Таким образом, в качестве целей реализации прокуратурой координирующей функции следует признать определение стратегии и тактики деятельности по борьбе с преступностью и коррупцией с учетом указанных выше задач.

Список использованных источников

1 Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Решение Всебелорусского народного собрания от 25.04.2024 № 5 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр законодательства и правовой информ. Респ. Беларусь. – Минск, 2024.

2 О борьбе с коррупцией [Электронный ресурс]: Закон Республики Беларусь от 15 июля 2015 г. № 305-З: с изм. и доп.: текст по состоянию на 24.05.2024 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр законодательства и правовой информ. Респ. Беларусь. – Минск, 2024.

3 О прокуратуре [Электронный ресурс]: Закон Республики Беларусь от 08.05.2007 г. № 220-З: с изм. и доп.: текст по состоянию на 03.01.2024 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2024.

4 Об утверждении положения о деятельности координационного совещания по борьбе с преступностью и коррупцией [Электронный ресурс]: Указ Президента Респ. Беларусь, 17 дек. 2007 г., № 644: с изм.и доп. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр законодательства и правовой информ. Респ. Беларусь. – Минск, 2024.

5 Пискунович Е.В. Прокурорский надзор за исполнением антикоррупционного законодательства/ Е.В. Пискунович // Вестник Полоцкого государственного университета. – 2016. – № 14. – С. 205–214

6 Василевич, Г.А. Актуальные направления противодействия коррупции в Республике Беларусь на современном этапе / Г.А. Василевич. – Минск: Беларуская навука, 2018. – 202 с. 7.

ГЛАВА 3. КИБЕРПРЕСТУПНОСТЬ КАК УГРОЗА НАЦИОНАЛЬНОЙ БЕЗОПАСНОСТИ

Переход человечества к новому этапу своего развития в результате становления «информационного общества» повлек за собой ряд изменений, которые характеризуются как с положительной, так и отрицательной стороны. В частности, внедрение и использование информационно-коммуникационных технологий (далее – ИКТ) в повседневную жизнь людей в значительной степени облегчили многие сферы жизнедеятельности и стали важной ступенью на пути развития. В свою очередь, слишком активное и быстрое внедрение ИКТ повлекло за собой появление новых угроз, которые представляют опасность для личной и общественной безопасности.

Одной из таких угроз на сегодняшний день является киберпреступность. Поскольку ежегодно количество зарегистрированных преступлений в сфере ИКТ растет как мире в целом, так и на национальном уровне, государства ставят перед собой цель по недопущению роста преступности в сфере ИКТ и обеспечению кибербезопасности.

Концепция национальной безопасности Республики Беларусь (далее – Концепция), утвержденная Решением Всебелорусского народного собрания № 5 от 25 апреля 2024 г., перечисляет основные угрозы национальной безопасности, среди которых выделяются такие, как: «нарушение киберустойчивости национального сегмента сети Интернет, критически важных объектов информатизации и государственных информационных систем; неправомерные действия в отношении персональных данных; утрата либо разглашение информации, распространение и (или) предоставление которой ограничено; дальнейшее развитие безопасной информационной среды и информационного общества» [1, п. 29]. Исходя из перечисленных угроз, Концепция устанавливает, что «в условиях глобальной цифровизации кибербезопасность критической инфраструктуры и больших данных приобрела исключительное значение для обеспечения устойчивости всех сфер жизнедеятельности» [1, п. 5].

Актуальность исследования определяется тем, что преступность в сфере ИКТ является относительно новым явлением, требующим постоянного совершенствования правового регулирования, криминализации новых общественно опасных деяний.

Целью исследования является разработка системы мер по противодействию киберпреступности и профилактике преступлений в области информационно-коммуникационных технологий на основе анализа национального законодательства и международных договоров, исследования особенностей, состояния и тенденций киберпреступлений и применяемых способов их профилактики.

Первые преступления в сфере ИКТ были зафиксированы в США. Процесс развития данного вида преступности можно подразделить на несколько этапов:

– первый этап, который характеризуется появлением первого компьютера в 1941 г. и зарождением Глобальной сети Интернет в 1960-х гг. на основе концепции Джозефа Леклайдера «Galactic Network» [2];

– второй этап связан с появлением компьютерных преступлений, в частности, в этот период времени активно действуют хакеры, которые изначально представляли собой преступников, совершающих противоправные действия с телефонами и телефонными звонками. В дальнейшем же хакерами стали называть всех лиц, которые совершают несанкционированный доступ к электронным источникам информации;

– на третьем этапе киберпреступность начинает приобретать мировые масштабы, что характеризуется переходом данных противоправных деяний на транснациональный уровень [2].

