Глава 11. Определение и описание киберпреступности

11.1. Понятие и сущность киберпреступности

Невозможно представить современный прогресс и развитие в XXI веке без знания компьютерных технологий. Однако, развитие современных технологий, наряду с сотнями преимуществ не обходится без проблем. Одной из таких проблем является распространение киберпреступности с использованием компьютерных технологий, борьба с которой началась во всех странах.

Информационные и коммуникационные технологии изменили способ ведения бизнеса, покупки товаров и услуг, отправки и получения денег, общения, обмена информацией, сотрудничества, формирования и развития отношений с различными юридическими лицами. Подобные изменения, а также более широкое использование и зависимость от ИКТ создают уязвимость в различных областях, которые и становятся целью преступников и других злоумышленников, которые используют ИКТ для совершения преступлений.

В первую очередь, киберпреступность направлена против компьютерных систем, которые определяется по-разному. Например, в статье 1 (a) Конвенции Совета Европы о киберпреступности 2001 года «компьютерная система» определяется как «любое устройство или группа взаимосвязанных или смешанных устройств, одно или несколько из которых действуют в соответствии с программой автоматически». Однако в 1 статье Конвенции Африканского союза о кибербезопасности и защите личных данных от 2014 года компьютерная система определяется как «электронное, магнитное, оптическое, электрохимическое или другое высокоскоростное устройство обработки данных или группы взаимосвязанных или арифметических функций; или хранилище, включая устройства хранения данных или средства прямой связи, связанные с этим устройством или аналогичными устройствами.

Преступления в сфере компьютерной информации и преступления, совершаемые с использованием компьютеров и иных устройств, представляют собой новый вид преступлений в уголовном праве, и эти виды преступлений по существу называются киберпреступлениями.

Общепризнанного определения киберпреступности не существует. Однако следующее определение включает элементы для всех определений киберпреступности. Киберпреступность - это действие, совершаемое с использованием информационных и коммуникационных технологий или направленное против сетей, систем, данных, веб-сайтов и / или технологий[1]. Киберпреступность отличается от традиционных преступлений тем, что «не признает физических или географических границ» и может быть совершена с меньшими усилиями, легкостью и скоростью, чем обычная преступность.

[1] Goodman, Marc D. and Brenner, Susan W. (2002). The Emerging Consensus on Criminal Conduct in Cyberspace. International Journal of Law and Information Technology, Vol. 10, No. 2, 139-223; Wilson, Clay. (2008). Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. https://fas.org/sgp/crs/terror/RL321 14.pdf.; International Telecommunication Union (ITU). (2012).

Европол в 2018 году разделил киберпреступность на две группы: 1) любые преступления, совершаемые исключительно с использованием компьютеров, компьютерных сетей или других форм информационных и коммуникационных технологий; 2) преступления, совершенные с помощью кибертехнологий (т.е. традиционные преступления, совершаемые с помощью Интернета и цифровых технологий). Основное различие между этими категориями киберпреступлений заключается в роли информационных и коммуникационных технологий в совершении преступлений, и это зависит от того, являются ли ИКТ целью преступления или неотъемлемой частью метода совершения преступления (метода воздействия), используемого преступником. Когда ИКТ становятся целью преступления, такое преступление отрицательно влияет на конфиденциальность, полноту, доступность компьютерных данных или компьютерных систем[2].

Конфиденциальность, целостность и доступ к информации - ключевые аспекты[3]: проще говоря, конфиденциальная информация должна оставаться конфиденциальной, ее нельзя изменить без разрешения ее владельца, а информация, услуги и системы всегда должны быть доступны владельцу. Когда ИКТ являются частью способа совершения преступления, киберпреступность включает традиционные преступления (такие как мошенничество и кражи), которые тем или иным образом совершаются через Интернет и цифровые технологии.

11.2. Проблемы в борьбе с киберпреступностью

Борьба с киберпреступностью в мире, в том числе в Таджикистане, сталкивается с несколькими проблемами, которые мы разделили на три вида:

Технические проблемы. Есть несколько технических причин, затрудняющих борьбу с киберпреступностью. Первая причина - это аффилированность (принадлежность). Любой компьютер, подключенный к Интернету, может взаимодействовать с любым другим компьютером, подключенным к Интернету. Подключение компьютеров через Интернет зависит от IP-адреса. IP-адрес обычно представляет собой единый глобальный номер и позволяет компьютеру подключаться к Интернету через провайдера определенной страны. Проблема в том, что у злоумышленника (хакера) есть много способов скрыть свой IP-адрес или даже сделать вид, что он подключается с другого IP-адреса. Более того, преступники могут использовать различные инструменты, чтобы избежать обнаружения правоохранительными органами, что затрудняет доступ.

Вторая техническая проблема связана с программным обеспечением. Компьютерные программы - это программное обеспечение. Набор программ,

[2] УНП ООН (2013). Проект доклада УНП ООН «Всестороннее исследование проблемы киберпреступности». https://www.unodc.org/documents/organizedcrime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf.

[3] Rouse, Margaret. Confidentiality, integrity and availability (CIA Triad). TechTarget. https://whatis.techtarget.com/definition/Confidentiality-integrity-andavailability-CIA (2014)

используемых на компьютере, называется компьютерным программным обеспечением. Современное программное обеспечение включает миллионы различных приложений. Некоторые из этих программ называются системными программами, другие - прикладными программами, третьи - информационными системами и так далее. Пользователь компьютера может использовать как готовые программы, так и сам создавать такие программы. На сегодняшний день построен очень большой набор различных программ, которые можно использовать для решения различных задач. С помощью программ можно решить как разные проблемы, так и самые сложные математические задачи. Они широко используются в банковском деле, финансах, подготовке документов, выставках и многом другом. Сложно назвать область, в которой не применяются компьютерные программы.

На вашем телефоне или планшете также есть приложения. Службы, которые вы подключаете к Интернету, например веб-сайты, также включены в программное обеспечение. Часто программное обеспечение уязвимо. Уязвимость может быть проблемой в программе или неправильной конфигурацией, которая позволяет злоумышленникам выполнять действия, которые они ранее не могли выполнить (например, загружать информацию о кредитной карте клиента).

Компаниям-разработчикам программного обеспечения трудно обнаружить уязвимости, особенно тем, которые участвуют в крупных проектах по разработке программного обеспечения, которые часто меняются. Иногда злоумышленники находят уязвимость раньше, чем компания-разработчик программного обеспечения. По словам Bilge and Dumitras, пока уязвимость остается неизвестной, уязвимость не может быть исправлена, а антивирусное программное обеспечение не может обнаружить атаку с помощью сканирования устройства. Компания признает эту уязвимость, как только она будет использована киберпреступниками для атаки на конфиденциальность, целостность или доступность программного обеспечения и пользователей программного обеспечения.

Еще одна техническая проблема - виртуальная инфраструктура ИКТ. Многие организации размещают свои информационные системы на серверах, принадлежащих другому серверу (хост-провайдеру). В таких случаях компания возлагает часть ответственности за кибербезопасность на поставщика услуг, а в случае нарушения безопасности компания должна сотрудничать с поставщиком услуг для расследования инцидентов, которые могут привести к техническим и юридическим проблемам.

Правовые проблемы. Киберпреступность - это вид транснациональной преступности, когда преступников и потерпевших можно найти в любой точке мира, где есть подключение к Интернету.

Поэтому следователям, расследующими киберпреступления, часто требуется международный доступ и обмен информацией в своей работе. Эта задача может быть выполнена, если запрошенная информация хранится у поставщиков услуг и приняты меры для обеспечения доступа правоохранительных органов к информации. В этом случае необходимо знать нормы главы 48 Уголовно-процессуального Кодекса Республики Таджикистан, т.е. взаимодействие судов,

прокуратуры, следователей и следственных органов с соответствующими органами и должностными лицами иностранных государств при оказании правовой помощи в уголовных делах.

Основными правовыми проблемами при расследовании киберпреступлений и судебном преследовании киберпреступников являются: существование разных правовых систем в разных странах; различия в национальных законах, касающихся киберпреступности; различия в правовых нормах доказывания и уголовного судопроизводства (например, в порядке доступа правоохранительных органов к цифровым доказательствам; в суде или без ордера на обыск); различия в практике и географическом применении региональных и многосторонних соглашений о киберпреступности; различия в подходах к защите данных и правам человека.

