тельности в этой сфере. При этом важное значение отводится усилению деятельности правоохранительных органов по предупреждению, выявлению и пресечению преступлений против информационной безопасности, а также надежному обеспечению безопасности информации, охраняемой в соответствии с законодательством.

УДК 343.8

А.Е. Сушко

ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Защита граждан, их прав и свобод, интересов общества и государства являются основными задачами, стоящими перед правоохранительными органами Республики Беларусь.

На современном этапе столь динамичного развития и применения информационных технологий неизбежно возникает проблема защиты от их использования в преступных целях. Преступность в сфере высоких технологий не имеет границ и составляет угрозу международной безопасности.

Киберпреступность является проблемой мирового уровня, так как подобные преступления совершаются, как правило, транснациональными организованными преступными группами, члены которых, используя возможности сети Интернет, виртуально пересекают границы между государствами и пользуются несовершенством законодательства различных государств. Преступления против информационной безопасности приобретают транснациональный и организованный характер. Преступление с использованием компьютерной техники и ресурсов интернета может быть совершено на территории другой страны и даже нескольких государств одновременно. При этом злоумышленник потратит на его совершение всего несколько минут, общаясь с представителями различных организаций (банковские учреждения, интернет-магазины, платежные системы, различные сервисы интернета) не выходя из своего дома.

Концепция национальной безопасности Республики Беларусь определяет информационную безопасность как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере и выделяет ее в самостоятельную составляющую национальной безопасности. К таким угрозам относятся и преступления против информационной безопасности, впервые отраженные в Уголовном кодексе Республики Беларусь

1999 г. Статистика последних лет свидетельствует об увеличении количества этих преступлений.

В 2016 г. в сравнении с 2015 г. количество выявленных преступлений в сфере высоких технологий увеличилось на 1,3 % (с 2 440 до 2 471), притом прирост преступлений против информационной безопасности (гл. 31 УК Беларуси) составил 63,6 % (с 404 до 651). Количество же фактов несанкционированного доступа к компьютерной информации возросло на 152,9 % (со 102 до 258).

Национальными интересами России в сфере информационных технологий является обеспечение прав и свобод граждан, а также неприкосновенность частной жизни, как определено в Доктрине информационной безопасности Российской Федерации.

Информационная безопасность приобрела особое значение в условиях глобализации и интенсивного информационного обмена в мировом масштабе. Дело бывшего сотрудника ЦРУ и агентства национальной безопасности США Эдварда Сноудена, хакерские атаки на серверы Демократической партии США, серверы Европейской комиссии подтверждают это.

Практически каждый белорус в настоящее время активно использует множество высокотехнологичных устройств (Smart TV, компьютеры, планшеты, мобильные телефоны и иные электронные устройства, банковские карточки). Международный союз электросвязи отметил, что Беларусь в 2016 г. улучшила позиции в рейтинге развития информационно-коммуникационных технологий (ИКТ) и заняла 31-е место среди 175 стран.

Очевидно, что в настоящее время подлежит защите любая информация, имеющая отношение к физическому лицу, которая включает его персональные данные, сведения о регистрации на различных сайтах в сети Интернет или в социальных сетях, сведения о покупках в интернет-магазинах. Минимизировать риски в указанной сфере, в частности со стороны операторов персональных данных, позволит принятие Закона «О персональных данных», целью которого является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну. Так как проблема информационной безопасности не носит региональный характер, а охватывает все государства мира, при разработке указанного Закона целесообразно ориентироваться на европейское и российское законодательства в данной сфере.

Управлением Следственного комитета по Минской области в январе 2017 г. завершено расследование уголовного дела в отношении группы лиц, занимавшихся хищениями денежных средств граждан.

Расследованием установлено, что трое граждан Российской Федерации, арендуя дом в Минском районе с ноября 2015 г. по февраль 2016 г., с целью завладения денежными средствами граждан использовали вредоносное программное обеспечение и от имени Министерства внутренних дел Республики Беларусь рассылали электронные уведомления о наложении административного взыскания за якобы имевший место просмотр видеоматериалов, содержащих элементы порнографического характера. Для оплаты штрафа предлагалось перевести денежные средства на счета абонентских номеров одного из белорусских операторов сотовой связи. В результате противоправных действий фигуранты дела произвели блокирование компьютерной информации более 900 граждан. Причиненный ущерб составил свыше 136 тыс. белорусских рублей.

