5. Felder R., Victor B. Getting Away With Murder: Weapons for the War Against Domestic Violence. – New York. 1997.
6. Бытовое насилие в Казахстане: «Все это свалилось на нас буквально за месяц» // Новости ООН. URL: https://news.un.org/ru/interview/2020/05/1377672].
7. file:///Users/zhuldyz/Downloads/latentnost-domashnego-nasiliya-v-respublike-kazahstan-na-sovremennom-etape%20(1).pdf
8. Юрченко Р. Применение судами норм Закона РК «О профилактике бытового насилия»: Комментарий к Закону Республики Казахстан «О профилактике бытового насилия»
9. Актуальные проблемы противодействия бытовому насилию: Материалы Правительственного часа в Мажилисе Парламента Республики Казахстан. – Астана, 2017. – 172 с.
10. Овчинский В. С. Криминальное насилие против женщин и детей: Международные стандарты противодействия // М.: Норма, 2008.

УДК 343.3/.7

## ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ В РЕСПУБЛИКЕ КАЗАХСТАН

**Мухамеджанов Алмасбек Бахытжанович**
**almasmv@gmail.com**
магистрант 2 курса кафедры уголовно-правовых дисциплин
ЕНУ им. Л.Н. Гумилева, Нур-Султан, Казахстан
Научный руководитель - Онгарбаев Е.А.

Современные тенденции преступного мира диктуют новые условия их предупреждения и противостояния. Широкое использование компьютерных технологий в общественных отношениях, в ежедневных бытовых условиях, способствует тому, что все больше преступлений совершается с использованием современных компьютерных технологий.

В преступной среде появился новый вид преступности, с использованием компьютерных технологий, который получил название «киберпреступность». Преступления, совершаемые с использованием компьютерных технологий увеличивают общественную опасность как отдельной личности, так и интересам общества и государства. Наибольшее количество киберпреступлений совершается в глобальной сети Интернет, с использованием компьютеров, сотовых телефонов, а также иных устройств, имеющих выход в сетевое пространство. Уголовное законодательство разных стран не адаптировано к киберпреступлениям, именно поэтому киберпреступники почти безнаказанно совершают преступления в компьютерной сфере, несмотря на то, что различные сферы общественной жизни адаптировались в информационной сфере, например такие, как наука, образование, финансовые операции, банковские услуги, торговая деятельность и ряд иных преступлений. С использованием компьютерных технологий совершаются даже преступления против личности, доведение до самоубийства.

Увеличение роста преступлений, связанных с использованием компьютерных технологий, повысил научный интерес к данной проблематике у практических работников и ученых-юристов. Вопросы, связанные с различными аспектами проблем об ответственности за преступления в сфере компьютерной информации, раскрывались в научных работах М.В. Богомолова, В.М. Быкова, А.Г. Волеводза, В.Д. Гавловского, А.Ю. Головина, В.О. Голубева, Е.В. Громова, Ю.В. Добрынина, К.Н. Евдокимова, А.П. Кузнецова, В.Е. Козлова, Ю.А. Мерзогитовой, О.В. Мосина, И.М. Рассолова, А.А. Протасевич, В.П. Сабадаш, А.Г. Серго, С.А. Середы, Н.А. Сивицкой, А.В. Сизова, В.С. Цымбалюка, В.Н. Черкасова, И.Г. Чекунова, А.Ю.Чупровой, Д.Л. Шиндер, и ряда других ученых.

Республика Казахстан, обретая государственный суверенитет, также предприняла ряд профилактических мер с целью предупреждения преступлений, связанных с использованием компьютерных технологий. Так, например, начиная с 1998 года, было принято постановление Правительства Республики Казахстан от 31 декабря 1998 года № 1384 "О координации работ по формированию и развитию национальной информационной инфраструктуры, процессов информатизации и обеспечению информационной безопасности".

Также было принято 3 новых редакции законов Республики Казахстан "Об информатизации" (2003, 2007, 2015 годы) и несколько специализированных законов Республики Казахстан о внесении в них соответствующих изменений по вопросам электронных форматов представления информации (данных) в том числе по вопросам информационно-коммуникационных сетей, "электронного правительства".

Позже, 30 июня 2017 года была разработана Концепция кибербезопасности ("Киберщит Казахстана") (далее – Концепция) разработана в соответствии с Посланием Президента Республики Казахстан "Третья модернизация Казахстана: Глобальная конкурентоспособность" с учетом подходов Стратегии "Казахстан-2050" по вхождению Казахстана в число 30-ти самых развитых государств мира. Данная Концепция формировалась с учетом требований Закона Республики Казахстан "О национальной безопасности" и основана на оценке текущей ситуации в сфере информатизации государственных органов, автоматизации государственных услуг, перспектив развития "цифровой" экономики и технологической модернизации производственных процессов в промышленности, расширения сферы оказания информационно-коммуникационных услуг.

Данная Концепция призвана обеспечить единство подходов к мониторингу обеспечения информационной безопасности государственных органов, физических и юридических лиц, а также выработку механизмов предупреждения и оперативного реагирования на инциденты информационной безопасности, в том числе в условиях чрезвычайных ситуаций социального, природного и техногенного характера, введения чрезвычайного или военного положения [1].

В новой редакции Уголовного кодекса Республики Казахстан [2], действующего с 1 января 2015 года, предусмотрена отдельная глава, посвящённая преступлениям, совершаемым в сфере информатизации и связи. С учётом квалифицирующих обстоятельств в ней содержится 38 составов преступлений против электронных информационных ресурсов и систем или сетей телекоммуникаций.

