

Предпосылки совершенствования уголовного законодательства в сфере защиты информационных объектов

Общеизвестно, что информация выступает как средство знакомства с миром, удовлетворения естественных потребностей, совершения для этого необходимых действий, в процессе общения людей между собой появляется язык, информационные механизмы становятся сложнее. Информационных потоков становится больше, происходит обмен информацией. При этом язык представляет собой чисто информационное средство, предназначенное для передачи информации от одного человека другому. Можно сказать, что язык - первый относительно обособленный информационный элемент в человеческом общении, но он появляется и развивается как средство общения. Современный период развития общества определяется повышением значимости информации как правовой категории и ее проникновением во все сферы общественной жизни.

Право на информацию только на конституционном уровне рассматривается более чем в двадцати конституционно-правовых установлениях, а на более широком - законодательном уровне, по оценкам специалистов, в этот институт входят нормы свыше трех десятков законодательных актов. Существующая система информационных отношений предполагает взаимосвязь между информацией и информационной сферой в целом. При этом стержневым системообразующим фактором для самой информационной сферы, в которой в настоящее время появляются новые субъекты отношений, является информация как явление¹. При этом определено, что информация является главным объектом интереса человека на протяжении развития и существования нашего общества.

¹ Бачило И. Л. Информационное право. Роль и место в системе права Российской Федерации // Государство и право, 2005, № 2. С. 13.

Многообразие форм существования информации в современном мире в условиях внедрения высокопроизводительных средств обработки информации определяет и множественность граней ее существования, свойств и признаков. Информация может быть представлена как сообщение, зафиксированное в традиционной для восприятия человека форме, а может быть представлена форме только образа того предмета, которое отражает информация. Высокотехнологичные средства формирования, хранения и использования информации могут преобразовать ее в символическом виде, который человек не воспринимает сенсорными средствами, наделенными его природой. Для того чтобы распознать информацию, необходимые вспомогательные средства «переводят» ее вновь в воспринимаемую форму. Таковы формы электронной информации. Названные вспомогательные средства являются также многообразной системой, которую принято называть информационной системой.

Само понятие информации, выступая в качестве центрального в ряде естественнонаучных отраслей знания, продолжает оставаться одним из наиболее спорных и противоречивых. Оно стало привлекать к себе особое внимание в начале XX века в результате совершенствования теории связи и возрастания роли обмена различными сведениями в общественной жизни и деятельности. Первые попытки уточнить понятие информации восходят к работам Р. Фишера 1921 г. (вероятностная концепция) и Р. Хартли 1928 г. (логарифмическая мера количества информации), которые предвосхитили появление классической статистической теории связи Н. Винера — К. Шеннона 1948 г. (количество информации как мера уменьшения неопределенности)².

² Fisher. Sir Ronald. *Statistical Methods for Research Workers*, Oliver & Boyd, Ltd, London. 1925; Hartley R.V.L. «Transmission of information». *Bell System Tech. V.*, 7. 1928; *Теории информации и ее приложения* / под ред. А. А. Харкевича. М., 1949; Шеннон К. *Работы по теории информации и кибернетики*. М., 1963; Винер И. *Кибернетика*. М., 1958

Учитывая изложенное в настоящее время происходит становление особой отрасли права, определяемой как информационное право, предметом познания которого выступают все формы существования информации, закономерности природы, все многообразие вспомогательных средств (информационная система или инфраструктура) распознавание информации, а также все виды человеческой деятельности по поводу поиска, производству, обработке, хранению, передачи и использованию информации.

Концептуальное поле информационного права отличается состоянием первоначальной рефлексии и обустройства основных проблем, перед правовым обеспечением предметной сферы, т.е. общественных отношений, складывающихся по поводу производства и использования информационных объектов и систем в целях удовлетворения информационных потребностей личности, общества и государства.

Следует иметь в виду, что информационное право России как самостоятельная отрасль права активно развивается в течение незначительного отрезка времени, во многом отставая от развития данной отрасли права за рубежом.³ При этом можно утверждать, что взаимосвязь между информационным и иными отраслями права (в частности – с уголовным правом) еще окончательно не сложилась. Так, первые попытки выделить информационный объект в качестве видового объекта преступления Главы 28 Уголовного кодекса Российской Федерации можно отнести к 1996 году, когда российский законодатель, исходя из новых экономических, политических и социальных отношений, складывающихся в обществе, с учетом международных правовых норм и стандартов, а также в соответствии с настоятельной потребностью в усилении борьбы с преступностью, впервые принял ряд уголовно-правовых норм о преступлениях в сфере компьютерной информации. Однако за время действия уголовного закона обнаружилось немало изъянов, в

³ Законотворчество в Российской Федерации (научно-практическое и учебное пособие) /Под ред. А.С.Пиголкина. М., 2000. С. 10, 234.

