4. Казанцев, С.Я. Авторские права и их защита в сети Интернет / С.Я. Казанцев, О. Э. Згадзай // Вестник Казанского юридического института МВД России. – 2010. – № 1. – С. 57–62.

5. Михайликов, В. Л. Формы защиты авторских прав / В.Л. Михайликов // Научные ведомости БелГУ. Серия: Философия. Социология. Право. 2010. – №2. – С. 136–137.

6. Алисова, Е.В. Актуальные проблемы защиты авторского права в сети Internet / Е.В. Алисова // Наука, образование и культура. – 2016. – №7 – С. 12 – 6.

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ МИРЕ

К.В. Санковский, С.М. Алексеенко

Ключевые слова: Интернет, цифровизация, информационно-коммуникационные технологии, киберпреступность, преступления в сфере информационной безопасности.

В эпоху цифровизации система социального взаимодействия основана на использовании интернета. Интернет делает более доступными общение и коммуникацию, способствует развитию самых разных сфер деятельности человека. Однако данное информационное пространство стало также полем для преступных деяний. В XXI в. человечество впервые столкнулось с новым, ранее неизвестным видом преступности -киберпреступностью. Киберпреступность основывается на взломе интернет-страниц, распространении вредоносных программ и противоправной информации людьми, осуществляющими преступную деятельность в виртуальном пространстве с помощью информационных технологий. Немаловажную роль для осуществления подобного рода противозаконной деятельности играет компьютер. Он является техническим средством, инструментом, позволяющим злоумышленникам не только похищать информацию, уничтожать или повреждать её, но и размещать вредоносные сайты, на которых содержатся компьютерные вирусы [1; 96].

Данный вид преступления, как, впрочем, и все другие, таит в себе угрозу информационной безопасности общества. Помимо кражи денежных средств с банковских карт киберпреступники научились похищать персональные данные человека, что может нанести непоправимый урон его репутации в случае опубликования этой информации в сети. Киберпреступность является проблемой не только каждого отдельного взятого интернет-пользователя, - её следует рассматривать в более широком, социальном и даже международном ключе. От роста киберпреступности страдают не только

физические, но и юридические лица; жертвами хакерских атак в нашей современности становятся целые страны, государства.

Целью данной работы является всестороннее исследование борьбы с киберпреступлениями в Республике Беларусь и зарубежных странах.

Основу методологии познания составили как общенаучные, так и частно-научные методы.

Уголовный кодекс Республики Беларусь (далее УК) содержит в себе раздел «Преступления против информационной безопасности» [2]. Однако, преступления, совершаемые посредством компьютера, находят своё отражение в статьях других разделов. Например, хищение путём использования компьютерной техники (ст. 212 УК) или причинение имущественного ущерба без признаков хищения (ст. 216 УК).

В уголовном кодексе Российской Федерации глава 28 (преступления в сфере компьютерной информации) содержит следующие статьи:

• неправомерный доступ к компьютерной информации (ст. 272);

• создание, использование и распространение вредоносных компьютерных программ (ст. 273);

• нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274);

• неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1) [3].

В законодательстве Германии, к преступлениям в сфере компьютерной информации относятся:

– действия лиц, неправомочно приобретающих для себя или иного лица непосредственно не воспринимаемые сведения, которые могут быть воспроизведены или переданы электронным, магнитным или иным способом (§ 202a);

– нарушение тайны телекоммуникационной связи (§ 206);

– действия лиц, учиняющих подделку или использующих поддельные технические записи, под которыми, в числе иного, понимаются данные, полностью или частично регистрируемые автоматическими устройствами (§ 268);

– аналогичная подделка данных, имеющих доказательственное значение (§ 269);

– действия лиц, уничтожающих, изменяющих или утаивающих технические записи (§ 274);

– действия лиц, противоправно аннулирующих, уничтожающих, приводящих в негодность или изменяющих данные (§ 303a);

– действия лиц, нарушающих обработку данных путём разрушения, повреждения, приведения в негодность установки для обработки данных или носителей информации (§ 303b);

– незаконное вмешательство в деятельность телекоммуникационных установок (§ 317) [4].

