МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ
РЕСПУБЛИКИ КАЗАХСТАН

АЛМАТИНСКАЯ АКАДЕМИЯ
ИМЕНИ МАКАНА ЕСБУЛАТОВА

А.А. Абдихаликов

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ ПО ПРОТИВОДЕЙСТВИЮ ПРЕСТУПНОСТИ В СФЕРЕ ИНФОРМАТИЗАЦИИ И СВЯЗИ

Учебно-методическое пособие

Алматы, 2024 г.

УДК 004.056.53:34
ББК 67.408.1
А13

Рецензенты:

Чукумов Г.Б. – начальник научно-исследовательского центра Алматинской академии МВД Республики Казахстан им. М. Есболатова, доктор (PhD), полковник полиции

Аратулы К. – доцент кафедры уголовного права, уголовного процесса и криминалистики юридического факультета КазНУ им. аль-Фараби, доктор (PhD).

А13 Информационные технологии по противодействию преступности в сфере информатизации и связи: учеб.-метод. пос. / Абдихаликов А.А. – Алматы: ООНИиРИР Алматинской академии МВД РК им. М. Есбулатова, 2024. – 124 с.

ISBN 978-601-360-141-0

Учебно-методическое пособие «Информационные технологии по противодействию преступности в сфере информатизации и связи» предназначено для студентов по специальностям «Информационная безопасность» уровней бакалавриат, магистратура и докторантура.

В пособии рассматриваются ключевые аспекты использования информационных технологий для борьбы с преступлениями в сфере информатизации и связи. Основное внимание уделяется видам уголовных правонарушений в сфере информатизации и связи, основные способам совершения уголовных правонарушений в сфере информатизации и связи, характеристика объективных и субъективных признаков состава правонарушения, взаимодействие государств в решении проблем, связанных с компьютерными преступлениями. Дан краткий анализ моделей и политики безопасности (разграничения доступа), а также международных стандартов в области информационной безопасности.

Пособие может использоваться студентами других специальностей при изучении курсов, связанных с информационными технологиями.

УДК 004.056.53:34
ББК 67.408.1

ISBN 978-601-360-141-0

ВВЕДЕНИЕ

В современном мире информационные технологии играют ключевую роль в различных сферах жизни, включая безопасность и правопорядок. С развитием цифровых технологий и увеличением объема данных, передаваемых через сети, возрастает и количество преступлений в сфере информатизации и связи. Киберпреступность становится все более сложной и изощренной, что требует применения передовых методов и технологий для ее предотвращения и расследования.

Цель данного учебно-методического пособия – предоставить студентам и специалистам в области информационных технологий и безопасности комплексные знания и практические навыки, необходимые для эффективного противодействия преступности в цифровой среде. В пособии рассматриваются основные виды киберпреступлений, методы их выявления и предотвращения, а также современные технологии и инструменты, используемые в борьбе с киберугрозами.

Пособие состоит из нескольких разделов, каждый из которых посвящен определенному аспекту уголовных правонарушений в сфере информатизации и связи. В первом разделе дается общая характеристика данных правонарушений, рассматриваются их виды и юридические понятия объекта и предмета. Во втором разделе проводится уголовно-правовой анализ состава правонарушений, таких как неправомерный доступ к информации и создание вредоносных программ. Третий раздел посвящен проблемам совершенствования мер противодействия компьютерным преступлениям, включая международное сотрудничество. Четвертый раздел рассматривает проблемы совершенствования мер противодействия компьютерным правонарушениям (преступлениям). В пятом разделе приведены практические задания и кейсы по противодействию преступности в сфере информатизации и связи.

Особое внимание уделяется вопросам правового регулирования и международного сотрудничества в области кибербезопасности, что является неотъемлемой частью эффективной борьбы с преступностью в сфере информатизации и связи. Пособие также включает практические задания и кейсы, которые помогут закрепить теоретические знания и развить навыки анализа и решения реальных задач.

Мы надеемся, что данное пособие станет полезным инструментом для всех, кто стремится внести свой вклад в обеспечение безопасности и правопорядка в цифровом мире.

1. Информационные технологии

1.1. Понятия информационных технологий

Доступ к информации играет ключевую роль во всех аспектах жизни человека. Он важен для охраны здоровья, получения образования, защиты трудовых прав, сохранения языков и культур, а также для активного участия в государственной и общественной жизни.

Право граждан на доступ к достоверной и объективной информации является важным аспектом в глобальном информационном обществе, так как оно связано с реализацией принципов справедливости и свободы в государственной политике. Важно помнить, что конечная цель создания информационного общества в Казахстане заключается в улучшении качества жизни каждого человека и расширении его социальных прав и возможностей.

Использование современных информационных технологий позволяет человеку более полно реализовать и другие, предоставленные ему Конституцией и законами права и свободы. Например, сегодня все больше государственных услуг предоставляется гражданам посредством так называемого «электронного правительства». Качество и повсеместная доступность предоставляемых государственных услуг направлены на создание благоприятных условий для развития предпринимательской деятельности, электронно-информационного взаимодействия между гражданами и государственными органами, позволяющего получать необходимые документы и услуги без необходимости посещать различные инстанции и непосредственно общаться с государственными служащими.

Итак, что такое информационные технологии – это процесс создания, хранения, передачи, восприятия информации и методы реализации таких процессов.

Большинство людей приравнивают понятие к компьютерным технологиям, потому что с их помощью информационные технологии (ИТ) стали развиваться быстрее [1].

Хотя информационные технологии часто ассоциируются с компьютерами и компьютерными сетями, их применение выходит далеко за рамки этих понятий. IT включает в себя широкий спектр технологий и процессов, которые используются для создания, хранения, обмена и управления информацией.

Информационные технологии состоят из таких компонентов, как:

1. программные средства – прикладные и системные;
2. организационно-методическое обеспечение;
3. технические средства ИТ.

Средства информационных технологий – это разновидности компьютерной техники, с помощью которых ищется, обрабатывается и передается информация.

Они нужны для того, чтобы ускорить и облегчить выполнение ряда задач.

Средства ИТ бывают трех видов:

1. вычислительные – автоматизированные устройства для сбора и обработки информации;
2. организационные – разные виды оборудования для выполнения технических задач;
3. коммуникационные – техника: ноутбуки, компьютеры, смартфоны, планшеты и прочие приборы.

Среднестатистический человек в повседневной жизни использует только коммуникационные средства. Вычислительные и организационные устройства предназначены для решения важных задач специалистами в сфере ИТ.

1.2. Этапы развития информационных технологий

Считается, что информационные технологии начали развиваться после появления компьютеров. Но на самом деле их история уходит далеко в прошлое вплоть до первобытных времен, когда люди делились данными с помощью наскальных рисунков.

Рассмотрим основные этапы развития информационных технологий:

1. Ручные ИТ (с античных времен до второй половины XIX века). Главными инструментами информационных технологий в то время были ручное перо, книга, чернильница.

Взаимодействие между людьми проходило путем отправки писем, а главной его целью являлось донесение информации до адресата таким образом, чтобы он понял, что ему хотели сообщить.

2. Механические ИТ (с конца XIX века по наше время). В качестве инструментов здесь выступают диктофоны, телефоны, пишущие машинки, современная почта. Цель и способы коммуникации прежние, но проходят в более удобной форме.

3. Электрические ИТ (с 1940-х по 1960-е годы). Эта эпоха характеризуется появлением первых ЭВМ и программного обеспечения , электрических пишущих машинок, портативных диктофонов. Акцент информационной технологии смещен с формы на содержание.

4. Электронные ИТ (с 1970-х годов по наше время). ЭВМ того времени становятся совершенными, создаются автоматизированные системы управления (АСУ) и информационно-поисковые системы (ИПС). Упор делается на создание содержательной информации.

5. Компьютерные ИТ (с 1980-х годов по наше время). Основной инструмент этой технологии – персональный компьютер (ПК) с набором программного обеспечения для выполнения задач разного назначения.

1.3. Современное развитие информационных технологий

Современный прогресс в области информационных технологий охватывает множество инновационных направлений, которые активно развиваются и внедряются в различных сферах. В настоящее время ключевыми считаются следующие технологии:

1. Искусственный интеллект (ИИ) и машинное обучение:

Искусственный интеллект и машинное обучение (МО) – это две тесно связанные, но разные области.

Искусственный интеллект – это область компьютерных наук, направленная на создание систем, способных выполнять задачи, требующие человеческого интеллекта. Это включает в себя такие способности, как обучение, рассуждение, восприятие и принятие решений.

Основные аспекты ИИ:

– обучение: Системы ИИ могут учиться на данных и опыте, улучшая свои способности со временем.

– рассуждение: ИИ может анализировать информацию и делать выводы, аналогично тому, как это делает человек.

– восприятие: ИИ может распознавать и интерпретировать данные из окружающей среды, такие как изображения и звуки.

– принятие решений: ИИ может принимать решения на основе анализа данных и установленных правил.

Примеры применения ИИ:

– Распознавание речи: Голосовые помощники, такие как Siri и Alexa.

– Компьютерное зрение: Системы распознавания лиц и автономные транспортные средства.

– Обработка естественного языка: Переводчики и чат-боты.

– Рекомендательные системы: Персонализированные рекомендации на платформах, таких как YouTube и Netflix.

ИИ активно развивается и находит применение в самых разных областях, от здравоохранения до финансов и развлечений.

Машинное обучение – это подмножество ИИ, которое фокусируется на разработке алгоритмов, позволяющих системам учиться на данных и улучшать свои результаты без явного программирования. Основные методы МО включают:

– Обучение с учителем (например, классификация и регрессия).

– Обучение без учителя (например, кластеризация и ассоциация).

– Глубокое обучение (например, нейронные сети и глубокие нейронные сети) [1].

Примеры применения

– Медицина: Диагностика заболеваний на основе анализа медицинских изображений.

– Финансы: Оценка кредитоспособности и обнаружение мошенничества.

– Маркетинг: Персонализация рекомендаций и прогнозирование спроса.

2. Интернет вещей (IoT):

Интернет вещей (IoT) – это концепция, в которой физические объекты, оснащённые встроенными средствами и технологиями, подключаются к интернету и обмениваются данными между собой или с внешней средой без необходимости прямого взаимодействия с человеком [2].

Основные компоненты IoT:

1. Устройства и датчики: Эти устройства собирают данные из окружающей среды. Примеры включают умные часы, термостаты, камеры наблюдения и промышленные датчики.

2. Средства подключения: Данные передаются через различные сети, такие как Wi-Fi, Bluetooth, спутниковая связь или мобильные сети.

3. Обработка данных: Собранные данные отправляются в облако, где они обрабатываются и анализируются.

4. Пользовательский интерфейс: Позволяет пользователям взаимодействовать с системой, например, через мобильные приложения или веб-интерфейсы.

Примеры применения IoT:

– Умный дом: Управление освещением, отоплением и бытовыми приборами через смартфон.

– Здравоохранение: Мониторинг состояния здоровья пациентов с помощью носимых устройств.

– Промышленность: Оптимизация производственных процессов и мониторинг оборудования.

– Транспорт: Управление трафиком и мониторинг состояния транспортных средств.

IoT активно развивается и находит применение в самых разных сферах, улучшая нашу повседневную жизнь и повышая эффективность различных процессов.

3. 5G и беспроводные технологии:

5G – это пятое поколение беспроводной сотовой технологии, которое обеспечивает значительно более высокую скорость передачи данных, низкую задержку и большую пропускную способность по сравнению с предыдущими поколениями, такими как 4G.

Основные характеристики 5G:

– высокая скорость: Скорость передачи данных может достигать до 20 Гбит/с, что позволяет мгновенно загружать и передавать большие объемы данных.

– низкая задержка: Время отклика сети составляет всего 1-2 миллисекунды, что особенно важно для приложений реального времени, таких как онлайн-игры и автономные транспортные средства.

– большая пропускная способность: 5G поддерживает подключение большого количества устройств одновременно, что важно для развития Интернета вещей (IoT).

Примеры применения 5G:

– автономные транспортные средства: Быстрая и надежная связь позволяет автомобилям обмениваться данными в реальном времени, что повышает безопасность и эффективность движения.

– телемедицина: Врачи могут проводить дистанционные операции и мониторинг пациентов с минимальной задержкой.

– умные города: Управление инфраструктурой, такой как освещение, транспорт и системы безопасности, становится более эффективным благодаря подключению множества устройств.

Беспроводные технологии:

Беспроводные технологии включают в себя различные методы передачи данных без использования проводов. Это могут быть Wi-Fi, Bluetooth, NFC и другие технологии, которые позволяют устройствам обмениваться данными на разных расстояниях и с разной скоростью.

Обеспечивают высокоскоростной интернет и поддерживают развитие умных городов и автономных транспортных средств.

4. Облачные вычисления:

Облачные вычисления – это модель предоставления вычислительных ресурсов и услуг через интернет по требованию. Вместо покупки и обслуживания физической инфраструктуры, компании и пользователи могут арендовать ресурсы у облачных провайдеров, таких как Amazon Web Services (AWS), Microsoft Azure или Google Cloud [3].

Основные характеристики облачных вычислений:

– гибкость: Возможность быстро масштабировать ресурсы в зависимости от потребностей бизнеса.

– эластичность: Автоматическое увеличение или уменьшение ресурсов в зависимости от нагрузки.

– оплата по факту использования: Пользователи платят только за те ресурсы, которые они реально использовали.

Примеры применения облачных вычислений:

– хранение данных: Облачные хранилища, такие как Google Drive или Dropbox.

– обработка данных: Анализ больших данных и машинное обучение.

– разработка и тестирование ПО: Виртуальные машины и контейнеры для разработки и тестирования приложений.

– резервное копирование и восстановление: Обеспечение безопасности данных и их восстановление в случае потери.

Преимущества облачных вычислений:

– снижение затрат: Нет необходимости в капитальных вложениях в оборудование.

– доступность: Доступ к ресурсам из любой точки мира с интернет-соединением.

– надежность: Высокий уровень отказоустойчивости и безопасности данных

5. Кибербезопасность:

Кибербезопасность – это совокупность методов и практик, направленных на защиту компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных от атак злоумышленников. Она охватывает несколько ключевых областей:

– безопасность сетей: Защита компьютерных сетей от различных угроз, таких как целевые атаки и вредоносные программы.

– безопасность приложений: Обеспечение защиты устройств от угроз, которые могут быть спрятаны в программах.

– безопасность информации: Обеспечение целостности и конфиденциальности данных как при хранении, так и при передаче.

– операционная безопасность: Управление разрешениями для доступа к сети и правилами хранения и передачи данных.

– аварийное восстановление и непрерывность бизнеса: Реагирование на инциденты безопасности и восстановление рабочих процессов после атак.

– повышение осведомленности: Обучение пользователей основным правилам безопасности для снижения риска человеческих ошибок.

Кибербезопасность становится все более важной в современном мире, где количество цифровых угроз постоянно растет.

6. Блокчейн:

Блокчейн – это децентрализованная цифровая технология, которая позволяет безопасно записывать и хранить данные о транзакциях на множестве компьютеров в сети. Вот основные аспекты блокчейна:

– цепочка блоков: Данные хранятся в блоках, которые связаны друг с другом в хронологическом порядке. Каждый

блок содержит информацию о предыдущем блоке, что делает цепочку неизменной.

– децентрализация: в блокчейне нет центрального органа управления. Все участники сети имеют равные права и могут проверять и записывать транзакции.

– безопасность: Данные в блокчейне защищены с помощью криптографии, что делает их практически невозможными для изменения или подделки.

– прозрачность: Все транзакции в блокчейне видны всем участникам сети, что повышает доверие и прозрачность.

Блокчейн используется не только для криптовалют, таких как биткойн, но и в других областях, таких как финансовые операции, идентификация пользователей и кибербезопасность.

7. Робототехника и автоматизация:

Робототехника и автоматизация – это две взаимосвязанные, но разные области технологий.

Робототехника – это наука и техника, занимающаяся проектированием, созданием и использованием роботов. Роботы – это механические устройства, которые могут выполнять различные задачи с минимальным или полным отсутствием человеческого контроля. Основные области применения робототехники включают:

– промышленность: Автоматизация производственных процессов.

– медицина: Хирургические операции и реабилитация.

– космос: Исследования и автономные миссии.

– образование: Обучение основам механики, электроники и программирования.

Автоматизация – это процесс использования технологий для выполнения задач без участия человека. Она может быть как физической, так и программной. Основные типы автоматизации включают:

– промышленная автоматизация: Использование машин и роботов для выполнения повторяющихся задач на производстве.

– программная автоматизация: Использование программного обеспечения для автоматизации бизнес-процессов, таких как обработка данных и управление проектами.

Робототехника часто используется для реализации автоматизации, особенно в промышленности, где роботы выполняют монотонные или опасные задачи, повышая производительность и снижая затраты

8. 3D-печать:

3D-печать, также известная как аддитивное производство, – это процесс создания трехмерных объектов путем послойного добавления материала на основе цифровой модели. Вот основные аспекты 3D-печати:

– проектирование: Создание цифровой 3D-модели с помощью программного обеспечения для автоматизированного проектирования (CAD).

– нарезка: Преобразование 3D-модели в серию горизонтальных слоев с помощью специального программного обеспечения.

– печать: Послойное нанесение материала (пластика, смолы, металла и т.д.) с использованием 3D-принтера.

– постобработка: Удаление опорных конструкций, шлифовка, покраска и другие этапы для улучшения внешнего вида и функциональности объекта.

3D-печать используется в различных областях, таких как медицина, архитектура, автомобильная промышленность и даже мода. Эта технология позволяет создавать сложные и индивидуальные объекты, которые трудно или невозможно произвести традиционными методами.

Контрольные вопросы

1. Что такое информационные технологии?
2. Какие компоненты входят в состав информационных технологий?
3. Как информационные технологии влияют на качество жизни граждан?
4. Какие виды средств информационных технологий существуют?

5. Какие основные этапы развития информационных технологий вы знаете?

6. Как изменились средства коммуникации с развитием механических информационных технологий?

7. Какие достижения характеризуют эпоху электрических информационных технологий?

8. Что такое искусственный интеллект и какие задачи он решает?

9. В чем разница между ИИ и машинным обучением?

10. Приведите примеры применения ИИ в различных областях.

11. Что такое Интернет вещей и как он работает?

12. Приведите примеры применения IoT в повседневной жизни и промышленности.

13. Что такое 5G и какие преимущества оно предоставляет по сравнению с предыдущими поколениями?

14. Как 5G влияет на развитие технологий и какие новые возможности оно открывает?

15. Приведите примеры применения 5G в различных сферах.

16. Какие методы используются для защиты компьютерных сетей?

17. Как обеспечивается безопасность приложений?

18. Почему важно обучение пользователей основным правилам безопасности?

19. Что такое блокчейн и как он работает?

20. В чем разница между робототехникой и автоматизацией?

21. Что такое 3D-печать и как она работает?

22. Какие преимущества дает 3D-печать по сравнению с традиционными методами производства?

2. Общая характеристика уголовных правонарушений в сфере информатизации и связи

2.1. Понятие и виды уголовных правонарушений в сфере информатизации и связи

Формирование глобального информационного общества вызывает множество важных вопросов, особенно касающихся положения личности в цифровом пространстве и защиты прав и свобод человека. Неконтролируемое распространение информации может угрожать конфиденциальности, свободе, а также физическому и психическому здоровью людей. В различных государственных и частных организациях накапливается огромный объем данных о каждом человеке. Эти данные, часто в электронном виде, плохо контролируются и слабо защищены от несанкционированного распространения. Центры обслуживания населения, банки, медицинские и образовательные учреждения, налоговые органы и другие инспекции ведут электронные базы данных, доступ к которым имеет широкий круг сотрудников, что увеличивает риск копирования и утечки информации [4].

В современном обществе существует огромный объем электронных персональных данных, которые сложно контролировать. Это часто наносит ущерб людям, их правам и свободам, что подтверждается многочисленными примерами. В частности, совершено немало преступлений, когда преступники, имея на руках личные данные других лиц, оформляют на последних банковские кредиты. Зафиксированы случаи хищений по «наводке» информационных баз супермаркетов о состоятельных клиентах, случаи разглашения банковской, медицинской тайны, тайны усыновления.

Необходимо подчеркнуть значимость Уголовного кодекса Республики Казахстан в вопросах уголовно-правовой защиты информационной безопасности. В УК Республики Ка-

захстан 2014 года предусмотрена специальная глава 7 «Уголовные правонарушения в сфере информатизации и связи» [5]. В нее включены такие преступные деяния, как, например, неправомерный доступ к информации; неправомерные уничтожение или модификация информации; нарушение работы информационной системы; неправомерное завладение информацией. Как можно заметить, все девять статей данной главы УК РК непосредственно связаны с информационными правоотношениями, то есть деятельностью с информацией как самостоятельным объектом. УК Республики Казахстан 1997 года изначально такой главы не содержал.

В настоящее время существуют два основных подхода к определению понятия «компьютерного правонарушения». Один из них включает действия, в которых компьютер выступает либо объектом, либо инструментом преступления. В этом случае кража компьютера также считается компьютерным правонарушением. Другая, что объектом посягательства является информация, обрабатываемая в компьютерной системе, а компьютер служит орудием посягательства [6, с.148]. Надо сказать, что законодательство многих стран, в том числе и в Республике Казахстан, стало развиваться именно по этому пути.

Термин «компьютерные правонарушения» можно рассматривать в трех аспектах:

– правонарушения, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых. Данные правонарушения не направлены на совершение противоправных операций с информацией, содержащейся в компьютерах и базах данных, и должны квалифицироваться по статьям гл. 6 УК РК – как уголовные правонарушения против собственности;

– правонарушения, направленные на получение несанкционированного доступа к компьютерной информации, созда-

ние компьютерных «вирусов» – вредоносных программ и заражение ими других компьютеров. Ответственность за такие правонарушения предусмотрена ст. ст. 205, 210 УК РК;

– правонарушения, в которых компьютеры и другие средства компьютерной техники используются злоумышленниками как средство совершения корыстного правонарушения и умысел направлен на завладение чужим имуществом путем внесения изменений в программы и базы данных различных организаций.