Главным следственным управлением Следственного комитета Республики Беларусь в 2016 г. при поддержке Европола, Секретной службы и ФБР США, полиции Кипра пресечена деятельность организованной преступной группы, жертвами которой стали более 130 тыс. держателей платежных карт из 29 стран. Преступная группа занималась компрометацией кредитных карт с использованием компьютерных технологий и вредоносных программ. Для этих целей были созданы несколько подставных онлайн-магазинов и фиктивная компания по разработке программного обеспечения. Киберпреступники связывались с легальными платежными онлайн-сервисами и имитировали проведение многочисленных международных транзакций. В дальнейшем похищенные средства переводились на банковский счет на Кипре. Благодаря большому числу транзакций с маленькими суммами преступникам несколько месяцев удавалось быть незамеченными. Сумма нанесенного ими ущерба составляет более 8 млн евро. Четыре участника группы, включая лидера, были установлены и задержаны Следственным комитетом Беларуси.

Европейский центр по борьбе с киберпреступностью, начавший свою работу в 2013 г., играет ведущую роль в борьбе с киберпреступностью на территории Европейского Союза, занимаясь созданием оперативных и аналитических мощностей, необходимых для обеспечения быстрого реагирования на киберпреступления, а также организацией взаимодействия официальных ведомств ЕС и стран-членов с международными партнерами. Сотрудники центра разрабатывают методы пресечения преступлений в сфере информационных технологий, в том числе завладения данными кредитных карточек, защищают от хакеров пользователей социальных сетей. Кроме того, центр обеспечивает безопасность стратегически важных интернет-ресурсов и коммуникационных систем ЕС, действует против распространения детской порнографии, занимается сбором и обработкой данных, оказанием информационной, технической и криминалистической поддержки соответст-

вующим подразделениям правоохранительных органов стран – членов ЕС, координацией совместных расследований, обучением и подготовкой специалистов. Европейский центр по борьбе с киберпреступностью содействует проведению необходимых исследований и созданию программного обеспечения, занимается оценкой и анализом существующих и потенциальных угроз, составлением прогнозов и выпуском заблаговременных предупреждений.

Так, 30 ноября 2016 г. был дан старт глобальной операции, получившей кодовое названия Avalanche («Лавина»). Для ликвидации огромной киберпреступной сети были объединены усилия правоохранительных органов и специалистов в области информационной безопасности из более чем 40 стран мира (Европол, ФБР, Интерпол, ICANN, Symantec, Shadowserver Foundation, Registrar of Last Resort и др.). Операцию предваряли расследования и другая подготовительная работа на протяжении четырех лет. В ходе проведения Avalanche прошли обыски в 37 местах и были арестованы пять подозреваемых, более 800 тыс. доменов перешли под контроль властей или были заблокированы, 39 серверов были изъяты и еще 221 сервер ушел в офлайн, после того как хостинг-провайдеров уведомили о нарушениях. Инфраструктура Avalanche использовалась для хостинга и распространения более чем 20 семейств различных вредоносных программ, в том числе таких известных, как GozNym, Marcher, Dridex, Matsnu, URLZone, XSWKit, Pandabanker, Cerber и Teslacrypt. Кроме того, злоумышленники занимались рассылкой спама, а также отмыванием денег, поиском и наймом так называемых денежных мулов. Огромный ботнет насчитывал как минимум 500 тыс. устройств по всему миру, которые за прошедшие годы успели атаковать более 40 крупных финансовых организаций, а также пользователей в более чем 180 странах мира. Суммарный ущерб от деятельности киберпреступников оценивается в сотни миллионов евро.

Указанные преступления, совершенные как на территории Республики Беларусь в отношении граждан Беларуси, так и на территории десятков государств организованными группами злоумышленников, подчеркивают опасность, исходящую от киберпреступников, и требуют от правоохранительных органов разных стран надлежащего уровня взаимодействия.