Что же следует понимать под киберпреступлениями? В настоящее время, несмотря на то, что термин «киберпреступления» в литературе используется довольно часто, в правовых источниках он встречается редко [3, с. 68]. Вместо данного термина чаще всего используются такие понятия, как: «компьютерные преступления», «преступления в сфере высоких технологий» и т.п.

В оборот термин «киберпреступность» был введен на X Конгрессе ООН в 2000 г. Киберпреступления, в соответствии с данным определением, рассматривались в смысловом плане различно:

в узком смысле – непосредственно сами компьютерные преступления, т.е. преступные деяния, которые направлены на преодоление защиты компьютерных систем;

в широком смысле – как преступления, в которых использовались компьютеры [4].

В Конвенции о киберпреступности 2001 г., открытой для подписания в г. Будапеште, вступившей в силу 1 июля 2004 г., под киберпреступлениями понимаются деяния, «направленные против конфиденциальности, целостности и доступности компьютерных систем, сетей и компьютерных данных, а также злоупотребления такими системами, сетями и данными» [4].

Следует отметить, что попытки определения понятия «киберпреступление» предпринимались неоднократно не только на международном правовом уровне, но также и в доктрине. В качестве примера можно привести определение К.Н. Евдокимова: «компьютерная преступность представляет собой совокупность преступлений, где основным непосредственным объектом преступного посягательства выступают общественные отношения в сфере компьютерной информации и информационных технологий, безопасного функционирования средств создания, хранения, обработки, передачи, защиты компьютерной информации, но при этом компьютерная информация, информационно-телекоммуникационные сети; средства создания, хранения, обработки, передачи компьютерной информации (компьютеры, смартфоны, айфоны, кассовые аппараты, банкоматы, платежные терминалы и иные компьютерные устройства) являются не только предметами преступного деяния, но и используются в качестве средства и орудия совершения преступления» [5].

В законодательстве Республики Беларусь также отсутствует легальное определение «киберпреступления», в то время как сам термин используется в наименовании главы 19 Концепции информационной безопасности Республики Беларусь.

Уголовный кодекс Республики Беларусь (далее – УК) содержит главу 31, которая называется «Преступления против компьютерной безопасности» и включает в себя 5 составов преступлений:

– несанкционированный доступ к компьютерной информации (ст. 349 УК);

– уничтожение, блокирование или модификация компьютерной информации (ст. 350 УК);

– неправомерное завладение компьютерной информацией (ст. 352 УК);

– разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программ, или аппаратных средств (ст. 354 УК);

– нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК) [6].

Киберпреступления можно охарактеризовать рядом признаков, среди которых наиболее значимыми являются:

– анонимность;

– трансграничный характер киберпреступлений;

– владение знаниями и умениями в области ИКТ;

– высокий уровень латентности;

– беспечность Интернет-пользователей;

– недостаточный уровень информационной грамотности населения;

– низкий уровень защиты.

Среди причин, способствующих совершению компьютерных преступлений, выделяют:

– недостаточный уровень подготовки правоохранительных органов;

– недостаточное количество ресурсов и технологий;

– темпы развития ИКТ опережают темпы развития законодательства;

– низкий уровень международного сотрудничества;

– увеличение количества Интернет-пользователей и др. [7].

Среди причин, способствующих увеличению числа регистрируемых киберпреступлений, особую роль играет постоянный рост количества пользователей Интернетом. Ежегодно количество интернет-пользователей значительно увеличивается. Так, например, если в 2013 году 58% населения Беларуси осуществляли пользование Интернетом, то в 2022 году этот показатель увеличился до 89,5% [8].

За последние годы отмечается увеличение количества зарегистрированных киберпреступлений на международном и национальном уровне. В Республике Беларусь особый прирост приходится на 2020 г. в связи с COVID-19. Так, во время пандемии было зарегистрировано около 25 561 преступлений в сфере высоких технологий. В 2021 и 2022 гг. происходит снижение показателей до 15 503 в 2021 г. и 11 707 в 2022 г. В 2023 г. опять наблюдается тенденция по увеличению киберпреступлений до 15 000 [9]. Следует иметь ввиду, что киберпреступность обладает высокой латентностью. Согласно экспертным данным, о 85–90% совершенных киберпреступлений не сообщается в правоохранительные органы, либо они остаются необнаруженными [10, с. 8].