Под компьютерным правонарушением следует понимать предусмотренные уголовным законом общественно опасные деяния, в которых компьютерная информация является либо средством, либо объектом посягательства [7].

Можно выделить следующие характерные особенности этого социального явления:

– неоднородность объекта посягательства;

– выступление электронной информации, как в качестве объекта, так и в качестве средства правонарушения;

– многообразие предметов и средств криминального посягательства;

– выступление компьютера либо в качестве предмета, либо в качестве средства совершения правонарушения.

Учитывая эти особенности, можно заключить, что компьютерное правонарушение представляет собой общественно опасное деяние, предусмотренное уголовным законом, которое совершается с использованием компьютерной техники.

В определении понятия «компьютерное правонарушение» выделяются следующие основные подходы:

1) К компьютерным правонарушениям относятся такие общественно опасные деяния, в которых компьютер является как объектом, так и орудием посягательства.

2) К компьютерным правонарушениям относятся общественно опасные деяния в сфере автоматизированной обработки информации.

3) Отрицание существования самостоятельных компьютерных правонарушений. Компьютер рассматривается как инструмент совершения известных уголовному закону криминальных посягательств.

Основное различие между предметом, орудием и средством совершения правонарушения следует определять по характеру использования материальных объектов в процессе посягательства. Если компьютерная информация на электронном носителе подвергается «атаке» в криминальных целях, речь идет о предмете правонарушения. Если с помощью одной компьютерной информации происходит посягательство на другую компьютерную информация, то компьютер по праву можно считать орудием или средством совершения правонарушения [8, с. 3].

Понятия «орудие» и «средство» совершения правонарушения схожи тем, что оба используются для достижения криминальной цели и воздействия на объект правонарушения. Поэтому сторонники третьей точки зрения считают, что использование компьютера как инструмента для совершения общественно опасного деяния является квалифицирующим признаком состава преступления и подпадает под понятие «применение технических средств».

Таким образом, «компьютерное правонарушение» можно признать либо как самостоятельную уголовно-правовую категорию, либо как «компьютерный аспект» совершения традиционных правонарушений.

Уголовным проступком признается совершенное виновно деяние (действие либо бездействие), не представляющее большой общественной опасности, причинившее незначительный вред либо создавшее угрозу причинения вреда личности, организации, обществу или государству, за совершение которого предусмотрено наказание в виде штрафа, исправительных работ, привлечения к общественным работам, ареста.

С этой позиции компьютерные правонарушения обладают всеми вышеперечисленными признаками:

1) Так как уголовный закон Республики Казахстан обозначил что уголовным проступком признается деяние, не представляющее большой общественной опасности чем преступление многие ученые ставят под сомнение наличие в целом такого признака как «общественная опасность». Тем не менее на наш взгляд, существует общественная опасность компьютерных правонарушений. Ущерб, наносимый компьютерными правонарушениями, значительно превышает ущерб традиционно совершаемых хищений. Повсеместное внедрение производственную и обыденную жизнь компьютеров, компьютеризированных расчетов и банковских операций, применений компьютерных технологий в документоведении, расширение диапазона возможностей выхода в иные, в том числе и зарубежные информационные сети

– все это делает компьютерные правонарушения общественно опасными. Причем наносимый ущерб может иметь как материальный, так и нематериальный характер, затрагивая интересы как личности, общества, так и государства в целом.

2) Вина в теории уголовного права определяется как психическое отношение виновного лица к совершенному им общественно опасному деянию и наступившим в результате общественно опасным последствиям, выраженное в форме умысла (ст. 20 УК РК) или неосторожности (ст. 21 УК РК). В случаях, когда в результате совершения умышленного правонарушения были причинены тяжкие последствия, которые по закону влекут боле строгое наказание и которые не охватывались умыслом лиц; возможны ситуации уголовной ответственность за совершение правонарушения с двумя формами вины (ст. 22 УК РК).

Применительно к компьютерным правонарушениям существует несколько точек зрения в отношении формы вины. По мнению таких авторов, как Т.Б. Сеитов, Б.Х. Толеубекова, Т.М. Лопатина данные правонарушения могут совершаться

как умышленно, так и неосторожно. Особенность компьютерных правонарушений обуславливается тем, что одни и те же действия с одним тем же умыслом могут приводить при различных состояниях компьютерной техники к не прогнозированным виновным последствиям. И, следовательно, неосторожная форма вины возможна. Вместе с тем, такой подход противоречит законодательному установлению, что деяние, совершенное по неосторожности, признается преступлением только в том случае, когда это специально предусмотрено соответствующей статьей Особенной части УК РК. Есть авторы, которые занимают иную позицию и считают, что субъективная сторона характеризуется только прямым умыслом [9, 10].

Разделяя последнюю точку зрения, необходимо внести некоторые уточнения. Совершая уголовно-наказуемое компьютерное правонарушение, виновное лицо действует умышленно, но мотивы и цели при этом могут быть различными. Одни занимаются компьютерными взломами с целью получения доступа к нематериальным эквивалентам материальных ценностей и их последующего присвоения, другие – действуют из «спортивных» целей. В результате, сознавая незаконность своих действий и предвидя возможность или неизбежность наступления общественно опасных последствий, виновное лицо действует с прямым или косвенным умыслом. Если же наступившие последствия не охватывались умыслом виновного, и влекут по закону более тяжкое наказание, то речь идет о двойной форме вины.

3) Факт существования компьютерных правонарушений признак уголовным законодательством не всех стран. Вместе с тем, признание их противоправности вытекает из высокой степени общественной опасности компьютерных правонарушений. Ни одна из отраслей права не обладает таким арсеналом санкций, как уголовное право, которые были бы адекватны ущербу, причиняемому компьютерными правонарушениями и реализовывали бы цели общей и частной пре-

венции. Богатый нормотворческий опыт ведущих индустриально развитых государств свидетельствует о том, что в таких странах как США, Япония, Великобритания, Германия проводится политика уголовно-правового преследования за компьютерные правонарушения. Существование последних этих странах расценивается как объективная реальность [11].

Таким образом, компьютерное правонарушение можно определить как общественно опасное деяние, предусмотренное уголовным законом, которое направлено на охраняемую законом компьютерную информацию и причиняет или создает угрозу причинения вреда правам и свободам человека, а также безопасности физических и юридических лиц, независимо от формы собственности, общества и государства.

Разнообразие научных взглядов на эту проблему указывает на существование другой точки зрения, согласно которой компьютерные правонарушения являются частью информационных правонарушений, затрагивающих информационные отношения. Информационные отношения, в свою очередь, представляют собой вид общественных отношений, возникающих при создании информационных ресурсов, функционировании информационных процессов, использовании информационных технологий и средств их обеспечения и защиты.

С развитием научно-технического прогресса и совершенствованием компьютерных технологий увеличивается количество криминальных схем и видов компьютерных правонарушений. Эксперты Организации экономического развития ООН предложили общую классификацию компьютерных преступлений, включающую: экономические компьютерные преступления; преступления, связанные с нарушением личных прав, особенно права на частную жизнь; и преступления против частных интересов.

Наиболее распространенными правонарушениями с использованием компьютерной техники являются: компьютерное пиратство, компьютерное мошенничество, распространение вредоносных (вирусных) программ и компьютерный саботаж. К компьютерному

пиратству относят, прежде всего, деятельность «хакеров» – неправомерный доступ к компьютерной информации с помощью подбора паролей, кодов, шифров, взломов электронных замков и т.п. Когда результатом подобной деятельности являются модификация информации и утечка денежных средств – она превращается в компьютерное мошенничество. Второй вид компьютерного пиратства - незаконное копирование, тиражирование и сбыт компьютерных программ. Подобная деятельность нарушает авторские права создателей и разработчиков программ, причиняет материальный ущерб им и законным владельцам компьютерных программ. К тому же страдают пользователи программного продукта, так как качество копий уступает качеству оригинала [12].

В настоящее время в научной литературе имеется обширный классификационный разброс:

1. В.Д. Курушин и А.В. Шопин классифицируют «компьютерные правонарушения» следующим образом:

– незаконное использование компьютера в целях моделирования или анализа преступных действий для осуществления в компьютерных системах;

– незаконное проникновение в информационно-вычислительные сети или массивы информации;

– хищение прикладного и системного программного обеспечения;

– несанкционированное копирование, изменение или уничтожение информации;

– шантаж, информационная блокада или другие виды компьютерного давления на соперника;

– передача компьютерной информации лицам, не имеющим к ней доступа;

– подделка, мистификация или фальсификация компьютерной информации;

– разработка и распространение компьютерных вирусов;

– несанкционированный просмотр или хищение информационной базы;

– небрежность при разработке, изготовлении и эксплуатации информационно-вычислительных сетей и программного обеспечения, приводящая к тяжким последствиям;

– механические, электрические, электромагнитные и другие виды воздействия на информационно-вычислительные сети, заведомо вызывающие их повреждение [13, с. 249].

2. Ю.М. Батурин, А.М. Жодзишский предлагают иную классификацию:

– нарушение правил обработки информации персонального характера;

– несанкционированный доступ в компьютерную систему;

– угроза возникновения конфликта;

– заражение компьютерным вирусом;

– уничтожение элементов компьютерной техники;

– изменение объектов компьютерной техники;

– изъятие объектов компьютерной техники;

– хищения [14, с. 372].

3. Б.Х. Толеубекова применительно к современным условиям Казахстана формулирует следующую классификацию:

– компьютерное мошенничество;

– информационное пиратство;

– незаконное копирование информации;

– кража компьютеров и их компонентов;

– кража из кассовых аппаратов [15, с. 190].

4. В руководстве ООН по «Профилактике и пресечению компьютерной преступности» предложена такая классификация:

– компьютерное мошенничество;

– компьютерный подлог;

– повреждение или модификация данных компьютера или программ;

– незаконный доступ в компьютерную систему;

– незаконное производство компьютерных программ [16].

Примеры классификации «компьютерных правонарушений» не являются исчерпывающими, и существуют другие виды. Их разнообразие объясняется следующими факторами: а) уровнем правового регулирования отношений в сфере компьютерной информации; б) степенью их теоретической проработки; в) глубиной криминальной пораженности информационного пространства; г) степенью использования международного законодательного опыта в национальной правоприменительной практике.

В нашем уголовном законе Казахстана «компьютерные преступления» теперь называются «уголовные правонарушения», которые делятся на уголовные проступки и преступления. В том случае, если деяние влечет наказание в виде лишения свободы, это является преступлением.

Кодификатор рабочей группы Интерпола, используемый Национальным центральным бюро Интерпола в более чем 10 странах, представляет значительный научный и практический интерес. Эта классификация не только учитывает возможность появления новых видов компьютерных преступлений, но и способствует укреплению международного сотрудничества.

Большинство компьютерных преступлений являются результатом профессиональной и организованной преступной деятельности, часто осуществляемой международными группами. Причем часто в состав группы входит непосредственный работник кредитной организации или иной компании, которая впоследствии оказывается пострадавшей (по некоторым оценкам, при хищениях с использованием компьютерных средств до 80% таких деяний совершались «изнутри»).

Транснациональный характер компьютерной преступности и её быстрое распространение требуют объединения усилий и ресурсов многих стран для противодействия этому явлению. В настоящее время существует острая необходимость в разработке международно-правовой базы для предотвращения инцидентов, связанных с обменом информацией,

борьбы с информационным терроризмом и создания комплекса международных мер, предотвращающих деструктивное использование средств воздействия на национальные и глобальные информационные ресурсы.

Можно сделать вывод, что понятие «компьютерного преступления» является одним из центральных в сегменте преступлений в сфере компьютерной информации, но до сих пор остается более чем не определенным. В мировой практике «… признано, что дать определение компьютерного преступления чрезвычайно сложно. Не всякое использование компьютерной системы образует состав компьютерного преступления» [17, с. 35]. Определение понятия «компьютерное преступление» сталкивается с трудностями из-за невозможности выделить единый объект криминального посягательства и множества предметов, подлежащих уголовно-правовой охране. В поисках точного юридического значения термина «компьютерное преступление» мнения ученых и практиков сильно разнятся. По поводу объекта данного преступления существуют как минимум три точки зрения: одни считают, что объектом является сам компьютер, другие – компьютерная информация, записанная на электронных носителях, а третьи - общественные отношения, связанные с безопасным (законным) использованием информации.

Компьютерное правонарушение по своей сути очень специфично и своими корнями уходит вглубь профессиональной среды специалистов в области информационных технологий. Это особый мир или отдельная страна со своими законами, понятиями, лидерами, целями и даже наказаниями. Здесь нельзя навести свой порядок, установить свой «устав». Единственный путь для уголовно-правовой науки видится в том, чтобы на основе глубокого анализа пытаться смоделировать юридические понятия и в дальнейшем грамотно регулировать отношения в данной области.

2.2. Юридическое понятие объекта и предмета уголовных правонарушений в сфере информатизации и связи

Для оценки характера и степени общественной опасности деяния и его правильной квалификации важно определить конкретное социальное благо, охраняемое уголовным законом, на которое направлено посягательство. Поэтому необходимо понять особенности непосредственного объекта уголовных правонарушений в области информатизации и связи.

Согласно теории уголовного права, непосредственным объектом является конкретное общественное отношение, которое защищается уголовно-правовой нормой, обеспечивая возможность действовать определенным образом или находиться в определенном состоянии.

Одни ученые считают, что непосредственным объектом компьютерных правонарушений являются общественные отношения, связанные с безопасностью информации. Другие полагают, что для каждого состава правонарушения существует свой непосредственный объект [18]. Наиболее последовательной, как нам представляется, является последняя позиция.

На основе этого, непосредственным объектом правонарушений в сфере информатизации и связи являются охраняемые уголовным законом общественные отношения, которые обеспечивают: а) конфиденциальность защищенной законом компьютерной информации; б) безопасность компьютерной информации и компьютеров; в) безопасность использования компьютера, информационной системы или информационно-коммуникационной сети.

Определяя понятие объекта правонарушений, необходимо остановиться на соотношении объекта и предмета криминального посягательства.

«Уголовно-правовое значение предмета правонарушения определяется не его физическими свойствами, а характе-

ром и содержанием выражающихся в нем общественных отношений. В уголовно-правовом смысле предмет всегда выступает в связи с конкретными общественными отношениями» [19]. Уголовный закон охраняет не вещи и предметы сами по себе, а те общественные отношения, на которые направлено посягательство. Иными словами, воздействуя на предмет криминального посягательства, правонарушитель нарушает (или предпринимает попытку нарушить) само общественное отношение, находящееся под охраной уголовного закона.

Соотношение объекта и предмета криминального посягательства в сфере компьютерной информации имеет важное значение для уголовно-правовой характеристики правонарушения, ввиду того, что компьютер и компьютерная информация (в таких формах, как цифровая, сжатая, зашифрованная) представляют собой особую материю.

В определении понятия предмета уголовного правонарушения в сфере информатизации и связи мнения ученых разделились. Одни считают, что предметом является компьютерная информация [20, с. 470], другие относят к предмету, компьютер, компьютерную систему или компьютерную сеть [21, с.23].

Нарушение нормального осуществления информационных отношений происходит посредством посягательства на информацию, которая выступает предметом рассматриваемых правонарушений, является общепризнанным фактом [22, с. 90].

Информация – это не просто совокупность знаний о фактических данных, это благо, которое имеет определенную ценность. С введением нового Гражданского кодекса Республики Казахстан (далее – ГК РК) информация стала самостоятельным объектом гражданских прав, наряду с деньгами, ценными бумагами, результатами интеллектуальной деятельности (ст. 115 ГК РК), т.е. товаром со всеми вытекающими из этой правовой дефиниции последствиями [23]. Отсюда любое «завладение» и «пользование» документированной информацией без согласия ее собственника или законного владельца (за исключением случаев, прямо указанных в законе) является

неправомерным, поскольку нарушает права последнего.

Информация признается одним из прав граждан. Всеобщая декларация прав человека и гражданина [24], принятая Генеральной Ассамблеей ООН 10 декабря 1948 г., в ст. 19 закрепила право каждого человека на свободу искать, получать и распространять информацию и идеи любыми средствами и независимо от государственных границ. Следуя приоритету норм международного права, Конституция Республики Казахстан, в ч. 4 ст. 29 подтвердила и гарантировала это право граждан, ограничив его сведениями, составляющими государственную тайну. Вместе с тем Конституция РК содержит ряд иных ограничений, связанных с распространением информации. В частности, ст. 23 закрепляет право граждан не неприкосновенность частной жизни, личную и семейную тайну, тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, а ст. 24 запрещает сбор, хранение, использование и распространение информации о частной жизни лица без его согласия.

В соответствии со ст. 2 Закона РК «Об информатизации» информация определяется как «сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления» [25].

В информационном обществе информация становится стратегическим ресурсом. В ближайшем будущем мировое сообщество может разделиться на два противоположных лагеря. Мощные индустриальные державы, благодаря своему высокому научно-техническому и экономическому потенциалу, а также высокому уровню информационной и образовательной подготовки населения, могут занять доминирующее положение и установить глобальный информационный контроль над миром.

Понятие «информация» может быть рассмотрено в различных аспектах:

Информация в философском понимании представляет

собой совокупность сведений о природе и обществе, процессах, протекающих в них и отражающихся в сознании людей.

Социальная информация включает все виды информации, проходящей через сознание людей: математическую, экономическую, правовую, статистическую т.д.

Информация с позиций кибернетики рассматривается как циркулирующая по электронным каналам связи.

Информация в техническом аспекте определяется как содержание данных, которое видят в них люди.

Информация в уголовно-правовом смысле представляет собой сведения о лицах, явлениях и процессах, содержащихся в информационных системах (банках данных).

Как научная категория информация представляет собой многоаспектное явление, которое имеет количественную и качественную стороны [26]. Количественная сторона информации фиксируется при помощи математических, статистических методов измерения, которые нашли свое применение как в науках о неживой природе (физике, химии, геологии), так и в науках об обществе (психологии, социологии, экономике). Качественная сторона информации характеризует ее содержание, смысл, социальную значимость и общественную (частную) ценность. Именно качественная характеристика социальной информации определяет необходимость в ее уголовно-правовой защите.

Социальную информацию можно классифицировать по разным основаниям:

– по сфере применения: массовая; персональная.

– по категориям: политическая; экономическая; правовая; военная; статистическая и т.д.

– по источникам: официальная; неофициальная.

– по объему: общая; отраслевая.

– по содержанию: документальная; иная.

– по режимам доступа: общедоступная; конфиденциальная (государственная, коммерческая, служебная тайна).

– по соотношению со временем: о прошлом; о настоящем; о будущем.

– по проблематике сведений: об экологии; о безопасности; о внешнеполитической обстановке и т.д.

– по мотивации: позитивная; нейтральная; негативная.

– по формам собственности: государственная; негосударственная (принадлежащая физическим и юридическим лицам).

– по форме выражения: устная; на бумаге; компьютерная: на электронных носителях, в компьютере, информационных системах или информационно- коммуникационных системах.

Социальная информация может быть представлена на электронных носителях и храниться в компьютерах, компьютерных системах и сетях. В этом контексте она называется компьютерной информацией. Здесь речь идет не просто об информации, а о данных, которые неразрывно связаны с компьютером.

Компьютерная информация – это информация, зафиксированная на электронном носителе и передаваемая по телекоммуникационным каналам в форме, доступной восприятию компьютера [27, с. 32].

Само понятие «компьютерная информация» как предмет криминального посягательства трактуется по-разному:

– как неотъемлемая инструментальная часть компьютера;

– как определенная совокупность данных, представляющая ценность для отдельного человека, организации, предприятия, учреждении, фирмы, общества, государства.

В первом случае «компьютерная информация» выступает как форма и является объектом гражданско-правовой охраны, объектом интеллектуальной собственности, авторского, патентного и изобретательского права. Во втором случае «компьютерная информация» выступает как содержание и в зависимости от категории доступа может являться объектом уголовно-правовой охраны.

На компьютерную информацию ограниченного доступа в процессе криминального посягательства осуществляется неправомерное воздействие, за которое предусматривается ответственность в ст. ст. 205, 206, 208, 211, ч.1 ст.

213 УК РК. В качестве предмета уголовного правонарушения в сфере информатизации и связи («пассивная информация») могут выступать банки данных, различные компьютерные программы, компьютеризованные объекты авторского права и т.д.

Когда компьютерная информация используется активно, она становится инструментом для совершения правонарушения, называясь «активной информацией». С её помощью воздействуют на «пассивную информацию». В любом компьютерном правонарушении можно воздействовать на объект правонарушения с помощью компьютерной информации, которая в этом случае выступает как орудие преступления. Примерами «активной информации» могут быть компьютерные команды или вирусные программы.

Ст. 210, ч. 2 ст. 213 УК РК предусматривает ответственность за создание, использование или распространение вредоносных компьютерных программ и программных продуктов, а также за создание, использование, распространение программ для изменения идентификационного кода абонентского устройства.

В таких случаях предметом криминального посягательства являются вредоносные программы или программные продукты, а также программы для изменения идентификационного кода абонентского устройства.

Законодатель определяет вредоносную программу как программу, способную уничтожать, блокировать, модифицировать или копировать информацию, нарушать работу компьютера, информационной системы или сети, выполняя эти действия без разрешения собственника или законного владельца информации.

К таким программам относятся «компьютерные вирусы» «черви», «троянцы», «программы-бомбы». Примером «программ-троянцев» являются программы-антивирусы, фото и видео галереи с «exe». «bat», «com» файлами и т.д.