В последние годы в Республике Таджикистан реализуется комплекс мер по повышению информационной безопасности. Правовая база для информационной безопасности создана и совершенствуется. Наряду с Уголовным кодексом Республики Таджикистан, были приняты Законы Республики Таджикистан «О государственной тайне», «О печати и других средствах массовой информации», «О телевидении и радиовещании», «Об издательской деятельности», «Об электрической связи», «Об авторском праве и смежных правах», «Об информатизации», «О национальных архивах и архивных учреждениях», «Об информации» и «О защите информации». Концепция информационной безопасности Республики Таджикистан, утвержденная Указом Президента Республики Таджикистан (7 ноября 2003 г. № 1176), является новым этапом в формировании государственной политики в области информационной безопасности. Таким образом, правовой вопрос противодействия киберпреступности находится в стадии рассмотрения и совершенствования.

Оперативные проблемы. Одна из основных оперативных проблем в расследовании киберпреступлений - сотрудничество с другими странами. Международное сотрудничество в расследовании киберпреступлений требует унификации законодательства в странах-партнерах. Такие средства, как соглашения о взаимной правовой помощи (т.е. соглашения, в которых стороны сотрудничают в расследовании и судебном преследовании преступлений, наказуемых в соответствии с их национальным законодательством), могут использоваться для отправки официальных запросов о помощи из одной страны в другую. Однако запросы о юридической помощи могут занять время и могут не дать ожидаемых результатов, таких как предупреждение преступности или представление доказательств для использования в суде.

На универсальном уровне Республика Таджикистан признает Конвенцию ООН против транснациональной организованной преступности, Конвенцию против пыток и других жестоких, бесчеловечных или унижающих достоинство видов обращения и наказания, Конвенцию о запрещении обработки, производства, накопления и применения химического оружия и о его уничтожении, Конвенцию Организации Объединенных Наций о наркотических средствах, Конвенцию ООН о психотропных веществах, Конвенцию Организации Объединенных Наций о

борьбе с незаконным оборотом наркотических средств и психотропных веществ, Конвенцию о борьбе с торговлей людьми и эксплуатацией проституции третьими сторонами, Шанхайскую конвенцию о борьбе с терроризмом, сепаратизмом и экстремизмом, Международную конвенцию о борьбе с финансированием терроризма, Конвенцию ООН против коррупции, и выполняет свои обязательства по этим документам в сфере борьбе с киберпреступностью.

На региональном уровне в Республике Таджикистан с 1993 года действуют: Конвенция о правовой помощи и правовых отношениях по уголовным, гражданским и семейным делам СНГ; Конвенция о правовой помощи и правовых отношениях по уголовным, гражданским и семейным делам, ратифицирована странами СНГ с 2002 г.. Вместе с тем заключены такие двусторонние соглашения с зарубежными странами, такие как: Соглашение между Республикой Таджикистан и Республикой Индия о взаимной правовой помощи по уголовным делам от 10 мая 2001 г.; Соглашение между Республикой Таджикистан и Объединенными Арабскими Эмиратами о взаимной правовой помощи по уголовным делам от 9 апреля 2007 г.; Соглашение между Республикой Таджикистан и Турецкой Республикой о сотрудничестве в области уголовных, коммерческих и гражданских дел от 6 мая 1996 г.; Соглашение между Республикой Таджикистан и Китайской Народной Республикой о правовой помощи по уголовным и гражданским делам от 16 сентября 1996 г.; Соглашение между Правительством Республики Таджикистан и Правительством Исламской Республики Пакистан о создании совместной рабочей группы по борьбе с международным терроризмом от 17 июня 2014 г.; Соглашение между Правительством Республики Таджикистан и Правительством Латвийской Республики о сотрудничестве в борьбе с терроризмом и незаконным оборотом наркотических средств, психотропных веществ, прекурсоров и другими преступлениями от 10 июня 2014.; Соглашение между Республикой Таджикистан и Украиной о возвращении осужденных к лишению свободы для дальнейшего отбывания наказания; Соглашение между Республикой Таджикистан и Китайской Народной Республикой о передаче; Соглашение между Республикой Таджикистан и Объединенными Арабскими Эмиратами об экстрадиции; Соглашение между Республикой Таджикистан и Китайской Народной Республикой об экстрадиции; Соглашение между Республикой Таджикистан и Исламской Республикой Афганистан о возвращении заключенных для дальнейшего отбывания наказания; Соглашение между Республикой Таджикистан и Исламской Республикой Иран об экстрадиции. В целом подобных двусторонних соглашений около 70. В будущем необходимо принятие двусторонних и многосторонних документов между странами мира и региона для адекватной борьбы с киберпреступностью.

11.3. Предупреждение киберпреступности

Киберпреступники часто используют технические и социальные методы для совершения преступлений. Предотвратить определенные виды киберпреступлений сложно, но пользователи технологий могут предпринять необходимые шаги для защиты (до некоторой степени) от киберпреступности.

Европейская полиция (Европол) на своем сайте опубликовала в 2018 году ряд руководящих принципов по информированию общественности и предупреждению преступности. Однако, даже небольшие действия могут иметь большое значение в этом направлении. Вот несколько советов, которые следует помнить при подключении к Интернету:

1) Регулярно обновляйте операционную систему и установленное программное обеспечение;

2) Удалите с устройства обычное программное обеспечение, которым вы больше не пользуетесь;

3) Используйте антивирусную программу, разработанную авторитетной компанией;

4) Не загружайте программное обеспечение, фильмы или музыку с общедоступных сайтов - они часто вредоносны;

5) Не вводите личную информацию на неизвестных сайтах;

6) Убедитесь в правильности адреса веб-сайта перед вводом финансовой информации.

Изучение ситуации показывает, что основной мерой борьбы с киберпреступностью на государственном уровне является правовое регулирование: совершенствование законодательства, криминализация новых преступлений, усиление ответственности за существующие киберпреступности. Несмотря на действующее законодательство разных стран, для киберпреступников нет границ. Киберпреступники совершают преступления по самым разным причинам и с разными целями. Однако стоит отметить, что киберпреступники, получившие доступ к конфиденциальной информации или слежке за ИТ-системами, иногда даже не понимают, что делать с полученной информацией.

С помощью набора доступных методов Марина Лепина предоставила список основных действий пользователя, которые играют важную роль в предотвращении киберпреступности:

1) Использование лицензионных компьютерных программ и антивирусных продуктов.

2) Использование электронного почтового адреса по конкретному назначению: для регистрации на сайтах, для оплаты услуг, для передачи важной информации (лучше защищенный).

3) Открытие вложений только от известных отправителей, если есть сомнения, необходимо связаться с отправителем иным способом.

4) Проверка вложения на наличие вирусов.

5) Нежелательность указания в полученных по электронной почте формах и анкетах личные данные, так как их безопасную передачу могут гарантировать только защищенные сайты.

6) Проверка запросов персональных данных из деловых и финансовых структур, путем обращения в эти структуры по контактам, указанным на официальном сайте, но не в электронном письме.

7) При общении с клиентами банки не осуществляют как правило массовую рассылку. Поэтому лучше связаться с офисом банка по контактным данным на его официальном сайте, чтобы прояснить ситуацию

8) Требования немедленных действий в чрезвычайных ситуациях с высокой степенью вероятности являются мошенничеством. Преступники вызывают ощущение тревоги, чтобы заставить пользователя действовать в критической ситуации быстро и неосмотрительно. Необходимо оценивать ситуацию и принимать взвешенное решение.

9) Выпуск дополнительной карты для оплаты товаров в интернете.

10) При взломе вашей страницы, если вами был скачан какой-либо файл, заходите на сайт для восстановления страницы с незараженного устройства. После выполните процедуру восстановления пароля, перед этим сменив учетные данные во всех сервисах, где они совпадали со скомпрометированными, для защиты других аккаунтов.

11) Никогда не открывайте файлы, запрашивающие использование компонентов ActiveX в браузере Internet Explorer, так как они позволяют JavaScript'ам, выполняющимся в контексте браузера IE, осуществлять доступ к объектам операционной системы, в том числе загружать на нее исполняемые файлы, которые с высокой вероятность могут оказаться вредоносными объектами и запускать их[4].

11.4. Походы к обеспечению кибербезопасности

Сегодняшний мир живет в эпоху глобальной конвергенцией цифровых, физических и биологических технологий, изменяя мир вокруг и понимание качества жизни. Цифровые технологии фундаментально изменили образ нашей повседневной жизни, способы работы и коммуникаций между людьми. Связь уже не просто соединяет людей: становятся реальностью концепции интернета вещей (IoT), больших данных и "умных" сетей.