В настоящее время, на наш взгляд, необходимо:

провести мероприятия для присоединения Республики Беларусь к международным правовым инструментам в сфере информационной безопасности, в том числе к Конвенции о защите физических лиц при автоматизированной обработке персональных данных, к Конвенции Совета Европы о борьбе с киберпреступностью, одними из участников которой являются члены СНГ – Азербайджан, Армения, Молдова, к Соглашению между правительствами государств – членов Шанхайской

организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности;

разработать и принять Стратегию обеспечения кибербезопасности (информационной безопасности) Республики Беларусь, в которой следует отразить основные современные угрозы интересам Беларуси, ее граждан и бизнес-сообщества в киберпространстве, определить основные мероприятия, направленные на защиту объектов критической инфраструктуры, прав граждан и государства, совершенствование национального законодательства в области информационной безопасности, закрепление статуса национального координатора, который объединит специалистов в сфере информационной безопасности из различных государственных органов и представителей частного сектора. Также целесообразно разработать Закон «Об обеспечении информационной безопасности» и Закон «О персональных данных»;

продолжить сотрудничество Следственного комитета Республики Беларусь с правоохранительными органами Российской Федерации, Европы и США, в частности с ФСБ, Европолом, полицией Нидерландов, ФБР, Секретной службой США, для организации борьбы с международными преступлениями против информационной безопасности, для обмена информацией с целью успешного раскрытия и расследования таких преступлений;

продолжить работу над реализацией инициативы Следственного комитета в создании национального киберцентра, который должен стать платформой сотрудничества и координации действий по вопросам расследования и профилактики преступлений, связанных с использованием сети Интернет, объединить экспертные знания правоохранителей, ученых, представителей частного сектора. Центром будут проводиться научные исследования, вырабатываться стратегические подходы в борьбе с преступностью, создаваться учебные и образовательные программы по данной тематике, раскрываться и расследоваться киберпреступления.

УДК343.54

О.О. Топорикова

СЕКСУАЛЬНОЕ КИБЕРВЫМОГАТЕЛЬСТВО (SEXTORTION)

Происходящие изменения форм социальной коммуникации, связанные с развитием функционально совместимых информационно-коммуникационных технологий, стимулируют возникновение новых форм сексуальной эксплуатации, в том числе путем модификации преступлений, которые традиционно относились к категории совершаемых только посредством личного (реального) контакта (например, преступления против половой свободы и половой неприкосновенности). К числу таких преступлений можно отнести сексуальное кибервымогательство (sextortion).

Сексуальное вымогательство относится к одной из новых форм сексуальной эксплуатации. Т.М. Лопатина отмечает, что для интернет-вымогательства как явления в целом характерны две тенденции: стремление придать требованиям правомерный вид и гиперлатентность.

Сексуальное кибервымогательство реализуется посредством информационно-коммуникационных технологий и нефизических форм принуждения с целью получения сексуальных услуг либо приватных материалов (изображения, видео сексуального содержания) от жертвы. При этом чаще всего физического контакта преступника и жертвы не происходит. Жертва совершает иные действия сексуального характера либо половые сношения с третьими лицами, которые транслируются преступнику в режиме реального времени с использованием web-камеры.

Сексуальное вымогательство может быть сопряжено с совершением таких преступлений, как изготовление и распространение порнографии (ст. 343 УК) и незаконное распространение информации о частной жизни (ст. 179 УК). В большинстве таких случаев, зарегистрированных на территории Республики Беларусь, преступник и жертва ранее были знакомы, состояли в супружеских отношениях либо проживали совместно. Мотивом распространения приватных материалов была либо месть из-за расставания либо принуждение к восстановлению отношений. Анализ правоприменительной практики показал, что чаще всего в таких случаях жертвы не подают заявления о привлечении виновного лица по ст. 179 УК. Кроме того, имеют место мотивированные примирения с преступниками, попытки потерпевших прекратить уголовное производство по ст. 343 УК.

Анализ национальной правоприменительной практики и зарубежного опыта позволил выделить две формы сексуального кибервымогательства, особенности которых влияют на квалификацию деяния по УК Республики Беларусь.

Например, может иметь место следующая картина преступления. Используя для общения социальные сети либо иные средства коммуникации, преступник устанавливает доверительный контакт с жертвой, после чего просит выслать изображение, видео сексуального характера либо осуществить сексуальные действия с трансляцией на web-камеру в режиме реального времени. Получив данный материал, он начинает шантажировать им жертву.