Наиболее известным случаем использования «логической бомбы» является инцидент, произошедший в начале 80-х годов на Волжском автомобильном заводе. Занимаясь программированием автоматизированной системы подачи механических узлов на главный конвейер, программист умышленно внес в программу команду, приведшую к остановке системы после прохождения заданного числа деталей. В результате с конвейера в срок не сошло 200 автомашин. Заводу был причинен значительный материальный ущерб [28, с. 206].

Вредоносные программы могут сочетаться. Широко известная пользователям компьютеров вредоносная программа «Чернобыль» сочетает в себе особенности «вируса» и особенности «временной бомбы».

Приведенные примеры показывают, что такие вредоносные программы могут представлять одинаковую угрозу как для отдельных пользователей компьютеров, так и для государственной безопасности. С ростом числа пользователей Интернета вероятность глобальной угрозы также увеличивается.

Новое уголовное законодательство Казахстана включает в себя новые виды правонарушений, среди которых есть законы, направленные на защиту компьютерной информации. Установление уголовной ответственности за вред, причиненный использованием компьютерной информации, стало необходимым из-за её растущего значения и широкого применения в различных сферах. Компьютерная информация более уязвима по сравнению с информацией, записанной на бумаге и хранящейся в сейфе, что делает её защиту особенно важной.

2.3. Основные способы совершения уголовных правонарушений в сфере информатизации и связи

Способы совершения правонарушений играют ключевую роль в их уголовно-правовой характеристике. Это совокупность методов, которые преступники используют для достижения своих целей. Правонарушения могут быть совершены различными способами, и иногда для достижения криминальных целей применяется комбинация этих методов. Компьютерные правонарушения не являются исключением. Техническая и правовая практика показывает, что компьютерные преступники проявляют огромную изобретательность. Рассмотрим наиболее распространенные методы совершения компьютерных правонарушений в Республике Казахстан.

По законодательству РК предусмотрены следующие способы совершения уголовно-наказуемых посягательств в сфере компьютерной информации:

1. Неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть.

Несанкционированный доступ к информации может осуществляться в широком диапазоне целей от удовлетворения бытового любопытства до компьютерного шпионажа, осуществляемого в криминальных целях.

Уголовная ответственность наступает в случае, если несанкционированный (неправомерный) доступ к защищенной законом информации приводит к общественно опасным последствиям.

Способы неправомерного доступа к защищенной законом компьютерной информации могут включать: использование чужого имени или пароля, изменение физических адресов устройств, модификацию программного обеспечения, нахождение уязвимостей и взлом системы, угадывание кодов, подключение к компьютеру через телефонную сеть и другие методы. Несанкционированный доступ к ограниченным интернет-ресурсам, который приводит к уничтожению, блокировке,

модификации или копированию информации, также считается неправомерным, если у лица не было права на такой доступ.

Так, с помощью методов «брешь», «люк», «неспешный выбор» находится ошибка в программе или слабое место в системе защиты и осуществляется несанкционированный доступ к информации. Преступник, используя метод «маскарад», выдает себя за законного пользователя и проникает в сеть. Несанкционированный доступ может осуществляться с использованием различных методов манипуляции. Преступник, используя «взламывающую программу», применяя метод «подмена кода», обходит систему защиты и проникает к информации. Зная пароль (код), преступник, применяя метод «троянский конь», внедряется в программное обеспечение компьютера [29].

Таким образом, применяя известные методы или их комбинации, можно получить несанкционированный доступ к защищенной законом компьютерной информации. Если наступают последствия, указанные в статье 205 Уголовного кодекса Республики Казахстан, возникает основание для уголовной ответственности. Эти методы требуют профессиональных знаний о логической структуре аппаратного и программного обеспечения компьютеров, что делает их недоступными для обычных пользователей.

2. Нарушение работы информационной системы или информационно-коммуникационной сети выражается в снижении работоспособности отдельных звеньев компьютера, отключении элементов компьютерной сети.

Нарушение работы информационной системы или информационно-коммуникационной сети выражается в нештатной технической ситуации (сбой в работе компьютера, информационной системы или информационно-коммуникационной сети, «зависание» компьютера и т.п.), при которой нормальное функционирование компьютерной техники невозможно. Обязательным условием при этом является сохранение физической целостности компьютерной системы [30, с. 32]. В противном случае содеянное дополнительно квалифицируется по

статьям о правонарушениях против собственности.

3. Создание компьютерной программы или программного продукта с целью неправомерного уничтожения, блокировки, модификации, копирования или использования информации, хранящейся на электронных носителях, в информационных системах или передаваемой по информационно-коммуникационным сетям, а также для нарушения работы компьютеров, абонентских устройств, программного обеспечения, информационных систем или сетей.

Создание программы для компьютера – это написание ее алгоритма, то есть последовательности логических команд с дальнейшим» преобразованиями его в электронном языке компьютера [31, с. 241]. Чаще всего для этого используется язык программирования АССЕМБЛЕР, СИ, СИ++, ТУРБО-СИ, ТУРБО-АССЕМБЛЕР.

Способ совершения правонарушения подразумевает создание не просто программ для компьютера, а вредоносных программ, т.е. программ, которые содержат «вирусы», «сетевые вирусы», «логические бомбы» с целью уничтожения, блокирования, модификации, копирования программного продукта, нарушение работы компьютера, информационной системы или информационно-коммуникационной сети. «Вирусы» могут быть внедрены в операционную систему, прикладную программу, в сетевой драйвер. Такие «вирусные программы» распространяются по коммуникационным сетям, проникают в компьютер и «заражают» его, присоединяясь к другим программам.

Наиболее сложной и опасной разновидностью компьютерный вирусов являются сетевые вирусы, иначе «компьютерные черви». Объектом нападения последних являются системы обработки данных, включающие в свой контур вычислительные комплексы, персональные компьютеры, соединенные в локальные, отраслевые, государственные или межгосударственные сети.

Общественная опасность создания «вирусных» программ состоит в том, что они могут в любой момент парализовать работу не только отдельного компьютера, но и целой

компьютерной сети.

Первым создателем «вируса» считается студент Калифорнийского университета (США) Фрэд Коуэн, который проводил опыты с компьютерными программами, в последствии названные «компьютерными вирусами». С первой компьютерной «эпидемией» связывается имя Роберта Таппана Морриса, студента Корнельского университета (США), который заразил «вирусом» более 6 тысяч компьютеров и 70 компьютерных систем, причинив ущерб около 100 миллионов долларов [32, с. 167].

«Логическая бомба» и ее разновидность «временная бомба» встраиваются в программный продукт путем внесения набора определенных команд, которые задействуются при определенных условиях или в определенный момент времени и приводят к общественно опасным последствиям.

Высокая общественная опасность вредоносных программ привела к тому, что законодатель связывает уголовную ответственность не с фактическим наступлением опасных последствий, а с самим фактом создания программ, которые могут привести к таким последствиям, как указано в статье. Из-за сложной структуры и принципа действия вирусных программ правильная квалификация действий преступника невозможна без участия специалиста в области компьютерных технологий.

4. Внесение вредоносных изменений в существующую программу или программный продукт.

Изменение существующих программ (или отдельной программы) включает модификацию алгоритма компьютера: изменение, удаление или замена фрагментов алгоритма, добавление новых частей и т.д. Такие изменения превращают программу в вредоносную, что может привести к различным нежелательным последствиям, вплоть до уничтожения информации.

Способ внесения изменений в программу может быть различным: декомпилирование программы, использование специального программного продукта и т.д. Законодателя свя-

зывает уголовную ответственность с фактом внесения изменений в программу, которые заведомо могут привести к наступлению общественно опасных последствий.

5. Использование вредоносных программ для компьютера.

Термин «использовать» обозначает что-либо употребить для какого-либо дела [33, с. 43]. Под использованием как способом совершения правонарушения понимается выпуск в свет, введение вредоносной программы (или программ) в хозяйственный оборот (в числе в модифицированном виде) для применения по назначению или воспроизведения.

Использование вредоносной программы происходит без согласия собственника или владельца информации. При этом виновное лицо осознает, что программа вредоносна и ее применение может привести к общественно опасным последствиям, таким как уничтожение, блокировка, модификация, копирование компьютерной информации, а также нарушение работы компьютера, информационной системы или сети. Такие программы обычно не входят в состав стандартного программного обеспечения и не проходят антивирусную проверку. Факт использования вирусной программы обычно устанавливается с помощью информационно-технологической экспертизы.

6. Распространение вредоносных программ для компьютера.

Распространение вредоносной программы (программ) означает ее передачу одному (или нескольким) пользователям компьютера. Распространение может осуществляться разными способами:

а) по компьютерной сети (локальной, региональной, государственной, международной);

б) путем предоставления доступа другим пользователям к «вирусной» программе;

в) путем воспроизведения на чужом компьютере записи вредоносной программы с дискеты, копирования вредоносной программы с диска на диск, через модем, компьютерную сеть, электронную почту;

г) созданием условий для самораспространения программы [34].

Распространение вирусных программ для компьютеров может происходить активно (внедрение вирусной программы в компьютер, информационную систему или сеть любым способом, обеспечивающим свободный доступ к ней) и пассивно (непрепятствование самораспространению вирусной программы или её распространению третьими лицами). Ответственность несут как разработчики, так и пользователи, сознательно распространяющие вирусные программы.

7. Использование или распространение вредоносных компьютерных программ и продуктов. Под использованием таких программ понимается их эксплуатация (или любое другое использование) с целью применения содержащейся в них вирусной программы.

Распространение вредоносных компьютерных программ включает их передачу третьим лицам через продажу, прокат, дарение, аренду, обмен, предоставление взаймы или копирование. Пользователи, сознательно распространяющие носители с вирусными программами, несут ответственность независимо от наступления общественно опасных последствий, так как они создают реальную угрозу уничтожения, блокировки, модификации, копирования информации или нарушения работы компьютеров, устройств, программного обеспечения, информационных систем или сетей.

Дополнительно, важно отметить, что распространение таких программ может происходить как в физической форме (например, через USB-накопители или диски), так и в цифровой форме (через электронную почту, файлообменные сети или вредоносные веб-сайты). В обоих случаях, действия по распространению вредоносных программ могут быть квалифицированы как преступные, если они направлены на причинение вреда или создание угрозы для информационной безопасности.

2.4. Характеристика субъективных признаков уголовных правонарушений в сфере информатизации и связи

Характеристика субъективных признаков уголовных правонарушений в сфере информатизации и связи включает анализ психического отношения лица к совершаемому преступлению. Это отношение выражается в форме вины, мотива и цели правонарушения. Важно учитывать, что правонарушением признается только такое деяние, которое было совершено осознанно и находилось под контролем воли и сознания лица.

Мотив и цель в некоторых случаях являются необходимыми элементами субъективной стороны умышленных уголовных правонарушений. Например, корыстный мотив при злоупотреблении должностным положением или цель похищения денежных средств при несанкционированном доступе к данным. В некоторых составах преступлений мотив и цель выступают в качестве квалифицирующих признаков, таких как корыстные побуждения при неправомерном распространении ограниченных электронных информационных ресурсов.

Некоторые мотивы указаны в уголовном законе как отягчающие или смягчающие обстоятельства. Это может быть совершение преступления из-за тяжелых личных или семейных обстоятельств, под влиянием угрозы или принуждения, материальной, служебной или иной зависимости, а также по мотивам национальной, расовой или религиозной ненависти, мести за правомерные действия других лиц, или с целью скрыть другое преступление или облегчить его совершение. Во всех этих случаях мотив и цель являются элементами уголовно-правовой характеристики преступлений.

Однако для большинства умышленных уголовных правонарушений мотив и цель не являются обязательными элементами субъективной стороны и, следовательно, не входят в их уголовно-правовую характеристику. Тем не менее, при расследовании конкретного преступления мотив и цель всегда должны быть установлены. Это важно не только для

определения справедливого наказания судом, но и для получения важной информации для предотвращения правонарушений в сфере информатизации и связи.

Исходя из результатов изучения зарубежных исследователей по этому вопросу, в настоящее время можно выделить, пять наиболее распространенных мотивов совершения компьютерных правонарушений, расположенных в рейтинговом порядке:

1. Корыстные соображения – 66% (совершаются в основном правонарушителями третьей группы, кракерами и ламмерами);
2. Политические цели – 17% (шпионаж, преступления направленные на подрыв финансовой и денежно-кредитной политики правительства, на дезорганизацию валютной системы страны, на подрыв рыночных отношений – совершаются хакерами по найму либо правонарушителями третьей группы);
3. Исследовательский интерес – 7% (студенты, молодые программисты-энтузиасты, называемые хакерами);
4. Хулиганские побуждения и озорство – 5% (хакеры, кракеры, ламмеры);
5. Месть – 5% (хакеры, кракеры, ламмеры)

Мотивы совершения правонарушений в сфере информатизации и связи разнообразны и не ограничиваются перечисленными. Они могут включать месть за негативное отношение работодателя, нанесение ущерба авторским правам, уничтожение секретных материалов, интеллектуальный вызов, безответственность, компьютерный шпионаж, самоутверждение и другие.

На основе криминального мотива формируется цель правонарушения, представляющая собой мысленную модель желаемого результата, к которому стремится правонарушитель, совершая противоправное деяние.

Анализ литературных источников позволяет выделить следующие типичные криминальные цели, для достижения ко-

торых используются компьютерные технологии: фальсификация платежных документов, хищение безналичных денежных средств, перечисление средств на фиктивные счета, отмывание денег, легализация преступных доходов (например, путем их дробления и перевода на законные счета с последующим снятием и многократной конвертацией), совершение покупок с фиктивной оплатой (например, с использованием сгенерированной или взломанной кредитной карты), продажа конфиденциальной информации, похищение программного обеспечения и его незаконное распространение и т.д.

В Уголовном кодексе Республики Казахстан, помимо обязательного признака субъективной стороны вины, в некоторых составах уголовных правонарушений выделяются специальные цели совершения деяний. Например, в части 2 статьи 209 "Принуждение к передаче информации" указана цель получения информации из национальных электронных информационных ресурсов или национальной информационной системы. В статье 210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» указана цель неправомерного уничтожения, блокирования, модификации, копирования или использования информации, хранящейся на электронных носителях, в информационных системах или передаваемой по информационно-коммуникационным сетям, а также нарушения работы компьютеров, абонентских устройств, программного обеспечения, информационных систем или сетей.

Блокирование информации – это запрещение дальнейшего выполнения последовательности команд или выключение из работы какого-либо устройства, или выключение реакции какого-либо устройства компьютера [35, с. 187].

В юридической литературе термин «блокирование информации трактуется по-разному: как невозможность ее использования при сохранение такой информации, как закрытие информации, что делает ее недоступной для использования правомочным пользователем, как создание условий (в том числе с помощью специальных программ), искусственно за-

трудняющих доступ пользователей или полностью исключающих пользование компьютерной информацией.

Из приведенных определений следует, что блокирование информации осуществляется путем воздействия на компьютерную информацию, при котором она сохраняется, но становится недоступной для выполнения своих функций. Это связано с таким техническим воздействием на компьютер, которое делает информацию недоступной для собственника или законного владельца с использованием существующих технических средств. Вряд ли можно говорить о блокировании информации в уголовно-правовом смысле, если доступ к ней невозможен из-за недостаточной квалификации пользователя.

Таким образом, блокирование информации следует понимать как результат воздействия на компьютер, который исключает доступ к информации при сохранении её целостности.

Модификация информации означает внесение любых изменений, за исключением тех, которые необходимы для функционирования программы или базы данных на конкретных технических средствах пользователя или под управлением его программ.

Модификация информации – наиболее сложный в правовом смысле вопрос. Модификация – это внесение изменений, не меняющих сущности объекта [36, с. 4]. Легальность внесенных изменений должна определяться с учетом норм авторского права.

В уголовно-правовом смысле под модификацией одни юристы понимают изменение первоначальной информации без согласия ее собственника или иного законного лица [37, с. 38]. Другие рассматривают модификацию информации как изменение логической и физической базы данных. Третьи полагают, что модификация заключается в несанкционированной переработке первоначальной информации (удаление и добавление записей, содержащихся в файлах, создание файлов, перевод программы компьютера или базы данных с одного языка на другой и т.п.).

Анализ мнений специалистов позволяет определить модификацию компьютерной информации как несанкционированная собственником или законным владельцем любая переработка первоначального состояния охраняемой законом информации, которая трансформирует ее содержание.

Копирование информации – создание копий файлов и системных областей дисков.

От копирования компьютерной информации следует отличать тиражирование (размножение) информации, преследующее иные цели.

Понятие копирование в уголовно-правовом смысле у ученых вызывает некоторые разногласия. В одних случаях, копирование рассматривается как снятие копии с оригинальной информации с сохранением ее не поврежденности и возможности использования по назначению [38]. В других, как изготовление второго и последующих экземпляров базы данных, файлов, а также их запись в память компьютера. В третьих – как тиражирование информации при сохранении оригинала. При этом способ копирования не имеет определяющего значения. Копирование по смыслу закона выступает способом несанкционированного проникновения, которое является уголовно наказуемым деянием. Поэтому нельзя согласиться с мнением, что копирование компьютерной информации от руки, ее фотографирование с экрана дисплея, считывание информации путем перехвата излучений компьютера не образуют состава данного преступления.

Нам представляется наиболее точным определение понятия «копирование информации» как перенос информации с одного электронного носителя на другой, если это осуществляется помимо воли собственника или владельца информации [39] при условии получения точного дубликата оригинала охраняемой законом компьютерной информации.

Личность человека, совершившего преступление, а теперь по нашему УК Республики Казахстан правонарушения, является объектом изучения наук криминалистического профиля, которые решают логически взаимосвязанные задачи: что такое личность преступника (правонарушителя); какие

признаки составляют ее содержание; какова ее роль в совершении преступления (правонарушения); как воздействовать на нее, чтобы предотвратить совершение преступления (правонарушения).

Понятие «личность» характеризует социальное качество человека, которое не возникает с рождением, а формируется в процессе общественных отношений. Личность человека – это система социально-психологических свойств и качеств, в которых отражены связи и взаимодействие человека с социальной средой посредством практической деятельности [40].

Личность человека, выступая в единстве всех ее социальных, нравственных и психологических свойств и признаков, формируется в процессе его жизни и деятельности.

Формирование личности является сложным, противоречивым и в общем необратимым процессом, развивающимся «по спирали». Этот процесс начинается в подростковом возрасте. Любое преступление (правонарушение), в какой бы форме оно не совершалось, не случайно по отношению к личности, поскольку оно подготовлено развитием его социальных, нравственных, психологических свойств. В криминологическом изучении личности преступника (правонарушителя) выделяются два основных подхода.

Первый подход предусматривает изучение личности конкретного преступника (правонарушителя). В данном случае о личности преступника (правонарушителя) можно говорить лишь применительно к субъекту преступления (правонарушения) в его уголовно-правовом представлении.

Второй подход дает представление об общих свойствах группы лиц, могущих совершить преступление (правонарушения). Применительно к компьютерным преступлениям (правонарушениям) диапазон таких лиц широк и включает в себя беспечных подростков, не достигших возраста уголовной ответственности и манипулирующих со своими компьютерами. Они сочетают в себе устойчивые элементы профессионализма в области информатики и программирования с элементами своеобразного фанатизма и изобретательности. Го-

воря о характеристике личности преступника (правонарушителя), необходимо учитывать следующие составляющие:

– пол,
– возраст,
– уровень образования,
– социальный статус,
– семейное положение,
– социально-полезная деятельность,
– характеристика преступной деятельности,
– мотивация преступной деятельности,
– нравственно-психологические особенности личности,
– уровень правового сознания и др.

Вышеперечисленные признаки не являются исчерпывающими. Они формируют содержание научного понятия «личность преступника», теперь с новым уголовным законодательством Казахстана мы будем их называть («личность правонарушителя»). В действительности эти признаки присущи конкретным правонарушителям в неодинаковой мере, их вариантность определяется личностными свойствами последних.

Применительно к уголовным правонарушениям в сфере информатизации и связи попытаемся рассмотреть основные характеристики личности правонарушителя по материалам отечественной и зарубежной литературы. Начнём с того, что, как и у обывателей, так и у работников следственных органов давно сложился яркий стереотип компьютерного правонарушителя. Это юнец 15-ти – 20-ти лет, с темными, длинными, чуть косматыми волосами, в очках, молчаливый, замкнутый, рассеянный, с блуждающим взглядом, помешанный на компьютерах, напрочь игнорирующий события в окружающем мире. Нельзя сказать, что данный стереотип не имеет права на существование и ни с чем с оригиналом не схож. Как показывает статистика и независимые исследования, 20 из 100 «обитателей» криминального мира с «компьютерным уклоном» являют собой стопроцентно «чистых» стереотипных компьютерных правонарушителей. Остальные 80 в это стереотип не вписываются либо вообще, либо частично [41, с. 146].

В личностном плане субъекты уголовных правонарушений в сфере информатизации и связи характеризуются противоречиво. От молодого человека, работающего за дисплеем по 12-16 часов подряд, неряшливого вида, питающегося урывками и неприхотливо, не обращающего внимание на внешний мир, до высококвалифицированных, респектабельных специалистов, занимающих высокое социальное положение. Свыше 80% правонарушителей в компьютерной сфере – мужчины [42, с. 148].

Обычно правонарушения в сфере компьютерной информации совершаются в одиночку, что характерно для мужчин. Женщины же, напротив, в большинстве входят в состав групп [43].

По уровню специального образования диапазон весьма широк – от высококвалифицированных специалистов до лиц, обладающих минимально необходимыми познаниями для работы в качестве пользователя: 40% – лица, имеющие среднее специальное образование; 40% – высшее; 20% – среднее [43].

По профессиональной подготовленности и социальному статусу выделяются следующие группы:

Первая группа характеризуется как самый низший уровень.

Сюда входят нарушители правил пользования компьютера, распространители вирусов и т.п.

