ЭВОЛЮЦИЯ КИБЕРПРЕСТУПНОСТИ И ЕЕ ПРОЯВЛЕНИЕ КАК СОВРЕМЕННОЙ УГРОЗЫ

Бутунбаев Тимур Нурйигитович
независимый соискатель Университета общественной безопасности Республики Узбекистан

Аннотация. *В данном тезисе анализируется процесс формирования киберпреступности, ее исторические этапы, а также специфические технологические и социальные аспекты каждого периода. На основе представленной информации раскрыты предварительные проявления киберпреступлений, механизмы их совершения с помощью технических средств, а также новые угрозы, возникающие в современную эпоху на глобальном и национальном уровнях.*

Ключевые слова: *киберпреступность, компьютерные преступления, киберпространство, информационная безопасность, правовое регулирование, эволюция, эпоха, хакерство, цифровая безопасность.*

Стремительно развивающиеся современные глобальные процессы ставят перед государствами задачу перехода к полноценной цифровой экономике путем разработки высокотехнологичных решений, создания передовых информационно-технических средств и развития программного обеспечения, внедрения современных инноваций во все отрасли экономики (производство, торговля, сфера услуг, коммуникации и образование).

В мире ущерб, причиняемый киберпреступлениями, увеличивается в среднем на 15% в год. Этот показатель в 2021 году составил 6 трлн., в 2022 году - 8 трлн., в 2023 году - 11 трлн. долларов США, к 2026 году прогнозируется достижение ущерба в 20 трлн долларов США. Это больше, чем незаконные доходы от стихийных бедствий, торговли оружием или наркотиками[1].

В Узбекистане данные тенденции также находят своё отражение в национальных показателях. В частности, согласно данным выборочного обследования домашних хозяйств, проведённого Комитетом по статистике, доля населения, пользующегося интернетом, в январе–августе 2025 года составила 94,2 %. В разрезе по годам данный показатель составлял: в 2021 году – 76,6 %, в 2022 году – 83,9 %, в 2023 году – 89 %, в 2024 году – 93,3 %, а по состоянию на август 2025 года – 94,2 % [2].

Известно, что понимание сущности каждого социального явления или действительности требует, прежде всего, глубокого изучения его

эволюционных корней и исторических источников. В связи с этим изучение возникновения информационных технологий или компьютерных преступлений, этапов историко-правового развития служит эффективному использованию этого института в правоприменительной практике, обеспечению сочетания теории и практики и его совершенствованию.

Преступления, связанные с незаконным (несанкционированным) использованием компьютерной информации, являются наиболее распространенными преступлениями в киберпространстве, которые можно разделить на следующие виды: мошенничество, связанное с платежами (хищение с использованием платежных карт или информации о них); скимминг (преступления, связанные с использованием банкоматов); хищения, связанные с вредными платежными программами (хищения, связанные с разработкой и использованием вредоносных программ); социальный инжиниринг (приобретение информации в корыстных целях); фишинг (приобретение права доступа к персональным данным путем распространения электронных писем); онлайн-мошенничество (хищения, связанные с уязвимостью платформ, таких как интернет-магазины, бронирование авиабилетов, аренда автомобилей) [3]; хакинг (действия после несанкционированного доступа к компьютерной системе); веб-джекинг (захват управления веб-сайтом для использования

в злонамеренных целях) [4]; кибersталлинг (преследование или вымогательство с использованием интернета); KRACK (атака путем переустановки защитного ключа, получение зашифрованных данных через Wi-Fi) и т.д.

Первые случаи такого рода преступлений были зарегистрированы еще до распространения Интернета. Компьютеры, компьютерные сети и Интернет специально созданы для хранения и передачи правительственных и корпоративных данных, которые влияют на государственную и общественную безопасность, и владение такой информацией всегда вызывает большой интерес у преступников.

Историю и эволюцию компьютерной преступности (киберпреступлений) можно изучать, разделив на пять периодов с учетом их особенностей и специфики каждого периода. Первые проявления киберпреступности были непосредственно связаны с развитием интернета, первоначально проявляясь в форме взлома местных телефонных сетей.

Первый период - пионерский и «экспериментальный» (1960 - 1978 гг.). В этот период начали появляться первые элементы киберпреступлений - случаи взлома телефонных сетей (фрикинга). В основном эксперименты проводились в Массачусетском технологическом институте (MIT) и на

телекоммуникационных системах США (например, Д. Дрейпер, известный как «Cap'n Crunch», обнаружил незаконный доступ к телефонным сетям с частотой 2600 Гц). В этот период противоправные деяния совершались преимущественно по мотивам опыта или интереса.

В качестве инструмента использовались такие устройства, как BlueBox, простые методы взлома кода. Хотя в начальный период киберпреступность находилась на уровне «хобби», именно этот фактор заложил основу для последующих процессов. В этот период в Узбекистане информационные технологии еще не проникли, и подобных экспериментов не наблюдалось.

Второй период - вторая большая волна компьютерной преступности начался в конце 80-х годов прошлого века с распространением электронной почты. При этом в электронные почтовые ящики пользователей были введены вредоносные программы и получены персональные данные.

В этот период появились коллективные формы хакерства. Появился активный обмен программным обеспечением, вирусами и паролями через Bulletin Board Systems (BBS), Usenet и электронную почту. Создавались хакерские группы, которые развивали обмен опытом и мошенническую деятельность. В то же время хакерство сформировалось как определенный образ в обществе через такие культурные феномены, как фильм «WarGames», журнал «2600». В этот период также были широко распространены ранние вирусы. Хотя эти процессы не были непосредственно заметны в Узбекистане, в 1980-х годах знания об информационных технологиях и программных рисках начали поступать через научно-техническую литературу.