Активное развитие информационно-коммуникационных технологий и растущее использование сети Интернет, с особой остротой определяет необходимость обеспечения безопасности в информационной среде, составной частью которой является киберпространство, и защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с киберпреступностью.

Транснациональный и трансграничный характер многих продуктов ИКТ и открытая природа Интернета используются международной преступностью в целях совершения противоправных действий с использованием ИКТ, что приводит к росту киберпреступности.

Увеличение числа пользователей Интернета повышает критичность и делает более ощутимыми последствия в случае отказов техники, ведет к увеличению количества атак на абонентские устройства. Пренебрежение требованиями

[4] 11 правил сетевой безопасности: как защититься от кибермошенников 22.03.2021 / Марина Лепина. URL: https://www.miloserdie.ru/article/11-pravil-setevoj-gigieny-kak-zashhititsya-ot-kiberprestupnosti/.

безопасности при использовании интернет-ресурсов и социальных сетей, игнорирование мер «цифровой гигиены» повышает риск неприкосновенности частной жизни, модификации или уничтожению персональных данных. Низкий уровень компьютерной грамотности конечных пользователей при отсутствии базовых знаний по общим методам компьютерных атак приводит к росту фактов кибер-мошенничества, противоправного использования ИКТ.

Меры, связанные с автоматизацией оказания государственных услуг, начавшаяся цифровизация государственных и муниципальных услуг, доступа к информации о деятельности государственных органов, создание государственных информационных ресурсов и систем, аккумулирование в них большого количества данных, в том числе критически важных (биометрика, данные, необходимые для выполнения государственных функций) также несут в себе определенные риски. Объем данных, обрабатываемых в государственном секторе, постоянно растет, что приводит к необходимости выработки новых форм их хранения и обеспечения их безопасности. Защита и безопасность данных, особенно критически важных, имеет сегодня решающее значение.

Беспечность в выборе поставщиков технологий обеспечения информационной и кибербезопасности государственных органов, отсутствие возможностей для аудита исходных кодов программного обеспечения, или непредставление таковых, также ведет к невозможности оценки рисков, связанных с намеренным внедрением в программное обеспечение или телекоммуникационное оборудование не декларируемых функций, которые потенциально могут быть использованы для нанесения ущерба государственным интересам.

Критичной является ситуация с обучением руководителей подразделений и всего задействованного в оказании электронных государственных и муниципальных услуг персонала принципам и технологиям защиты конфиденциальной информации.

Не всегда оценивается важность совместных усилий по формированию безопасного киберпространства внутри страны. Недостаточная обеспеченность бизнес сектора в технологиях защиты информации, зачастую не желание признавать потребности в защите информации и сетевой безопасности, приводит к большому количеству остающихся латентными инцидентов информационной и кибербезопасности.

Остро ощущается общая нехватка экспертов по информационной и кибербезопасности, особенно в государственном секторе. Программы обучения и подготовки специалистов в этой сфере, не в полной мере отвечают сегодняшним тенденциям и реалиям.

Вместе с тем, оперативное, проактивное и эффективное противодействие киберугрозам, киберпреступности требует принятия адекватных мер реагирования на уровне государственных органов, и прежде всего - концептуального закрепления необходимых мер на доктринальном и нормативно-правовом уровне, создания государственной политики в области обеспечения

информационной и кибербезопасности с вовлечением всех заинтересованных сторон.

Вопросы кибербезопасности следует решать, принимая во внимание глобальный, транснациональный характер киберугроз.

Концепция кибербезопасности должна обеспечить единство подходов к формированию и реализации общенациональной политики обеспечения безопасности защищаемых законом видов информации, защиты электронных информационных ресурсов и систем, информационно-коммуникационной инфраструктуры, а также методологической базы и нормативных правовых актов, регулирующих сферу безопасного использования ИКТ.

Необходимой мерой является и создание организационных киберструктур, специальных подразделений в правоохранительных органах, развитие сети центров реагирования на компьютерные инциденты (CERT) для определения киберугроз, управления операциями и реагирования на них, а также участия в механизмах сотрудничества на внутригосударственном, региональном и международном уровнях, привлечение технического и экспертного сообщества по вопросам потенциальных решений в сфере кибербезопасности.

Общая цель таких мер должна состоять в создании и постоянном поддержании системы управления кибербезопасностью, обеспечивающей устойчивое развитие страны при использовании информационно-коммуникационных технологий.

Необходимо развитие национального потенциала в области кибербезопасности, обмен информацией о передовом опыте, привлечение всего сообщества в целом. Формирование культуры кибербезопасности путем распространения передового опыта, повышение уровня осведомленности по вопросам кибербезопасности, создании необходимого потенциала, совершенствования средств кибербезопасности, укрепление и поддержание согласованности усилий в сфере кибербезопасности;

Вопросы кибербезопасности должны включать состояние защищенности средств телекоммуникаций (средств связи), цифровых (электронных) информационных ресурсов информационных систем, информационно-коммуникационной инфраструктуры от внешних и внутренних угроз.

Основными направлениями обеспечения кибербезопасности должны стать:

- правовое обеспечение (принятие и применение правовых норм в сфере кибербезопасности);
- организационное обеспечение (регламентация деятельности, исключающая нанесение ущерба, наличие соответствующих служб);
- инженерно-техническое обеспечение (использование технических средств, препятствующих нанесению ущерба, физические, аппаратные, программные и криптографические средства защиты).

Принятие подобных мер в качестве доктринальных, правовых будет означать значимый шаг в выстраивании адекватных сегодняшнему дню методов и способов защиты достаточно уязвимого киберпространства.

Необходимо разработать мероприятия, направленные на реализацию стратегических целей по повышению институционального и человеческого потенциала обеспечения кибербезопасности, созданию и защите кибер-физических систем, информационных ресурсов, критической инфраструктуры от киберугроз. Должны быть четко определены органы/организации, ответственные за осуществление мер, сроки выполнения мероприятий. Все это должно быть подкреплено прописанными финансовыми ресурсами с четким распределением на каждое конкретное мероприятие.

Опираясь на международный опыт обеспечения кибербезопаности можно сформулировать следующие общие **выводы и рекомендации** для страновой доктрины:

1) выстроить на национальном уроне систему органов государственного управления, задействованных в определении политики кибербезопасности и ее реализации на организационном (управление), нормативно-правовом (доктринальном), инженерно-техническом уровне;

2) создать уполномоченный государственный орган по реагированию на возникающие угрозы и киберинциденты (CERT); ежегодно публиковать отчеты о киберугрозах и рисках, информировать общественность в целях повышения осведомленности, в том числе через веб-сайт такого уполномоченного органа (CERT); указанный уполномоченный CERT должен нести ответственность за (обладать следующими функциями):

Предотвращение киберугроз:

- предупреждение организаций и широкой общественности о значимых инцидентах кибербезопасности;
- подготовка аналитических отчетов об известных угрозах;
- отслеживание инцидентов кибербезопасности;

Реагирование на киберугрозы:

- распространение соответствующей информации об инцидентах кибербезопасности;
- гарантировать быстрое реагирование на широкомасштабные национальные кризисные инциденты;
- подготовка отчетов об инцидентах, ежегодно подготавливать, по крайней мере, один публичный отчет;
- выступать в качестве контактного пункта в случае инцидентов кибербезопасности на международном уровне в режиме 24/7;
- обеспечить партнерство отечественных и международных заинтересованных сторон по обмену опытом в области кибербезопасности;
- быть членом признанной международной организации по реагированию на инциденты кибербезопасности;

Прогнозирование киберугроз:

- подготовка и распространение образовательных материалов по повышению потенциала кибербезопасности;
- проведение учений по кибербезопасности;

- подготовка и поддержка руководств по лучшей практике по всем аспектам работы CERT, включая создание, управление, расследование инцидентов и использование форензик инструментов.
- предусмотреть на законодательном уровне, что субъекты государственного сектора и операторы критической информационной инфраструктуры обязаны сообщать об инцидентах кибербезопасности;
- в соответствии с правовыми актами установить, что субъекты государственного и частного сектора обмениваются соответствующей информацией о кибреугрозах, киберицидентах.
- рассмотреть вопрос о создании в вооруженных силах страны отделы, ответственные за защиту национальное киберпространства (подразделение по кибероперациям/кибероборонe).