Необходимо также отметить, что доля компьютерных преступлений в общей структуре преступности также увеличивается из года в год. Если

в 2022 г. в общей структуре насчитывалось 16,5% киберпреступлений, то уже в 2023 г. их доля от общего числа составила 21,5% [9].

По Витебской области количество киберпреступлений в общей структуре составило в 2023 г. около 19%, при этом более 80% преступлений пришлось на долю мошенничества и хищения имущества путем модификации компьютерной информации. На начало 2024 г. по Витебской области пострадало от киберпреступлений свыше 800 человек [11].

В настоящее время провести классификацию киберпреступлений довольно затруднительно, так как в каждой стране есть свои особенности, характеризующие данные преступные деяния, разные составы. Немаловажным является и тот факт, что появляются новые составы компьютерных преступлений в связи с развитием ИКТ. В соответствии с законодательством Республики Беларусь преступления в сфере высоких технологий можно разделить на следующие группы:

1 преступления против собственность, квалифицирующиеся по главе 24 УК Республики Беларусь (это, например, преступления, связанные с завладением, повреждением или уничтожением средств компьютерной техники или сети, носителей информации);

2 преступления против компьютерной безопасности, которые закреплены в главе 31 УК Республики Беларусь [12].

Среди названных групп компьютерных преступлений наиболее часто в Республике Беларусь совершаются деяния, предусмотренные ст. 212 УК – «хищение имущества путем модификации компьютерной информации». Под «модификацией компьютерной информации» следует понимать «противоправное изменение компьютерной информации либо внесение в компьютерную систему заведомо ложной компьютерной информации» [6]. В общей доле компьютерных преступлений они составляют около 90%. Отличительными признаками данных преступлений являются два показателя:

– совершение хищения имущества – путем модификации компьютерной информации осуществляется посредством использования компьютерной техники;

– возможность совершения данного вида киберпреступления, не выходя из дома.

Обращаясь к судебной практике, в качестве примера можно привести дело, рассмотренное судом Докшицкого района по ч. 1 ст. 212 УК Республики Беларусь. Исходя из материалов дела было установлено, что лицо, умышленно завладев банковской картой жертвы, осуществляло на протяжении определенного промежутка времени платежи в различных торговых объектах. При осуществлении данных платежей лицо выдавало себя за владельца банковской карты. По итогам рассмотрения дела суд постановил обвинительный приговор и назначил наказание в виде штрафа в размере 60 базовых величин [13].

Немаловажной и неотъемлемой частью при рассмотрении киберпреступлений является криминологическая характеристика лиц, которые совершают киберпреступления и их жертв. Исследование особенностей личности киберпреступников и жертв данных преступлений, будут способствовать в расследовании и раскрытии преступлений, их профилактике и предупреждении.

Рассмотрим более подробно некоторые характеристики лиц, совершающих киберпреступления.

– социально-демографические свойства указывают на то, что наиболее склонны к совершению компьютерных преступлений лица мужского пола (около 70%) в возрасте от 18 до 24 лет (около 38%), которые не работают и имеют образование среднее либо высшее в сфере высоких технологий;

– социально-психологические и уголовно-правовые свойства характеризуются, наряду с прочими, следующими элементами: мотив – то, что «толкает» лиц на совершение противоправных действий или бездействие (например, стремление лица самоутвердиться) и цель – это конечный результат, к которому стремится лицо (например, получение денежной выгоды);

– нравственно-психологические свойства: к совершению киберпреступлений склонны лица, которые не состоят в браке, у них низкий уровень сопереживания, а, также высокий уровень эгоцентричности [14, с. 66].

В литературе приводятся различные классификации киберпреступников. Так, выделяются, например, следующие группы: хакеры и кракеры; лица, страдающие компьютерными фобиями; профессиональные преступники [15, с. 298].

Подразделяют киберпреступников также на начинающих киберпреступников – лиц, которые ранее не совершали противоправные деяния в сфере высоких технологий и только начинают свой криминальный путь, устойчивых киберпреступников – лиц, которые раньше совершали киберпреступления, но не были привлечены к уголовной ответственности за противоправные деяния, профессиональных киберпреступников – лиц, которые уже раньше были осуждены за совершенные киберпреступления [16, с. 104].