Третий период совпадает с развитием веб-браузеров в 1991 году.

С популяризацией Интернета и развитием веб-браузеров киберпреступления перешли на новый уровень. Появились «черви (warm)» и макровирусы, распространяемые по электронной почте, а также первые проявления мошенничества. Когда пользователи посещают подозрительные сайты, компьютер начинает работать медленно из-за отправленных вирусов, на экране неожиданно появляются реклама и объявления, или пользователь перенаправляется на порнографические сайты.

Арест Kevin Mitnicka и «Morris worm»а, созданный Робертом Моррисом, привлекли всеобщее внимание. В этот период усилилось совершение киберпреступлений в погоне за экономическими интересами. В Узбекистане же, поскольку интернет начал широко распространяться с конца 1990-х годов, в этот период наблюдались первые проявления фишинга, вирусов и программных атак.

Четвертый период - период DoS-атак, ботнетов и корпоративных рисков (2001-2010 гг.). В 2000-х годах киберпреступления вышли на новый уровень, широко распространились DoS/DDoS-атаки, ботнеты и автоматизированные вредоносные программы. Ярким примером являются атаки, которые привели к краху таких крупных сайтов, как Yahoo!, eBay, Amazon. В то же время удаленно управляемые программы, такие как Back Orifice, резко обострили проблемы безопасности.

Хотя, по данным лаборатории Касперского, за 15 лет (1992 - 2007 годы) было выявлено около 2 миллионов вредоносных программ, только в 2008 году этот показатель достиг 15 миллионов. В первом квартале

2013 года было выявлено 22 750 новых модификаций вредоносных программ для мобильных телефонов, что составляет более половины модификаций, обнаруженных в 2012 году. В 2020 году было обнаружено более 33,4 миллиона вредоносных объектов, и каждый десятый компьютер интернет-пользователей подвергался атаке в виде вредоносного программного обеспечения хотя бы один раз [7].

Именно события, произошедшие в четвертый период, стали причиной возникновения и развития социальных сетей. Люди добровольно размещают свою личную информацию в Интернете, что делает их лёгкой жертвой для хакеров. При этом были похищены персональные данные, предоставлен незаконный доступ к банковским счетам и различные финансовые мошенничества. В этот период основной мотив киберпреступлений был направлен на получение финансовой выгоды. В Узбекистане, наряду с расширением интернет-сетей, широко распространились «компьютерные вирусы», и информационные системы государственных органов и крупных предприятий начали серьезно страдать от кибератак.

Пятый период - эпоха мобильных, социальных сетей

и профессиональных киберпреступлений (с 2010 года по настоящее время). Главным признаком этого этапа является развитие смартфонов, социальных сетей и технологий IoT. Киберпреступления теперь совершаются в глобальном масштабе на уровне профессиональных групп и даже государств. Широкое распространение получили такие передовые методы, как вымогательство, фишинг, социальная инженерия, атака цепочки поставок. Киберпреступность теперь поднята до уровня «услуги» (crime-as-a-service), активно используется в экономических, политических и разведывательных целях. В Узбекистане в последние годы, наряду с ростом использования интернета и мобильных приложений, наблюдаются случаи

мошенничества с банковскими картами, кражи персональных данных в социальных сетях и атаки на государственные информационные системы.

Из вышеизложенного можно сделать вывод, что системное изучение историко-эволюционных этапов киберпреступности, факторов их формирования, технологических основ и социально-правовых последствий создает важную научную основу для глубокого понимания этого явления. Анализ, подобный приведенному выше, позволяет не только выявить тенденции развития киберпреступлений, но и научно сформировать их структурные особенности, субъект-объектные отношения и правовые механизмы. В результате, на основе изученных периодических этапов, можно оптимизировать правовые, организационные и технические направления борьбы с современной киберпреступностью, приблизить национальное законодательство к международным стандартам и усовершенствовать политику кибербезопасности.

СПИСОК ИСПОЛЬЗОВАННЫХ ЛИТЕРАТУР:

1. Estimated cost of cybercrime worldwide 2018-2029. https://www. statista.com/forecasts /1280009/cost-cybercrime-worldwide. (Дата обращения к электронному источнику: 2025-yil 18-avgust)

2. https://t.me/statistika_lotin/1604. (Дата обращения к электронному источнику: 03.10.2025)

3. Jahankhani H., Al-Nemrat A., Hosseinian-Far A. Cybercrime classification and characteristics // Cyber Crime and Cyber Terrorism Investigator’s Handbook. Waltham, 2015. p. 215–221. (Дата обращения к электронному источнику: 9.02.2023)

4. https://digit.in/technology-guides/fasttrack-to-cyber-crime/the types-of-cyber-crime. https://kaspersky.ru/(Дата обращения к электронному источнику: 12.02.2023)

5. https://securelist.ru/kaspersky-security-bulletin-2009-razvitie-ugroz-v-2009-godu/1383/ (Дата обращения к электронному источнику: 13.02.2023)

6. https://securelist.ru/razvitie-informatsionny-h-ugroz-v-perv-3/216/ (Да т а обращения к электронному источнику: 13.02.2023)

7. www.securelist.com/kaspersky-security-bulletin-2020-statistics/99804 (Дата обращения к электронному источнику: 13.02.2023).