3) принять меры к пересмотру образовательных стандартов от общешкольного до ВУЗовского и послеВУЗОвского образования, чтобы основные знания в области кибербезопасности приобретались в рамках общего образования; внедрить программы профессионального и высшего образования для подготовки технических, правовых и полиси специалистов по кибербезопасности; в целом принимать регулярные меры к повышению потенциала в сфере кибербезопасности;

4) внедрить нормативные правила и принять стандарты для управления безопасностью ИКТ в государственном секторе; в том числе предусмотреть, что до внедрения ИКТ-решений в государственном секторе, при государственных закупках проводился обязательный аудит по безопасности, как программных, так и технических средств (исходных программных кодов, бэк-доров); предусмотреть регулярность такого аудита ИТК-решений в государственном секторе;

5) пересмотреть законодательство с целью внедрения правовой базы для электронной аутентификации и электронной подписи на принципах технологической нейтральности, универсальности, соответствия требований к шифрованию признанным современным международным принципам; выстроить надлежащую систему сертификации средств шифрования, в соответствии с которыми требования к цифровой подписи и устройствам электронной подписи соответствуют надлежащим требованиям к безопасности;

6) законодательно выстроить меры к защите критической информационной инфраструктуры, пересмотреть законодательство о стратегически объектах; нормативно в правовых актах определить понятия и критерии критически важных секторов и критической информационной инфраструктуры; в структуре Госкомитета информационных технологий и связи создать отдел, специализирующийся на защите критической информационной инфраструктуры на национальном уровне; для операторов критической информационной инфраструктуры установить обязательные требования к обработке данных и непрерывности услуг с обязательством назначить сотрудника, ответственного за кибербезопасность;

7) разработать план управления в случае кризисной ситуации, связанной с кибербезопасностью; проводить регулярные учения по управлению в случае

кризисной ситуации, связанной с кибербезопасностью, и по возможности обеспечивать участие специалистов в учениях на международном уровне; проводить учения по киберзащите;
8) принять меры к законодательному (на уровне процессуального законодательства) закреплению методов и средств цифровой криминалистики (компьютерной форензики), внедрить соответствующие методы и способы фиксации цифровых доказательств в целях расследования, их исследования в суде;
9) рассмотреть вопрос об усилении международного сотрудничества, заключению соглашений по вопросам кибербезопасности с другими странами и/или международными организациями.

11.5. Классификация преступлений против информационной безопасности (киберпреступность)

Киберпреступность, в первую очередь включает в себя преступления, нацеленные на системы, сети и информацию с целью нарушения конфиденциальности (т. е. когда системы, сети и данные защищены и только авторизованные пользователи имеют к ним доступ), целостности (т. е. когда данные точны и надежны и не изменились) и их доступности (т. е. когда данные, услуги и системы доступны по первому запросу). Эти киберпреступления представляют собой хакерские атаки; создавать, поддерживать и распространять вредоносное ПО; атаки для отказа в обслуживании (DoS); Широкомасштабная DoS атак (DDoS) и причинение вреда веб-сайтам (то есть форма онлайн-взлома, направленная на содержание веб-сайта).

Согласно Уголовному кодексу Республики, Таджикистан, эти преступления перечислены в главе 28, которая называется преступлениями против информационной безопасности. Основываясь на этой главе, преступления против информационной безопасности включают:

1. Неправомерный доступ к компьютерной информации (статья 298 УК РТ). Этот вид преступления включает в себя неправомерный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты (п. 1. ст. 298 УК РТ), а также те же деяния, повлекшие по неосторожности изменение, уничтожение или блокирование информации, а равно вывод из строя компьютерного оборудования, либо значительный ущерб, (п. 2 ст. 298 УК РТ).

Согласно закону, каждое преступление должно иметь как объективные (объект и объективная сторона), так и субъективные (субъект и субъективная сторона) элементы, которые адекватно описывают состав преступления. Объектом преступления несанкционированного доступа к компьютерной информации являются связи с общественностью, обеспечивающие защиту информации и компьютерного оборудования, а также возможность их дальнейшего использования в интересах владельца и пользователей. Защита информации - комплекс мер, принимаемых для предотвращения утечки, кражи, потери, несанкционированного уничтожения, неверного толкования, изменения,

несанкционированного копирования и блокирования распространения информации.

Одной из категорий, входящих в составную структуру объекта преступления, является предмет преступления. Предметом преступления является неправомерный доступ к электронной информации, то есть компьютерной информации, хранящейся в компьютерной системе, сети или на машинных носителях. Информация - сведения о лицах, предметах, событиях, явлениях и процессах независимо от формы их представления[5]. Электронные данные (электронное сообщение) - электронное представление любой информации, воспринимаемой электронной вычислительной машиной[6].

Объективной стороной данного преступления (ч.1 ст.298 УК РТ) является активное действия в форме неправомерного доступа (несанкционированного доступа) к информации, содержащейся в системе или компьютерной сети либо в базе данных машин. Несанкционированный доступ — это доступ к защищенной информации заинтересованным лицом с нарушением прав или правил доступа к защищенной информации, установленных правовыми документами или владельцем информации.

Практический пример данного преступления: «*В ходе розыскных операций сотрудниками Управления по борьбе с организованной преступностью МВД РТ по подозрению в незаконном доступе к компьютерной информации был задержан гражданин И.С. 1984 года рождения, житель Душанбе. Подозреваемый в апреле 2013 г. перед зданием «Фарханг» в Душанбе встретился с гражданином РФ, П.А 1987 г.р., и по предварительному сговору с ним, незаконно ввел в компьютер информацию. Они, используя специальное оборудование, две единицы техники «Шлюз-GSM» с использованием высокоскоростного оптического Интернета г. Душанбе, шестью SIM-картамы «Шлюз-GSM», тремя «WIMAX», пятью SIM-карт «Симбанк» мобильной компании «Вавилон М» используя специальные компьютерные программы, незаконно проникли в защищенную систему, занимались незаконной терминацией входящих международных звонков и в результате нанесли материальный ущерб компании и госбюджету*”[7].

Чтобы деяние, указанное в этой статье, было признано преступлением, оно должно быть связано с нарушением системы защиты информации, установленной в компьютерной системе или в компьютерной сети. В противном случае, если человек незаконно обращается (получает доступ) к информации без нарушения системы безопасности, то совершенное действие не считается преступлением. Нарушение системы защиты информации может осуществляться разными способами, например, с помощью:

а) использования специальных технических или программных материалов, позволяющих разрушить существующую систему безопасности;

[5] Закон Республики Таджикистан об информации// http://www.mmk.tj/library/dar_borai_ittiloot.rar

[6] Закон Республики Таджикистан об электронной цифровой подписи// mmk.tj/library/dar_borai_imzoi_elektroni.doc

[7] https://mvd.tj/old/index.php/tj/asosi/3521-ajri-onun-daromadan-ba-ittilooti-kompyuter

б) незаконного использования рабочего имени (пароля) или пароля (кода) для входа в компьютер;
в) хищения носителей информации при принятии мер по их защите;
г) для выполнения других операций с целью доступа к компьютерной системе или сети в качестве законного пользователя[8].

Субъективная сторона данного преступления выражается в прямом умысле, то есть преступник осознает незаконность своих действий, что выражается в нарушении системы компьютерной безопасности доступа к информации, и желает их осуществить.

Субъект преступления - лицо, достигшее 16-летнего возраста. В то же время субъектом преступления может быть также специальный субъект, который совершает такое преступление, используя свое служебное положение, то есть лицо, имеющее прямой доступ к компьютеру, компьютерной системе или ее сети.

Часть 2 ст. 298 УК РТ устанавливает уголовную ответственность за совершение данного преступления по неосторожности, повлекшего изменение, уничтожение или блокирование информации, а также выход из строя компьютерной техники или причинение серьезного ущерба. Из положений данной статьи следует, что объективная сторона состоит из следующих альтернативных действий:

Модификация информации - изменение информации, требующее разрешения автора или владельца информации;

Удаление информации - это умышленное или неосторожное действие, в результате которого доступ к информации юридическому или физическому лицу прекращается полностью или частично. Следует отметить, что возможность пользователя восстановить удаленные данные с помощью программных средств или получить эту информацию от другого пользователя не освобождает правонарушителя от уголовной ответственности. Сохранение файла, содержащего информацию, а также автоматическая замена старых версий файлов на самые свежие с течением времени не считается удалением информации.