Вторая группа представлена «хакерами» и «кракерами». «Хакеры» (hacker) – пользователи компьютеров, занимающиеся доскональным изучением и поиском слабых мест компьютерных сетей, операционных систем и систем информационной безопасности. Иногда в литературе и средствах массовой информации (далее – СМИ) таких лиц называют: «киберпанками».

К хакерам относятся увлеченные компьютерной техникой лица, преимущественно из числа молодежи – школьники и студенты, совершенствующиеся на взломах различных защитных систем. Хакеры объединены в региональные группы, издают свои СМИ (газеты, журналы, BBS (bulletin board system – электронные доски объявления), Web-странички), проводят электронные конференции, кодекс хакерской чести,

имеют жаргонный словарь, который постоянно пополняется и распространяется, также имеются все необходимые сведения для повышения мастерства начинающего – методики проникновения в конкретные системы и взлома систем защиты [44].

К хакерам следует относить лиц, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма, и изобретательности. По мнению некоторых авторов, эти субъекты воспринимают средства компьютерной техники как своеобразный вызов их творческим и профессиональным знаниям, умениям и навыкам. Именно это и является в социально-психологическом плане побуждающим фактором для совершения различных деяний, большинство из которых имеют криминальный характер.

Под воздействием указанного выше фактора лицами рассматриваемой группы изобретаются различные способы несанкционированного проникновения в компьютерные системы, нередко сопровождающиеся преодолением постоянно усложняющихся средств защиты данных. Следует подчеркнуть, что характерной особенностью правонарушителей этой группы является отсутствие у них четко выраженных противоправных намерений. Практически все действия совершаются ими с целью проявления своих интеллектуальных и профессиональных способностей. Ситуация здесь условно сравнима с той, которая возникает при различного рода играх, стимулирующих умственную активность игроков, например при игре в шахматы. Когда в роли одного игрока выступает гипотетический правонарушитель, а в роли его соперника – обобщенный образ компьютерной системы и интеллект разработчика средств защиты от несанкционированного доступа. Подробно данная ситуация исследуется в математической науке в теории игр – модели поведения двух противоборствующих сторон. При этом одной из сторон является человек, а другой – компьютер. Взаимодействие человека с компьютером осуществляется по определенному игровому алгоритму с целью обучения, тренировки, имитации обстановки и с развлекательными целями.

Обобщенные данные позволяют обозначить следующую социально-психологическую характеристику этого круга лиц. Представители данной специальности обычно весьма любознательны и обладают незаурядным интеллектом и умственными способностями. При этом не лишены некоторого своеобразного озорства и «спортивного» азарта. Наращиваемые меры по обеспечению безопасности компьютерных систем ими воспринимаются в психологическом плане как своеобразный вызов личности, поэтому они стремятся, во что бы то ни стало найти эффективные способы доказательства своего превосходства.

Как правило, это и приводят их к совершению правонарушения. Постепенно некоторые субъекты рассматриваемой категории не только приобретают необходимый опыт, но и находят интерес в этом виде деятельности. В конечном итоге происходит переориентация их целеполагания, которое из состояния «бескорыстной игры», переходит в свое новое качество: увлечение заниматься подобной «игрой» лучше всего с получением некоторой материальной выгоды.

Обобщенный портрет «хакера» примерно выглядит так: мужчина в возрасте от 15 до 45 лет, имеющий многолетний опыт работы на компьютере; в прошлом к уголовной ответственности не привлекался; является яркой мыслящей личностью, способной принимать ответственные решения; хороший, добросовестный работник; по характеру нетерпимый к насмешкам и к потере своего социального статуса в рамках группы окружающих его людей: любит уединенную работу: приходит на службу первым и уходит последним; часто задерживается на работе после окончания рабочего дня и очень редко использует отпуска и отгулы [45, с. 12].

В виртуальном мире, как и в реальном уже сложилась четкая классификация. Есть хакеры – программисты энтузиасты, а есть кракеры. Кракерами стали называть хакеров совершающих хищения. К ним также относятся и компьютерные хулиганы, и вандалы, которые просто крушат сайты.

Кракеры, как и хакеры, занимаются поиском уязвимых мест в вычислительных системах и осуществлением атак на них.

Принципиальное различие между хакерами и кракерами состоит в целях, которые они преследуют. Основная задача хакера в том, чтобы, исследуя информационную систему, обнаружить слабые места (уязвимости) в ее системе безопасности и информировать пользователей и разработчиков системы с целью последующего устранения найденных уязвимостей. Другая задача хакера – проанализировав существующую безопасность информационной системы, сформулировать необходимые требования и условия повышения уровня ее защищенности.

Основная задача кракера состоит в непосредственном осуществлении взлома системы с целью получения несанкционированного доступа к чужой информации – обычно для ее копирования, подмены или для объявления факта взлома. Итак, кардинальное различие между хакерами и кракерами в том, что первые - исследователи компьютерной безопасности, а вторые – непосредственно преступники.

Общими признаками для хакеров и кракеров являются: завышенная оценка своих профессиональных и, как следствие, интеллектуальных способностей; использование специфического жаргона не только в кругу специалистов, но и при повседневном общении; отсутствие интереса к проблемам повседневной жизни [45, с. 12]. Хакерство и кракерство – это образ жизни, который накладывает отпечаток на внешность, поведение, круг общения, личностные цели и социальные ориентиры. Правонарушения, как правило, совершаются открыто, могут использоваться оригинальные способы, собственные ноу-хау; методы взлома атакованного компьютера, информационной системы или информационно-коммуникационной сети могут тиражироваться среди «коллег».

Два наиболее опасных типа злонамеренных кракеров – это так называемые информационные маклеры и мета-хакеры. Информационные маклеры нанимают хакеров и оплачивают их услуги, чтобы получить интересующую информацию, а затем продают ее правительствам иностранных государств или деловым конкурентам.

Мета-хакеры – более изощренные хакеры, контролирующие других хакеров, причем делающие это порой незаметно для последних. Как правило, с корыстной целью используются уязвимые места, обнаруженные этими подконтрольными хакерами. Мета-хакер эффективно использует других хакеров фактически как интеллектуальные инструментальные средства.

Другой типичной разновидностью хакеров являются бригады, известные как «элита». Они формируют закрытые клубы, члены которых свысока смотрят на обычных хакеров, использующих традиционные инструментальные средства для взлома. Эта так называемая элита разрабатывает собственные инструментальные средства и всегда пользуется дружеской поддержкой и оценкой своего мастерства со стороны себе подобных.

Еще одной характерной разновидностью является группа, известная как «темные хакеры» («darksiders»). Они используют хакерство для финансовых махинаций или для создания злонамеренных разрушений. Они не согласны с классической мотивацией для хакеров, которая заключается лишь в получении ощущения успеха и власти. Эти хакеры не считают электронное нарушение границ нечестным по своей сути. Однако важнейшей их особенностью является скорее то, что darksiders переступают невидимую границу, проведенную другими хакерами, и сами становятся вне законов этики хакерского мира. Не секрет, что этические нормы «хакерского большинства» осуждают хакерство для получения нечестных денег или причинения явного вреда.

К числу особенностей, указывающих на совершение уголовного правонарушения в сфере информатизации и связи лицами рассматриваемой категории, можно отнести следующие:

1. Отсутствие целеустремленной, продуманной подготовки к уголовному правонарушению;

2. Оригинальность способа совершения уголовного правонарушения;

3. Непринятие мер к сокрытию уголовного правонарушения;

4. Совершение озорных действий на месте происшествия.

Близко к рассматриваемой выше группе лиц способных совершить компьютерное правонарушение можно отнести, как мне представляется, еще одну, группу лиц отличающихся от хакеров и кракеров непрофессионализмом, дилетантством и наивностью.

Ламмеры – это лица, которые на волне всеобщего «Интернет психоза» пытающиеся быть хакерами. В последнее время участились случаи, когда компьютерными правонарушениями начинают заниматься «чайники» (неопытный пользователь ПК), считающие что компьютерные правонарушения остаются безнаказанными. Для совершения криминальных деяний ими используются готовые рецепты вроде программ генерации фальшивых номеров кредитных карточек и т.д. Компьютерные правонарушения с использованием генерированных номеров кредитных карточек приняли сегодня широко распространились по странам СНГ.

Попытки «выхватить» что-нибудь из сети предпринимают многие любители Интернета, причем большинство из них и не подозревает, что за ними «могут прийти». Ламмеры по неопытности полагают, что за хищение виртуальных денег им ничего не будет. Вообще большинство людей, искренне считающих себя хакерами, таковыми не являются. Они используют заранее написанные «программы-ломалки» и очень слабо представляют себе, как работает сеть. К сожалению подобных правонарушителей-дилетантов, становится слишком много. Так что средний «правонарушитель» теперь обыкновенный «lamer», т.е. малоквалифицированный человек.

Третья группа характеризуется более высоким социальным положением и респектабельностью. В нее входят бухгалтера, управляющие финансами фирм, адвокаты и т.д. – воспитанники экономико – политической среды. Они вовремя осознали свои возможности в конкретный момент времени и в потенциале, определили «рыночную» цену своих знаний, сделали из увлечения карьеру. Их знания в большинстве случаев обширнее и систематизированнее, а следовательно и ценнее,

чем у представителей второй группы. Они – настоящая сила как в бизнесе, так и в криминальном мире.

В связи с этим представляет интерес профиль типичного «беловоротничкового» компьютерного правонарушителя, составленный консультативно-исследовательской фирмой Managment Safeguards INc. (США):

– приходит на работу очень рано, задерживается дольше других, иногда работает в выходные дни;
– хорошо знает, как работает система охранной сигнализации;
– имеет ключи от всех основных замков в служебных помещениях;

– делает все возможное, чтобы завоевать доверие руководства и работать самостоятельно без контроля;

– не поддерживает дружеских и деловых отношений с другими сотрудниками, предпочитая работать самостоятельно, потому что мало кому доверяет [46, с. 8].

Правонарушители третьей группы характеризуются организованностью совершения компьютерных правонарушений с обязательным использованием действий, направленных на их сокрытие, и обладающие в связи с этим устойчивыми криминальными навыками.

Лиц данной группы можно охарактеризовать как высококвалифицированных специалистов, имеющих высшее техническое образование, возможно более одного высшего образования (техническое + экономическое и/или юридическое).

Знания в области компьютерных технологий практически исчерпывающие: люди этой группы владеют несколькими языками программирования всех уровней, в совершенстве знают особенности аппаратной части современных компьютерных систем (не только персональных, но и сетевых систем и специализированных информационных комплексов), имеют навыки профессиональной работы с несколькими компьютерными платформами (IBM PC, Apple Macintosh, SUN Microsystems), основными операционными системами (UNIX и клоны, LINUX в различных вариантах), MS DOS, Windows 3.X/NT/9X, OS/2, Novell NetWare/IntranetWare, SUN OS) и

большинством пакетов прикладного программного обеспечения специализированного назначения (любое офисное, сетевое программное обеспечение, пакеты разработки приложений и др.), прекрасно информированы об основных системах электронных транзакций (сетевые протоколы, протоколы защищѐнной связи (биржевые, банковские и правительственные каналы), системах сотовой связи, системах и методах стойкой и супер-стойкой криптографии и успешно используют эти знания в «повседневной деятельности».

Имеют связи во многих властных структурах (приём многие «покровители» обязаны им за определённые услуги), которые используют при необходимости для проникновения на закрытые объекты и для получения кодов доступа в сильно защищённые от «взлома» системы.

Работают в основном «для прикрытия», обычно начальниками или замами начальников отделов информационных технологий в банках, в иностранных компаниях и государственных учреждениях, основная же деятельность развёртывается в нелегальной и полулегальной сфере. Связь с «соратниками по ремеслу» поддерживают практически постоянную, но в основном на чрезвычайно конфиденциальном и индивидуальном уровне, крайне редко в прямом общении, в основном через сетевую связь, защищённую стойкой криптографией. Постоянно совершенствуют приемы и инструменты «работы». Практически недосягаемы для органов правосудия. В общем, на лицо стопроцентные профессионалы своего дела.

Именно эта группа правонарушителей и представляет собой основную угрозу для общества. На долю именно этих правонарушителей приходится максимальное число совершенных особо опасных посягательств, например, до 79% хищений денежных средств в крупных и особо крупных размерах и различного рода должностных преступлений, совершаемых с использованием средств компьютерной техники.

В этой группе выделяются «узкие профессионалы», технический уровень которых позволяет заниматься созданием вредоносных компьютерных программ или их модификацией.

Создание такой программы представляет собой комплекс операций, состоящих из подготовки исходных данных, предназначенных для управления процессами уничтожения, блокирования, модификации или копирования информации, нарушения работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети. Такую работу могут исполнить только высококвалифицированные специалисты: профессионально подготовленные компьютерщики; программисты; лица, могущие модифицировать программу с целью сделать ее вредоносной. К ним примыкают и лица, занимающиеся незаконным обращением вредоносных программ или электронных носителей с такими программами [47, с. 129].

Четвертая группа представлена самой высокой ступенью. Сюда входят лица, занимающиеся компьютерным шпионажем. Представители этой группы хорошо подготовлены в техническом и организационном отношениях. Их целью является получение стратегических важных данных о противнике в экономической, технической и других сферах.

На основании вышеизложенного, а также с учетом анализа специальной литературы, обобщенную характеристику личности «компьютерного» правонарушителя, данные которой в равной степени можно отнести к любой из рассмотренных групп, представляется возможным изложить следующим образом.

Возраст правонарушителей колеблется в широких границах (от 15 до 45 лет): на момент совершения правонарушения возраст 33% правонарушителей не превышал 20 лет, 13% – были старше 40 лет и 54%- имели возраст 20-40 лет. Большинство лиц данной категории составляют мужчины (80%), но доля женщин быстро увеличивается из-за профессиональной ориентации некоторых специальностей и профессий (секретарь, делопроизводитель, бухгалтер, кассир, и т.д.)

По уровню специального образования диапазон также весьма широк – от высоко квалифицированных специалистов до лиц, обладающих минимально необходимыми познаниями для работы в качестве пользователя. 52% правонарушителей

имели специальную подготовку в области автоматизированной обработки информации, а 97% – являлись служащими государственных учреждений и организаций, использующих компьютерную технологию в своих производственных процессах, а 30% из них имели непосредственное отношение к эксплуатации средств компьютерной техники.

Большинство правонарушителей (77%) при совершении правонарушения имели средний уровень интеллектуального развития, 21% – выше среднего и только 2% – ниже среднего. При этом 40% правонарушителей имели средне специальное образование, 40% – высшее и 20% – среднее. С исследовательской точки зрения интересен тот факт, что из каждой тысячи компьютерных правонарушений только семь совершаются профессиональными программистами.

В последнее время, как свидетельствует статистика, резко увеличивается количество уголовных правонарушений, совершенных в составе организованных групп и сообществ за счет активного участия в них правонарушителей третьей группы. Так, 39% правонарушителей действовали без соучастников, тогда как 62% – в составе преступных групп. В поведении правонарушителей рассматриваемой группы, как правило, не наблюдается отклонений от принятых общественных норм и правил. По своему общественному положению большинство из них являются служащими, нередко занимающими ответственные руководящие посты и соответственно обладающие доступом либо к средствам компьютерной техники, либо к учету и распределению материальных ценностей и благ, либо и то и другое вместе. В этом случае необходимо отметить высокий удельный вес руководящих работников всех рангов (более 25%), обусловленный тем, что управляющим обычно является специалист долее высокого класса, обладающий профессиональными знаниями, имеющий право отдавать распоряжения исполнителям и непосредственно не отвечающий за работу средств компьютерной техники.

Вместе с этим более высокий удельный вес руководящих работников среди совершивших хищения (23%) и более высокий процент правонарушений, совершенных в составе

организованной преступной группы (35%), характеризуют компьютерные хищения как организованные и групповые правонарушения. К косвенным признакам представителя рассматриваемого нами социального типа можно отнести внимательность, бдительность, осторожность, оригинальность (нестандартность) мышления и поведения, активную жизненную позицию.

В профессионально-классификационном плане круг «компьютерных» правонарушителей чрезвычайно широк. Обычно это разные категории специалистов и руководителей: бухгалтеры, программисты, системные администраторы, инженеры, финансисты, банковские служащие, адвокаты, начальники отделов и служб и т.д. Всех их можно разделить на две основные группы, исходя из классифицирующего признака категории доступа к средствам компьютерной техники:

1. Внутренние пользователи.
2. Внешние пользователи, где пользователь – субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Пользователи бывают двух видов: зарегистрированные (санкционированные) и незарегистрированные (несанкционированные, незаконные).

По оценкам основная опасность в плане совершения компьютерного правонарушения исходит именно от внутренних пользователей: ими совершается 94% правонарушений, тогда как внешними пользователями – только 6%, при этом 70%-клиенты пользователи, 24 обслуживающий персонал.

Правонарушителями из числа внешних пользователей, как свидетельствует практика, обычно бывают лица, хорошо осведомленные о деятельности потерпевшей стороны. Их круг настолько широк, что уже не поддается какой-либо систематизации, и классификации им может быть любой даже случайный человек. Например, представитель организации, занимающейся сервисным обслуживанием, ремонтом, разработкой программных средств, хакеры, кракеры, ламмеры и т.д.

Рассмотрение характеристик личности компьютерного

правонарушителя имеет важное значение в практической деятельности по предупреждению рассматриваемой категории правонарушений и учитываются при статистическом анализе уголовных правонарушений по лицам; при установление причин и условий, способствующих совершению компьютерных правонарушений; при профилактике соответствующих правонарушений. Уголовно-правовой анализ состава уголовных правонарушений в сфере информатизации и связи.

Контрольные вопросы

1. Какие основные виды уголовных правонарушений в сфере информатизации и связи вы можете назвать?
2. Какое значение имеет Уголовный кодекс Республики Казахстан в обеспечении информационной безопасности?
3. Какие примеры реальных преступлений в сфере информатизации и связи вы можете привести?
4. Какие общественные отношения охраняются уголовным законом в сфере информатизации и связи?
5. В чем заключается разница между объектом и предметом уголовного правонарушения?
6. Какие примеры предметов уголовных правонарушений в сфере информатизации и связи вы можете привести?
7. Какие способы неправомерного доступа к информации вы знаете?
8. В чем заключается нарушение работы информационной системы или сети?
9. Какие методы используются для несанкционированного доступа к информации?
10. Какие мотивы чаще всего встречаются при совершении компьютерных правонарушений?
11. Как мотивы и цели влияют на квалификацию правонарушений?
12. Какие примеры целей правонарушений в сфере информатизации и связи вы можете привести?

3. Уголовно-правовой анализ состава уголовных правонарушений в сфере информатизации и связи

3.1. Характеристика объективных и субъективных признаков состава правонарушения «Неправомерного доступа к информации, в информационную систему или информационно-коммуникационную сеть»

Согласно статье 205 Уголовного кодекса Республики Казахстан, непосредственным объектом неправомерного доступа к защищенной законом информации, хранящейся на электронных носителях, в информационных системах или сетях, являются общественные отношения, которые обеспечивают сохранность и конфиденциальность этой информации.

Под собственником информационных ресурсов, информационных систем, технологий и средств их обеспечения понимается субъект, имеющий право в полном объеме реализовывать полномочия владения, пользования и распоряжения указанными объектами [48, с. 274]. Под владельцем информационных ресурсов, информационных систем, технологий и средств их обеспечения понимается субъект, имеющий право в полном объеме реализовывать полномочия владения, пользования и распоряжения в пределах, установленных законом. Под пользователем информации понимается субъект, обращающийся к информационной системе за получением необходимой информации с целью ее пользования.

Анализируемая диспозиция правонарушения указывает на неправомерность доступа не ко всей защищенной законом компьютерной информации, а только к той, которая хранится на электронных носителях, в информационных системах или информационно-коммуникационных сетях.

К электронным носителям относятся устройства, используемый для записи, хранения и воспроизведения информации, обрабатываемых с помощью средств вычислительной

техники: магнитные диски, дискеты, магнитные ленты, оптические диски, стримеры и т.п. В компьютере информация может находиться в оперативном запоминающем устройстве (далее – ОЗУ), в котором при запуске компьютера определенное время может храниться, обрабатываться и передаваться охраняемая законом компьютерная информация. В информационной системе компьютера информация может находиться в ОЗУ периферийных устройств (к примеру, в лазерном принтере могут выстроиться «в очереди» на печать несколько документов, которые содержат охраняемую законом информацию). ОЗУ устройств связи, сетевые устройства и каналы связи относятся к информационно-коммуникационной сети компьютера, в которых также может находиться охраняемая законом информация (к примеру, модемы и факс-модемы имеют свои ОЗУ и «буферные» устройства, в которых некоторое время может находиться предназначенная для дальнейшей передачи информация).

Уголовно-правовой запрет на доступ к информации, содержащейся на электронном носителе, в информационную систему или информационно- коммуникационную сеть распространяется только на охраняемую законом информацию. Применительно к уголовному законодательству Республики Казахстан охраняются следующие виды информации:

Сведения, отнесенные к государственной тайне (ст.ст. 175, 176, 185 УК РК); Сведения, носящие конфиденциальный характер: персональные данные, сведения о частной жизни (ст.ст. 138, 147 УК РК);

Сведения, связанные с выполнением профессиональных функций; врачебная тайна, адвокатская тайна, тайна вклада, тайна переписки, телефонных, переговоров, почтовых отправлений и сообщений (ст. ст. 148, 321 УК РК);

Сведения, являющиеся служебной тайной, банковской тайной коммерческой тайной (ст. 223 УК РК);

Сведения, являющиеся объектом авторских и смежных прав (ст. 198 УК РК).

К обязательным признакам объективной стороны неправомерного доступа к информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть относятся:

– общественно опасное деяние в виде неправомерного доступа к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть;

– общественно опасные последствия в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства;

– причинная связь между совершенным общественно опасным деянием и наступившими общественно опасными последствиями.