Для жертв киберпреступлений характерны два типа поведения:

– активное поведение, которое заключается в частом пользовании Интернетом, социальными сетями и т.д. В этом случае лица зачастую утрачивают бдительность и забывают о безопасном пользовании Интернетом, в результате чего становятся легкой «мишенью» для киберпреступника;

– агрессивное поведения, которое разделяется на проактивное (когда жертва сама своими действиями провоцирует другое лицо на совершение противоправных действий) и реактивное (здесь агрессия проявляется именно у киберпреступника и на такое поведение реагирует жертва) [17, с. 38].

Основываясь на статистических показателях, которые отражают характерные данные жертв киберпреступлений, можно сделать вывод о том, что жертвами выступают лица мужского пола в возрасте от 30 до 60 лет

[18, с. 62]. Однако в последние годы отмечается тенденция к увеличению количества жертв женского пола, в частности, за 2023 г. по Витебской области этот показатель превысил 60% [11].

К числу криминогенных условий, детерминирующих киберпреступления, можно отнести:

– недостаточный уровень контроля (надзора) со стороны общества и государства за преступлениями в сфере высоких технологий либо вообще отсутствие такого контроля (надзора);

– появление новых видов киберпреступлений, а также трансформация старых преступлений в новые, которые совершаются посредством ИКТ [19, с. 37];

– правовой фактор, который заключается в недостаточном уровне развития соответствующего законодательства, когда темпы развития киберпреступности опережают их криминализацию;

– организационно-технический фактор, связанный с недостаточным уровнем подготовки правоохранительных органов, нехваткой современных технических средств, способствующих расследованию и раскрытию рассматриваемых преступлений.

Мировые тенденции киберпреступности и ее состояние находят свое отражение в ежегодном отчете Европола IOCTA–2023. В последних отчетах отмечается, что компьютерные преступления все больше становятся взаимосвязанными и дополняющими друг друга. Это вызвано тем, что преступникам, действующим в сфере высоких технологий, выгоднее сотрудничать друг с другом для проведения успешной преступной деятельности [20].

Исходя из отчета IOCTA–2023, можно сделать вывод о том, что основными направлениями в современной киберпреступности являются:

– использование VPN (в качестве маскировки и скрытия сведений о лице, которое совершает компьютерное преступление. Их популярность среди киберпреступников обусловлена тем, что провайдеры не предоставляют сведения о своих клиентах правоохранительным органом, в результате поймать таких лиц практически невозможно);

– использование Darknet («теневой» Интернет используется среди злоумышленников как средство общения, а также как основной источник получения запрещенной или ограниченной в распространении информации);

– использование вредоносных программ (которые нацелены на получение данных других лиц с последующим их использованием в противоправных намерениях) [20].

При рассмотрении основных направлений и тенденций в Республике Беларусь в области киберпреступлений, можно сделать вывод о том, что они, в принципе, совпадают с мировыми. Так, на национальном уровне характерны следующие преступления в области высоких технологий:

– использование вредоносных программ, а частности программ–вымогателей паролей, которые направлены на завладение чужих данных

с целью их дальнейшего использования. Такие программы могут рассылать сообщения через электронные почты или SMS-сообщения лицам с ложными уведомлениями о денежных и вещевых выигрышах или трудоустройстве;

– распространение контента сексуального характера с участием несовершеннолетних. Следует также отметить, что в последнее время участились случаи, когда именно сами несовершеннолетние распространяют такой контент;

– в связи с развитием электронных приложений, которые значительно облегчили жизнь общества, появились и новые преступления в данной области, в частности, такие преступления связаны с мобильным банкингом, а также с созданием специальных онлайн-платформ, которые копируют оригинальные сайты;

– использование Глобальной сети Интернет для совершения преступлений, связанных с незаконным оборотом наркотических средств, психотропных веществ и иных запрещенных веществ [21, с. 269].

Поскольку на данный момент киберпреступность приобрела транснациональный характер и является глобальной угрозой, государства осуществляют международное сотрудничество путем проведения международных конференций и форумов, обмена опытом между сотрудниками и т.д. Примером может служить форум «ЦИФРОПОЛ–2024», в котором участвуют МВД государств-участников СНГ. В ходе данного форума рассматриваются вопросы, связанные с осуществлением международного сотрудничества в целях снижения количественных и качественных показателей киберпреступности, в частности проблемы борьбы с преступлениями в сфере высоких технологий посредством DarkNet и искусственного интеллекта [22].