том числе и юридико-технического плана, в нормах о преступлениях в сфере компьютерной информации. Анализ состояния информационной безопасности Российской Федерации показал, «что ее уровень не в полной мере соответствует потребностям общества и государства».⁴

Конечно, при возникновении новых общественных отношений первое время они законом не защищаются. Но достаточно быстро общество осознает необходимость защиты новых прав, особенно в тех случаях, когда указанные отношения приобретают особую общественную значимость, возникает необходимость в их государственно – правовом регулировании. На первых порах в практической деятельности осуществляются попытки правоприменения существующих нормативных актов. Иногда это удается, а порой возникают забавные или трагические казусы. Новейшая история показывает, что от момента возникновения нового общественного отношения до момента, когда возникнет более-менее единообразная юридическая практика его защиты, проходит от 5 до 8 лет.

Следует также иметь в виду, что в области информационных отношений, которые только что возникли или возникнут в ближайшие годы как результат высоких технологий, уже возникли или в ближайшее время возникнут следующие:

- отношения по поводу прав на доменные имена и, возможно, некоторые другие средства индивидуализации в глобальных сетях;
- отношения по поводу виртуальных предметов, персонажей, недвижимости и иных активов, существующих в виртуальных мирах;
- отношения по поводу рекламных возможностей и иного влияния на людей различных сетевых ресурсов - веб-сайтов, блогов, сетевых сервисов, поисковых систем и т.п.;
- отношения по поводу прав интеллектуальной собственности на результаты работы отдельных программ и комплексов программ, в том числе комплексов независимых друг от друга программ;

⁴ Концепция развития законодательства Российской Федерации в сфере информации и информатизации // <http://www.isn.ru/zakon/concept.htm>.

- отношения по поводу новых видов использования интеллектуальной собственности.

- отношения по поводу технических стандартов, форматов и протоколов, которые формально являются добровольными, но фактически обязательны для всех и вследствие этого служат механизмом недобросовестной конкуренции и т.д.

Таким образом, в настоящее время остро встает вопрос о необходимости правовой защиты в сфере обращения информации. При том обстоятельстве, что наше общество горячо принимает и поддерживает саму идею указанной защиты, практическая деятельность в данной сфере осуществляется сравнительно медленными темпами, в настоящее время сложилась ситуация, когда проблема недостаточной защищенности информации поднимается не только специалистами в области информационного права, но и иными участниками гражданского общества.⁵

Между тем, можно сказать, что домашний пользователь на широком канале - это массовое явление, в том числе и в нашей стране.⁶ При этом широкополосный доступ выглядит крайне привлекательно, с точки зрения киберпреступников. Домашние пользователи не в состоянии защитить свои компьютеры от внедрения вредоносных программ, в отличие от корпоративных компьютеров, здесь отсутствуют какие-либо дополнительные средства защиты информации - сервера доступа с трансляцией адресов, межсетевые экраны, системы обнаружения атак. Можно быть уверенным, что из нескольких миллионов таких компьютеров несколько десятков тысяч (на основе которых формируются зомби – сети) наверняка обладают значительной уязвимостью.

Персональные компьютеры, обслуживаемые неквалифицированными пользователями и подключенные к широкополосным линиям связи, будут в

⁵ Федотов Н.Н. Форензика – компьютерная криминалистика. М., 2007. С. 50

⁶ Дешевый широкополосный доступ в Интернет для частных (домашних) пользователей начал предоставляться в массовых масштабах в развитых странах в 2000-2001 годах. Чуть позже такой доступ появился в других странах. В России широкополосный доступ для домашних пользователей приобрел массовый характер в Москве уже с 2005 года, а в областных центрах внедрен в 2008-2009 годах.

дальнейшем только множиться. Значит, на этом ресурсе будут основаны многие технологии злоумышленников - рассылка спама, DoS-атаки, хостинг нелегальных материалов, методы анонимизации, хищение персональных данных и т.п.