Общественно опасное деяние в данном составе всегда проявляется в активной форме поведения виновного, то есть в действии. Неправомерный доступ к информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть в форме бездействия осуществить нельзя.

Под неправомерным доступом к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть следует понимать самовольное получение виновным лицом информации или распоряжение ею (уничтожение, блокирование, модификация, копирование) по своему усмотрению без разрешения ее собственника или законного владельца.

Чтобы вменить лицу проанализированные выше общественно опасные последствия и квалифицировать его действия по ст. 205 УК РК, необходимо установить наличие причинной связи между совершенным, деянием в виде неправомерного доступа к охраняемой законом компьютерной инфор-

мации и наступившими последствиями, обозначенными в диспозиции статьи. Для этого требуется доказать тот факт, что деяния было необходимым и закономерным условием наступления вредных последствий и предшествовало этим последствиям по времени.

Помимо обязательных признаков объективной стороны состава теория уголовного права выделяет факультативные к которым относятся место, время, обстановка, орудия, средства и способ совершения преступления. Применительно к составу неправомерного доступа к охраняемой законом компьютерной информации, факультативные признаки объективной стороны на квалификацию содеянного не влияют, но могут учитываться при индивидуализации наказания.

Состав правонарушения, предусмотренного ст. 205 УК РК, является материальным, поэтому квалифицирующее уголовно-правовое значение отводится моменту окончания правонарушения. Одни авторы правонарушение связывают с моментом отсылки компьютеру последней команды вызова хранящейся информации [29, с. 14]. Другие, и их большинство, с моментом наступления хотя бы одного из последствий, перечисленных в законе [35, с. 187].

Таким образом, моментом окончания неправомерного доступа к охраняемой законом информации, содержащейся на электронном носителе, информационную систему или информационно-коммуникационную сеть следует считать наступление общественно опасных последствий: существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства.

Совершение деяний, не повлекших перечисленные выше последствия, состава данного правонарушения не образуют либо образуют стадию покушения на совершение неправомерного доступа к охраняемой законом информации, содержащиеся на электронном носителе, в информационную систему или информационно-коммуникационную сеть.

Таким образом, имеющаяся у законного владельца или пользователя возможность восстановить неправомерно уничтоженную информацию с помощью программных средств, получить ее от другого пользователя или использовать имеющуюся копию уничтоженной информации не освобождает виновного от уголовно-правовой ответственности.

В науке уголовного права субъективная сторона состава правонарушения рассматривается как «психическое отношение лица к совершенному им правонарушению, которое характеризуется конкретной формой вины, мотивом и целью правонарушения» [49, с. 104].

Установление субъективной стороны состава неправомерного доступа к охраняемой законом компьютерной информации обусловлено определенной сложностью. Ведь безошибочных программ не бывает. Доказать умысел в действиях виновного лица нелегко: на его стороне презумпция невиновности. Сложность доказывания умысла затрудняется и сложностью доказывания совершенных им действий, ставших причиной наступления указанных в законе последствий. «Это затруднение связано с большой сложностью компьютерных систем и большим кругом лиц, имеющих прямое или косвенное отношение к последствиям преступления» (в нашем государстве - правонарушения) [50, с. 193].

В отношении субъективной стороны рассматриваемого состава наличествует несколько диаметрально противоположных точек зрения. По мнению одних ученых данное правонарушение может быть совершено как умышленно, так и по неосторожности. Другие предполагают наличие только прямого умысла. Последняя позиция разделяется большинством авторов осуществляя неправомерный доступ к информации, в информационную систему или информационно-коммуникационную сеть виновное лицо сознает общественно опасный характер своего действий, предвидит возможность или неизбежность наступления общественно – опасных последствий, указанных в диспозиции статьи Уголовного кодекса, желает их

наступления (прямой умысел) или не желает, но сознательно допускает наступления этих последствий либо относится к ним безразлично (косвенный умысел).

Интеллектуальный элемент умысла при неправомерном доступе к охраняемой законом информации к информации, в информационную систему или информационно-коммуникационную сеть характеризуется: осознанием субъектом правонарушения, совершаемого им деяния и предвидением возможности (или вероятности) того, что охраняемая законом информация может повлечь существенное нарушение прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства.

Волевой элемент умысла определяется желанием (или сознательным допущением) либо безразличным отношением к наступлению указанных в статье общественно-опасных последствий.

Говоря об умысле, необходимо учитывать то обстоятельство, что неправомерный доступ к охраняемой законом информации, в информационную систему или информационно-коммуникационную сеть совершаются субъектами, которые обладают достаточной профессиональной эрудицией, чтобы отдавать отчет своим действиям и предвидеть вариантность будущих последствий. Совершение волевого осознанного действия виновным лицом, которое обладает личной технической осведомленностью, компьютерной грамотностью, предполагает видимость и наступивших последствий. Все это позволяет признать, что уголовно наказуемый неправомерный доступ к охраняемой законом информации, в информационную систему или информационно- коммуникационную сеть совершается с умышленной формой вины.

Субъекты компьютерных правонарушений являются технически образованными лицами, которые управляют компьютеризированными системами, эксплуатируют и обслуживают их. Поэтому совершение ими общественно опасных де-

яний с использованием компьютерных технологий происходит с осознанием возможности наступления последствий, представляющих опасность для компьютерных программ, для работы компьютера, информационной системы или информационно- коммуникационной сети.

Как было отмечено выше в науке уголовного права часто возникают вопросы: может ли быть уголовно наказуемо несанкционированное проникновение к охраняемой законом компьютерной информации с неосторожной формой вины?

Теория уголовного права по степени общественной опасности дифференцирует неосторожность на такие формы как самонадеянность и небрежность. Моделирование преступного умысла применительно к анализируемому составу позволяет предположить, что при самонадеянности виновное лицо предвидит наступление общественно опасных последствий своего «легкомысленного» обращения (в виде неправомерного доступа) с информацией, но рассчитывает без достаточной на то аргументации их предотвратить; при небрежности виновное лицо не предвидит возможности наступления общественно опасных последствий в результате действий, связанных с неправомерным доступом к компьютерной информацией, хотя при должной внимательности и осмотрительности оно должно было и могло предвидеть эти последствия.

Нельзя не принимать во внимание и вероятность наступления в результате самонадеянного или небрежного обращения с компьютерной техникой в процессе неправомерного доступа к охраняемой законом информации общественно опасных последствий. Разработчики компьютеров приблизились к технологиям, позволяющим, через информационные системы управлять производственными процессами, переводить вредные технологии на обслуживание вычислительной техникой. В таких условиях и самонадеянность, и небрежность могут вызвать катастрофические последствия, в том числе и тяжкие.

В формировании формы вины большую роль играет мотив и цель поведения. Мотив – психическое переживание, побуждение, которое вызывает у человека решимость к действию или благоприятствующее его совершению. Цель – желаемый результат конкретного преступного акта. Мотивы и цель совершения данного преступления могут быть самыми разными; от корысти, мести, исследовательского интереса, злобы до хулиганских побуждений, политического и служебного эгоцентризма.

Зарубежные и отечественные исследователи излагают перечень мотивов неправомерного доступа, связывая их в одних случаях, с социально-психологическими свойствами различных групп преступников, в других – с особенностями способов совершения преступления. Так, у «неквалифицированных» пользователей мотивы и цели могут отсутствовать полностью. Для «любителей» характерны такие мотивы, как хулиганские побуждения, самоутверждение, исследовательский интерес. Для «профессиональных» компьютерных правонарушений характерны корыстные мотивы. Для «пользователей» компьютеров мотивы и цели могут быть самыми разнообразными [43, с. 12].

Для данного состава мотив и цель не являются обязательным элементом субъективной стороны и на квалификацию содеянного не влияют, но учитываются при индивидуализации наказания.

По общему правилу субъектом неправомерного доступа к охраняемой законом компьютерной информации может быть любое вменяемое физическое лицо, достигшее к моменту совершения правонарушения шестнадцатилетнего возраста. Особенность субъекта анализируемого правонарушения состоит в том, что пользователь, не обладающий специальными знаниями, вряд ли может причинить компьютерной информации вред, за который законодатель предусматривает уголовную ответственность.

Опасность неправомерного доступа к охраняемой законом информации, содержащейся на электронном носителе, в информационную систему или информационно-коммуникационную сеть заключается в том, что в сферу криминальной деятельности втягиваются профессионалы из не криминогенного контингента: а) лица, не связанные трудовыми отношениями с организацией, «атакованной» в криминальных целях; б) сотрудники-пользователи компьютеров, злоупотребляющие своим должностным положением или положением в компании. К первой группе относятся:

– «профессионалы» – это высококвалифицированные специалисты, действия которых характеризуются предварительной подготовкой, целеустремленностью, сокрытием следов правонарушения, прямым умыслом и корыстной направленностью;

– «любители» – это лица, сочетающие профессионализм в области компьютерной техники и программирования с элементами своеобразного фанатизма, и изобретательности;

– «пользователи» компьютеров – это лица, обладающие достаточными навыками в работе с компьютерами и совершающими правонарушения

«разово», то есть в случае, когда представляется возможность совершить незаконную операцию при помощи компьютера;

– жертвы «компьютерной революции» – это лица, имеющие ограниченные знания в области эксплуатации информационных технологий, в результате чего их неосторожными действиями уничтожается компьютерная информация.

Ко второй группе относятся внутренние пользователи компьютера, которые по роду своей деятельности имеют доступ к компьютеру, информационно-коммуникационным сетям и осведомленные об используемых компанией способах и средствах защиты компьютерной техники.

Западные специалисты подразделяют представляющий опасность персонал на следующие категории в зависимости от

сфер деятельности:

а) операционные правонарушения – совершаются операторами, периферийных устройств ввода информации в компьютер и обслуживающими линии телекоммуникации;

б) правонарушения, основанные на использовании программного обеспечения, совершаются лицами, в чьем ведении находятся библиотеки программ, системными программистами, прикладными программистами, хорошо подготовленными пользователями;

в) для аппаратурной части компьютерных систем опасность совершения правонарушения представляют: инженеры-системщики, инженеры по терминальным устройствам, инженеру, связисты, инженеры-электронщики;

г) определенную угрозу совершения компьютерных правонарушений представляют и сотрудники, занимающиеся организационной работой: управлением компьютерной сетью, руководством операторами, управлением базами данных, руководством работой по программному обеспечению;

д) определенную угрозу могут представлять также разного рода клерки, работники службы безопасности, работники, контролирующие функционирование компьютеров;

е) особую опасность могут представлять специалисты в случае вхождения ими в сговор с руководителями подразделений и служб самой коммерческой структуры или связанных с ней систем, а также с организованными преступными группами, поскольку в этих случаях причиняемый ущерб от совершенных преступлений и тяжесть последствий значительно увеличиваются.

Отечественные исследователи внутренних пользователей подразделяют на следующие группы:

К первой группе относятся служащие, которые в силу функциональных обязанностей имеют доступ к компьютерной информации.

Ко второй группе относится вспомогательный техниче-

ский персонал, по востребованности имеющий доступ к компьютерной информации.

К третьей группе относятся лица, косвенно имеющие доступ к средствам компьютерной техники в силу занимаемого ими служебного положения.

К четвертой группе относятся лица, которые не имеют доступа к средствам компьютерной техники, к компьютерной информации и не имеет специальных познаний в этой области (например, уборщики помещений, сотрудники службы охраны и т.д.) [43, с. 12].

Несмотря на то, что особое внимание исследователей уделяется «внешним» правонарушителям, в действительности подавляющее большинство правонарушений совершается «внутренними» правонарушителями. Около 90% злоупотреблений в финансовой сфере, – связанных с нарушениями в области информационной безопасности, происходит при прямом или косвенном участии действующих работников банков. Причем на криминальный путь становятся самые квалифицированные, обладающие максимальными правами в автоматизированных системах категории служащих.

Компьютерные правонарушения, совершаемые в компаниях, связаны, как правило, с ошибками или умышленным «нападением» служащих компаний:

– ошибки персонала – 55%:
– проблемы физической защиты – 20%;
– нечестные сотрудники – 10%:
– обиженные сотрудники – 9%;
– распространение «вирусов» – 4%;
– внешнее нападение – 1-3% [31, с. 43].

Выделение типовых моделей разных категорий правонарушителей, знание их основных черт способствует процессу определения круга лиц, среди которых может оказаться субъект правонарушения.

Лицо, использующее свое служебное положение или имеющее доступ к компьютеру, информационной системе

или информационно-коммуникационной сети, – это законный пользователь, обладающий правом доступа и обработки определенного рода информации в связи с выполнением своих служебных обязанностей, вытекающих из трудовых отношений (заключенного контракта) [51].

Неправомерный доступ осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

Хакеры «электронные корсары», «компьютерные пираты» – так называют компьютерных правонарушителей, осуществляющих противоправный несанкционированный доступ в чужие информационные сети. Техника правонарушения проста – набирая один номер за другим, они дожидаются, пока на другом конце провода не отзовется чужой компьютер. После этого телефон подключается к приемнику сигналов в собственном компьютере и устанавливается автоматическая связь и необходимый код. Таким образом, можно внедриться в чужую компьютерную систему.

Несанкционированный противоправный доступ к файлам и информации законного пользователя осуществляется также нахождением слабых мест в компьютерной защите системы. Однажды обнаружив их, правонарушитель может не спеша исследовать содержащуюся в системе информацию, копировать ее, возвращаться к ней много раз, подобно покупателю, изучающему товары на витрине.

Также программисты иногда допускают ошибки в программах, которые не удается обнаружить в процессе отладки. Авторы больших сложных программ могут не заметить некоторых слабостей компьютерной логики. Уязвимые места иногда обнаруживаются и в электронных цепях. Все эти небреж-

ности, ошибки приводят к появлению возможности совершения противоправного деяния. Обычно они все-таки выявляются при проверке, редактировании, отладке программы, но абсолютно избавится от них невозможно.

Бывает, что правонарушитель проникает в компьютерную систему, выдавая себя за законного пользователя. Системы, которые не обладают средствами аутентичной идентификации (например, по физиологическим характеристикам: по отпечаткам пальцев, по рисунку сетчатки глаза, голосу и т. п.), оказываются без защиты против этого способа правонарушения. Самый простейший путь его осуществления – это получить коды и другие идентифицирующие шифры законных пользователей. Это возможно:

– приобретением (обычно подкупом персонала) списка пользователей со всей необходимой информацией;

– обнаружением такого документа в организациях, где не налажен достаточный контроль за их хранением;

– незаконным, несанкционированным подслушиванием через телефонные линии.

Иногда случается, как например, с ошибочными телефонными звонками, что пользователь с удаленного терминала подключается к чьей-то системе, будучи абсолютно уверенным, что он работает с той системой, с какой и намеревался. Владелец системы, к которой произошло фактическое подключение, формируя правдоподобные отклики, может поддерживать это заблуждение в течение определенного времени и таким образом незаконно получить некоторую ценную информацию, в частности коды.

В любом компьютерном центре имеется особая программа, применяемая как системный инструмент в случае возникновения сбоев или других отклонений в работе компьютера, своеобразный аналог инструкций и приспособлений, помещаемых в транспорте под надписью «разбить стекло в случае аварии». Такая программа – мощный и опасный инструмент в руках преступника. Несанкционированный доступ

также может осуществляться в результате системной поломки компьютера. Например, если некоторые файлы пользователя остаются открытыми, он может получить доступ к не принадлежащим ему частям банка данных. Говоря фигурально, все происходит так словно клиент банка, войдя в выделенную ему в хранилище комнату, замечает, что у хранилища нет одной стены. В результате он может проникнуть в чужие сейфы и похитить все, что в них хранится.

3.2. Характеристика объективных и субъективных признаков состава правонарушения. Создания, использования и распространения вредоносных компьютерных программ и программных продуктов

Следует отметить, что данное правонарушение отнесено к наиболее общественно опасным деяниям из числа правонарушений, посягающих на компьютерную информацию, что выражается в размере санкций и в конструировании ч. 1 ст. 210 УК РК в виде формального состава. Наибольший вред собственникам, владельцам и законным пользователям компьютерных средств и информационных ресурсов приносят именно вредоносные программы.

Объектом данного правонарушения являются общественные отношения по безопасному использованию информации, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, а также программного обеспечения компьютерной информации.

В качестве предмета правонарушения выступают компьютерные программы и программные продукты, которые являются разновидностью компьютерной информации. Законодатель в ч. 1 ст. 210 УК РК предусматривает возможность «...внесение изменений в существующую программу или программный продукт», тем самым определяет программные средства в качестве предмета правонарушения, которые могут

быть подвергнуты противоправному воздействию, оговоренному в уголовном законе: уничтожению, блокированию, модификации, копированию и др.

К обязательным признакам объективной стороны правонарушения, предусмотренного ч. 1 ст. 210 УК РК относится общественно опасное деяние в виде: а) создания компьютерной программы, программного продукта б) внесение изменений в существующую программу или программный продукт, в) использование такой программы или программного продукта, г) их распространение.

Общественно опасное деяние в данном составе всегда проявляется в активной форме поведения виновного, то есть в действии. Понятие «создание вредоносной компьютерной программы» – это сложный многоэтапный процесс написания программы: от возникновения идеи и определения основных принципов работы программы до написания ее исходного текста и компилирования. В диспозиции статьи подразумевается создание программ для компьютеров, которые могут быть «вредными» и «безвредными». Определение вредоносности программы осуществляется только специалистами на основании информационно-технологической экспертизы и с учетом установления общественно-опасного характера последствий их действия.

С программно-технической точки зрения «компьютерный вирус» – это специальная компьютерная программа, способная самопроизвольно присоединяться к другим программам и при запуске последних выполнять самые различные нежелательные Действия (например, испортить, стереть файл, засорять оперативную память компьютера, создавать помехи в работе компьютера и т.п.). «Компьютерные вирусы» способны к само воспроизводству, модификации, маскировке и даже консервации на определенный период, они могут порождать новые вирусы. Они являются средством несанкционированного уничтожения, блокирования модификации, копиро-

вания компьютерной информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети.

В современном мире существует более 5 млн. видов программ-вирусов, и их количество ежегодно возрастает. По некоторым данным, в мире ежедневно создается от пяти до десяти новых вирусных программ [52, с. 197].

В последнее время появились программы – генераторы вирусов, которые позволяют получить текст нового вируса. Сам же процесс создания «вируса» может осуществляться одним из следующих способов: непосредственно в компьютере, информационной системе или информационно- коммуникационной сети, вне компьютерной системы с последующим внедрением «вируса».

Количество вирусов постоянно увеличивается. Все «вирусы» можно разбить на несколько групп:

а) системные вирусы (поражают загрузочные секторы электронной памяти);

б) файловые вирусы (поражают исполняемые файлы);

в) комбинированные вирусы (сочетающие свойства вышеуказанных вирусов в определенной алгоритмической совокупности).

По способу заражения компьютерной техники вирусы подразделяются на: а) резидентные (находится в оперативной памяти компьютерной системы потерпевшей стороны и является активным вплоть до ее выключения или перезагрузки. Активизируется после каждого включения компьютерной системы);

б) нерезидентные (не заражают оперативную память компьютерной системы, являются активными некоторое время и не имеют способности к распространению).

По алгоритму строения вирусы подразделяются на:

а) «вульгарный вирус» (компьютерная программа, написанная единым блоком);

б) «раздробленный вирус» (компьютерная программа,

разделенная на части, содержащие инструкции как, в какой последовательности, в какое время собрать их воедино).

Помимо вирусов, по характеру своего действия выделяют следующие вредоносные программы:

– «троянский конь», когда под известную программу вуалируется другая, которая, проникнув в информационно-вычислительные системы, внедряется в иные программы (иногда методом вставки операторов), начинающие работать неожиданно для законного пользователя по-новому;

– «троянская матрешка» (вредоносные команды формируются опосредованно через другие команды), «салями» и другие разновидности «троянского коня», «салями» применяется к программам, используемым в бухгалтерии. С помощью этой программы осуществляются компьютерные хищения. Принцип ее работы заключается в изъятии малых средств с каждого большого числа при совершении определенных операций, например, зачислении денег на счет или конвертации из одного вида валюты в другой. Программа названа так ввиду сходства с процессом отрезания тонких ломтиков одноименной колбасы. Программа эта весьма удобна для преступников, так как хищение оказывается высоко латентным ввиду того, что пропажу мизерных сумм выявить весьма сложно. Вместе с тем, учитывая скорость работы компьютера и частоту совершаемых операций (например, в пределах крупного банка), суммы, похищенные таким образом, оказываются в результате достаточно велики;

– «логическая бомба» – срабатывание определенных команд, неправомерно внесенных в какую-либо программу при определенных обстоятельствах, часто направленных на уничтожение данных. Иногда выделяют такой подвид, как «временная бомба», когда вредоносная программа или команда срабатывает по истечении определенного времени;

– компьютерные «черви». По характеру эта программа схожа с компьютерными вирусами. Отличие состоит в том, что «червь» – это самостоятельная программа.

Вредоносные программы могут сочетаться. Общественная опасность создания вредоносной программы определяется не столько способностью уничтожать, блокировать, модифицировать, копировать информацию, сколько способностью выполнять эти функции без получения санкции (согласия) собственника или законного владельца информации. Вредоносные программы содержат либо «вирусы», либо команды («троянский конь», «люк», «асинхронная атака», «логическая бомба» и т.п.), либо обладают свойствами, предназначенными для выполнения неправомерных действий.

Объемы и характеристики вредоносных программ разнообразны. Объединяющим является их разрушительное воздействие на информационные ресурсы, а в некоторых случаях и на сам компьютер.

