**Уголовные правонарушения в сфере информатизации и связи.**

**План:**

1. Уголовно-правовая характеристика уголовных правонарушений с сфере информатизации и связи;
2. Общие определения уголовных правонарушений в сфере информатизации и связи;
3. Разбор уголовных правонарушений в сфере информатизации и связи по составу.

 Список использованной литературы.

1. **Уголовно-правовая характеристика уголовных правонарушений с сфере информатизации и связи.**

Информатизация - организационный, социально-экономический и научно-технический процесс, направленный на автоматизацию деятельности субъектов информатизации. Субъекты информатизации - государственные органы, физические и юридические лица, осуществляющие деятельность или вступающие в правоотношения в сфере информатизации. [1]

Под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах, со­держащиеся в информационных системах (банках данных). Компьютерной информацией следует считать информацию, зафиксированную на машинном носителе или передавае­мую по телекоммуникационным каналам и доступную к вос­приятию ЭВМ. К компьютерной информации относится ин­формация, содержащаяся на машинном носителе (в нако­пителях информации на гибких или жестких магнитных дис­ках, кассетных магнитных лентах), в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети. Эта информация может храниться или передаваться с по­мощью указанных устройств. В систему ЭВМ включаются дополнительные устрой­ства, обеспечивающие ввод или передачу информации: мо­дем (устройство для подключения компьютера в телефон­ную сеть), принтер (печатающее устройство), плоттер (уст­ройство для вывода чертежей на бумагу), сканер (устройст­во ввода текстов в компьютер). Сеть ЭВМ - эта соединение нескольких компьютеров или систем ЭВМ друг с другом при помощи специальных кабелей или использования телефонной сети. В результате такого объединения обеспечивается обмен информацией, совместное использование периферийных устройств и за­пуск общих программ через базовый компьютер. Под программой для ЭВМ следует понимать объек­тивную форму представления совокупности данных и ко­манд, которые предназначены для функционирования элек­тронной вычислительной техники с целью получения опре­деленного результата. Программа, в которой находится вирус, называется вредоносной. Такая программа, получив управление, может сама размножаться, порождать новые вирусы для выполне­ния различных нежелательных действий на компьютере (например, испортить, стереть файлы, засорять оператив­ную память компьютера, создавать помехи в работе ЭВМ и т. п.). Создание вредоносной программы представляет со­бой комплекс операций, состоящий из подготовки исходных данных, предназначенных для управления процессами уничтожения, блокирования, модификации или копирования информации, а также нарушения работы ЭВМ, системы ЭВМ и их сетей. Внесение изменений в существующие программы -это модификация программы с целью сделать эту програм­му вредоносной. Использование вредоносных программ означает умышленное их воспроизведение, установку (введение в память компьютера) в процессе технического обслуживания ЭВМ. Распространение вредоносных программ означает их передачу другим пользователям электронно-вычислитель­ной техники путем продажи, проката, передачи в обмен и т. п. К понятию распространения можно отнести и такие дей­ствия, когда лицо сознательно представляет доступ другим пользователям к воспроизведенной вредоносной программе или работает на чужом компьютере с использованием дис­кеты с записью, содержащей вредоносную программу. Рас­пространение вируса может быть осуществлено по­средством копирования вредоносной программы с диска на диск, а также через модем или компьютерную сеть, через электронную почту.

1. **Общие определения уголовных правонарушений в сфере информатизации и связи.**