Среди международных актов, регулирующих вопросы международного сотрудничества в странах СНГ, можно выделить Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере компьютерной информации (далее – Соглашение) от 01.06.2001 г. Данное соглашение выделяет формы сотрудничества, которые могут быть осуществлены между странами:

– обмен информацией;

– исполнение запросов;

– сотрудничество в области осуществления кадровой политики;

– создание информационных систем и др. [23].

Сотрудничество в противодействии киберпреступности осуществляется на основе следующих принципов:

– уважение суверенитета государств-участников, их национального законодательства, общепризнанных принципов и норм международного права;

– равноправие сторон;

– приоритет защиты прав и свобод человека и гражданина;

– совершенствование сотрудничества компетентных органов государств-участников;

– создание благоприятных условий для совместных усилий в противодействии киберпреступности [24, с. 405].

В Республике Беларусь в структуре государственных органов, составляющих систему органов, осуществляющих противодействие киберпреступности, особую роль играет оперативно-аналитический центр при Президенте Республики Беларусь, который осуществляет регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты и иные сведения. В 2023 г. на основании Указа Президента Республики Беларусь № 40 от 14.02.2023 «О кибербезопасности» была создана новая «национальная система обеспечения кибербезопасности, элементами которой являются: Оперативно-аналитический центр при Президенте Республики Беларусь; Национальный центр обеспечения кибербезопасности и реагирования на киберинциденты; центры обеспечения кибербезопасности и реагирования на киберинциденты объектов информационной инфраструктуры государственных органов и иных организаций; оператор электросвязи по взаимодействию Национального центра кибербезопасности, центров кибербезопасности, а также государственных органов и иных организаций; объекты информационной инфраструктуры государственных органов и иных организаций; сети передачи данных, используемые для взаимодействия элементов национальной системы обеспечения кибербезопасности» [25].

Республика Беларусь, как и другие государства, ставит перед собой задачу по обеспечению информационной безопасности общества и государства. Среди направлений обеспечения кибербезопасности, можно выделить следующие:

– правовое: совершенствование действующей системы законодательства, с целью устранения пробелов, введение новых норм и изменений, дополнений или отмена уже существующих норм в соответствии с развитием ИКТ;

– организационно-техническое: обеспечение правоохранительных органов необходимым оборудованием, средствами и устройствами для осуществления расследования и раскрытия преступлений;

– организационно-управленческое: защита информации от несанкционированного доступа [26, с. 129].

Правоохранительные органы принимают все меры по обеспечению кибербезопасности и проводят профилактику киберпреступлений посредством, в числе прочего, проведения мероприятий для граждан любого возраста, которые нацелены на повышение информационной и правовой грамотности населения. В качестве примера можно привести «Декаду кибербезопасности», которая проводится ежегодно на протяжении последних нескольких лет [27, с. 449].

Анализ современного состояния и тенденций развития киберпреступности на международном и национальном уровне, показывает, что

в связи с увеличением числа регистрируемых компьютерных преступлений, основной задачей как международного сообщества, так и отдельных государств является снижение количественных и качественных показателей киберпреступности, прежде всего, путем проведения профилактических мероприятий и усовершенствования действующего законодательства, как на международном уровне, так и на национальном. Помимо этого, необходимо проведение политики повышения цифровой грамотности населения посредством использования современных средств массовой информации, проведения различного уровня мероприятий, направленных на решение этой задачи. Мы полагаем, что также будет способствовать снижению уровня киберпреступлений разработка и реализация комплексных планов мероприятий по профилактике и противодействию киберпреступности на всех уровнях, от общенационального и регионального, до локальных – на предприятиях, в учреждениях, по месту жительства граждан.

Успех в противодействии киберпреступности зависит от слаженного сотрудничества между государственными, правоохранительными органами, структурами гражданского общества.

Список использованных источников

1. Концепция национальной безопасности Республики Беларусь: утверждена Решением Всебелорусского народного собрания № 5 от 25.04.2024 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр законодательства и правовой информ. Респ. Беларусь. – Минск, 2024.

2. История Интернета (краткая история) [Электронный ресурс]. – Режим доступа: https://ria.ru /20210806 /internet-1744333745.html?clckid = 58b9d736. – Дата доступа: 22.06.2024.

