

разом, сам доступ является правомерным, преступник при DDoS-атаке злоупотребляет предоставленным правом на доступ к сайту-жертве. В этой связи автор предлагает для надлежащей уголовно-правовой защиты от данного вида кибератак внести изменения в ст. 272 УК Российской Федерации, убрав из объективной стороны такое обстоятельство, как неправомерность доступа, заменив его признаками несанкционированности и умышленности в отношении последствий.

Т.Л. Тропина считает, что понятие неправомерного доступа является оценочным. Неправомерность может означать как несоответствие нормам права, так и совершение действия при отсутствии прав на его совершение. Автор также предлагает заменить термин «неправомерный» термином «несанкционированный».

В Положении о технической и криптографической защите информации в Республике Беларусь, утвержденном Указом Президента Республики Беларусь от 16 апреля 2013 г. № 196, несанкционированный доступ к информации определяется как доступ к информации, осуществляемый с нарушением установленных прав или правил разграничения доступа. В п. 20 постановления Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 «О применении судами уголовного законодательства по делам о хищениях имущества» разъясняется, что несанкционированным при хищении с использованием компьютерной техники считается доступ к компьютерной информации лица, не имеющего права на доступ к этой информации либо имеющего такое право, но осуществляющего его помимо установленного порядка. Кроме того, в технической литературе употребляется именно термин «несанкционированный доступ». Также прилагательное «несанкционированный» по отношению к доступу используется и в государственных стандартах.

На наш взгляд, несанкционированное ознакомление означает, что у лица нет ни прав на ознакомление с информацией, ни разрешения (санкции) владельца информации. Ведь ситуацию, когда у лица имеется право на доступ к информации, но такой доступ осуществлен помимо установленного порядка, относят к несанкционированному доступу. Поэтому считаем традиционное использование прилагательного «несанкционированный» более приемлемым.

Таким образом, несанкционированный доступ к компьютерной информации состоит из представленных в единстве получения и реализации возможности – ознакомления и использования указанной информации, сопряженных с нарушением системы ее защиты. При этом действие осуществляется лицом, не имеющим права на ознакомление с информацией либо имеющим такое право, но осуществляющим его с

нарушением установленного порядка. В предметно-содержательном аспекте несанкционированный доступ состоит из ознакомления с полученной информацией и из возможного затем ее использования, независимо от фактической реализации этой возможности. В организационно-управленческом аспекте несанкционированный доступ – это нарушение установленных правил и порядка доступа, связанных с системой защиты.

УДК 504.75.05

С.Л. Яблочников, И.О. Яблочникова, М.С. Яблочникова

АЛЬТЕРНАТИВНЫЙ ВЗГЛЯД НА ПРОБЛЕМЫ, СВЯЗАННЫЕ С ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Как правило, научные публикации в сфере обеспечения информационной безопасности в первую очередь касаются вопросов разработки методов и средств защиты информации от несанкционированного доступа к ней, ее искажения, уничтожения, модификации или же создания условий гарантированного доступа для определенного круга пользователей. Мероприятия, связанные с защитой информации, реализуются при ее приеме, передаче, хранении, обработке, визуализации и т. д. Таким образом, в качестве объектов, на защиту которых направлены соответствующие действия в рамках выработанной политики безопасности, рассматриваются либо некоторые информационные ресурсы, либо совокупность информационных процессов, осуществляемых в сложных технических системах. Также речь идет об обеспечении бесперебойного функционирования программно-технических комплексов, непосредственно реализующих указанные выше защищаемые информационные процессы.

Упомянутые сложные технические системы, существующие для обеспечения информационных процессов, в большинстве случаев являются человеко-машинными. Конечная цель функционирования таких систем – информационная поддержка производственной, экономической, технологической, социальной и иной деятельности отдельных личностей, определенных групп людей или же социума в целом. При этом общая логика совокупности действий в рамках обеспечения информационной безопасности такова: необходимо защитить информационные ресурсы или информационные процессы, которые человек (общество), в конечном счете, использует себе во благо.

Фактически мало кто из исследователей задумывается о том факте, что кроме негативных, несанкционированных воздействий (внешних и

внутренних по отношению к информационной системе, естественных и искусственных, преднамеренных и непреднамеренных) на информационные ресурсы, процессы и программно-технические средства, вполне реально существует целый ряд существенных угроз для отдельных личностей и социальных групп, возникающих вследствие их взаимодействия с информационными ресурсами, оборудованием, а также вольного или невольного участия в процессах передачи, приемки, хранения, отображения, обработки и синтеза информации. В некотором роде такой подход определяет альтернативную трактовку сущности основ информационной безопасности, вполне имеющую право на существование.

В последнее время в ряде публикаций высказывается мнение о необходимости активного формирования теоретических основ нового направления в науке – информационной экологии. Отправная точка для обоснования ее сущности – признание того факта, что помимо природной и социальной сред обитания человека объективно существует также информационная среда, являющаяся агрессивной по отношению к нему. Роль и значение такой среды в современном информационном обществе и в условиях реализации так называемой четвертой промышленной революции постоянно возрастает по мере дальнейшего развития компьютерных технологий, средств массовой информации и современных телекоммуникаций.

Информационная среда оказывает на человека весьма активное воздействие. Она существенно влияет (в том числе и негативно) на формирование и функционирование личности, на его духовное, интеллектуальное и психическое развитие, состояние психического и физического здоровья. Таким образом, при использовании упомянутого выше подхода к рассмотрению роли информационных ресурсов и информационных технологий объектом защиты становится человек и как достаточно сложная биологическая система, и как необъемлемая часть (социальная подсистема) другой сложной и глобальной системы – социума.

Смещение акцентов в сторону информационной безопасности непосредственно конкретного человека, а не совокупности современных средств обеспечения его продуктивной жизнедеятельности позволяет рассматривать обсуждаемую проблему несколько в ином ракурсе, как и саму информационную безопасность, в классическом ее понимании, в качестве составной части комплексной безопасности жизнедеятельности.

Также вполне понятен тезис о том, что перед человечеством стоит следующая дилемма: активное использование информационных ресур-

сов и информационных технологий для эффективного достижения определенных целей с обеспечением защиты информации и функционирования средств ее обработки или же обеспечение с наименьшими затратами комплексной безопасности жизнедеятельности человека в процессе решения им глобальных и локальных задач, возникающих перед ним. Все зависит от того, как именно будет трактоваться понятие «эффективность жизнедеятельности»: как максимизация объемов обработки информации и обусловленное этим максимальное извлечение некоторой выгоды (в том числе и финансовой) или же как некоторое достаточное для обеспечения эволюционного развития человечества информационное взаимодействие при минимизации рисков возникновения негативных последствий в настоящем и будущем.

По нашему мнению, социум со временем в качестве приоритетного изберет для себя путь развития, при котором минимизируются всевозможные риски и подлежат максимизации возможности сохранения и непрерывной эволюции человеческого потенциала. Обеспечение физического и психического здоровья отдельной личности и общества в целом является более важной и глобальной проблемой, чем создание некоторого валового продукта, который со временем, может быть, позволит решить указанную выше задачу наряду со многими остальными. Таким образом, создание теоретических основ информационной экологии – это в некотором роде попытка изменить парадигму эволюции общества.