Под программой для компьютера следует понимать объективную форму представления совокупности данных и команд, которые предназначены для функционирования компьютерной техники с целью получения определенного результата [53, с. 4]. Из определения следует, что создание программы следует считать оконченным с момента завершения процесса компилирования [54, с. 25]. Программой можно считать лишь реализованный алгоритм (совокупность данных и команд) в виде компилированного текста, декомпилированная, не переведенная на электронный язык программа, представляет собой обыкновенный текст. Законодатель устанавливает ответственность за создание таких вирусных программ, которые обладают способностью несанкционированного уничтожения, блокирования, модификации, копировании информации либо нарушению работы компьютера, информационной системы или информационно-коммуникационной сети.

Внесение изменений в существующую программу или программный продукт для компьютера означает изменение теста программы путем исключения его отдельных фрагментов, замены их другими либо их дополнения новыми фрагментами посредством специального программного продукта или

вручную. Внесение изменений в существующие программы – это комплекс операций с целью модификации ее во вредоносную. Причем «вирусной» программа становится именно в результате этих изменений.

Использование вредоносной программы для компьютера – это умышленное воспроизведение, распространение, установка или иные действия по введению программы в оборот в первоначальной или измененной форме. Под использованием понимается применение, запуск, вредоносной программы для осуществления функций, для которых она предназначена. Таким образом, использование вредоносной программы заключается во всяком ее употреблении по прямому назначению.

Распространение вредоносных программ для компьютера – это предоставление доступа к программе для компьютера в компилированном виде, в том числе сетевыми и иными способами, а также путем продажи, проката, сдачи внаем, предоставления взаймы либо создание условий для самораспространения программы.

Распространение вредоносных программ для компьютера возможно следующими способами:

– активным (посредством внедрения ее в компьютер, информационную систему или информационно-коммуникационной сеть);

– пассивным (не воспрепятствование самораспространении вредоносной программы или распространению ее третьими лицами).

К понятию распространение можно отнести и действия по сознательному представлению доступа другим пользователям к воспроизведенной вредоносной программе и программных продуктов или работа на чужом компьютере с использованием дискеты с записью вредоносной программы. Распространение «вируса» может осуществляться посредством копирования вредоносной программы с диска на диск или через модем, компьютерную сеть, электронную почту.

Использование электронных носителей с вредоносными программами и продуктами заключается во всяком их употреблении с целью использования записанной программы для компьютера. При этом под электронным носителем понимаются устройства, позволяющие сохранять вне компьютера компьютерную информацию: дискеты, магнитные ленты, магнитооптические диски, флешки, жесткие диски.

Распространение электронных носителей с вредоносными программами и программными документами означает передачу электронных носителей третьим лицам как возмездно, так и безвозмездно либо предоставление им возможности пользования этими носителями. Распространение электронных носителей с вредоносными программами и программными документами представляет собой один из способов их распространения (к примеру, сетевой способ) и по сути дела является альтернативным распространению вредоносных программ и программных продуктов деянием.

Состав уголовного правонарушения является формальным, поэтому для уголовной ответственности не требуется наступления каких-либо общественно опасных последствий. На формальный характер конструкции состава указывает факт заведомости приведения к общественно опасным последствиям созданной вредоносной программы и программных продуктов, внесенных в программу и программные документы изменений, а также их использование и распространение. Такое построение состава связано с характером перечисленных в диспозиции статьи деяний.

Правонарушение признается оконченным в момент завершения создания компьютерной программы и программного документа или их использования, распространения, независимо от того, наступили общественно опасные последствия или нет.

Большинство ученых полагает, что психическое отношение к выполнению действий, образующих объективную сторону состава правонарушения, предусмотренного ч. 1 ст. 210 УК РК, характеризуется прямым умыслом. Виновное лицо сознает, что его действия по созданию, использованию или

распространению соответствующих программ носят общественно опасный характер, предвидит неизбежность наступления несанкционированного уничтожения, блокирования, модификации, копировании информации, нарушения работы компьютера, информационной системы или информационно-коммуникационной сети и желает их наступления.

Единообразного определения признака заведомости в юридической литературе нет. Одни рассматривают «заведомость» в ряду с факультативными признаками субъективной стороны [55, с. 14], другие как обстоятельство, характеризующее интеллектуальный момент вины, третьи как признак волевого момента [56, с. 159]. Вместе с тем, учеными не уделяется достаточного внимания субъективному признаку «заведомости».

Признак «заведомости» характеризует осознание субъектом правонарушения социальной опасности и противоправности совершаемого им деяния в виде создания вредоносных программ для компьютера или внесения вредоносных изменений в существующие программы или программные продукты, а равно использования либо распространения таких программ или электронных носителей с такими программами. Для признания прямого умысла в действиях виновного лицо, необходимо установить, что степень осведомленности последнего вредоносности программы была исключительно велика. Лицо не обязательно должно быть достоверно уверено в наличии вредоносности компьютерной программы, достаточно того, что оно с высокой степенью вероятности это допускает.

Таким образом, интеллектуальный элемент прямого умысла при создании, внесении изменений, использовании и распространении вредоносной компьютерной программы определяется как такое состояние сознания виновного лица, когда он знал (или допускал с высокой степенью вероятности), что данная программа может привести к несанкционированному уничтожению, блокированию, модификации, копированию информации, нарушению работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной

сети. Волевой элемент прямого умысла характеризуется желанием совершить действия, образующие объективную стороны рассматриваемого формального состава правонарушения.

Ученые, считающие возможным признание косвенного умысла в рассматриваемом составе, признак сознательного допущения относят к характеристике волевого момента умысла. Нам представляется, что с учетом сложности технических процессов, протекающих в компьютерных системах, законодательно установленный признак «заведомости» осознания виновным лицом возможности наступления общественно опасных вредоносных последствий, указанных в диспозиции ч. 1 ст. 210 УК РК, является достаточным основанием расценивать поведение виновного лица как совершаемого с прямым умыслом.

Данный подход позволяет облегчить в значительной степени правильное применение рассматриваемой нормы права, т.к. не требует установления абсолютно четкого знания виновным свойств вредоносной программы и безусловного представления картины возможных общественно опасных последствий. При обращении с техникой столь высокого класса можно говорить только о высокой степени вероятности предположений, что идентично «желанию» в обычных материальных составах.

В последнее время исследователи поднимают вопрос о существовании «компьютерной» этики и «компьютерной» морали. Так, «хакеры» имеют собственную этику. Не видя жертву, они не осознают противоправность своего поведения, полагая, что нажатие кнопки на компьютере не образует преступления. Кроме того, для них характерно чувство безнаказанности. Они не устанавливают прямого контакта с жертвой, могут действовать из собственной квартиры, способ совершения преступления позволяет не оставлять материальных следов криминальной деятельности, а для установления личности правонарушителя потребуется длительный промежуток времени, применение сложных технических устройств и привлечение специалистов.

Не менее важным обстоятельством, определяющим характер субъективной стороны, является то, что использование программного продукта и различные манипуляции с ним предполагает наличие у виновного лица большого аспекта разветвленных в: от узко операциональных (простая работа с клавиатурой) до ориентации в сетевом пространстве.

Цель данного правонарушения -неправомерное уничтожение, блокирование, модификация, копирование, использование информации, хранящейся на электронном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети, нарушение работы компьютера, абонентского устройства, компьютерной программы, информационной системы или информационно-коммуникационной сети.

Субъект данного правонарушения является общим: физическим вменяемым лицом, достигшим установленного законом возраста уголовной ответственности. Ответственность за незаконное обращение с вредоносными программами наступает с шестнадцати лет. Однако субъект данного правонарушения должен обладать и определенными профессиональными навыками и знаниями. Вредоносную программу создать или ее модифицировать может только человек, обладающий навыками в обращении с компьютерной техникой и в написании программы (профессиональные программисты, лица, освоившие основы программирования).

Законодатель в части 2 ст. 210 УК РК предусматривает повышенную уголовную ответственность за те же деяния, совершенные группой лиц по предварительному сговору, лицом с использованием своего служебного положения, в отношении национальных электронных информационных ресурсов или национальной информационной системы.

В части 3 вышеуказанной статьи установлена уголовная ответственность за те же деяния, совершенные преступной группой или повлекшие тяжкие последствия.

На основании вышесказанного необходимо сделать некоторые выводы:

1. Уголовные правонарушения в сфере информатизации и связи, особенно это касается взлома удаленных компьютеров, практически являются идеальной возможностью для правонарушителей совершать свои деяния без наказания. Практическая возможность доказательства этих правонарушений сводится к цифре очень приближенной к нулю. Конечно, особо громкие дела известны всему миру, но в связи с компьютерной и законодательной безграмотностью нашего населения дела, связанные с хищением информации, взломов компьютеров и тому подобное, почти никогда не заводятся, а если такое случается, то редко и сложно доказуемые.

2. Все компьютерные правонарушения условно можно подразделить на две большие категории – правонарушения, связанные с вмешательством в работу компьютеров и правонарушения, использующие компьютеры как необходимые технические средства.

Контрольные вопросы

1. Какие общественные отношения охраняются при неправомерном доступе к информации?
2. Какие действия могут квалифицироваться как неправомерный доступ к информации?
3. Какие мотивы и цели могут быть у правонарушителей при совершении неправомерного доступа к информации?
4. Почему неправомерный доступ к информации не может быть осуществлен в форме бездействия?
5. Какие действия могут квалифицироваться как неправомерный доступ к информации?
6. Как устанавливается причинная связь между неправомерным доступом и наступившими последствиями?
7. Какие факультативные признаки могут учитываться при индивидуализации наказания?

4. Проблемы совершенствования мер противодействия компьютерным правонарушениям (преступлениям)

4.1. Взаимодействие государств в решении проблем, связанных с компьютерными преступлениями (правонарушениями)

Развитие научно-технического прогресса в XX в., обусловившее появление научно-технических достижений глобального значения, связано с новыми проблемами, затрагивающими интересы не только отдельных лиц и государств, но и международного сообщества в целом. Появление новых научно-технических объектов как результат извечного и постоянного стремления человечества к познанию окружающего мира относится, несомненно, к прогрессивным явлениям, но использование этих объектов может повлечь как позитивные, так и негативные последствия, так как неразрывно связано с рядом этических, политических и правовых проблем ответственности государств и индивидов.

С распространением производства компьютеров в 50-х гг. XX в. и появлением технологий электронных коммуникаций в 70-х гг. преодоление негативных последствий использования новых технических достижений постепенно трансформировалось из проблемы, разрешаемой в пределах отдельных государств, в проблему межгосударственного сотрудничества.

Для анализа проблем межгосударственного сотрудничества по борьбе с компьютерными преступлениями (в данном случае речь идет именно о преступлениях, так как сотрудничество на международном уровне возможно только по наиболее общественно опасным деяниям в вышеуказанной сфере) первостепенное значение имеет определение компьютерного преступления как международно-правовой категории.

В настоящее время термин «компьютерные преступления» используется в ряде международно-правовых документов.

Под международным преступлением понимается деяние, возникающее в результате нарушения государством международного обязательства, столь основополагающего для жизненно важных интересов международного сообщества, что его нарушение международным сообществом рассматривается как преступление. При использовании глобальных компьютерных систем будут действовать положения ст. 4 Международной конвенции о ликвидации всех форм расовой дискриминации [57] от 07 марта 1966 года об осуждении государствами-участниками всякой пропаганды, основанной на идеях превосходства одной расы или группы лиц определенного цвета кожи или этнического происхождения, или пытающейся оправдать или поощрять расовую дискриминацию в какой бы то ни было форме. Кроме того, пункт «с» ст. 3 Конвенции о предупреждении преступления геноцида и наказании за него от 09 декабря 1948 года содержит запрет на прямое и публичное подстрекательство к совершению геноцида, которое может быть осуществлено с использованием технологий электронных коммуникаций. Более того, компьютерные сети могут быть использованы для подготовки и координации совершения других международных преступлений, а компьютеры, управляющие военными объектами, могут непосредственно служить средством агрессии. Представляется вполне обоснованным отнесение международных преступлений, связанных с использованием компьютерной техники, к особой группе компьютерных преступлений.

С использованием компьютеров может быть совершен также и ряд преступлений международного характера - деяний, предусмотренных международными договорами и посягающих на нормальные отношения между государствами, наносящих ущерб мирному сотрудничеству в различных областях отношений, а также организациям и гражданам, наказуемых либо согласно нормам, установленным в международных договорах, либо нормам национального законодательства

в соответствии с этими договорами. В частности, противоправным является распространение по компьютерным сетям порнографических предметов, анонсирование или оглашение каким бы то ни было путем (в целях поощрения оборота или торговли порнографическими предметами), что какое-либо лицо занимается их распространением или торговлей, а также способов их получения, что следует из положений ст. 1 Международной конвенции о пресечении обращения порнографических изданий и торговли ими от 12 сентября 1923 года [58].

Следует отметить, что в настоящее время глобальный характер приобрели различные способы мошенничества с использованием компьютеров, в частности в банковских сетях, распространение программного обеспечения и баз данных без получения необходимых лицензий от лица, обладающего правами на соответствующие объекты интеллектуальной собственности, и другие правонарушения, связанные с функционированием компьютеров. Не могут не вызывать опасений за состояние международного мира и безопасности периодически появляющиеся в печати сообщения о «взломе» хакерами баз данных и программного обеспечения Пентагона.

В целях эффективной борьбы с неправомерным использованием компьютерной техники компьютерные преступления не должны пониматься в узком смысле, как они понимаются в актах ОЭСР и Совета Европы, предусматривающих достаточно ограниченный перечень преступлений, непосредственно связанных с нарушением нормального функционирования компьютеров. Для определения понятия компьютерных преступлений в первую очередь следует учитывать способ их совершения.

Таким образом, к компьютерным следует отнести все преступления, совершаемые с использованием отдельных компьютеров либо технологий электронных коммуникаций.

Не исключено, что с развитием компьютерных сетей государства будут согласовывать новые нормы, содержащие

меры по борьбе с преступлениями, связанными с использованием компьютеров и круг преступлений международного характера расширится.

Компьютерная преступность в условиях функционирования глобальных компьютерных сетей приобретает транснациональный характер, вследствие чего меры борьбы с ней должны предусматриваться не только в национальном законодательстве.

Информационная безопасность страны – это «состояние защищенности страны (жизненно важных интересов личности, общества и государства на сбалансированной основе) в информационной сфере от внутренних и внешних угроз» [59, с. 247].

Проблемы, возникающие в процессе сотрудничества государств в борьбе с компьютерными преступлениями, равно как и проблемы, связанные с сотрудничеством по пресечению и наказанию иных категорий преступлений, можно подразделить на следующие группы:

1) определение места совершения преступления;
2) выявление преступления и выдача преступников;
3) расследование преступления;
4) судебное преследование, в том числе передача судопроизводств;
5) определение места отбывания наказания за совершенное преступление.

В отношении компьютерных преступлений проблемы определения места совершения преступления, выявления преступления и его расследования являются наиболее сложными. Указанные преступления имеют высокую степень латентности, способы их совершения обусловливают значительные трудности в раскрытии, поскольку преступники, используя компьютер и коды доступа, остаются, по существу, анонимными. Более того, раскрытие таких преступлений возможно только вследствие привлечения высококвалифицированных специалистов в области компьютерной техники, обладающих

не меньшим уровнем знаний, чем хакеры. Раскрытие преступлений усложняется и тем, что преступник, как правило, может находиться в одном государстве, а результаты преступной деятельности проявляются на территориях других государств.

Что касается определения места совершения преступления, то государства могли бы установить соответствующие правила путем заключения многостороннего договора. Представляется целесообразным предусмотреть в договоре положение, согласно которому местом совершения компьютерного преступления должна признаваться территория того государства, где наступили последствия совершенного деяния. Но в случае, когда известно, с какого компьютера был произведен ввод данных и иные действия, представляющие собой преступное вмешательство в функционирование других компьютеров, в том числе и находящихся на территории иностранных государств, место нахождения такого компьютера должно признаваться местом совершения преступления. Место совершения преступления может быть определено отдельно для каждого деяния, даже если они совершались одним и тем же лицом.

Более сложной является проблема указания национальных органов, которые компетентны расследовать компьютерное преступление. В многостороннем договоре можно согласовать общее правило о расследовании компьютерных преступлений по месту их совершения с рядом исключений из общего правила. Во-первых, компьютерные преступления могут быть совершены на территории государства, которое не обладает необходимыми техническими приспособлениями, а также не имеет специалистов для их расследования. В таком случае возможна передача возбужденного уголовного дела для расследования органам другого государства после консультаций между компетентными представителями соответствующих государств. Во-вторых, если компьютерные преступления совершены одним и тем же лицом, возможна пере-

дача дела для расследования органам государства, где соответствующее лицо имеет место жительства, либо гражданином которого указанное лицо является. В-третьих, при совершении одним и тем же лицом компьютерных преступлений, последствия которых имели место в нескольких государствах, уголовные дела в отношении данного лица могут быть возбуждены в каждом из государств. Затем путем взаимных консультаций государства могут договориться о расследовании дела органами одного государства либо создании совместного органа по расследованию данного дела. В-четвертых, передача материалов уголовного дела, возбужденного по факту совершения компьютерного преступления, возможна и компетентным органам по месту жительства либо нахождения потерпевшего, если расследование дела этими органами будет соответствовать интересам потерпевшего и целям быстрого и полного установления всех обстоятельств дела.

В.П. Талимончик считает, что наиболее полно интересы государств в борьбе с компьютерными преступлениями могут быть обеспечены вследствие создания системы международного контроля за передачей информации в компьютерных сетях и расследования правонарушений, связанных с использованием глобальных компьютерных сетей и отдельных компьютеров, имеющих трансграничные последствия [60, с. 17]. При этом должны соблюдаться специальные принципы международного обмена информацией, и в первую очередь принцип свободного, широкого и сбалансированного распространения информации. Система международного контроля и расследования может быть создана только при условии использования средств, которые не будут препятствовать свободному распространению правомерной информации и создавать условия для неправомерного доступа к информации, затрагивающей права человека.

Контроль за содержанием информации, расследование наиболее сложных либо затрагивающих интересы двух и более государств преступлений, координация деятельности

национальных органов по расследованию компьютерных преступлений должны осуществляться в рамках международной организации.

Возможно, контроль за содержанием электронных данных и расследование будет входить в функции Интерпола. Но в таком случае нельзя не учитывать, что Интерпол координирует сотрудничество национальных органов уголовной полиции, борьба с международными преступлениями непосредственно в ее компетенцию не входит. Видимо, для координации сотрудничества государств в борьбе с международными компьютерными преступления и компьютерными преступлениями международного характера будет создана единая международная организация.

Создание международной организации по борьбе с компьютерными преступлениями будет способствовать эффективности межгосударственного сотрудничества в данной области. В частности, государства, не обладающие высококвалифицированными кадрами и развитыми системами коммуникаций, смогут обращаться к ней за помощью. Даже государства, которые обладают всем необходимым для расследования компьютерных преступлений, нуждаются в информационном обеспечении своей деятельности, получении данных об опыте других государств. Для расследования в рамках такой организации могут быть переданы преступления, затрагивающие интересы множества государств и требующие совместных усилий по их раскрытию.

Таким образом, можно сделать вывод, что борьба с компьютерной преступностью связана как с использованием традиционных средств, применяемых государствами (в рамках существующих международных организаций, а также на основе двусторонних договоров о правовой помощи и многосторонних договоров по вопросам борьбы с отдельными видами правонарушений и оказанию правовой помощи по уголовным делам), так и с созданием новых, более эффективных средств.

4.2. Меры противодействия компьютерным преступлениям (правонарушениям)

Правоприменительная практика свидетельствует, что одним из главных направлений в борьбе с преступностью (правонарушениями) является её предупреждение. Идея о том, что предупреждение преступности (правонарушений) должно иметь приоритет перед карательной политикой государства, была высказана еще Платоном в IV в. до н.э. Суть кардинального подхода к вопросам борьбы с преступностью (правонарушениями) закрепилась в следующей формуле: «Мудрый законодатель предупредит преступление, чтобы не быть вынужденным наказывать за него».

Предупреждение преступлений (правонарушений) в «широком» смысле слова представляет собой систему экономических, социально-культурных, воспитательных и правовых мер, осуществляемых органами государственной власти в процессе формирования правового государства и гражданского общества. Предупреждение преступности (правонарушений) выступает особым видом деятельности в области социального управления.

Предупреждение преступлений (правонарушений) в «узком» смысле – это комплекс специальных мер, предпринимаемых правоохранительными органами, по недопущению или пресечению криминальных посягательств и осуществляемый различными предусмотренными законом средствами [61, с. 692].

Криминология, разрабатывающая вопросы предупреждения преступности, выделяет несколько таких систем:

1. в зависимости от иерархии причин и условий преступности:

– общесоциальный уровень предупреждения,

– специально-криминологический уровень предупреждения;

– индивидуальный уровень предупреждения.

2. в зависимости от конкретного содержания:

– экономические меры предупреждения,
– социальные меры предупреждения,
– идеологические меры предупреждения,
– технические меры предупреждения,
– организационные меры предупреждения,
– правовые меры предупреждения.

Рядом ученых компьютерные системы рассматриваются как источник повышенной опасности, нарушающие отношения общественной безопасности, призванные удерживать указаны технические системы в безопасном, упорядоченном состоянии.

Поэтому предупредительные меры применительно к преступлениям (правонарушениями) в сфере информатизации и связи неразрывно связаны с таким более широким понятием как обеспечение информационной безопасности, которая предполагает наличие целостной системы отслеживания обстановки в различных странах и своевременного обмена информацией внутри государства.

К основным источникам угроз информационной безопасности относятся:

1. Естественные, вызванные объективными природными явлениями, не зависящими от деятельности человека;

2. Искусственные, порожденные деятельностью человека, которые обусловлены:

а) непреднамеренной деятельностью человека (неумышленные ошибки в разработке компьютерных программ, в разработке программного продукта, в процессе эксплуатации компьютера и т.п.);

б) преднамеренная деятельность человека, сопряженная с умыслом, корыстными устремлениями, имеющая уголовно-правовую мотивацию и преследующая противоправные цели.