Блокировка информации - это выполнение действия, ограничивающего или блокирующего доступ к компьютерной системе и предоставляемым ею информационным ресурсам;

Отключение компьютерного оборудования (нарушение работы компьютера, компьютерной системы или ее сети) - нарушение каких программ, базы данных, источника искаженной информации, а также работы непрофильного оборудования и стабильности сети периферийных устройств[9].

В этом случае одно из условий квалификации - только по ч. 2 ст. 298 УК РТ - защита физической неприкосновенности компьютера. Если, помимо вышеперечисленных последствий, физическая целостность компьютерной системы нарушается как товар, то такое деяние требует дополнительной квалификации согласно соответствующим статьям УК РТ, устанавливающим уголовную ответственность за преступления против собственности.

[8] Комментарий к Уголовному кодексу Республики. Душанбе: Глобус, 2005. С. 397-398
[9] См.: Там же.

Состав данного преступления материальный и требует причинения серьезного вреда. Серьезное повреждение - означает, что компьютерная система или компьютерная сеть выходит из строя, ценные данные изменены или удалены и так далее.

Субъективная сторона преступления по ч.2 статьи 298 УК РТ выражается в неосторожности. Преступление, совершенное по неосторожности признается общественно опасное деяние совершенное по самонадеянности или небрежности. Преступлением считается совершенное по самонадеянности, если лицо считает возможность последствий своих действий (бездействия) опасными для общества, но без достаточных оснований верить в это, что исключает последствия. Преступление, совершенное по неосторожности, считается совершенным, если лицо не предвидело возможность последствий своих действий (бездействия) для общества, даже если оно должно и могло предвидеть последствия с должной осторожностью и предусмотрительностью.

Субъект преступления (п. 2 ст. 298 УК РТ) - лицо, достигшее 16-летнего возраста.

Часть 3 этой статьи предусматривает ответственность за действия, предусмотренные частью первой или второй ст. 298 УК РТ повлекшие по неосторожности тяжкие последствия

Субъективная сторона преступления, предусмотренного п. 3 ст 298 УК РТ выражается в неосторожности.

2.Модификация компьютерной информации (статья 299 УК РТ).

Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации, причинившее значительный ущерб или создавшее угрозу его причинения признается преступлением, и это деяние квалифицируется ст. 299 УК РТ.

Модификация компьютерной информации - это самостоятельная форма незаконного доступа к компьютерной информации. Состав данного преступления по своей структуре является материальным и предусматривает как последствие причинение тяжкого вреда. Его объективная сторона состоит из двух альтернативных действий:

1. изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях;
2. внесение в них заведомо ложной информации в компьютерной системе, сети или на машинных носителях.

Понятие изменения информации можно выявить из анализа ст. 298 УК РТ.

Модификация информации влечет за собой уголовную ответственность только в том случае, если изменение информации не связано с адаптацией приложения к компьютеру или базе данных, которая осуществляется только для обеспечения работы приложения на определенных технических средствах или под контролем конкретных пользовательских приложений.

Использование программного обеспечения, которое изменяет информацию без изменения ее содержания, позволяя восстановить ее в исходной форме –

архиваторы, кодировщики и т.д., не должно толковаться как «изменение» в уголовно-правовом смысле.

Внесение информации в эту систему является преступлением по настоящей статье только в том случае, если она содержит заведомо ложную информацию.

Информация считается ложной, если она не соответствует действительности и вводит в заблуждение пользователей[10].

Субъективная сторона выражается в прямом умысле.

Субъект - общий, то есть человек, достигший 16-летнего возраста.

В ч. 2 ст. 299 УК РТ уголовная ответственность предусмотрена за изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации, сопряженное с неправомерным доступом к компьютерной системе или сети и повлекшее по неосторожности тяжкие последствия.

Первый признак описывает деяния - его состояние, а второй - его последствия. Анализируя ч. 2 ст. 299 УК РТ следует отметить, что содержание данных квалифицирующих норм являются материальным, так как законодатель использовал термин «изменение компьютерной информации» без каких-то условий. Термин «модификация компьютерной информации», согласно первой части ст. 299 УК РТ предусматривает причинившее значительного ущерба. Таким образом, изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации сопряженное с неправомерным доступом к компьютерной системе или сети считается уголовным преступлением только в случае умышленного причинения серьезного вреда. Изменение компьютерной информации, повлекшее по неосторожности тяжкие последствия, является неосторожным преступлением так как это указано в самом тексте закона.

3. Компьютерный саботаж (статья 300 УК РТ).

Компьютерный саботаж в УК РТ толкуется как изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, а равно внесение в них заведомо ложной информации, причинившее значительный ущерб или создавшее угрозу его причинения.

Объективная сторона компьютерного саботажа выражается в совершении одного (или нескольких) из следующих действий:

А) Уничтожение компьютерной информации. Уничтожение информации - это умышленное действие, которое приводит к полному или ограниченному прекращению доступности информации для юридического или физического лица.

Б) Уничтожение компьютерной программы. Компьютерная программа - это последовательность инструкций, предназначенных для управления компьютерами с помощью оборудования. Программа является одним из элементов программного обеспечения. В зависимости от содержания термин также может использоваться в качестве исходного кода. Программа представляет собой набор данных и команд,

[10] Комментарий к Уголовному кодексу Республики Таджикистан. Душанбе: Глобус, 2005. С. 398

которые могут использоваться для управления электронными машинами и другим компьютерным оборудованием с целью достижения желаемого результата, включая учебные материалы, полученные в ходе разработки программы для компьютера, а также для генерации звука и изображений[11].

Уничтожение компьютерной программы означает, что в результате такой операции компьютерная программа удаляется с компьютера, и в результате она не может нормально функционировать или деятельность, контролируемая компьютерной программой, перестает работать. Например, в результате уничтожения компьютерной программы торгового центра Ашан, из-за продажи продукции, деятельность этого центра будет приостановлена до восстановления программы, и ему будет нанесен материальный ущерб. Или в случае уничтожения компьютерных программ, связанных с денежными переводами, таких как: «Контакт», «ЛИДЕР», «Юнистрим», «Анелик» их деятельность будет приостановлена до их восстановления, в результате чего пострадают владельцы этих систем, получив материальный ущерб.

В) блокирование информации или компьютерной программы - выполнение действия, которое приводит к ограничению или блокировке (блокировке) доступа к компьютерной системе и предоставляемым ею информационным ресурсам;

Г) приведение в непригодное состояние компьютерной информации или программы. Это движение означает, что в компьютере присутствует информация или компьютерная программа, но из-за отсутствия или разрушения его основных частей он не может полностью выполнять свою функцию. Например, компьютерная программа больше не может отличить один фрагмент информации от другого;

Д) вывод из строя компьютерного оборудования. Как известно, ПК IBM выпускаются двух типов - настольные и совместные. К основным настольным устройствам этого персонального компьютера относятся системный блок, монитор (экран), клавиатура и мышь. Дополнительное аппаратное обеспечение персонального компьютера может включать в себя различные входные и выходные данные аппаратного обеспечения. Количество, тип и качество такого оборудования зависит от вида деятельности и финансовых возможностей пользователя компьютера. Пользователи в основном используют принтеры, джойстики, сканеры, плоттеры, дигитайзеры, веб-камеры, цифровые камеры, акустические системы и модемы. Вывод из строя компьютерного оборудования считается компьютерным саботажем. Вывод из строя компьютерного оборудования во всех его формах должно быть отнесено к преступлениям с материальными элементами, т.е. последствия вреда обществу в виде вреда (серьезного, в больших количествах, особенно в больших количествах) должны быть указаны в диспозиции статьи. Однако, по неизвестным причинам это преступление установлено в ч. 1 статьи. 300, что может затруднит квалификацию преступления или же по нему могут привлечь к ответственности за незначительный ущерб, такой как повреждение компьютерной мыши.

