс переведения осужденных в специальные учреждения должен проходить дифференцированно, через общую пенитенциарную систему, с обязательной работой экспертов-психологов, которые смогут охарактеризовать степень достоверности раскаяния осужденных.

Следует указать, что в международно-правовых актах и законодательстве передовых демократических государств закреплено правовое положение осужденных, при котором осужденным предоставляется рентабельная, доходная работа, отвечающая способностям, подготовке и склонностям осужденного [8, 9]. Здесь обязанность трудиться (при наличии физических способностей к соответствующей работе) согласовывается с возможностями осужденного к возмещению затрат, связанных с содержанием под стражей, погашением исков и т. п.

Следует также добавить, что в законодательных актах Украины необходимо предусмотреть создание специализированных рабочих мест для лиц, которые освобождаются из мест лишения свободы, имеют высокие профессиональные качества специалистов и обладают навыками квалифицированной работы в области компьютерных технологий.

Использование потенциала хакеров в "мирных" целях происходит, судя из официальных и неофициальных сведений, как зарубежными, так и отечественными спецслужбами, но эта ситуация требует правового закрепления с целью соблюдения законности таких действий.

Кабинет Министров Украины 2 декабря 1996 года принял постановление № 1454 "О неотложных мерах по привлечению к труду лиц, отбывающих наказание в местах лишения свободы", в котором обязал Министерство экономики Украины ежегодно предусматривать в проекте государственного заказа объемы поставок продукции для хозяйственных нужд, которые будут изготавливаться предприятиями уголовно-исполнительной системы. В связи с этим видится целесообразность скорейшей разработки аналогичного постановления относительно интеллектуальной продукции, которая могла бы производиться в местах лишения свободы [10].

III Выводы

Для того чтобы Украина заняла соответствующее положение в мире, чтобы к ней относились с уважением, она должна всячески проявлять заботу о плодотворном использовании интеллектуальных ресурсов. И пусть осужденные, в нашем случае владельцы этого интеллекта, приносят пользу государству и обществу. Для достижения этой цели необходимо:

1. Изменить виды и размер наказания за компьютерные преступления, предусмотренные Разделом XVI УК Украины, приведя их в соответствие с:
   A. Наносимыми убытками (расходы потерпевшей стороны, включая затраты на восстановление техники и понесенные моральные потери);
   B. Доходами, полученными правонарушителем в результате противоправной деятельности;
   C. Пользой, которую может принести государству осужденный за компьютерные преступления.
2. Создать или модернизировать специализированные пенитенциарные учреждения (так называемые пенитенциарные центры), которые позволят использовать интеллектуальный потенциал осужденных с пользой для государства.
3. Изложить в новой редакции отдельные статьи Раздела XVI УК Украины:

“Стаття 361. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж.

(1) Незаконне втручання в роботу автоматизованих електронно-обчислювальних машин, систем чи комп'ютерних мереж, що призвело до перекручення чи знищення комп'ютерної інформації або носіїв такої інформації, а також розповсюдження комп'ютерного вірусу шляхом застосування програмних і технічних засобів, призначених для незаконного проникнення в ці машини, системи чи комп'ютерні мережі і здатних спричинити перекручення або знищення комп'ютерної інформації чи носіїв такої інформації, –

караються штрафом не менше трьохсот неоподатковуваних мінімумів доходів громадян, або обмеженням волі строком до двох років.

(2) Ті самі дії, якщо вони заподіяли шкоду, що перевищує три тисячі неоподатковуваних мінімумів доходів громадян або вчинені повторно чи за попередньою змовою групою осіб, –

караються обмеженням волі на строк до п'яти років або позбавленням волі на строк від трьох до п'яти років з відбуванням покарання в спеціалізованих пенітенціарних закладах.

Стаття 362. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем.

(1) Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службової особи своїм службовим становищем –

караються штрафом, сума якого відшкодовує завдані збитки, але не менше п'ятисот неоподатковуваних мінімумів доходів громадян, або обмеженням волі на строк до двох років.

(2) Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, –

караються штрафом не менш тисячі неоподатковуваних мінімумів доходів громадян, або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк з відбуванням покарання в спеціалізованих пенітенціарних закладах.

(3) Дії, передбачені частинами першою або другою цієї статті, якщо вони заподіяли шкоду, яка перевищує три тисячі неоподатковуваних мінімумів доходів громадян –

караються позбавленням волі на строк від двох до п'яти років з відбуванням покарання в спеціалізованих пенітенціарних закладах.

Стаття 363. Порушення правил експлуатації автоматизованих електронно-обчислювальних систем

(1) Порушення правил експлуатації автоматизованих електронно-обчислювальних машин, систем чи комп'ютерних мереж особою, що відповідає за їх експлуатацію, якщо це спричинило викрадення, перекручення чи знищення комп'ютерної інформації, засобів її захисту, або незаконне копіювання комп'ютерної інформації, або істотне порушення роботи таких машин, систем чи комп'ютерних мереж, –

карається штрафом не менш трьохсот неоподатковуваних мінімумів доходів громадян, або обмеженням волі на строк до двох років.

(2) Те саме діяння, якщо воно заподіяло шкоду, яка перевищує три тисячі неоподатковуваних мінімумів доходів громадян –

карається штрафом, сума якого відшкодовує завдані збитки, або обмеженням волі на строк до п’яти років”.

Литература: 1. Computer Security Institute. – 2000. 2. По материалам www.sec.ru. 3. Уголовный Кодекс Украины. 4. Sec. 1030. Fraud and related activity in connection with computers. http://www4.law.cornell.edu/uscode/18/1030.html. 5. Информационно-методический журнал "Защита информации. Конфидент", № 2 (№ 30), 2000. 6. Информационно-методический журнал "Защита информации. Конфидент", № 3 (№ 31), 2000. 7. П. И. Орлов. Информация и информатизация: Нормативно-правовое обеспечение: Научно-практическое пособие. – Харьков: Вид-во НУВС, 2000. – 576 с. 8. Kaiser / Kerner / Schoch. Strafvollzug // Ein. Lehrbuch. C. F. Muller Juristischer Verlag, 1982. p. 121 – 126. 9. Бандурка О. М., Севостянов В. П. Правовое положение осужденных к лишению свободы: Пособие. – Х.: Основа, Ун-т внутр. справ, 1997. – 242 с. 10. Информационно-аналитический журнал "Служба безопасности". № 1–2, 2000.