Поскольку услуги связи постоянно дешевеют, внедряются новые, более производительные технологии и протоколы (например, Wi-Max), а тарифы используются преимущественно безлимитные, то пользователи не очень заинтересованы заботиться о защищенности своих компьютеров. В аналогичной ситуации находится интернет-провайдер зараженного пользователя: При этом провайдеры и пользователи не несут прямых убытков, когда вредоносные программы функционируют в сети, однако заинтересованы, чтобы в сетях иных провайдеров вредоносных программ не было. Указанные обстоятельства создают основу для заключения многосторонних соглашений между операторами связи или объединения их под эгидой государства для совместной борьбы, взаимодействия и оказания взаимной помощи. Например, из событий последних двух лет стоит отметить появление объединения операторов «Networks Fingerprint Sharing Alliance» для борьбы с DoS-атаками на основе продукта «Arbor Peakflow».

В то же время компьютерные технологии сделали необычайно легким отчуждение произведения от его носителя. Копирование и передача объектов интеллектуальной собственности в цифровой форме имеют ничтожную себестоимость и доступны практически всем. При этом следует иметь в виду, что повышение роли интеллектуальной собственности выражается в увеличении доли нематериальных вложений в стоимости почти всех видов продукции. От величины этой стоимости существенным образом зависит стабильность экономики государств, где расположены крупнейшие правообладатели и производители «творческой» продукции. Размер стоимости авторских и патентных прав в товарообороте развитых стран таков, что сильные колебания этой стоимости могут привести к краху экономики. А стоимость интеллектуальной собственности поддерживается соответствующим законодательством и практическими мерами по его исполнению — то есть не рыночным, а административным механизмом.

Понятно, что государство придает большое значение поддержанию стоимости нематериальных активов. Установление выгодных правил в области торговли интеллектуальной собственностью - одна из приоритетных задач внешней политики развитых стран, в связи с чем следует ожидать усиления борьбы с нарушениями авторских прав, патентных прав, прав на товарные знаки и иных прав интеллектуальной собственности на цифровой контент. Круг преступных деяний, скорее всего, расширится, поскольку, когда затруднительно пресекать сами нарушения (воспроизведение, например), пытаются запрещать то, что способствует таким нарушениям (например, файлообменные сети). Соответственно будут ужесточаться и наказания за соответствующие нарушения.

В настоящее время специалистами в области защиты информации определен ряд обстоятельств, способствующих совершению преступлений в области высоких технологий, к которым относятся следующие⁷:

- не разработаны положения о защите информации, или они не соблюдаются, и не назначен ответственный за информационную безопасность. Пароли пишутся на компьютерных терминалах, помещаются в общедоступные места, ими делятся с другими, или они появляются на дисплее во время ввода;

- удалённые терминалы и компьютеры оставляются без присмотра в рабочие и нерабочие часы, данные отображаются на дисплеях, оставленных без присмотра;

- не существует ограничений на доступ к информации или на характер её использования, все пользователи имеют доступ ко всей информации и могут использовать все функции системы;

- не ведутся системные журналы, и не хранится информация о том, кто, когда, как и в каких целях использует компьютер;

⁷ Федотов, Н.Н. Форензика – компьютерная криминалистика, М., 2007, С. 132

- отсутствует документация, или она не позволяет понимать получаемые отчёты и формулы, по которым рассчитываются результаты, модифицировать программы, готовить данные для ввода, исправлять ошибки, производить оценку мер защиты и понимать сами данные - их источники, формат хранения, взаимосвязи между ними;

- делаются многочисленные попытки войти в систему с неправильными паролями;

- вводимые данные не проверяются на корректность и точность, или при их проверке много данных отвергается из-за ошибок в них, требуется делать много исправлений в данных, не ведутся записи в журналах об отвергнутых транзакциях;

- имеют место приносящие большие убытки случаи выхода системы из строя;

- не производится анализ информации, обрабатываемой в компьютере, с целью определения необходимого для неё уровня безопасности;

- мало внимания уделяется информационной безопасности, и, хотя политика безопасности существует, большинство пользователей считает, что на самом деле она не нужна;

- изменения в компьютерные программы вносятся без предварительного уведомления и утверждения руководством;

- изменения в аппаратные средства вносятся без предварительного уведомления и утверждения руководством;

- не применяются, неправильно подобраны и установлены (или установлены устаревшие) программные средства защиты;

- не применяются, неправильно выбраны и установлены (или установлены устаревшие) аппаратные средства защиты прослушивать даже армированные бетонные и кирпичные стены около метра толщиной. Специальная техника может снимать информацию на значительном расстоянии от объекта, улавливая акустические, электромагнитные и другие

излучения, передаваемые в окружающую среду строительными конструкциями зданий и сооружений, с помощью лазерных устройств можно без особых проблем получить необходимые данные через стёкла окон;

- существуют специальные устройства, способные давать точное изображение людей и отчётливую запись конфиденциальных переговоров, ведущихся за закрытыми окнами с металлическими решётками на них и плотно задёрнутыми шторами. Практически во всём мире в поте лица трудятся целые артели «Кулибиных», способных поставить и ставящих на поток производство фальшивых CD-ROM и электронных карточек, качество которых если и не выше, то и не ниже настоящих.