[11] https://tg.wikipedia.org/wiki/компьютерная программа

Е) разрушение компьютерной системы, сети или машинного носителя. Чтобы определить суть этого действия, необходимо определить следующие понятия:

1. Компьютерная система. Компьютерная система - это организованный набор информационных технологий, в том числе с использованием компьютерного и коммуникационного оборудования, обеспечивающий поток информации;

2. Компьютерная сеть. Если два или более компьютера каким-либо образом связаны друг с другом (проводным, волновым и т. Д.) и могут обмениваться данными друг с другом, то считается, что они соединены в компьютерную сеть. Компьютерная сеть - мощное средство обмена информацией между компьютерами. На практике, в зависимости от количества информации, необходимой для решения проблем, используются локальные, региональные, глобальные компьютерные и т.п. сети

Д. Базы данных являются носителями информации, например, флэш-карты, оборудование, CD-COM, DVD-COM, оптические приводы и т. д.

В качестве неисправности компьютерной системы следует рассматривать разрушение как всего оборудования этой системы, так и некоторых из них, которые не могут работать без этой компьютерной системы. Например, удаление монитора в качестве устройства вывода не приведет к остановке системного блока, но без отображения информации на экране системный блок будет бесполезен для пользователя.

Суть разрушения (диверсии) компьютерной сети заключается не в уничтожении отдельных компьютеров в сети, а только в уничтожении сервера или линий связи между сервером и другими компьютерами в сети.

Уничтожение машинной базы данных означает полное уничтожение или повреждение ее (без каких-либо признаков разрушения) любого типа машинной базы данных, за исключением хранящихся в ней данных.

Субъективная сторона преступления выражается в форме прямого умысла.

Субъект – вменяемое физическое лицо, достигший 16-летнего возраста.

Если уничтожение, блокирование либо приведение в непригодное состояние компьютерной информации или программы, вывод из строя компьютерного оборудования, а равно разрушение компьютерной системы, сети или машинного носителя, сопряженное с неправомерным доступом к компьютерной системе или сети; повлекшее по неосторожности тяжкие последствия, то такие опасные действия должны быть квалифицированы по ч. 2 ст. 300 УК РТ.

Субъективная сторона преступления (ч. 2 ст. 300 УК РТ) вина в форме как умысла так и в неосторожности.

Субъект (с.2 ст. 300 УК РТ) – вменяемое физическое лицо, достигший 16-летнего возраста.

4. Незаконное завладение компьютерной информацией (статья 301 УК РТ)

Данное преступление в ст. 301 УК РТ определяется как незаконное копирование или иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, а равно перехват информации, передаваемой с использованием компьютерной связи (ч.1 ст. 301), также характеризуется как принуждение к передаче информации, хранящейся в

компьютерной системе, сети или на машинных носителях, под угрозой оглашения позорящих сведений о лице или его близких, предания гласности сведений о таких обстоятельствах, которые потерпевший желает сохранить в тайне, а равно под угрозой применения насилия над лицом или его близкими либо под угрозой уничтожения или повреждения имущества лица, его близких и других лиц, в ведении или под охраной которых находится эта информация, (ч. 2 ст. 301 УК РТ).

Основной целью установления уголовной ответственности за незаконное завладение компьютерной информацией (статья 301) является, прежде всего, защита информации, которая предусмотрена в ст. 1 Закона Республики Таджикистан «О защите информации» от 2 декабря 2002 года. К целям защиты информации относятся:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предупреждение санкционированных и несанкционированных действий, которые могут повлечь за собой преднамеренное или непреднамеренное уничтожение, блокирование, искажение (подделку), хищение, копирование, утечку, модифицирование и преобразование информации

Объективная сторона данного преступления состоит из следующих альтернативных действий:

1. Копирование информации, содержащуюся в компьютерной системе или компьютерной сети, или в базе данных машины. Копирование информации, хранящейся в компьютерной системе или компьютерной сети или в базе данных машины, означает получение исходной копии информации без ее повреждения и с сохранением ее способности его использоваться по назначению (в отличие от уничтожения, изменения или блокировки информации) без разрешение владельца и уполномоченных лиц или законного пользователя;
2. Иными неправомерными способами завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях- любые незаконные средства получения информации без согласия ее владельца или их уполномоченных лиц, а также законного пользователя или с их согласия, но против их волеизъявление, выраженное с целью использования этой информации по своему усмотрению. Примером такого хищения является кража системного блока, а также носителей информации - компакт-дисков, флеш-карт и т. д., взятых с целью считывания информации. В этом случае хищение компьютерной системы или носителей данных требует дополнительной упаковки как преступление против собственности - кража, грабеж, вымогательство и т.д. (В зависимости от вида кражи), поскольку результатом такой кражи является не только нарушение безопасности информации, но и причинение имущественного ущерба.
3. Перехват информации, передаваемой с использованием компьютерной связи.

Перехват информации, передаваемой с использованием компьютерной связи возможен, например, в случае отправки информации по электронной почте на адрес другого пользователя.

Субъективная сторона (п.1 ст. 301 УК РТ) выражается в прямом умысле.

Субъектом (ч. 1 ст. 301 УК РТ) – вменяемое физическое лицо, достигший 16-летнего возраста.

Часть 2 данной статьи предусматривает более серьезную уголовную ответственность за принуждение к передаче информации. Передача (раскрытие защищенной информации) - это несанкционированная доставка защищенной информации потребителям, не имеющим права доступа к ней. Способы такого принуждения предусмотрены диспозицией статьи и включают[12]:

а) путем угрозы оглашения позорящих сведений о лице или его близких;

б) путем угрозы предания гласности сведений о таких обстоятельствах, которые потерпевший желает сохранить в тайне;

в) путем угрозы применения насилия над лицом или его близкими;

г) угрозой уничтожения или повреждения имущества лица, его близких и других лиц, в ведении или под охраной которых находится эта информация.

В частях 3 и 4 статьи 301 УК РТ предусмотрена уголовная ответственность за совершение данного преступления с применением насилия в отношении человека или его родственников; совершенные по предварительному сговору группой лиц; в) причинившие значительный ущерб потерпевшему; г) совершенные с целью получения особо ценной информации; совершенные повторно; б) совершенные организованной группой; в) повлекшее по неосторожности смерть человека либо иных тяжких последствий;

5. Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети (статья 302 УК РТ).

В статье 302 УК РТ за изготовление с целью сбыта, а равно сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети предусматривается уголовная ответственность.

Предметом этого преступления являются специальные средства. Такие как шпионские клавиатуры, вирусные программы, специализированные программы (для отправки информации на другой адрес электронной почты) и так далее. Среди этих инструментов трекеры и шпионские клавиатуры являются наиболее распространенными формами специальных инструментов для незаконного доступа к компьютерной системе или сети.

Трекеры (трекеры) или маяки предоставляют злоумышленнику информацию о местоположении устройства, веб-сайтах, документах, списках контактов, маршрутах путешествий, часто посещаемых местах и многом другом. Трекеры бывают двух типов: аппаратные и программные. Типы трекеров, которые открыто размещаются в Интернете: Reptilicus; Ear Agent; Intruder Selfie; Alfred Camera; iKeyMonitor; Cocospy и другие.

Шпионские клавиатуры - это специальные программы и устройства, которые по нажатию клавиш на клавиатуре переключаются на запись работы компьютера. Как и трекеры, шпионские клавиатуры делятся на два типа: аппаратные и программные.

[12]Комментарий к Уголовному кодексу Республики Таджикистан. Душанбе: Глобус, 2005. С. 400

Такие инструменты обычно называются Spyware, то есть вредоносной программой, которая собирает и передает информацию с устройств без согласия человека злоумышленнику.

Объективная сторона данного преступления выражается в:

а) Изготовление специальных программ;

б) Изготовление специального оборудования;

в) Сбыт специальных программ другому лицу;

г) Сбыт аппаратных средств другому лицу.

Изготовление указанного средства составляет объективную сторону рассматриваемого преступления только в том случае, если оно совершено с целью сбыта таких средств другому лицу.

Сбыт другому человеку означает продавать, дарить, обменивать, давать такие особые средства.

Эти действия могут быть квалифицированы по данной статье только в том случае, если они были совершены с целью получения неправомерного доступа к защищенной компьютерной системе или сети.

В противном случае, если такая цель не определена, действия лица по изготовлению и передаче другому лицу специальных программ и средств специальной техники должны квалифицироваться по статье 302 УК РТ[13].

Состав данного преступления носит формальный характер, то есть преступление считается оконченным с момента совершения одного из вышеуказанных действий.

Субъективная сторона этого преступления выражается в прямом умысле.

Субъект преступления - вменяемый человек, достигший 16-летнего возраста.

6. Разработка, использование и распространение вредоносных программ (статья 303).