Законодательство Германии устанавливает уголовную ответственность за мошенничество в сфере интернет, под которым понимается умышленное деяние с намерением получить для себя или третьих лиц имущественную выгоду, заключающееся в причинении вреда чужому имуществу путём воздействия на результат обработки данных путём неправильного создания программ, использования неправильных или данных, неправомочного использования данных или иного воздействия на результат обработки данных (§ 263a) [4].

Правовая система Люксембурга предусматривает ответственность за неправомочный доступ к системе или части системы обработки данных и незаконное пребывание в такой системе. Законодательство запрещает преднамеренное затруднение или изменение функционирования системы автоматической обработки данных [5]. Таким образом, основной целью законодательства Люксембурга в вопросе киберпреступности является охрана целостности и качества данных.

В законодательстве данного государства также предусмотрено, что лицо, умышленно и без надлежащих полномочий вводящее данные в электронную систему их обработки, удаляющее или изменяющее данные, находящиеся в этой системе, изменяющее действие системы или способ передачи данных, подлежит уголовной ответственности. Любое вмешательство в телекоммуникации является преступлением, за которое лицо может быть подвергнуто штрафу или заключению от 1 месяца до 3 лет [5].

В современном мире киберпреступность представляет собой серьёзную угрозу обществу и его информационной безопасности. Киберпреступность порождает комплекс социальных проблем, которые требуют незамедлительного реагирования и эффективного разрешения. С совершенствованием информационных технологий совершенствуется и киберпреступность, находящая проявление во многих сферах жизни и деятельности человека и общества в целом. Защита от данного вида преступлений предполагает корреляцию усилий на уровне международного сотрудничества и взаимодействия: совершенствование технологий, содействующих выявлению киберпреступлений; развитие ресурсов искусственного интеллекта и их последовательное внедрение в сферу расследования киберпреступлений; ужесточение ответственности за совершение киберпреступлений.

Список использованных источников:

1. Тимофеев, А.В., Комолов, А.А. Киберпреступность как социальная угроза и объект правового регулирования. А.В.Тимофеев [и др.] // Вестник МГОУ. Серия: Философские науки. – №1. – 2021. – С. 95–101.

2.Уголовный кодекс Республики Беларусь [Электронный ресурс]: 9 июля 1999 г., №275-З: принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г.: в ред. Закона Респ. Беларусь

от 26.05.2021 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. –Минск, 2021.

2. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс]: 6 января 2021 г., №91-З: принят Палатой представителей 18 дек. 2020 г.: одобр. Советом Респ. 18 дек. 2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

3. Уголовный кодекс Российской Федерации от 13 июня 1996 г. №63-ФЗ [Электронный ресурс] // СПС «Гарант». – 2021.

4. Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 [Elektronische ressource]. – Zugriffsmodus: https: // www.legislationline.org / download/id / 8253/file/Germany_CC%20am2019_de.pdf. Access-datum: 02.11.2021.

5. Code pénal du 1er novembre 2018 [Ressource électronique]. – Mode d'accès: https://www.legislationline.org/download/id/8273/file/Luxembourg_Criminal_Code_am2018_fr.pdf. Date d'accès: 02.11.2021.

ПОНЯТИЕ И ВИДЫ ИНФОРМАЦИОННОГО ОРУЖИЯ

Т.В. Сафонова, А.В. Будько

Ключевые слова: информационное оружие, информационная война, информационное противоборство, международное информационное право.

Информационное оружие представляет собой технические, программные и психологические приемы и способы информационного воздействия на противника, применяемые в условиях информационного противоборства (информационной войны).

Информационная война – война нового типа, объектом которой являются объекты информатизации, включая интернет-ресурсы, информационные системы, сети и сознание людей [1, с.134].

В соответствии с Соглашением, заключенным между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области обеспечения международной информационной безопасности от 25 декабря 2013 года, информационная война представляет собой противоборство между двумя или более государствами в информационном пространстве в целях нанесения ущерба информационным системам, процессам и ресурсам, критически важным и другим объектам, подрыва политической, экономической и социальной систем, массированной психологической обработки населения для дестабилизации общества и государства, а