По всей видимости, особая значимость указанной проблемы в нашей стране была определена еще в 2000 году, поскольку с принятием Доктрины информационной безопасности⁸ остро встает вопрос об уголовном нормотворчестве в указанной сфере, определяемый объективными, общепризнанными критериями социальной ценности информации (информационного объекта, информационной безопасности) как объекта преступления. Степень защищенности или повреждаемости указанного объекта определяет потенциальные последствия преступления. Они проявляются в возможном изменении к худшему общего состояния и параметров информационной безопасности, характером причиненного ущерба и потребностью информационных объектов в уголовно – правовой защите.

В настоящее время все более очевидным становится факт, что ныне действующее уголовное законодательство не позволяет эффективно бороться с преступлениями в сфере защиты информационных объектов (обеспечения информационной безопасности), поскольку существующее информационное

⁸ Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. N Пр-1895

законодательство России «не свободно от недостатков⁹, во многом декларативно и противоречиво»¹⁰.

Между тем, эффективность деятельности правоохранительных органов во многом зависит от того, насколько четко, с соблюдением существующих принципов технико-юридического конструирования формулируются в уголовном праве РФ нормы, предусматривающие ответственность за совершение преступлений. В этой связи решение практических проблем противодействия преступности невозможно без глубокой проработки теоретических вопросов законодательной техники построения уголовно-правовых норм о преступлениях в сфере компьютерной информации, внесения ряда существенных изменений и дополнений в законодательство, регулирующее информационные отношения.

Наиболее концептуальные положения, связанные с охраной информации закреплены в нормах Федерального закона «Об информации, информационных технологиях и о защите информации» N 149-ФЗ от 27 июля 2006 года. Так, ст. 16 указанного Федерального Закона в качестве мер обеспечения защиты информации предусматривает принятие правовых, организационных и технических мер, направленных на обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации; соблюдение конфиденциальности информации ограниченного доступа и - реализацию права на доступ к информации. При этом определено, что государственное регулирование отношений в сфере защиты информации осуществляется путем установления требований о защите информации, а также

⁹ Крылов В.В. Основы криминалистической теории расследования преступлений в сфере информации: Дис...д-ра юрид. наук. М., 1998. С. 13; Воробьев В.В. Преступления в сфере компьютерной информации (юридическая характеристика составов и квалификация): Дис...канд. юрид. наук. Н.Новгород, 2000. С. 5; Ушаков С.Н. Преступления в сфере обращения компьютерной информации (теория, законодательство, практика): Дис...канд. юрид. наук. Ростов-на-Дону. 2000. С.

¹⁰ Лопатин В.Н. Информационная безопасность России: Человек. Общество. Государство. СПб. 2000. С. 132, 139.

ответственности за нарушение законодательства Российской Федерации об информации, информационных технологиях и о защите информации.

Значимость государственного регулирования в данной сфере в настоящее время определяется также и тем обстоятельством, что Указом Президента от 12 мая 2009 года Российской Федерации утверждена Стратегия национальной безопасности Российской Федерации до 2020 года, представляющая собой официально признанную систему целей и мер в области внутренней и внешней политики, определяющую состояние национальной безопасности, уровень устойчивого развития государства на долгосрочную перспективу, а также стратегические национальные приоритеты создания безопасных условий реализации конституционных прав и свобод граждан Российской Федерации, осуществления устойчивого развития страны, сохранения территориальной целостности и суверенитета государства.

При этом положениями Раздела 2¹¹ настоящей Стратегии определяется круг задач, направленных на обеспечение национальной безопасности в сфере государственной и общественной безопасности исходя из необходимости постоянного совершенствования правоохранительных мер по выявлению, предупреждению, пресечению и раскрытию актов терроризма, экстремизма, других преступных посягательств на права и свободы человека и гражданина, собственность, общественный порядок и общественную безопасность, конституционный строй Российской Федерации. При этом главными направлениями государственной политики в сфере обеспечения государственной и общественной безопасности на долгосрочную перспективу должны стать, помимо прочего, также и совершенствование нормативного правового регулирования предупреждения и борьбы с преступностью.