УК РТ в статье 303 предусматривает уголовную ответственность за разработку компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, а также разработка специальных вирусных программ, заведомое их использование или распространение носителей с такими программами.

Общественная опасность этого преступления проявляется в том, что вредоносные программы могут в любой момент парализовать работу компьютерной системы или сети, что может иметь серьезные последствия.

Вредоносные программы являются предметом преступления. Вредоносное ПО - это программы, специально разработанные для нарушения нормальной работы компьютерных систем и программ.

Одна из самых распространенных форм вредоносного ПО - это вирусы. Компьютерные программы, которые распространяются независимо, размножаются и заряжают компьютерную систему, сеть или базу данных машин, появились на заре развития информационных технологий и называются вирусами.

---

[13] Комментарий к Уголовному кодексу Республики. Душанбе: Глобус, 2005. С. 400

«Компьютерные вирусы» - это тип программ, которые могут быть размножены до нескольких копий, изменять включенные в них программы и тем самым нарушать их нормальную работу.

Обычно каждый вирус после запуска выполняет разные операции.

В самом общем виде можно выделить основные операции, которые выполняют вирусы после взятия под контроль[14].

1. *Резидентные* вирусы после их активизации полностью или частично перемещаются из среды обитания (сеть, загрузочный сектор, файл) в оперативную память ЭВМ. Эти вирусы, используя, как правило, привилегированные режимы работы, разрешенные только операционной системе, заражают среду обитания и при выполнении определенных условий реализуют деструктивную функцию.
2. *Нерезидентные* вирусы попадают в оперативную память ЭВМ только на время их активности, в течение которого выполняют деструктивную функцию и функцию заражения. Затем вирусы полностью покидают оперативную память, оставаясь в среде обитания.
3. *Загрузочные* вирусы. От программных вирусов загрузочные вирусы отличаются методом распространения. Они поражают не программные файлы, а определенные системные области магнитных носителей. Кроме того, на включенном компьютере они могут временно располагаться в оперативной памяти.
4. *Макровирусы*. Когда макровирус активирован, он заражает шаблоны, по которым документы обрабатываются в текстовом редакторе. Например, при заражении шаблона Normal.dot заражаются все документы текстового процессора, которые были скомпилированы или отредактированы на данном компьютере.
5. *Сценарные* вирусы. Сценарные вирусы были задуманы как инструмент для сетевых администраторов для удаленного управления управляемыми компьютерами. Например, вирус-сценарий, содержащий сценарий для сервера WSH, может войти в компьютер через веб-страницу или электронную почту. Согласно командам скрипта, сервер компилирует вредоносный код и автоматически включает его запуск при запуске компьютера.
6. *Почтовые* вирусы. Сейчас, к сожалению, существует множество вирусов, которые легко могут проникнуть в компьютер. Для таких вирусов достаточно компьютера, подключенного к сети. После заражения компьютер становится источником заражения для других компьютеров в глобальной сети.
7. *Троян.* Троян относится к программе, которая обычно выдает себя за безобидную и очень важную программу. Как видите, само слово «троян» фактически произошло от словосочетания «троянский конь» в древнегреческой мифологии. Теперь это слово более тесно связано со словом «вирус». Трояны - это программы, которые выполняют серию невидимых, но

[14] Защита компьютерной информации антивирусной программой // https://allinweb.ru/informatika/26076/

вредоносных операций на компьютере. Например, они могут получать доступ к данным с одного компьютера на другой без разрешения (BackDoor). Также трояны могут отправлять необходимую информацию с компьютера жертвы на определенный адрес (Trojan.PSW).

8. *«Электронная бомба» (Емейл-бомба), (на анг.яз email-bomb)* - простой и невидимый метод кибератаки, суть которого заключается в нарушении нормальной работы электронной почты получателя путем отправки больших сообщений или сообщений в больших количествах на его электронную почту. Это один из вариантов DoS-атак, он может быть осуществлен путем отправки повторяющегося сообщения. Для тех, кто пользуется платными услугами, такая атака может увеличить их ценность.

Объективную сторону данного преступления составляют следующие деяния:
а) Разработка компьютерных программ. Концепция разработки вредоносных компьютерных программ состоит в том, чтобы записать свой текст (алгоритм) в виде последовательности логических команд, а затем перевести его на машиночитаемый язык, независимо от того, встроен он в память компьютера или нет.
б) внесение изменений в существующие программы. Внесение изменений в существующие приложения означает их изменение, то есть изменение текста программы путем удаления ее частей, замены их другими, а также текста программы. Изменение является наказуемым только в том случае, если нарушитель исправил программу на компьютере или каким-либо образом распространил исправленную программу. Исправление программы, представленной на бумаге, не является преступлением.
в) разработка специальных вирусных (вредоносных) программ. Под разработкой специальных зараженных вирусами программ для компьютера, записывающих свой текст (алгоритм), понимается последовательность логических команд, вне зависимости от того, встроены они в память компьютера или нет.
г) использование специальных вирусных программ. Использование специальной вирусной программы - это действие, направленное на введение таких программ в оборот, за исключением распространения ссылок ресурсов таких программ (это самостоятельное деяние, согласно статье 303 Уголовного кодекса РТ) или их преднамеренное использование против информации чужого компьютера. Известно, что распространение приложений без передачи их ссылок возможно только через компьютерную сеть - локальную, региональную и международную. Использование таких программ в личных целях, например, для уничтожения информации на вашем компьютере, не является преступлением.
д) распространение ресурсов с вредоносными программами - передача ссылок таких ресурсов третьим лицам за плату или безвозмездно, на постоянной или временной основе.

Состав преступления формальный и не требует наступления последствий и считается прекращенным с момента совершения одного из указанных действий.

Субъективная сторона преступления – прямой умысел.

Субъектом преступления может быть вменяемое физическое лицо, достигшее 16-летнего возраста.

Часть 2 ст. 303 УК РТ предусматривает отягчающий признак, повлекшее по неосторожности тяжкие последствия. Создавать вредоносные программы могут только высококвалифицированные программисты, которые в зависимости от уровня подготовки должны предвидеть последствия использования таких программ. Однако, уголовная ответственность предусмотрена ч. 2 ст. 303 УК РТ, если такие специалисты не предвидели возможности наступления общественно опасных последствий своего действия (бездействия), хотя при внимательности и дальновидности должно было и могло их предвидеть[15].

7. Нарушение правил эксплуатации компьютерной системы или сети (статья 304 УК РТ).

В ст. 304 УК РТ предусматривается уголовная ответственность за нарушение правил эксплуатации компьютерной системы, или сети лицом, имеющим доступ к этой системе или сети, если это повлекло по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования или причинение иного значительного ущерба.

Фактически, такое нарушение может выражаться в нарушении определенных правил безопасности оборудования или программного обеспечения компьютерной системы или сети. Например, использование запоминающих устройств без тестирования «вирусных» программ, несоблюдение последовательности операций, неправильное подключение периферийных устройств и так далее.

Как известно, диспозиция ч.1 преступления носит бланкетный характер. Правила эксплуатации компьютерных систем и сетей определяются нормативными правовыми актами других отраслей, разрабатываются и устанавливаются производителями технического оборудования, либо определяются владельцем этого технического оборудования. Поэтому всегда необходимо обращаться к этим правилам, чтобы определить, какие конкретные требования и какие нормативные акты, инструкции, правила использования были нарушены. Следует отметить, что согласно этой статье, наказуемо нарушение не всех правил работы с компьютером, а только технических.

Объективной стороной данного преступления является нарушение правил использования компьютерной системы или сети. Нарушение таких правил может быть совершено как путем действия, так и бездействия. Однако такое деяние считается преступлением, если оно имеет одно или несколько из следующих последствий:

а) уничтожение, блокирование, модификацию компьютерной информации;

б) нарушение работы компьютерного оборудования;

в) причинение значительного ущерба.

Субъективная сторона преступления вины неосторожность в форме самонадеянности и небрежности.

---

[15] Комментарий к Уголовному кодексу Республики Таджикистан. Душанбе: Глобус, 2005. С. 401

Субъект специальный - то есть человек, которому дано право доступа к такой системе или компьютерной сети. Поэтому на основании соответствующих документов (постановления, приказа) необходимо определить, обладает ли лицо такими полномочиями или нет.