В условиях стремительного развития информационных технологий меры противодействия компьютерным правонарушениям должны являться составной частью всего комплекса экономических, политических, правовых, организационных мероприятий по

обеспечению информационной безопасности общества и государства. Сущность противодействия компьютерным правонарушениям заключается в выработке комплексной системе мер, предопределенных особенностями компьютеров как технических сооружений и спецификой обрабатываемой и получаемой с ее помощью информации.

На этот процесс оказывают влияние такие объективные факторы как:

а) непотребляемость информационных ресурсов (они подвержены лишь моральному износу);

б) их нематериальность (они не сводимы только к электронным носителям, в которых воплощаются);

в) их высокий экономический потенциал (за счет сокращения людских, сырьевых, энергетических и т.п. ресурсов);

г) наличие мощного потенциала организационно-технических средств защиты;

д) варьирование информационной ценности и функционального значения программного продукта от детской игры до схем обслуживания военно-промышленного комплекса.

Почти все виды компьютерных правонарушений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать различные профилактические меры. В данном случае профилактические меры следует понимать как деятельность, направленную на выявление и устранение причин, порождающих правонарушения и условий, способствующих их совершению.

Каких-то особых методов для борьбы с правонарушениями в сфере информатизации и связи в Казахстане нет. Используются те же методы, что и во всем мире. В мировой практике борьбы с компьютерной преступностью (компьютерными правонарушениями) применяются в совокупности правовые, организационные и технические методы [62, с. 175].

На основе данных, полученных в ходе анализа отече-

ственной и зарубежной специальной литературы и публикаций в периодической печати по вопросам теории и практики борьбы с компьютерной преступностью (компьютерными правонарушениями), можно выделить три основные группы мер предупреждения:

1) правовые;
2) организационно-управленческие;
3) технические.

К правовым мерам предупреждения правонарушений в сфере информатизации и связи в первую очередь относятся нормы законодательства, устанавливающие уголовную ответственность за указанные выше противоправные деяния.

К правовым методам относятся разработка норм, устанавливающих ответственность за правонарушения в сфере информатизации и связи, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства, принятие международных договоров в данной сфере.

История развития законодательства зарубежных стран в этом направлении показывает, что впервые подобный шаг был предпринят законодательными собраниями американских штатов Флорида и Аризона уже в 1978 году. Принятый закон назывался «Computer crime act of 1978» и был первым в мире специальным законом, устанавливающим уголовную ответственность за компьютерные преступления. Затем практически во всех штатах США (в 45 штатах) были приняты аналогичные специальные законодательства [63].

Эти правовые акты стали фундаментом для дальнейшего развития законодательства в целях осуществления мер предупреждения компьютерных правонарушений. Отечественное законодательство движется в этом направлении следующими шагами.

Первым из них по праву законодательным шагом можно считать принятие в июле 1997 года Уголовного Кодекса Республики Казахстан и выделяющего информацию в качестве

объекта уголовно-правовой охраны.

Этим актом отечественное уголовное законодательство приводится в соответствие с общепринятыми международными правовыми нормами развитых в этом отношении зарубежных стран.

Вторым прогрессивным шагом является принятие Закона РК «О связи» в 1999 году и его переиздание в 2004 году [64].

Следующим важным шагом является принятие в 2007 году Закона РК «Об информатизации».

Данные нормативные акты дают юридическое определение основных компонентов информационной технологии как объектов правовой охраны; устанавливают и закрепляют права и обязанности собственника на эти объекты; определяют правовой режим функционирования средств информационных технологий; определяют категории доступа определенных субъектов к конкретным видам информации; устанавливают категории секретности данных и информации.

Между тем общеизвестно, что одними правовыми мерами не всегда удается достичь желаемого результата в деле предупреждения правонарушений.

Тогда следующим этапом становится применение мер организационно- управленческого характера для защиты средств компьютерной техники (далее – СКТ) от противоправных посягательств на них.

Организационно-управленческие мероприятия направлены на исключение (или по крайней мере затруднение) возникновения ситуаций, угрожающих безопасности. Они носят сугубо персональный характер и «лежат» в основании политики безопасности конкретного объекта. Данный аспект профилактики наиболее широкий и включает в себя как меры оперативного, так и факультативного характера. В 97% случаях утечки информации причины происшедшего связаны с изъянами в организационно-управленческой сфере.

К ним относятся мероприятия:

а) регламентирующие процессы функционирования

компьютерной системы;

б) осуществляемые при проектировании, строительстве и оборудовании объектов систем обработки информационных данных;

в) определяющие политику безопасности;

г) устанавливающие систему надежной охраны и действенного пропускного режима;

д) распределяющие реквизиты разграничения доступа;

е) направленные на осуществление явного и скрытого контроля за пользователями и т.п.

К организационно-управленческим мерам примыкают кадровые вопросы. Превентивная функция в этой части осуществляется опосредованно. В этих целях проводится тестирование кандидатов на работу; в заключаемых контрактах отражаются условия конфиденциальности на весь период работы и на определенный срок после расторжения трудового соглашения; периодическое проведение ротации сотрудников; создание служб компьютерной безопасности; обучение персонала правилам защиты информации с учетом последних нововведений и т.п.

При этом различается несколько групп риска:

а) группа малого риска – ранее у сотрудника не отмечались случаи совершения правонарушения в работе с компьютером;

б) пограничная группа риска – у сотрудника в прошлом имелся единичный случай совершения правонарушения при работе с компьютером;

в) группа высокого риска – имеются сведения о неоднократном совершении сотрудником правонарушений при обращении с компьютерной информацией.

Организационные меры защиты СКТ включают в себя совокупность организационных мероприятий: по подбору, проверке и инструктажу персонала; разработке плана восстановления информационных объектов после входа их из строя; организации программно-технического обслуживания СКТ;

возложению дисциплинарной ответственности на лиц по обеспечению безопасности конкретных СКТ; осуществлению режима секретности при функционировании компьютерных систем; обеспечению режима физической охраны объектов; материально-техническому обеспечению и т.д.

Организационные меры являются важным и одним из эффективных средств защиты информации, одновременно являясь фундаментом, на котором строится в дальнейшем вся система защиты.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных правонарушений в большинстве случаев стали:

1) неконтролируемый доступ сотрудников к клавиатуре компьютера, используемого как автономно, так и в качестве автоматизированной сети для передачи данных первичных бухгалтерских документов в процессе осуществления финансовых операций;

2) бесконтрольность за действиями обслуживающего персонала, что позволяет правонарушителю свободно использовать компьютер в качестве орудия совершения правонарушения;

3) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

4) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

5) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации;

6) отсутствие категоричности допуска сотрудников к документации строгой финансовой отчетности;

7) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Для эффективной безопасности от компьютерных правонарушений всего лишь необходимо:

1) просмотреть всю документацию в учреждении, организации;

2) ознакомиться с функциями и степенью ответственности каждого сотрудника;

3) определить возможные каналы утечки информации;

4) ликвидировать обнаруженные слабые звенья в защите.

Зарубежный опыт показывает, что наиболее эффективной мерой в этом направлении является введение в штатное расписание организации должности специалиста по компьютерной безопасности (администратора по защите информации) либо создание специальных служб как частных, так и централизованных, исходя из конкретной ситуации. Наличие такого отдела (службы) в организации снижает вероятность совершения компьютерных правонарушений вдвое.

Кроме этого, в обязательном порядке должны быть реализованы следующие организационные мероприятия:

1) для всех лиц, имеющих право доступа к СКТ, должны быть определены категории допуска;

2) определена административная ответственность для лиц за сохранность и санкционированность доступа к имеющимся информационным ресурсам;

3) налажен периодический системный контроль за качеством защиты информации посредством проведения регламентных работ как самим лицом, ответственным за безопасность, так и с привлечением специалистов;

4) проведена классификация информации в соответствии с ее важностью;

5) организована физическая защита СКТ (физическая охрана).

Помимо организационно-управленческих мер, существенную общепрофилактическую роль в борьбе с компьютерными правонарушениями могут играть также меры технического характера.

Технические меры предназначены для защиты от нежелательного физического воздействия на аппаратные средства и средства связи компьютерной техники, а также для закрытия возможных каналов утечки конфиденциальной информации за счет применения лазерных, радиотехнических и других способов перехвата, а также средства визуального наблюдения, средства связи и охранной сигнализации.

Данный аспект профилактики (посредством технических или программно-аппаратурных мер) опирается на положения физической и интеллектуальной компьютерной безопасности.

Группа технических мер предназначена для закрытия возможных каналов утечки: а) конфиденциальной информации; б) данных, образующихся за счет побочных электромагнитных излучений; в) вибрационных и акустических сигналов, образующихся на перегородках строительных конструкций, окон; г) данных с помощью применения лазерных, радиотехнических и других способов перехвата.

Реализация этих методов осуществляется путем применения различных технических разработок, устройств и специального оборудования. Для защиты информации используется программное обеспечение антивирусного контроля; применяются различные методы шифрования данных; применение новейших технических мер, обеспечивающих реализацию организационно- управленческого уровня профилактики компьютерных правонарушений.

Различают следующие виды технических мер безопасности:

а) пассивные меры, которые предназначены для погашения или снижения уровня излучения от работающего компь-

ютера (экранирование помещений, использование экранирующих средств, к примеру: металлических штор, специальных аэрозолей);

б) активные меры, которые включают применение специальных генераторов помех, охранной сигнализации, средств защиты портов компьютерной техники, устройств, обеспечивающих только санкционированный доступ идентифицированных пользователей к конфиденциальной информации, к компьютерным системам или сетям и др.

Наиболее важной и значимой в системе технических мер является защита программного обеспечения. В настоящее время к наиболее распространенным способам защиты относятся; дублирование файлов, применение паролей, кодирование, применение защитной оболочки вокруг файла, применение антивирусных программ. Последние являются в настоящее время одним из действенных способов борьбы с компьютерными вирусами, которые способны самопроизвольно присоединяться к другим программам, «заражая» их и вызывая различные нежелательные последствия в виде порчи файлов, искажение результатов вычислений, «засорение» ала стирание памяти и т.п. Современные антивирусные программы способны распознавать и уничтожать как известные, так и неизвестные вирусы и их модификации.

Как разновидность технических средств защиты выделяются физические меры, основанные на применении различных устройств и сооружений, препятствующих проникновению к защищаемой информации, компьютерным системам и сетям, а также технические средства связи, охранной и пожарной сигнализации. К таким мерам можно отнести найтование компьютеров, т.е. прикрепление компьютеров к столам, консолям при помощи специальных зажимов, освобождение от которых возможно с помощью специальных инструментов; использование «стальных рубашек», которые надеваются по окончании работы на компьютер; технические средства визуального наблюдения за компьютерными залами; применение

аккумуляторных батарей, обеспечивающих бесперебойное электропитание в экстренных случаях и при авариях и т.п.

Условно технические меры можно подразделить на три основные группы в зависимости от характера и специфики охраняемого объекта, а именно: аппаратные, программные и комплексные.

Аппаратные методы предназначены для защиты аппаратных средств и средств связи компьютерной техники от нежелательных физических воздействий на них сторонних сил, а также для закрытия возможных нежелательных каналов утечки конфиденциальной информации и данных, образующихся за счет побочных электромагнитных излучений и наводок, виброакустических сигналов, и т.п.

Практическая реализация данных методов обычно осуществляется с помощью применения различных технических устройств специального назначения. К ним, в частности, относятся:

1) источники бесперебойного питания, предохраняющие от скачкообразных перепадов напряжения;

2) устройства экранирования аппаратуры, линий проводной связи и помещений, в которых находятся СКТ;

3) устройства комплексной защиты телефонии;

4) устройства, обеспечивающие только санкционированный физический доступ пользователя на охраняемые объекты СКТ (шифрозамки, устройства идентификации личности и т.п.);

5) устройства идентификации и фиксации терминалов и пользователей при попытках несанкционированного доступа к компьютерной сети;

6) средства охранно-пожарной сигнализации;

7) средства защиты портов компьютерной техники (наиболее эффективны для защиты компьютерных сетей от несанкционированного доступа) и т.д.

Программные методы защиты предназначаются для

непосредственной защиты информации по трем направлениям: а) аппаратуры; б) программного обеспечения; в) данных и управляющих команд.

Для защиты информации при ее передаче обычно используют различные методы шифрования данных перед их вводом в канал связи или на физический носитель с последующей расшифровкой. Как показывает практика, методы шифрования позволяют достаточно надежно скрыть смысл сообщения.

Все программы защиты, осуществляющие управление доступом к электронной информации, функционируют по принципу ответа на вопросы: кто может выполнять, какие операции и над какими данными.

Доступ может быть определен как:

– общий (безусловно предоставляемый каждому пользователю);

– отказ (безусловный отказ, например разрешение на удаление порции информации);

– зависимый от события (управляемый событием);

– зависимый от содержания данных;

– зависимый от состояния (динамического состояния компьютерной системы);

– частотно-зависимый (например, доступ разрешен пользователю только один или определенное число раз);

– по имени или другим признаком пользователя;

– зависимый от полномочий;

– по разрешению (например, по паролю);

– по процедуре.

Также к эффективным мерам противодействия попыткам несанкционированного доступа относятся средства регистрации. Для этих целей наиболее перспективными являются новые операционные системы специального назначения, широко применяемые в зарубежных странах и получившие название мониторинга (автоматического наблюдения за возможной компьютерной угрозой).

Мониторинг осуществляется самой операционной системой (далее – ОС), причем в ее обязанности входит контроль за процессами ввода-вывода, обработки и уничтожения электронной информации. ОС фиксирует время несанкционированного доступа и программных средств, к которым был осуществлен доступ. Кроме этого, она производит немедленное оповещение службы компьютерной безопасности о посягательстве на безопасность компьютерной системы с одновременной выдачей на печать необходимых данных (листинга).

В последнее время в США и ряде европейских стран для защиты компьютерных систем действуют также специальные подпрограммы, вызывающие самоуничтожение основной программы при попытке несанкционированного просмотра содержимого файла с секретной информацией по аналогии действия «логической бомбы».

При рассмотрении вопросов, касающихся программной защиты информационных ресурсов особо надо подчеркнуть проблему защиты их от компьютерных вирусов.

Здесь необходимо активно использовать специальные программные антивирусные средства защиты (как зарубежного, так и отечественного производства). Антивирусные программы своевременно обнаруживают, распознают вирус в информационных ресурсах, а также «лечат» их.

Однако, наряду с использованием антивирусных программ, для уменьшения опасности вирусных посягательств на СКТ необходимо предпринять комплексные организационно-технические меры.

1. Информировать всех сотрудников учреждения, организации, использующих СКТ, об опасности и возможном ущербе в случае совершения вирусного посягательства.

2. Запретить сотрудникам приносить на рабочее место программные средства (далее – ПС) «со стороны» для работы с ними на СКТ учреждения, организации по месту работы сотрудника.

3. Запретить сотрудникам использовать, хранить на

носителях и в памяти компьютера компьютерные игры.

4. Предостеречь сотрудников организации от использования ПС и носителей электронной информации, имеющих происхождение из учебных заведений различного уровня и профиля.

5. Все файлы, которые поступают из внешней компьютерной сети должны обязательно тестироваться.

6. Создать архив копий ПС, используемых в непосредственной работе организации.

7. Регулярно просматривать хранимые в компьютерной системе ПС, создавать новые их архивные копии; где это возможно, использовать защиту типа «только чтение» для предупреждения несанкционированных манипуляций с ценными данными.

8. Периодически проводить ревизионную проверку контрольных сумм файлов, путем их сличения с эталоном.

9. Использовать для нужд электронной почты отдельный стендовый компьютер или ввести специальный отчет.

10. Установить системы защиты информации на особо важных компьютерах. За активировать на них специальные комплексные антивирусные ПС.

11. Постоянно контролировать исполнение установленных правил обеспечения безопасности СКТ и применять меры дисциплинарного воздействия к лицам, сознательно или неоднократно нарушавшим их и т.д.

В настоящее время идеальной всеохватывающей системы противодействия компьютерным правонарушениям не существует. Абсолютно надежные технические и физические средства защиты даже в сочетании со стойким персоналом сотрудников не могут обеспечить идеально надежную систему защиты. Только комплексный подход к рассматриваемой проблеме и сочетание различных мер противодействия позволять добиться такой степени защиты компьютерных систем и сетей от криминальных посягательств, которая позволить избежать

общественно опасных последствий утечки защищаемой информации.

Комплексные меры защиты, с одной стороны, должны сочетать организационно-управленческие, физические и технические меры, а с другой – кадровые, правовые и морально-этические.

Таким образом, предупреждение преступности (правонарушений) в сфере обращения компьютерной информации рассматривается как средство регулирования информационных отношений; как взаимодействие мер социально-экономического, организационно-правового и воспитательного порядка; как сочетание различных уровней предупреждения компьютерной преступности (правонарушений), воплощенных в деятельности неоднородных субъектов, осуществляющих эту функцию.

Прогрессирование уголовных правонарушений в сфере информатизации и связи в Казахстане пока не имеет больших статистических показателей. На современном этапе развития общества проблема правонарушений в сфере информатизации и связи не грозит обрести те масштабы, которые она имеет в развитых странах. В государстве происходит процесс осваивания рынка локальных и межрегиональных информационных сетей, вхождения в международные сети; решение вопросов компьютерной оснащенности финансовых, управленческих и иных структур на периферии; невелик кадровый потенциал специалистов по созданию современных информационных технологий.

Указанные факторы носят временный характер и в процессе интегрирования Казахстана в мировое информационное пространство будут изжиты. Увеличивающиеся темпы заполнения отечественного рынка средствами информационных технологий, внедрение в повседневную жизнь компьютерной техники, выявление отдельных фактов совершения компьютерных правонарушений свидетельствует о том, что в ближай-

шем будущем эта проблема может проявиться. Поэтому вопросы разработки и совершенствования эффективности мер предупреждения уголовных правонарушений в сфере информатизации и связи являются современными, призваны содействовать нейтрализации или минимизации криминогенных последствий от криминальной деятельности и упреждению процессов формирования компьютерных правонарушений.

Контрольные вопросы

1. Почему проблема борьбы с компьютерными преступлениями требует международного сотрудничества?
2. Какие международные документы упоминают компьютерные преступления?
3. Какие примеры преступлений международного характера могут быть совершены с использованием компьютеров?
4. Почему предупреждение преступлений должно иметь приоритет перед карательной политикой государства?
5. Какие уровни предупреждения преступности выделяет криминология?
6. Какие меры предупреждения преступлений существуют в зависимости от их содержания?
7. Какие источники угроз информационной безопасности существуют?
8. Какие меры противодействия компьютерным правонарушениям вы можете назвать?

5. Практические задания и кейсы по противодействию преступности в сфере информатизации и связи

5.1. Практические задания

Целью практических заданий является оценка уровня осведомленности и выявить области, требующие дополнительного обучения.

Вот несколько примеров практических заданий:

1. Анализ фишинговых писем:

Задание: Соберите примеры фишинговых писем и проанализируйте их. Определите, какие элементы указывают на мошенничество.

Цель: Научить обучающихся распознавать фишинговые атаки и понимать, как они работают.

2. Создание безопасных паролей:

Задание: Попросите обучающихся создать несколько паролей и оцените их безопасность с помощью специальных инструментов.

Цель: Показать важность создания сложных и уникальных паролей для защиты аккаунтов.

3. Расследование киберпреступлений:

Задание: Смоделируйте кибератаку и попросите обучающихся провести расследование, используя методы цифровой криминалистики.

Цель: Ознакомить обучающихся с процессом расследования киберпреступлений и инструментами, которые используются в этой области.

4. Разработка плана защиты от DDoS-атак:

Задание: Попросите обучающихся разработать план защиты для компании от DDoS-атак.

Цель: Научить обучающихся разрабатывать стратегии защиты и понимать, как работают DDoS-атаки.

5. Создание фальшивого интернет-магазина:

Задание: Создайте фальшивый интернет-магазин и попросите обучающихся выявить признаки мошенничества.

Цель: Показать, как можно распознать поддельные сайты и защитить себя от интернет-мошенничества.

6. Опрос и анализ осведомленности о киберпреступности:

Задание: Проведите опрос среди обучающихся или сотрудников компании о их знаниях и опыте в области киберпреступности.

7. Анализ инцидента с фишингом:

Ситуация: Несколько сотрудников компании получили фишинговые письма, что привело к утечке конфиденциальной информации.

Задание: Проведите анализ фишинговых писем, определите, как злоумышленники получили доступ к данным, и предложите меры по предотвращению подобных атак в будущем.

8. Расследование DDoS-атаки:

Ситуация: Веб-сайт компании подвергся DDoS-атаке, что привело к его недоступности на несколько часов.

Задание: Определите источник атаки, проанализируйте ее последствия и предложите меры по защите от подобных атак в будущем.

9. Анализ вредоносного ПО:

Ситуация: Вредоносное ПО было обнаружено на нескольких компьютерах компании, что привело к утечке данных.

Задание: Проведите анализ вредоносного ПО, определите его источник и предложите план по восстановлению системы и предотвращению повторных атак.

10. Инцидент с утечкой данных:

Ситуация: В результате утечки данных были скомпрометированы личные данные клиентов компании.

Задание: Проведите расследование, чтобы выяснить, как произошла утечка, и предложите меры по защите данных и уведомлению пострадавших клиентов.

11. Расследование инцидента с неправомерным доступом:

Ситуация: Внутренняя сеть компании была взломана, и злоумышленники получили доступ к конфиденциальной информации.

Задание: Определите, как произошел взлом, какие данные были скомпрометированы, и предложите меры по усилению защиты сети.