Для современных преступлений, совершаемых с использованием компьютерных технологий характерны следующие особенности:

1) сложные преступные схемы, с участием представителей различных структур;

2) совершение киберпреступлений организованной преступной группой, участники которой могут быть как в государственных, так и частных структурах;

3) сочетание киберпреступлений с различными видами уголовных преступлений, нанося неоценимый вред общественным отношениям;

4) расширение транснациональной структуры преступлений, совершаемых с использованием современных компьютерных технологий.

5) использование в процессе совершения киберпреступлений несовершеннолетних лиц с учетом отсутствия уголовной ответственности несовершеннолетних по многим видам преступлений;

6) совершение киберпреступлений в отношении самих несовершеннолетних, используя их наивность и доверие.

Современные компьютерные технологии, глобальные сети Интернет, создают удобные предпосылки для совершения различных видов уголовных преступлений, собственно, такие технологии представляют собой весьма удобное орудие и средство для совершения общественно опасных деяний. Ежедневно появляются новые компьютерные технологии, которые способствуют облегчению трудовых процессов, но вместе с тем, облегчается совершение преступных деяний по многим статьям уголовного законодательства. Такие возможности особо привлекают преступников, совершающих преступления террористического и экстремистского характера, экономические преступления, а также преступления против собственности, против личности и иных общественных интересов.

Также, привлекательной стороной таких видов преступлений является и то, что большая часть преступлений в сети Интернет не оставляет ярко выраженных следов, охватывает большой круг лиц, требует специальной подготовки и хорошие познания в информационных технологиях. В качестве примера можно привести мессенджер «Telegram», которым активно пользуются преступники, так как данный мессенджер с помощью шифрования полностью защищает данные пользователя, в связи с чем его сложно найти и привлечь к уголовной ответственности.

Особо распространенным видом преступлений в глобальной сети Интернет является мошенничество в отношении личного имущества граждан. Такие характерные особенности киберпреступлений как высокая степень анонимности, бесконтрольность и неподчиненность глобальной сети, низкие затраты на организацию деятельности очень привлекают мошенников, которые все чаще используют ее возможности для реализации своих преступных замыслов. К основным способам мошенничества в глобальной сети можно отнести:

1) Организация мошенниками фиктивных «банков» и «инвестиционных фондов»;

2) Организация фиктивных Интернет–магазинов, аукционов, торговых платформ;

3) Предложение помощи в отмывании крупных сумм;

4) Организация Интернет-казино и лотерей;

5) Интернет–благотворительность. Спам рассылки и сайты с просьбой о материальной помощи под трогательную историю, просьбами внести денег в фиктивный благотворительный фонд и т д;

6) Фишинг - вид Интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей - логинам и паролям путем обмана или злоупотребления доверием [3];

7) Подделка платежных систем и взлом аккаунтов – т.е. записей, содержащих сведения, которые пользователь сообщает о себе некоторой компьютерной системе;

8) Кардинг - вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем.

В связи с вышеуказанным, представляется возможным выделить уровни предупреждения киберпреступности: общесоциальный, специально-криминологический и индивидуальный [3].

Применяемые меры предупреждения преступлений в Республике Казахстан на наш взгляд не достаточно эффективны, поскольку уровень преступлений с применением компьютерных технологий растет, соответственно растет и количество жертв данных видов преступлений. Для повышения эффективности борьбы с данными видами преступлений, необходимо усиление правовых и организационных мер, разработка новых мер борьбы с данными преступлениями, изучить опыт зарубежных стран в предупреждении данных видов преступлений, а также просвещение населения о таких видах преступности.

**Список использованных источников**:

1. Об утверждении Концепции кибербезопасности ("Киберщит Казахстана"). Постановление Правительства Республики Казахстан от 30 июня 2017 года № 407.

2. Уголовный кодекс Республики Казахстан, принятый в 2014 году и действующий с 1 января 2015 года.

3. Бородкина Т.Н., Павлюк А.В., Киберпреступления: понятие, содержание и меры противодействия . №1 - 2018. - С. 120-127.

УДК 343.148

## СУДЕБНАЯ ЭКСПЕРТИЗА В ПРОЦЕССЕ ДОКАЗЫВАНИЯ

**Нургазиева Меруерт Аниаркызы**
m.nurgaziyeva@icloud.com
Магистрант 1 курса, специальность «Судебная экспертиза», ЕНУ им.Л.Н.Гумилева,
Нур-Султан, Казахстан
Научный руководитель – Бекмагамбетов А.Б.

Анализ судебной практики и законодательства о судебной экспертизе позволяют утверждать, что нередко участники судопроизводства, в том числе судьи и суды, заблуждаются относительно судебной экспертизы как судебного доказательства. Например, в одних случаях игнорируются и не используются возможности доказывания обстоятельств, подлежащих установлению, с помощью судебных экспертиз, а в других – наоборот, судебная экспертиза без достаточных к тому оснований считается самым «главным» доказательством.

В соответствии с действующим законодательством судебной экспертизой является только такое исследование, которое выполнил эксперт на основании постановления лица, производящего дознание, следователя, определения суда о назначении экспертизы в порядке, предусмотренном уголовно-процессуальным законодательством.

Только указанные лица и суд уполномочены назначать судебные экспертизы с обязательным предупреждением эксперта об уголовной ответственности по ст. 420 УК РК за дачу заведомо ложного заключения [1].

Исследования, выполненные по заданиям других лиц, могут быть приобщены к материалам дела и могут выступать в качестве доказательств как «иные документы», если изложенные в них сведения имеют значение для установления обстоятельств, подлежащих доказыванию, указанных в ст. 73 УПК РК [2].

Вызов эксперта, назначение и производство судебной экспертизы осуществляются в порядке, предусмотренном главой 35, а также статьей 373 УПК РК.