Задачи

Граждане Д. Р., Дж. Дж. и П. По предварительному сговору арендовали комнату на проспекте Шерози в г.Душанбе и в течении майя-октября 2012 года незаконно установили техническое оборудование - системный блок и шесть USB-HUB с 58 модемами 3G, с помощью специального компьютерного программного обеспечения незаконно использовали систему компании «XXX» на общую сумму 1 000 000 сомони и 300 SIM-карт компании «EEE» на сумму 200 000 долларов США, тем самым нанесли ущерб в крупном размере указанным компаниям.

1. Оцените деяние этих людей?
2. Определить объект преступления?
3. По какой статье УК РТ квалифицируются данное деяние?

Тесты

№1. Укажите субъективную сторону нарушения правил эксплуатации компьютерной системы или сети:

А) Умышленно;
Б) Смешанный;
В) Прямой умысел;
Г) Неосторожность.

№2. Укажите состав разработки, использования и распространения вредоносных программ:

А) Материальный;
Б) Формальный;
В) Усеченный;
Г) Формально-материальный.

№3. Укажите субъект нарушения правил эксплуатации компьютерной системы или сети:

А) Должностное лицо;
Б) Государственный служащий;
В) Должностное лицо или лицо, занимающее государственные должности в Республике Таджикистан, либо руководитель органа местного самоуправления;
D) Лицо, которому предоставлено право доступа к подобной компьютерной системе или сети.

№4. Уничтожение машинных носителях это:

А) полное уничтожение или повреждение (без указания разрушения) любого типа машинной базы данных, что исключает извлечение данных, хранящихся в ней;

Б) частичное разрушение компьютера;

В) изменение текста программы, удаление ее части, замена их другими и текстом

Г) запись своего текста (алгоритма) в виде последовательности логических команд вне зависимости от того, введен он в память компьютера или нет.

№5. Субъектом компьютерного саботажа является:

А) вменяемое физическое лицо достигшее 14 лет;

Б) вменяемое физическое лицо достигшее 16 лет;

В) вменяемое физическое лицо достигшее 18-лет;

Г) вменяемое физическое лицо достигшее 14-16 лет.

№6. Защита информации это?

А) комплекс мер, направленных на предотвращение утечки, кражи, потери, несанкционированного уничтожения, неверного толкования, изменения, несанкционированного копирования и блокирования распространения информации;

Б) частичное разрушение компьютера;

В) изменении текста программы путем удаления его частей, замены их другими и текста программы;

Г) запись своего текста (алгоритма) в виде последовательности логических команд вне зависимости от того, введен он в память компьютера или нет.

№7. Уничтожение информации:

А) является умышленным действием, в результате которого доступность информации для юридического или физического лица прекращается полностью или частично;

Б) комплекс мер, направленных на предотвращение утечки, кражи, потери, несанкционированного уничтожения, неверного толкования, изменения, несанкционированного копирования и распространения информации;

В) частичное разрушение компьютера;

Г) изменение текста программы путем удаления его частей, замены их другими и текста программы.

№8. Блокировка информации - это:

А) принятие мер, ограничивающих или блокирующих доступ к компьютерной системе и предоставляемым ею информационным ресурсам;

Б) изменение информации, требующее разрешения автора или владельца информации;

В) умышленное или неосторожное действие, в результате которого доступность информации юридическому или физическому лицу прекращается полностью или частично;

Г) защита информации от умышленного или неосторожного действия злоумышленника.

№9. Изменение информации - это:

А) принятие мер, ограничивающих или блокирующих доступ к компьютерной системе и предоставляемым ею информационным ресурсам;

Б) изменение информации, требующее разрешения автора или владельца информации;

В) умышленное или неосторожное действие, в результате которого нарушается целостность информации;

Г) нарушение программ, базы данных, выдача искаженной отдельной информации, в том числе во время работы непрофильного и периферийного оборудования, либо нарушение нормальной работы сети.

№10. Вывод из строя компьютерного оборудования- это:

А) принятие мер, ограничивающих или блокирующих доступ к компьютерной системе и предоставляемым ею информационным ресурсам;

Б) изменение информации, требующее разрешения автора или владельца информации;

В) умышленное или неосторожное действие, в результате которого доступность информации юридическому или физическому лицу прекращается полностью или частично.

Г) нарушение программ, базы данных, выдача искаженной отдельной информации, в том числе во время работы непрофильного и периферийного оборудования, либо нарушение нормальной работы сети.

Вопросы для письменной работы:

1. Способы предотвращения киберпреступности;
2. Объективные элементы компьютерного уничтожения;
3. Субъективные элементы преступлений против информационной безопасности;
4. Информационная безопасность как объект преступления.

Вопросы для самотестирования:

1. Что такое киберпреступность?
2. Что является предметом преступлений в сфере информационной безопасности?
3. В каких действиях отражается объективный аспект разработки, использования и распространения вредоносных программ?
4. Предоставьте информацию о субъекте преступлений против информационной безопасности
5. Что такое вирус?
6. Что такое компьютерная сеть?
7. Как вы понимаете уничтожение компьютерной информации?
8. Что такое взлом компьютеров?
9. Что имеется в виду под изменением компьютерной информации?

Литература:

1. Jody R. Westby. Laws on Crimes against Computer Systems // International Guide to Combating Cybercrime. -- ABA Publishing, 2003.
2. Megan McAuliffe «Australian hackers face jail time». - ZDNet Australia, 09.04.01;
3. David Adams «Momentum grows for e-crime center». - Fairfax. IT, 28.03.01.
Thomas J Holt,Adam M Bossler,Kathryn C Seigfried-Spellar. Legal challenges in dealing with malware // Cybercrime and Digital Forensics: An Introduction. New York: Routledge, 2015.
4. Андреев Б.В., Пак П.Н., Хорст В.П. Расследование преступлений в сфере компьютерной информации. - М.: Юрлитинформ, 2001. - 152с.
5. Беляев Е.В. Типы личности «компьютерного преступника» / Е.В. Беляев // Законодательство и экономика. - № 5. - 2014. - С.74-77.
6. Волеводз А. Международная взаимопомощь при расследовании компьютерных преступлений (анализ международно-правовых документов) // Вопросы правоведения. Межвузовский сборник научных трудов. № 4. - Ереван: Изд-во Ереван. ун-та, 2001. - С.11-26.
7. Гаврилов М.В. Противодействие преступлениям, совершаемым в сфере компьютерной информации. - М.: Юрлитинформ, 2007. - 188 с.
8. Дворецкий М.Ю. Преступления в сфере компьютерной информации. Научно-практический комментарий к главе 28 Уголовного кодекса Российской Федерации. - Тамбов, 2015. - 474с.
9. Евдокимов К.Н. Актуальные вопросы предупреждения преступлений в сфере компьютерной информации в Российской Федерации // Академический юридический журнал. - № 1 (59). - 2015. - С.21-31.
10. Зинина У.В. Международное сотрудничество в сфере борьбы с компьютерными преступлениями // Право и безопасность. - № 3. -2005. - С.92-99.
11. Иванов В.П. Защита от электронного шпионажа // Сети и системы связи. - 2006. - №3. - С.110-111.
12. Калиниченко И.А., Коробов А.А. и др. Теоретические основы противодействия неправомерному доступу в сфере информационных технологий. Под общ. ред.: Калиниченко И.А. - Орел, 2013. - 179с.
13. Косынкин А.А., Подольный Н.А. Преодоление противодействия расследованию преступлений в сфере компьютерной информации: - Москва: Юрлитинформ, 2013. - 216с.
14. Крылов В.В. Информационные компьютерные преступления. - М.: Инфра-М-Норма, 2007. - 285с.
15. Сизов А.В. Причины и условия совершения преступлений в сфере компьютерной информации // Информационное право. - № 2. - 2008. - С.38-41.
Степанов-Егиянц В.Г. Криминологическая характеристика личности компьютерного преступника // Российский следователь. - № 19. - 2014. - С.41-44.
16. Федоров В. Компьютерные преступления: выявление, расследование и профилактика // Законность. - № 6. - 2004. - С.44-47.

17. Халиуллин А.И. Место совершения преступления как признак состава преступления в сфере компьютерной информации // Актуальные проблемы экономики и права. - № 1 (21). - 2012. - С.291-294.
18. Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. - 2014. - № 2. - С. 37 - 44.
19. Комиссаров В.С. Преступления в сфере компьютерной информации: понятие и ответственность. – Юридический мир. 1998. № 2. С.9-19.