12. Анализ инцидента с использованием социальной инженерии:

Ситуация: Злоумышленники использовали методы социальной инженерии, чтобы получить доступ к конфиденциальной информации компании.

Задание: Определите, какие методы социальной инженерии были использованы, и предложите меры по обучению сотрудников для предотвращения подобных инцидентов.

13. Расследование инцидента с криптовымогательством (ransomware):

Ситуация: Система компании была заражена программой-вымогателем, и данные были зашифрованы.

Задание: Проведите анализ программы-вымогателя, определите, как она проникла в систему, и предложите план по восстановлению данных и предотвращению подобных атак в будущем.

14. Анализ инцидента с компрометацией электронной почты (BEC):

Ситуация: Злоумышленники получили доступ к корпоративной электронной почте и отправили фальшивые письма от имени руководства компании.

Задание: Определите, как произошла компрометация, и предложите меры по усилению безопасности электронной почты и предотвращению подобных инцидентов.

15. Инцидент с утечкой данных через облачные сервисы:

Ситуация: Конфиденциальные данные компании были скомпрометированы через уязвимость в облачном сервисе.

Задание: Проведите расследование, чтобы выяснить, как произошла утечка, и предложите меры по защите данных в облачных сервисах.

16. Расследование инцидента с использованием IoT-устройств:

Ситуация: Злоумышленники использовали уязвимости в IoT-устройствах для проникновения в сеть компании.

Задание: Определите, какие уязвимости были использованы, и предложите меры по защите IoT-устройств и сети компании.

5.2 Кейсы

Давайте подробно рассмотрим кейс о фишинговой атаке на крупную компанию, анализ данного кейса позволяет понять, как фишинговые атаки могут нанести значительный ущерб компании и какие меры необходимо предпринять для защиты от подобных угроз в будущем. Важно не только внедрять технические решения, но и повышать осведомленность сотрудников о возможных угрозах.

Кейс: Фишинговая атака на крупную компанию

Описание ситуации – в 2020 году крупная компания стала жертвой фишинговой атаки. Злоумышленники отправили поддельные электронные письма сотрудникам компании, выдавая себя за руководство. В результате атаки были украдены данные сотрудников и клиентов, что привело к значительным финансовым потерям и репутационному ущербу.

Пункты для анализа

1. Предыстория

Описание компании: размер, сфера деятельности, количество сотрудников.

Текущие меры безопасности до атаки: используемые системы защиты, политика безопасности.

2. Описание атаки

Тип фишинговой атаки: целевая (спирфишинг) или массовая.

Методы, использованные злоумышленниками: поддельные электронные письма, фальшивые веб-сайты.

Примеры фишинговых писем: анализ содержания, выявление признаков мошенничества.

3. Уязвимости

Какие уязвимости были использованы злоумышленниками: недостаточная осведомленность сотрудников, слабые пароли, отсутствие многофакторной аутентификации.

Анализ причин, по которым атака была успешной: недостаточная подготовка сотрудников, отсутствие регулярных тренировок по безопасности.

4. Последствия атаки

Финансовые потери: прямые и косвенные затраты.

Репутационный ущерб: влияние на доверие клиентов и партнеров.

Влияние на операционную деятельность: временная недоступность систем, утечка данных.

5. Меры по устранению последствий

Действия, предпринятые компанией после атаки: уведомление пострадавших, восстановление систем, сотрудничество с правоохранительными органами.

Внедрение дополнительных мер безопасности: усиление политики безопасности, обучение сотрудников, внедрение многофакторной аутентификации.

6. Рекомендации по предотвращению подобных атак в будущем

Обучение сотрудников: регулярные тренировки и повышение осведомленности о фишинговых атаках.

Технические меры: использование антифишинговых фильтров, многофакторная аутентификация, регулярные обновления программного обеспечения.

Политика безопасности: разработка и внедрение строгих правил и процедур по защите данных.

Примеры кейсов по киберпреступности, задача: изучить методы социальной инженерии, использованные в данном случае, и предложить меры по повышению осведомленности сотрудников о подобных угрозах.

1. Кейс: Атака с использованием программ-вымогателей (Ransomware)

Описание: В 2022 году больница подверглась атаке с использованием программ-вымогателей, что привело к блокировке доступа к медицинским данным.

Задача: Исследовать, как была проведена атака, какие уязвимости были использованы и какие меры можно принять для защиты от подобных угроз.

2. Кейс: Взлом интернет-магазина

Описание: В 2024 году интернет-магазин был взломан, и данные о кредитных картах клиентов были украдены.

Задача: Рассмотреть методы, использованные хакерами для взлома, и предложить стратегии для улучшения безопасности интернет-магазинов.

3. Кейс: DDoS-атака на финансовую организацию

Описание: В 2023 году финансовая организация подверглась DDoS-атаке, что привело к временной недоступности онлайн-сервисов.

Задача: Проанализировать, как была организована атака, какие меры были предприняты для её отражения и как можно улучшить защиту от DDoS-атак.

4. Кейс: Фишинговая атака на крупную компанию

Описание: В 2024 году крупная компания стала жертвой фишинговой атаки, в результате которой были украдены данные сотрудников и клиентов.

Задача: Проанализировать, как произошла атака, какие меры безопасности были нарушены и какие шаги можно предпринять для предотвращения подобных инцидентов в будущем.

Заключение

Проведенное исследование казахстанского уголовного законодательства, регулирующего ответственность за правонарушения в сфере информатизации и связи, а также анализ отдельных видов компьютерных преступлений и методов защиты компьютерной информации от криминальных посягательств, позволяет сделать следующие выводы:

1) В нашей стране накоплена значительная научно-теоретическая база, свидетельствующая о формировании устойчивого правового механизма для защиты компьютерной информации. Логическим развитием правовой системы, обеспечивающей безопасность компьютерной информации, стало введение в новом Уголовном кодексе Республики Казахстан 2014 года специальной главы 7 «Уголовные правонарушения в сфере информатизации и связи», включающей 9 статей.

2) Компьютерная преступность не знает границ, она выходит за пределы казахстанской действительности. Это международное понятие и бороться с ней надо согласованно и сообща. С внедрением в человеческую жизнь новых компьютерных технологий, когда обмен информацией стал быстрым, дешевым и эффективным, преступность в информационной сфере переросла за рамки уголовно-правовых норм, направленных для борьбы с ней. Компьютерные правонарушения условно можно подразделить на две большие категории - правонарушения, связанные с вмешательством в работу компьютеров и правонарушения, использующие компьютеры как необходимые технические средства.

3) Проблемы информационной безопасности постоянно усугубляется процессами незаконного несанкционированного проникновения практически во все сферы деятельности общества технических средств обработки и передачи данных и прежде всего информационных систем. Неслучайно, поэтому защита компьютерной информации становится одной из самых острых проблем в современной информатике. На сегодняшний день сформулировано четыре базовых прин-

ципа информационной безопасности, которая должна обеспечивать:

– целостность данных – защиту от несанкционированных сбоев, ведущих к потере информации, а также неавторизованного, несанкционированного, противоправного создания или уничтожения данных;

– конфиденциальность (законность) информации;

– доступность для всех авторизованных зарегистрированных пользователей;

– защита компьютерной информации от противоправного посягательства (копирование, хищение, распространение, подделка).

Анализ действующего казахстанского уголовного законодательства, устанавливающего ответственность за правонарушения в сфере информатизации и связи позволяет говорить о необходимости решения нескольких правовых проблем, которые могут быть рассмотрены в качестве составных частей правового механизма защиты компьютерной информации:

1) Установление контроля над несанкционируемым, противоправным доступом к компьютерным информационным данным системы.

2) Ответственность за выполнение технологических операций, связанных с противоправной деятельностью в отношении компьютерной информации.

Среди наиболее эффективным мер, направленных на предупреждение правонарушений в сфере компьютерной информации выделяются правовые, организационные и технические.

К правовым мерам относятся разработка норм, устанавливающих уголовную ответственность за компьютерные преступления, защита авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства. Также сюда входят вопросы государственного контроля за разработчиками программного обеспечения и принятие международных договоров, ограничивающих их деятельность, если она влияет или может повлиять на военные, экономические и социальные аспекты

стран.

К организационным мерам относятся охрана информационного центра, тщательный подбор персонала, исключение случаев выполнения особо важных работ одним человеком, наличие плана восстановления работоспособности центра после сбоев, организация обслуживания центра сторонними организациями или лицами, незаинтересованными в сокрытии нарушений, универсальность средств защиты для всех пользователей (включая руководство), возложение ответственности за безопасность центра на определенных лиц, выбор места расположения центра и т.д.

К техническим мерам относятся защита от несанкционированного доступа к системе, резервирование важных компьютерных подсистем, организация сетей с возможностью перераспределения ресурсов при сбоях, установка оборудования для обнаружения и тушения пожара, обнаружения воды, принятие мер защиты от хищений, саботажа, диверсий, взрывов, установка резервных систем электропитания, оснащение помещений замками, установка сигнализации и многое другое.

Подводя некоторые итоги, можно сделать выводы о том, что сложность компьютерной техники, латентность компьютерных правонарушений, а также трудность сбора доказательственной информации не приведет в ближайшее время к появлению большого числа уголовных дел, возбужденных по статьям 205-213 главы 7 «Уголовные правонарушения в сфере информатизации и связи» УК Республики Казахстан.

К сожалению, даже обладая достаточно полным набором значащих элементов портрета компьютерного правонарушителя, мы лишь на 30-49% приближаемся к конкретному правонарушителю. Самое печальное, что дальнейшее продвижение по процентной шкале практически исключено – любое высокотехнично исполненное правонарушение не раскрываемо, если правонарушитель не допустил серьезных ошибок или его не сдали подельщики. В целом, значительное обновление уголовного законодательства современного Казахстана в сфере борьбы с киберпреступностью поможет более эффек-

тивно противодействовать современным угрозам безопасности личности, общества и государства за счет введения новых норм, направленных на борьбу с данными преступлениями. Конечно одними только уголовно-правовыми мерами невозможно полностью предотвратить эти деяния. Это в принципе относится к противодействию преступности. Определенный задел в виде нормативной основы (разработка уголовно-правового инструментария) создан, однако не стоит абсолютизировать или преувеличивать их значение.

В этой связи следует согласиться с мнением Н.А. Биекенова, о том, что Казахстан становится частью более широкого киберпространства и поэтому представляется необходимым разработать и принять свою государственную программу (концепцию, стратегию) киберзащиты информационного пространства, предусматривающей:

– создание системы постоянного мониторинга киберугроз;

– развитие национальных систем оперативного обнаружения кибератак и противодействия им;

– совершенствование системы взаимодействия государственных силовых структур, отвечающих за кибербезопасность и общественных организаций, работающих в области информационной безопасности;

– организацию программы научно-технических работ по проблемам кибербезопасности [5, с.29].

Думается в свете системного подхода первый шаг сделан: компьютерные правонарушения получили свое признание в качестве самостоятельной группы криминальных деяний.

Следующий шаг – формирование необходимой концептуальной и институциональной базы, наработка правоприменительного опыта. И этому должно быть уделено самое серьезное внимание, иначе шансы на реальные успехи в противодействии с компьютерными правонарушениями будут не высоки, в то время как социальные риски и колоссальные экономические потери от них станут возрастать в геометрической прогрессии.

Список использованных источников

1. Информационные технологии (IT) – что это такое (ktonanovenkogo.ru) //ktonanovenkogo.ru/voprosy-i-otvety/informacionnye-tekhnologii-chto-ehto-takoe. html

2. Что такое интернет вещей? Определение и описание//www.kaspersky.ru/resource-center/definitions/what-is-iot

3. Что такое облачные вычисления? //aws.amazon.com/ru/what-is-cloud-computing/

4. Казахстан в новой глобальной реальности: рост, реформы, развитие: Послание Президента Республики Казахстан от 30 ноября 2015 года // Каз. правда. – 1 декабря 2015г. – №230 (28106).

5. Уголовный кодекс Республики Казахстан от 3 июля 2014 года №226-V // http://adilet.zan.kz/rus/docs/ K1400000226

6. Исмагулова А.Т. Уголовные правонарушения в сфере информатизации и связи: законодательные новеллы Казахстана / Уголовно-правовая охрана информационного пространства в условиях глобализации: коллективная монография по материалам XII Международной научно-практической конференции, посвященной памяти М.И. Ковалева (Екатеринбург, 20-21 февраля 2015г.)/ Под ред. И.Я. Козаченко. Екатеринбург: Издательский дом Уральского государственного юридического университета, 2016. – С. 148.

7. Химченко А.И. Информационное общество: правовые проблемы в условиях глобализации: автореф. дис. … канд. юрид. наук. – М., 2014. – С. 24.

8. Компьютерные преступления и обеспечение безопасности ЭВМ. Проблемы преступности в капиталистических странах. – М.: Винити, 1983. – №6. – С. 3

9. Сеитов Т.Е. Правовые аспекты компьютерной преступности в зарубежных странах и в Казахстане. Учебное пособие. – Алматы: Данекер, 2004. – С. 328.

10. Толеубекова Б.Х. Компьютерная преступность. Монография. – Караганда, 2005. – С. 295.

11. Кочои С., Савельев Д. Ответственность за неправомерный доступ к компьютерной информации // Российская юстиция. – 1999. – №1. – С. 11.

12. Назмышев Р.А. Криминально-правовая сущность преступлений в сфере компьютерной информации как критерий оценки понятия «компьютерные преступления» // Фемида. – 2003. – №4. – С. 74.

13. Курушин В.Д., Шопин А.В. Предупреждение и раскрытие преступлений, совершаемых с использованием компьютерной техники. – М., 2004. – С. 249.

14. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юрид. лит., 2004. – С. 372.

15. Толеубекова Б.Х. Проблемы совершенствования борьбы с преступлениями, совершаемыми с использованием компьютерной техники / Автореферат дисс. докт. юрид. наук. – Астана, 1998. – С. 190.

16. Воздействие организованной преступности на общество в целом // Материалы Комиссии ООН по предупреждению преступности и уголовному правосудию. Вена. 13 – 23 апреля 1993. – http://www. consultant.ru.

17. Оспанов Е.Т. Орудие преступления – компьютер // Бюллетень ГСУ и ЭКУ МВД РК. – Алматы: МВД РК, 2005. – №1-2(1-5). – С. 35-41.

18. Карпинский О. Защита информации, виртуальные частные сети (VPN). Технология ViPNet / По материалам компании Infotecs. – http://www.Gazeta.Ru.

19. Уголовное право. Особенная часть: Учебник для ВУЗов / Под ред. Н.И. Ветрова, Ю.И. Ляпунова. – М.: Новый юрист, 2008. – С. 768.

20. Лунеев В.В. Преступность 21 века. Мировой криминологический анализ. – М.: Норма, 2007. – С. 470.

21. Сальников В.П. Компьютерная преступность: уголовно-правовые и криминологические проблемы. Материалы

Международной научно- практической конференции // Государство и право. – 2005. – №9. – С. 101.

22. Тихомиров В.П. Зачем рынку информационные технологии? // Новин-тех. – 2001. – №1. – С. 17.

23. Гражданский кодекс Республики Казахстан (Общая часть) №269-XII от 27 декабря 1994 года. // Сайт законодательства РК. – http://www.zakon.kz.

24. Всеобщая декларация прав человека (принята на 3-ей сессии Генеральной Ассамблеи ООН) от 10 декабря 1948 года // Российская газета. – 1995. – 5 апреля. – http://www.iacis.ru.

25. Закон Республики Казахстан от 24 ноября 2015 года №418-V ЗРК «Об информатизации» //http://adilet.zan.kz/rus/docs/Z1500000418

26. Конвенция о преступности в сфере компьютерной информации. – http://www.oprave.ru.

27. Крылов В.В. Информация как элемент криминальной деятельности // Вестник Моск. ун-та. Сер. 11. Право. – М., 2008. – №4. – С. 50-64.

28. Кутузов В., Гуцалюк М., Цимбалюк В. Преступления в сфере высоких технологий. – Минск, 2002. – С. 268.

29. Аманов Ж.К. О некоторых вопросах уголовной ответственности за неправомерный доступ к компьютерной информации // Свобода слова и информационная безопасность государства, общества, личности: Сб. матер. межд. конф. 01-02 марта 2001 г. – Алматы: Интернет трейнинг центр, 2006. – С. 14.

30. Скородумов Е.И. Безопасность информационных технологий – человеческий фактор // Экономика и производство, 2006. – №3. – С. 32.

31. Медведовский И.Д. Атака через Internet / Под науч. ред. проф. Зегжды П.Д. - СПб.: Мир и Семья – 95, 2007. – С. 214.

32. Айков Д., Сейгер К.. Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями. Перевод с английского. – М.: Мир, 2004. – С. 167.

33. Катаев С.Л. Социальные аспекты компьютерной

преступности // Центр исследования проблем компьютерной преступности. – Киев, 2008. – С. 43.

34. Ладный В. Проблема распространения в сети информации порнографического характера // Комсомольская правда. – 2004. – 26 января. – №14 (22479).

35. Анин Б. Защита компьютерной информации. – СПб.: BHV, 2006. – С. 187.

36. Черкасов В. Информация защищена – нет проблем ? // Мир безопасности. – 2007. – №11. – С. 4.

37. Фролов Д.Б., Старостина Е.В. Новая система страха - кибертерроризм // Безопасность информационных технологий. – 2004. – №2. – С. 38.

38. Голубев В.А. Проблемы борьбы с кибертерроризмом в современных условиях. – http://www.crime-research.ru.

39. Мониторинг состояния сети Интернет и нарушений прав ее пользователей в Казахстане в августе 2008 года. – http://www.info@adilsoz.kz.

40. Бельгибаев С. Интеллектуальный взлом. – http://www.iim.kz.

41. Дагель П.С., Котов Д.П. Субъективная сторона преступления и ее установление. – Воронеж, 2004. – С. 215.

42. Мазуров В.А. Компьютерные преступления: классификация и способы противодействия. – М.: Палеотип; Логос, 2009. – С. 148.

43. Хакеры угрожают Казахстану. – http://www.crime-research.org.kz.

44. Модельный уголовный кодекс для стран-участников СНГ от 17 февраля 1996 года. – http://www.iacis.ru.

45. Хакеры: компьютерная преступность. Можно ли ей противостоять? // Мир безопасности. – №11. – 2007. – С. 12.

46. Расследование компьютерных преступлений // Проблемы преступности в капиталистических странах. – 2002. – №6. – С. 8.

47. Борьба с компьютерной преступностью за рубежом. – М.: Академия МВД РФ, 2005. – С. 129.

48. Крылов В.Б. Информационные компьютерные преступления. – М.: ИНФРА-М-НОРМА, 2007. – С. 274.

49. Волеводз А.Г. Противодействие компьютерным преступлениям: Правовые основы международного сотрудничества. – М.: Юрлитформ, 2002. – С. 496.

50. Панфилова Е.И., Попов А.Н. Компьютерные преступления: Серия «Современные стандарты в уголовном праве и уголовном процессе» // Науч. редактор проф. Волженкин Б.В. – СПб., 2008. – С. 193.

51. Постановление Правительства Республики Казахстан от 29 июля 1998 года №715 «О Концепции единого информационного пространства Республики Казахстан и мерах http://adilet.zan.kz/rus/docs/P980000715_#z0

52. Карпец И.И. Международная преступность. – М., 1998. – С. 197.

53. Проблемы борьбы с компьютерной преступностью // Борьба с преступностью за рубежом (по материалам зарубежной печати): Ежем. информ. бюл. ВИНИТИ. – М., 2006. – № 4. – С. 3-5.

54. Гульбин Ю. Преступления в сфере компьютерной информации // Российская юстиция. – 2007. – №10. – С. 25.

55. Ляпунов Ю., Максимов В. Ответственность за компьютерные преступления // Законность. – 2006. – №1. – С. 14.

56. Исаев А.А. Применение специальных познаний для квалификации преступлений. – Алматы: Мектеп, 2007. – С. 159.

57. Международная конвенция о ликвидации всех форм расовой дискриминации (Принята 21 декабря 1965 г. Резолюцией 2106 (XX) Генеральной Ассамблеи ООН) // Ведомости ВС СССР. – 1969. – №25. – Ст. 219. – http://www.medialaw.ru.

58. Международная конвенция о пресечении обращения порнографических изданий и торговли ими (заключена в г. Женеве 12 сентября 1923 г.) // Сборник действующих дого-

воров, соглашений и конвенций, заключенных СССР с иностранными государствами. Вып. IX. – М., 1938. http://www.medialaw.ru.

59. Вехов В.Б. Компьютерные преступления: способы совершения, методики расследования. – М: Право и закон, 2006. – С. 247.

60. Талимончик В.П. Компьютерные преступления и новые проблемы сотрудничества государств // Законодательство и экономика. – 2005. – № 5. – С. 17.

61. Комментарий к Уголовному кодексу Республики Казахстан / Под ред. Борчашвили И.Ш.– А., 2007. – С. 692.

62. Лопатина Т.М. Проблемы компьютерной преступности. Учебное пособие. Петропавловск: Северо-Казахстанская юридическая академия, 2003. – С. 175.

63. Международный обзор уголовной политики ООН. Нью-Йорк. – 2004. – http://www.iacis.ru.

64. Закон Республики Казахстан «О связи» №567 от 05 июля 2004 года. – // Сайт законодательства РК. – http://www.zakon.kz.

СОДЕРЖАНИЕ

Беттеу:
Туренова Б.Ю.

Қазақстан Республикасы ІІМ
М. Есболатов атындағы Алматы академиясы
ғылыми-зерттеу және редакциялық-баспа жұмыстарын ұйымдастыру бөлімі
050060, Алматы қ., Өтепов көш., 29

Басуға 23 қазан 2024 ж. жіберілді.
Пішімі 60×84 1/8. №1 баспаханалық қағаз.
Ризографтық басылыс. Есептік баспа табағы 5.
Таралымы 100.