¹¹ П.п.37-39 Раздела 2 Указа Президента Российской Федерации № 537 от 12 мая 2009 года «О стратегии национальной безопасности Российской Федерации до 2020 года»

При этом, несомненно, следует соотносить положения указанного Раздела 2 Стратегии национальной безопасности в соотнесении с положениями Раздела 6 того же нормативного акта, определяющего стратегические цели обеспечения национальной безопасности в сфере науки, технологий и образования. Следует также иметь в виду, что в числе прочих мер противодействия угрозам в сфере науки, технологий и образования силам обеспечения национальной безопасности во взаимодействии с институтами гражданского общества надлежит обеспечить эффективность государственно-правового регулирования в области интеграции науки, образования и высокотехнологичной промышленности, а "средствами обеспечения национальной безопасности" определены в том числе и правовые средства.

Что характерно, указанная Стратегия национальной безопасности во многом перекликается с положениями Стратегии развития информационного общества в Российской Федерации¹² предусматривающей меры противодействия использованию потенциала информационных и телекоммуникационных технологий в целях угрозы национальным интересам России, к которым относит: обеспечение безопасности функционирования информационно-телекоммуникационной инфраструктуры; обеспечение безопасности функционирования информационных и телекоммуникационных систем ключевых объектов инфраструктуры Российской Федерации, в том числе критических объектов и объектов повышенной опасности; повышение уровня защищенности корпоративных и индивидуальных информационных систем; создание единой системы информационно-телекоммуникационного обеспечения нужд государственного управления, обороны страны, национальной безопасности и правопорядка; совершенствование правоприменительной практики в

¹² Стратегия развития информационного общества в Российской Федерации утверждена Президентом Российской Федерации 07 февраля 2008 года № Пр -212

области противодействия угрозам использования информационных и телекоммуникационных технологий во враждебных целях; обеспечение неприкосновенности частной жизни, личной и семейной тайны, соблюдение требований по обеспечению безопасности информации ограниченного доступа.

Следует иметь в виду, что в Доктрине информационной безопасности определен круг общественных отношений определенных действующим законодательством и требующих наиболее пристального внимания со стороны государственных правовых институтов, наиболее остро нуждающихся в обеспечении государственно – правовой охраны, в том числе и уголовно – правовыми средствами.

К сожалению, существующая в настоящее время система уголовно – правовой защиты информационных объектов, позволяет определить указанные объекты как предмет преступления и, мягко говоря, не отличается достаточной системностью и работоспособностью. При этом все многообразие информационных объектов, защита которых осуществляется нормами действующего уголовного законодательства, раскрываемые лишь через категорию предмета преступления, можно свести к следующим: информация, зафиксированная на материальных носителях; информация ограниченного доступа, подразделяемая на сведения, содержащие государственную тайну (ст.ст. 275, 276, 283, 284 УКРФ) и сведения конфиденциального характера (соотносимые с Перечнем сведений конфиденциального характера, определенным Указом Президента Российской Федерации № 188); информационные объекты, образующие предмет преступления (информационный объект, образующий заведомые знания субъекта преступления в части личностного отношения лица, как к потерпевшему, так и к предмету преступления; применение угроз; обращение вредоносной информации, к которой относится информация, подрывающая основы морали, нравственности и правопорядка в обществе;

информация, унижающая человеческое достоинство; ложная, фальсифицированная информация; распространение информации, направленной на осуществление противоправного информационного воздействия; информацию, способствующую совершению преступлений.¹³

Что самое интересное, в существующем уголовном законодательстве сложилась такая ситуация, когда при значительном количестве информационных объектов как предметов уголовно – правовой охраны, имеет место отсутствие системного подхода к охране общественных отношений в данной сфере и, как следствие, проявляется невозможность формирования научного подхода к вопросам уголовно – правовой охраны информационных объектов.

Так, например, проведенное Суловой С.И. исследование показало, что в случаях нарушения правил обращения с информацией с ограниченным доступом, уголовная ответственность может наступить лишь для 12 из 40 видов указанной категории информационных объектов, а административная ответственность может наступать только в одном случае, что свидетельствует декларативность действующих законов в области защиты информационных объектов и делает маловероятным реализуемость данных законов¹⁴.

