Заключение. На сегодняшний день промышленность Республики Беларусь имеет высококвалифицированную рабочую силу и наиболее развитое техническое оборудование, которое дает возможность получить качественный результат. Улучшение материально-технической базы, выявление новых приоритетных направлений, осуществление инновационной деятельности, реализация научно-технических достижений формируют более конкурентные преимущества государства в промышленной сфере и являются факторами развития производственного сектора в стране.

1. Структура объёма промышленного производства в 2021 году [Электронный ресурс]: [стат. бюл.] / Нац. стат. ком. Респ. Беларусь. – Минск, 2021. – Режим доступа: prom_konkurent_rate2022.pdf (belstat.gov.by). – Дата доступа: 06.07.2023.
2. Промышленность в Беларуси [Электронный ресурс]. – Режим доступа: Промышленность в Беларуси | Официальный интернет-портал Президента Республики Беларусь (president.gov.by). – Дата доступа: 06.07.2023.

КРИМИНАЛИСТИЧЕСКАЯ ХАРАКТЕРИСТИКА КИБЕРПРЕСТУПЛЕНИЙ

Козел А.Н.,
студентка 4 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – ***Алхимина И.А.,*** *ст. преподаватель*

Ключевые слова. Киберпреступления, компьютерная информация, информационно-коммуникационные технологии, криминалистическая характеристика компьютерных преступлений, преступления.

Keywords. Cybercrimes, computer information, information and communication technologies, criminalistic characteristics of computer crimes, crimes.

Внедрение в повседневную жизнь человека информационно-коммуникационных технологий (далее – ИКТ) способствовало созданию ряда перспектив для всего общества [4]. Несмотря на то, что ИКТ несут в себе положительные моменты, например, рост компьютерной грамотности, есть и обратная сторона, в которой стремительное развитие ИКТ повлекло за собой появление новых видов преступлений – киберпреступления. Актуальность исследования заключается в том, что ИКТ являются довольно новой отраслью права, поэтому многие вопросы по охране и защите прав так и не закреплены и не урегулированы в нормативно-правовых актах (далее – НПА), что порождает киберпреступления. Специфика совершения данного вида преступлений вызывает трудности при их раскрытии и расследовании. Целью исследования является всестороннее и полное изучение специфики криминалистической характеристики киберпреступлений.

Материал и методы. Материалом исследования в данной работе являются нормы национального законодательства: Уголовный кодекс Республики Беларусь, статистические данные и публикации по данной теме. Также в работе использованы нормы международного законодательства. В работе использованы сравнительно-правовой и формально-юридический методы исследования.

Результаты и их обсуждение. Криминалистическая характеристика киберпреступлений представляет собой совокупность наиболее характерной, наиболее значимой, взаимосвязанной информации, ее признаках и свойствах, способной служить основанием для выдвижения версий о событии преступления и личности преступника, позволяющей верно оценить ситуации, возникающие в процессе раскрытия и расследования компьютерных преступлений, и обуславливающей применение необходимых криминалистических методов, приемов и средств [2, с. 304]. Значение криминалистической характеристики заключается в том, что она задает направление в деятельности для следователя благодаря наличию специальных признаков, которые образуют структуру, а также определяет ход расследования и способствует выдвижению версий.

Киберпреступления представляют собой преступную деятельность, которая осуществляется с использованием ИКТ, либо в информационном пространстве [1]. Общим для преступлений, входящих в состав киберпреступлений, являются средства их совершения – киберпространство, информационно-коммуникационные сети и средства компьютерной техники.

Поскольку данный вид преступлений обладает определенной спецификой их совершения, то раскрытие и расследование компьютерных преступлений, а также противодействие им вызывает трудности.

При анализе киберпреступлений может выделить следующие проблемные моменты: высокий уровень латентности, трудность обнаружения и изъятия следов, недостаточная подготовка и практика судей и следователей, а также отсутствие необходимых средств, позволяющих раскрыть данный вид преступлений.

Прежде всего, чтобы дать криминалистичесекую характеристику преступлениям, которые совершаются в данной сфере, необходимо выяснить, что представляет собой понятие «компьютерная информация».

Под компьютерной информацией, в соответствии с Уголовным кодексом Республики Беларусь (далее – УК), следует понимать информацию, которая хранится в компьютерной системе, сети или на машинных носителях, обрабатываемая компьютерной системой либо передаваемая в пространстве с помощью любых программно-технических средств [5]. Если обратиться к Уголовному кодексу Российской Федерации (далее – УК РФ), то под компьютерной информацией следует понимать сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи [6]. Без знания этих понятий невозможно дать криминалистическую характеристику киберпреступлений.

Криминалистическая характеристика киберпреступлений имеет следующую структуру:

1. предмет преступного посягательства;
2. способы совершения преступлений;
3. особенности обстановки совершения преступления;
4. особенности следовой информации;
5. личность преступника [2, с. 304].

Предметом преступного посягательства являются компьютерные системы и их сети. Что касается способов совершения преступления, то их можно разделить на следующие группы:

1. методы перехвата (например: непосредственный перехват, «уборка мусора»;
2. методы несанкционированного доступа (например: подмена пользователя, подбор паролей);
3. методы манипуляции (например: подмена данных, «троянский конь»);
4. комбинированное использование.

Следы, отражающие неправомерный доступ к компьютерной информации, можно подразделить на два типа: традиционные (они включают в себя следы-отображения; следы-предметы и следы-вещества) и нетрадиционные (информационные следы) [2, с. 307].