3. Овчинский, В.С. Криминология цифрового мира: учебник для магистратуры / В.С. Овчинский. – М.: Норма: ИНФРА-М, 2018. – 352 с.

4. ETS 185 – Convention on Cybercrime, 23.XI.2001[Электронный ресурс]. – Режим доступа: https: // www.europarl.europa.eu / meetdocs / 2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf. – Дата доступа: 22.06.2024.

5. Киберпреступность: криминологический, уголовно-правовой, уголовно-процессуальный и криминалистический анализ / науч. ред. И.Г. Смирнова; отв. ред. О.А. Егерева, Е.М. Якимова. – М., 2016.

6. 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 / Нац. центр законодательства и правовой информ. Респ. Беларусь. – Минск, 2024.

7. Компьютерная безопасность: правовая характеристика и ответственность [Электронный ресурс]. – Режим доступа: https://normativka.by/lib/

document/106659/sid/505bbec85c074ad7a3ec1648dc97b33c?clckid=f14b77f0. – Дата доступа: 23.06.2024.

8. Информационное общество в Республике Беларусь – 2023 / Национальный статистический комитет Республики Беларусь; редкол.: Т.В. Максимова [и др.]. – Минск: Национальный статистический комитет Республики Беларусь, 2024. – 65 с.

9. Сведения о совершенных правонарушениях на территории Республики Беларусь / Информационный центр МВД Республики Беларусь. – Минск, 2004 – 2022; Национальный статистический комитет Республики Беларусь [Электронный ресурс]. – Режим доступа: http://dataportal.belstat.gov.by/Indicators/Search?code=1063066. – Дата доступа: 14.06.2024.

10. Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений для специальности II ступени высшего образования (магистратура) 1-24 80 01 Юриспруденция: учебно-методический комплекс по учебной дисциплине / сост.: Т.Ф. Дмитриева, В.Г. Стаценко. – Витебск: ВГУ имени П.М. Машерова, 2022. – 83 с.

11. Жертвами кибермошенников в Витебской области с начала года стали более 800 человек [Электронный ресурс]. – Режим доступа: https://www.belta.by/regions/view/zhertvami-kibermoshennikov-v-vitebskoj-oblasti-s-nachala-goda-stali-bolee-800-chelovek-637094-2024/. – Дата доступа: 19.06.2024.

12. Правотворчество и правоприменение в контексте Концепции правовой политики Республики Беларусь [Электронный ресурс]: монография: текстовое электронное издание / В.В. Козловская [и др.]; под ред. С.В. Агиевец; М-во образования Республики Беларусь, Учреждение образования «Витебский государственный университет имени П.М. Машерова», Юридический фак. – Витебск: ВГУ имени П.М. Машерова, 2023. – 143 с. URL.: https://rep.vsu.by/handle/123456789/40740 (дата обращения: 25.06.2024).

13. Архив суда Докшицкого района за 2023 г. – Уголовное дело № 31У2336.

14. Беломытцев, Н.Н. О лице, совершившем хищение путем использования компьютерной техники / Н.Н. Беломытцев // Юстиция Беларуси. – 2019. – № 1(202). – С. 61–66.

15. Козел, А.Н. Личность киберпреступника / А.Н. Козел // IV Международная научно-практическая конференция молодых ученых «Вектор 3.0» = IV International scientific and practical conference of young researcher «Vector 3.0»: материалы IV Международной научно-практической конференции, Витебск, 17 апреля 2024 г.: электронное научное издание / редкол.: И. В. Николаева (гл.ред.) [и др.]. – Витебск: Витебский филиал Международного университета «МИТСО», 2024. – С. 137–140.

16. Григорян, С.А. Особенности личности современного «киберпреступника» / С.А. Григорян // Наука и образование: хозяйство и экономика; предпринимательство; право и управление. – 2022. – № 8(147). – С. 103–106.

17. Айнутдинова, К.А. Виктимологические особенности киберпреступности в условиях цифровой трансформации общества / К.А. Айнутдинова // Наука, образование: современные цифровые технологии формирования экосреды инновационного развития региона в условиях системных преобразований: материалы национальной научно-практической конференции, Казань, 2 декабря 2022 г. / редкол.: А.Н. Грязнова, А.М. Найда [и др.]. – В 2-х ч. – Казань: ИЦ Университета управления «ТИСБИ», 2022. – Ч. 1. – С. 34–40.