Существующее строение Особенной части Уголовного кодекса позволяет использовать правоотношения по поводу информационного объекта (объекта информационной безопасности) для обоснованного и четкого построения системы родового и видовых объектов по характеристике угроз, поскольку Доктрина информационной безопасности Российской Федерации определяет виды угроз информационной безопасности по общей направленности, раскрывая содержание каждой из них.

¹³ Елин В.М. Информационный объект как предмет уголовно –правовой охраны\\ Конфликты в информационной сфере. Материалы теоретического семинара Сектора информационного права ИГП РАН 2008.М..2009.С.127-146

¹⁴ Сулова С.И. Тайна в праве России: цивилистический аспект. Дисс.канд.юрид.наук.Иркутск.2003.С. 64

Разрешая вопрос о необходимости отнесения правоотношений по поводу информационных объектов (объектов информационной безопасности) к самостоятельной группе объектов уголовно правовой охраны следует иметь в виду, что указанное выделение информационного объекта в определенную группу ценностей, подлежащих уголовно – правовой охране, на которые могут быть совершены преступные посягательства основано на том обстоятельстве, что информационные объекты, как и все охраняемые и, соответственно, входящие в общий объект преступления социальные феномены, социальные блага, общественные отношения имеют не только общие свойства, порождающие необходимость в уголовно-правовой их охране, но также и имеют такие особенности, которые позволяют сводить их в отдельные группы и тем самым разграничивать друг от друга на основе различающих их признаков.

При этом следует учитывать то обстоятельство, что в работах по Общей части уголовного права объект преступления иногда определяется как то, на что посягает субъект преступления, чему преступлением причинен или может быть причинен определенный вред¹⁵. При этом на протяжении длительного периода, начиная едва ли не с появления первых советских уголовных законов, существовало единодушное мнение, что преступление посягает на внешние для него общественные отношения, которые и являются его объектом¹⁶.

Следует иметь в виду, что правоотношения в информационной сфере как объект преступления в настоящее время могут рассматриваться как часть действительности, имеющая определенные материальные либо нематериальные формы, границы, состояния, закономерности

¹⁵ Историю развития уголовно-правовых воззрений по этой проблеме см.: *Таганцев Н.С.* Русское уголовное право. Лекции. Т. 1. Спб., 1902. С. 484. и сл. (Многие положения исторического характера, к сожалению, отсутствуют в изд. лекций Н.С. Таганцева 1994 г.)

¹⁶ *Тацый В.Я.* Объект и предмет преступления в советском уголовном праве. Харьков, 1988.

существования, наконец, ценность, что соотносит его с существующим материально – формальным определением преступления, предусмотренного ч. 1 ст. 14 УК РФ.

Выделение информационного объекта (объекта информационной безопасности) в категорию родового (видового) объекта преступления позволяет охарактеризовать отдельные свойства информационного объекта как элемента состава преступления: ценность, степень защищенности (повреждаемость), интенсивность потребности в защите имеют конкретные проявления и степень выраженности, поскольку:

- потребность информационного объекта в уголовно-правовой защите отражает ценность информационного объекта — его поврежденность (нарушенность) и парадоксальным образом — возможность защиты

- социальная ценность информации как объекта преступления в самом общем виде оправдывает применение уголовного наказания к посягающим на нее лицам и отражает невозможность общества обходиться без нее;

- степень защищенности или повреждаемости информационного объекта определяет потенциальные последствия преступления в информационной сфере, которые могут проявляться в возможности: а) изменить к худшему общее состояние и параметры информации; б) полностью ликвидировать одну из составных частей информационного объекта или сам информационный объект в его индивидуальном предметном выражении;

- глубина повреждения информационного объекта может измеряться характером нанесенного ему ущерба, возможностью и стоимостью восстановления объекта, влиянием изменений в состоянии объекта на иные стороны действительности, что в полной мере отвечает совокупным требованиям, предъявляемым к объекту преступления.¹⁷

¹⁷ См., например, Уголовное право. Учебник. Под общ.ред. Л. Д. Гаухмана, С.В. Максимова и Л.М. Колодкина, М., 1999.С. 63-66, Уголовное право Российской Федерации. Общая часть: Учебник // Под ред.