В литературе выделяют три группы лиц, которые совершают киберпреступления. Первая группа – хакеры и крэкеры. Данная группа характеризуется тем, что лица сочетают профессионализм и фанатизм. Ко второй группе относятся лица, страдающие компьютерными фобиями (игроманы). И третья категория лиц включает в себя профессиональных преступников, которые действуют из корыстных побуждений [2, с. 310].

В Республике Беларусь за первый квартал 2023 г. было зафиксировано более 10 тыс. киберпреступлений, 90% составляют мошенничество и хищение денежных средств. Данные показатели значительно превысили показатели по сравнению с 2022 г. – 11 707) [3]. Следует отметить, что IP-адрес большинства лиц, совершающих данный вид преступления, был выдан провайдерами зарубежных стран, что значительно осложняет возможности раскрытия преступлений, а также возможность установить личность преступника.

Среди международных НПА, регулирующих вопрос международного сотрудничества по оказанию помощи в расследовании и раскрытии киберпреступление, отсутствует единый унифицированный акт, который регулировал бы данную сферу и закреплял формы сотрудничества. Следует отметить, что Республикой Беларусь ратифицирована Конвенция «О правовой помощи и правовых отношениях по гражданским, семейным и уголовным делам», а также Соглашение о сотрудничестве государств-участников СНГ в

борьбе с преступлениями в сфере компьютерной информации. Наличие международных договоров и соглашений о сотрудничестве позволяют оказывать содействие по раскрытию киберпреступлений, а также способствуют передаче лица, совершившего преступление, в другое государство для отбывания наказания.

Заключение. Таким образом, криминалистическая характеристика киберпреступлений выделяет специфические признаки отдельных видов преступлений и способствует их расследованию и раскрытию. Противодействие совершению преступлений в сфере ИКТ является одной из основных задач международной и национальной безопасности. Для решения проблем, возникающих в результате совершения киберпреступлений, на мировом уровне, на наш взгляд, необходимо разработать единый НПА, который позволял бы странам сотрудничать между собой для более быстрого раскрытия преступлений. Подписание международных договоров и соглашений о сотрудничестве, также значительно было повысило уровень раскрытия данных преступлений и снизило бы их латентность.

Что касается национального уровня, то для решения проблем, связанных с борьбой с киберпреступлениями, на наш взгляд следует разработать и внедрить в практику программу углубленного обучения следователей и судей, которые специализируются по расследованию данного вида преступлений.

1. Буз, С.И. Киберпреступления: понятия, сущность и общая характеристика / С.И. Буз // Юристъ-правоведъ. – 2019. – № 4 (91). – С. 78–82.
2. Дмитриева, Т.Ф. Криминалистика: курс лекций / Т.Ф. Дмитриева. – 2-е изд., с изм. и доп. – Витебск: ВГУ имени П.М. Машерова, 2018. – 341 с.
3. МВД: 10 тыс. киберпреступлений зафиксировано в Республике Беларусь [Электронный ресурс]. – Режим доступа: https://www.belarus.kp.ru/online/news/5431533/. – Дата доступа: 10.09.2023.
4. Стаценко, В.Г. Проблема определения и латентности преступлений в сфере информационно-коммуникационных технологий / В.Г. Стаценко // Наука - образованию, производству, экономике [Электронный ресурс]: материалы 75-й Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов, Витебск, 3 марта 2023 г. – Витебск: ВГУ имени П.М. Машерова, 2023. – С. 556–558. – Библиогр.: с. 558 (4 назв.). URL: https://rep.vsu.by/handle/123456789/36994 (дата обращения: 09.09.2023).
5. Уголовный кодекс Республики Беларусь [Электронный ресурс]: Кодекс Республики Беларусь от 09.07.1999 № 275-З (в ред. от 09.03.2023) // ЭТАЛОН. Законодательство Республики Беларусь / Национальный центр правовой информации Республики Беларусь. – Минск, 2023.
6. Уголовный кодекс Российской Федерации [Электронный ресурс]: 13.06.1996 № 62-ФЗ: принят Гос. Думой 24.05.1996 (ред. от 04.08.2023) // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2023.

ИНСТИТУЦИОНАЛЬНОЕ ЗАКРЕПЛЕНИЕ ВСЕБЕЛОРУССКОГО НАРОДНОГО СОБРАНИЯ

Козлова К.А.,
студентка 2 курса ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – ***Петров А.П.,*** *канд. юрид. наук, доцент*

Ключевые слова. Всебелорусское народное собрание, Президент Республики Беларусь, Конституция Республики Беларусь, Президиум Всебелорусского народного собрания, институт государственного управления.

Keywords. All-Belarusian People's Assembly, President of the Republic of Belarus, Constitution of the Republic of Belarus, Presidium of the All - Belarusian People 's Assembly, institute of Public Administration.

Актуальность выбранной темы обусловлена недавним закреплением Всебелорусского народного собрания, как отдельного государственного института, в Конституцию Республики Беларусь после внесения в неё изменений и дополнений на республиканском референдуме 27 февраля 2022 года, добавили отдельную главу, посвящённую Всебелорусскому народному собранию. Целью исследования является детальное рассмотрение институционального закрепления Всебелорусского народного собрания.

Материал и методы. Нормативно-правовые акты Республики Беларусь, Конституция Республики Беларусь, Закон Республики Беларусь о Всебелорусском народном собрании. В работе использованы общенаучные и специальные правовые методы исследования, такие как формально-юридический и структурно-правовой.