18. Стаценко, В.Г. Особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь / В.Г. Стаценко // Правотворчество и правоприменение в контексте концепции правовой политики Республики Беларусь: монография: текстовое электронное издание / В.В. Козловская [и др.]; под ред. С.В. Агиевец; М-во образования Республики Беларусь, Учреждение образования «Витебский государственный университет имени П.М. Машерова», Юридический фак. – Электрон. текст. дан. (1 файл, 1,13 МБ). – Витебск: ВГУ имени П.М. Машерова, 2023. – С. 57–72. URL: https://rep.vsu.by/handle/123456789/40740 (дата обращения: 25.06.2024).

19. Евдокимов, К.Н. Противодействие компьютерной преступности: автореф. дис. … 12.00.08 / К.Н. Евдокимов; Университет прокуратуры Российской Федерации. – Москва, 2022. – 73 с.

20. Отчет Европола IOCTA–2023 показывает, что киберпреступники становятся все более взаимозависимыми [Электронный ресурс]. – Режим доступа: https://www.techrepublic.com/article/europol-internet-organised-crime-threat-assessment/?clckid=ac843f17. – Дата доступа: 25.06.2024.

21. Третьяков, Г. Сравнительный анализ тенденций развития преступлений, совершаемых путем использования компьютерной техники, в Республике Беларусь и за рубежом / Г. Третьяков // Підприємництво, господарство і право – 2020. – № 11. – С. 266–270.

22. 18 апреля 2024 года в Московском университете МВД России имени В.Я. Кикотя состоялся Международный форум «ЦИФРОПОЛ–2024» [Электронный ресурс]. – Режим доступа: https://pravo.hse.ru/proclaw/news/919711131.html. – Дата доступа: 26.06.2024.

23. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. [Электронный ресурс] // ЭТАЛОН. Законодательство Республики Беларусь / Национальный центр правовой информации Республики Беларусь. – Минск, 2024.

24. Бородич, А.И. Международное право: учебное пособие / А.И. Бородич; учреждение образования «Акад. М-ва внутр. Дел Респ. Беларусь». – Минск: Академия МВД, 2020. – 462 с.

25. О кибербезопасности [Электронный ресурс]: Указ Президента Республики Беларусь от 14.02.2023 г. № 40 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр законодательства и правовой информ. Респ. Беларусь. – Минск, 2024.

26. Черняк, С.А. О профилактике киберпреступности в Республике Беларусь / С.А. Черняк // Проблемы борьбы с преступностью и подготовки кадров для правоохранительных органов: междунар. науч.-практ. конф., Минск, 28 января 2022 г.: тез. докл. / редкол.: П.В. Гридюшко (отв. ред.) [и др.]. – Минск: Академия М-ва внутр. дел Респ. Беларусь, 2022. – С. 128–130.

27. Татарчук, Е.И. Особенности профилактики киберпреступности в Беларуси / Е.И. Татарчук // Научный поиск курсантов: сборник материалов Международной научной конференции, Могилев, 16 февраля 2022 г.: Министерство внутренних дел Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь» / редкол.: В.В. Борисенко (отв. ред.) [и др.]. – Могилев: Могилев. Институт МВД, 2022. – 1 электрон. опт. диск (CD-R). – С. 449–450.

ГЛАВА 4. ПРЕДУПРЕДИТЕЛЬНАЯ ДЕЯТЕЛЬНОСТЬ КАК СПОСОБ СДЕРЖИВАНИЯ ПРЕСТУПНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Предупреждение преступности несовершеннолетних – актуальная и сложная задача для каждого государства. Значительная часть преступлений, совершаемых данными лицами, воспринимается окружающими как, проявление возрастной незрелости, неумения правильно оценивать факты и явления общественной жизни, сопоставлять свои поступки с требованиями общественной необходимости. Поэтому о многих из них не сообщается в правоохранительные органы, что увеличивает их латентность.

Проблема преступности среди подростков сохраняет свою актуальность вне зависимости от существенного сокращения объема и уровня преступности. Несмотря на усеченный круг лиц (в возрасте 14–17 лет) и преступлений, за которые подросток может быть привлечен к уголовной ответственности, преступность несовершеннолетних в общем числе лиц, совершивших преступление, остается относительно высокой и составляет порядка 3–4% (таблица 1).