Выделение информационных отношений в самостоятельную категорию охраняемых нормами уголовного права объектов преступления позволяет указать на более высокую социальную ценность информационного объекта, в практическом плане этим можно обосновать возможность применения мер уголовно – правового воздействия в отношении лиц, совершающих неправомерные воздействия в отношении объектов информационной безопасности; выделить признаки информационных объектов как различных объектов преступного посягательства, произведя их тщательное разграничение как по категории социальной значимости, так и по категории общественной опасности, отграничив различные деяния в указанной сфере. Иначе говоря, указанное выделение с одной стороны позволяет продемонстрировать сравнительную социальную ценность информационного объекта как группы благ, охраняемых уголовным законом, включая степень потребности в их уголовно-правовой охране, с другой стороны - свойства информационных объектов как охраняемых благ, программирующих возможные способы наказуемого уголовно-правового поведения, а также выделить признаки, позволяющие описать определяемые содержанием родового объекта способы преступного посягательства, а также позволит использовать свойства информации, информационного объекта, либо информационной безопасности как родового объекта для обоснованного и четкого построения системы родового и видовых объектов по характеристике угроз, поскольку Доктрина информационной безопасности Российской Федерации определяет виды угроз информационной безопасности по общей направленности и раскрывая содержание каждой из них.

Таким образом, на основании положений Доктрины, можно сделать вывод о целесообразности дополнения родовых объектов

составов преступлений дополнительным родовым объектом – общественными отношениями в сфере защиты информационных объектов (обеспечения информационной безопасности). Преступления в сфере информационной безопасности подлежат разделению на четыре категории преступлений, создающих соответствующие видовые объекты и определяющиеся соответствующей группой угроз информационной безопасности:

-преступления в сфере конституционных прав и свобод человека и гражданина в области духовной жизни и информационной деятельности;

- преступления в сфере обеспечения государственной политики Российской Федерации;

- преступления в сфере развития отечественной индустрии информации;

- преступления в сфере безопасности информационных и телекоммуникационных средств и систем;

С учетом изложенного к дальнейшей разработке могут быть предложены отдельные составы преступлений по каждому из видовых объектов.

Преступления в сфере конституционных прав и свобод человека и гражданина в области духовной жизни и информационной деятельности могли бы включать в себя следующие деяния:

- принятие руководителями федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации нормативных правовых актов, ущемляющих конституционные права и свободы граждан в области духовной жизни и информационной деятельности;

- неисполнение руководителями федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, организаций и гражданами требований

федерального законодательства, регулирующего отношения в информационной сфере;

- нерациональное, чрезмерное ограничение доступа к общественно необходимой информации, неправомерное ограничение доступа граждан к открытым информационным ресурсам федеральных органов государственной власти, органов государственной власти субъектов Российской Федерации, органов местного самоуправления, к открытым архивным материалам, к другой открытой социально значимой информации;

- создание монополий на формирование, получение и распространение информации в Российской Федерации, в том числе с использованием телекоммуникационных систем, нарушение конституционных прав и свобод человека и гражданина в области массовой информации;

- вытеснение российских информационных агентств, средств массовой информации с внутреннего информационного рынка и усиление зависимости духовной, экономической и политической сфер общественной жизни России от зарубежных информационных структур;

- противодействие реализации гражданами своих конституционных прав на личную и семейную тайну, тайну переписки, телефонных переговоров и иных сообщений;

- противоправное применение специальных средств воздействия на индивидуальное, групповое и общественное сознание, манипулирование информацией (дезинформацию, сокрытие или искажение информации);

- девальвацию духовных ценностей, пропаганду образцов массовой культуры, основанных на культе насилия, на духовных и нравственных ценностях, противоречащих ценностям, принятым в российском обществе, дезорганизацию и разрушение системы накопления и сохранения культурных ценностей, включая архивы;

- снижение духовного, нравственного и творческого потенциала населения России, что существенно осложнит подготовку трудовых ресурсов

для внедрения и использования новейших технологий, в том числе информационных.

Преступления в сфере обеспечения государственной политики Российской Федерации могут определяться следующими составами:

- монополизация информационного рынка России, его отдельных секторов отечественными и зарубежными информационными структурами;
- блокирование деятельности государственных средств массовой информации по информированию российской и зарубежной аудитории;
- снижение эффективности информационного обеспечения государственной политики Российской Федерации вследствие дефицита квалифицированных кадров, отсутствия системы формирования и реализации государственной информационной политики.