Состав преступления, предусмотренного частью пер­вой анализируемой статьи УК, является материальным. Преступление считается оконченным с момента наступле­ния хотя бы одного из следующих последствий: уничто­жения, блокирования, модификации либо копирования ин­формации, нарушения работы ЭВМ, системы ЭВМ или их сети. Необходимым признаком рассматриваемого преступ.ления является причинная связь между деянием виновного и наступившим последствием, которую необходимо уста­навливать в каждом случае привлечения к уголовной от­ветственности по рассматриваемой статье УК. Для этого требуется проведение технической экспертизы. Под уничтожением понимается полное либо частич­ное удаление (стирание, порча) информации с машинных носителей. Блокирование - это закрытие информации, что делает ее недоступной для использования правомочным пользователем. Модификация заключается в несанкциони­рованной переработке первоначальной информации, ее из­менении. Например, удаление и добавление записей, со­держащихся в файлах, создание файлов, перевод програм­мы ЭВМ или базы данных с одного языка на другой и т. п. Копирование - это перенос информации с одного ма­шинного носителя на другой, если это осуществляется по­мимо воли собственника или владельца такой информации. Например, запись с диска в память ЭВМ. Нарушение работы ЭВМ, системы ЭВМ или их сети предполагает сбой в работе вычислительной техники при сохранении ее физической це­лостности. Например, полный или частичный вывод компь­ютера, компьютерной системы или их сети из строя. Состав преступления, предусмотренный частью третьей рассматриваемой статьи УК, является формаль­ным. Для признания преступления оконченным достаточно установления факта создания указанных программ для ЭВМ или внесения изменений в существующие программы, а также использования или распространения вредоносных программ или машинных носителей с такими программами независимо от наступления последствий. Такое построение состава связано с характером перечисленных в диспози­ции, содержащейся в части 3 статьи 210 УК, деяний. Соз­дание вредоносных программ, внесение изменений в суще­ствующие программы с целью сделать их вредоносными, а также их использование или распространение представля­ют реальную опасность уничтожения, блокирования, мо­дификации либо копирования информации или нарушения работы электронно-вычислительной техники. [2]

1. **Разбор уголовных правонарушений в сфере информатизации и связи по составу.**

Объектом данного преступления следует считать общественные отношения, связанные с охраной безопасно­сти информации и систем их обработки с использованием ЭВМ.

Объективная сторона преступления выражается: а) в неправомерном доступе к охраняемой законом компьютерной информации; б) в создании программ для ЭВМ, заведомо приводя­щих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети (статья 210 УК); в) внесение изменений в существующие программы, приводящее к одному из перечисленных последствий (статья 206 УК); г) использование таких программ, повлекших те же последствия (статья 207 УК); д) распространение таких программ, повлекших ука­занные выше последствия (часть 3 статьи 211 УК).

С субъективной стороны преступление, предусмот­ренное частью 3, характеризуется прямым или косвенным умыслом. Виновный сознает, что совершает неправомерный доступ к компьютерной информации, предвидит возмож­ность и неизбежность уничтожения, блокирования, модифи­кации или копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети и желает наступления таких последствий (при прямом умысле) или не желает наступле­ния перечисленных выше последствий, однако сознательно допускает возможность их наступления либо относится к их наступлению безразлично.

Мотивы и цель совершения данного преступления мо­гут быть самыми разнообразными (месть, злоба, хулиганст­во, корысть, с целью устранения конкуренции и т. п.) и на ответственность и квалификацию преступления не влияют. Субъектом анализируемого состава преступления может быть физическое вменяемое лицо, достигшее 16-летнего возраста.

Квалифицирующие признаки статей 205-213 УК РК применяется, если непра­вомерный доступ к компьютерной информации был совер­шен: а) группой лиц по предварительному сговору или ор­ганизованной группой лиц; б) лицом с использование своего служебного положе­ния; в) лицом, имеющим доступ к ЭВМ, системе ЭВМ или их сети.

Использование лицом своего служебного положения предполагает доступ к охраняемой законом компьютерной информации благодаря занимаемому лицом служебному положению. К таким лицам можно отнести тех, кто по роду своей деятельности имеет право эксплуатировать элек­тронно-вычислительную технику и знакомиться с хранящей­ся в ней информацией, а также тех, кому подчиняются лица, непосредственно работающие на ЭВМ. К лицам, имеющим доступ к ЭВМ, системе ЭВМ или их сети можно отнести пользователей информации, которые непосредственно работают на электронно-вычислительной технике. К ним относятся операторы, программисты, або­ненты, техники, обслуживающие ЭВМ или их сеть.

**Список использованной литературы:**

1. <https://articlekz.com/article/18691>
2. https://studall.org/all-58285.html