Преступления в сфере развития отечественной индустрии информации определяются категориями угроз развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в ее продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов и могут включать в себя:

- противодействие доступу Российской Федерации к новейшим информационным технологиям;
- противодействие взаимовыгодному и равноправному участию российских производителей в мировом разделении труда в индустрии информационных услуг, средств информатизации, телекоммуникации и связи, информационных продуктов;
- создание условий для усиления технологической зависимости России в области современных информационных технологий;
- закупка руководителями органов государственной власти импортных средств информатизации, телекоммуникации и связи при наличии

отечественных аналогов, не уступающих по своим характеристикам зарубежным образцам;

- деятельность, направленная на вытеснение с отечественного рынка российских производителей средств информатизации, телекоммуникации и связи;

- деятельность, направленная на увеличение оттока за рубеж специалистов и правообладателей интеллектуальной собственности.

Преступления в сфере безопасности информационных и телекоммуникационных средств и систем определяются угрозами безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории России, могут включать в себя:

- противоправные сбор и использование информации;
- нарушения технологии обработки информации;
- внедрение в аппаратные и программные изделия компонентов, реализующих функции, не предусмотренные документацией на эти изделия;
- разработка и распространение программ, нарушающих нормальное функционирование информационных и информационно-телекоммуникационных систем, в том числе систем защиты информации;
- уничтожение, повреждение, радиоэлектронное подавление или разрушение средств и систем обработки информации, телекоммуникации и связи;
- воздействие на парольно-ключевые системы защиты автоматизированных систем обработки и передачи информации;
- компрометация ключей и средств криптографической защиты информации;
- деятельность, направленную на осуществление утечек информации по техническим каналам;

- внедрение электронных устройств для перехвата информации в технические средства обработки, хранения и передачи информации по каналам связи, а также в служебные помещения органов государственной власти, предприятий, учреждений и организаций независимо от формы собственности;

- уничтожение, повреждение, разрушение или хищение машинных и других носителей информации;

- перехват информации в сетях передачи данных и на линиях связи, дешифрование этой информации и навязывание ложной информации;

- использование несертифицированных отечественных и зарубежных информационных технологий, средств защиты информации, средств информатизации, телекоммуникации и связи при создании и развитии российской информационной инфраструктуры;

- несанкционированный доступ к информации, находящейся в банках и базах данных;

- нарушение законных ограничений на распространение информации.

Таким образом, предлагаемый раздел Особенной части Уголовного кодекса Российской Федерации «Преступления в сфере информационной безопасности» может включать в себя 4 главы, отнесенные соответственно к преступлениям в сфере:

- конституционных прав и свобод человека и гражданина в области духовной жизни и информационной деятельности;

- информационного обеспечения государственной политики Российской Федерации;

- развития отечественной индустрии информации;

- безопасности информационных и телекоммуникационных средств и систем.

В связи с изложенным неизбежным является вывод о том, что в настоящее время в нашей стране существует достаточное количество

предпосылок и оснований для совершенствования уголовного законодательства в сфере защиты информации (информационных объектов, информационной безопасности), поскольку:

- принятие программных нормативных актов в данной сфере обособляет данную категорию правоотношений, определяя ее общественную значимость и исключительное положение в сфере иных общественных отношений;

- существующими охранительными нормами безопасность в данной сфере обеспечивается недостаточно, поскольку административная ответственность за совершение правонарушений в данной сфере практически не предусматривается, а разработка и принятие норм уголовной ответственности в данной сфере носила достаточно бессистемный характер, затрудняющий как исследования в области уголовно – правовой защиты информации, так и практическое применение указанных норм;

- существующие положения теории уголовного права не исключают возможности его совершенствования, в том числе и путем включения дополнительного родового объекта в действующее законодательство, определяющего общественные отношения данной сфере;

- информационные объекты, имеют не только общие свойства, порождающие необходимость в уголовно-правовой их охране, но также и имеют такие особенности, которые позволяют сводить их в отдельные группы и тем самым разграничивать друг от друга на основе различающих их признаков

- включение в действующее уголовное законодательство соответствующего раздела, предусматривающего уголовную ответственность за совершение преступлений в сфере защиты информации (или информационной безопасности) позволит подчеркнуть значимость информации в современных условиях и ее потребность в уголовно –правовой охране;

- в основу изменений действующего уголовного законодательства могут быть положены концептуальные положения Доктрины информационной безопасности, раскрывающей виды угроз информационной безопасности по общей направленности, раскрывая содержание каждой из них, причем при формулировке диспозиций новых составов преступлений существует реальная возможность учесть и «традиционные» уже существующие составы преступлений, что в свою очередь, может способствовать построению обоснованной и четкой системы родового и видовых объектов.