Академии правоохранительных органов
при Генеральной прокуратуре Республики Казахстан

КҮНҒОЖИНОВ ҚАНАТ ӘУЕЛБЕКҰЛЫ

Организационно-процессуальные особенности расследования и доказывания транснациональных киберпреступлений

Магистерский проект на соискание степени магистра национальной безопасности и военного дела

по направлению образовательной программы послевузовского образования
«7М12301 - Правоохранительная деятельность»
(профильное направление)

Научный руководитель:
Заведующий кафедрой ОЮД,
Сырбу А.В.
кандидат юридических наук,
доцент (ассоциированный профессор),
старший советник юстиции
_____

Косшы – 2021 г.

РЕЗЮМЕ

Магистерский проект состоит из введения, двух разделов, семи подразделов, заключения, списка использованных источников, примеры образцов процессуальных документов.

В ходе исследования проведен анализ расследования транснациональных киберпреступлений, необходимость дальнейшего повышения практического опыта органов уголовного преследования по досудебному расследованию киберпреступлений совершенных транснациональными преступными группами. Автором выработаны предложения по проблемным вопросам регулирования получения электронных доказательств у отечественных и заграничных Поставщиков Услуг, о развитии взаимоотношении между АО «Государственная техническая служба» и органами уголовного преследования и совершенствования законодательства для нужд практической деятельности

ҚОРЫТЫНДЫ

Магистрлік жоба кіріспеден, екі бөлімнен, жеті бөлімшеден, қорытындыдан, пайдаланылған дереккөздер тізімінен және іс жүргізу құжаттарының үлгілерінен тұрады.

Зерттеу барысында трансұлттық киберқылмыстарды тергеу, қылмыстық қудалау органдарымен трансұлттық қылмыстық топтар жасаған киберқылмыстар бойынша сотқа дейінгі тергеп-тексерудің практикалық тәжірибесін одан әрі жетілдіру қажеттілігіне талдау жасалды.

Автор отандық және шетелдік Қызмет Көрсетушілерден электронды дәлелдемелерді алуды реттеудің өзекті мәселелері жөнінде, «Мемлекеттік техникалық қызмет» АҚ мен қылмыстық қудалау органдарының арасындағы қарым-қатынасты дамыту және тәжірибелік қызметтің қажеттілігі үшін заңнаманы жетілдіру бойынша ұсыныстар әзірленді.

RESUME

The master's project consists of an introduction, two sections, seven subsections, a conclusion, a list of sources used, and examples of samples of procedural documents.

The study analyzes the investigation of transnational cybercrimes, the need to further improve the practical experience of criminal prosecution authorities in the pre-trial investigation of cybercrimes committed by transnational criminal groups. The author has developed proposals on the problematic issues of regulating the receipt of electronic evidence from domestic and foreign Service Providers, on the development of relations between JSC "State Technical Service" and criminal prosecution authorities, and on improving legislation for the needs of practical activities.

СОДЕРЖАНИЕ

Обозначения и сокращения

УПК	— Уголовно-процессуальный кодекс
РК	— Республика Казахстан
ст.	— статья
СНГ	— Содружество независимых государств
УКПС и СУ	— Управление Комитетом по правовой статистики и специальным учетам
МВД	— Министерство внутренних дел
МОиН	— Министерство образования и науки
СССР	— Союз советских социалистических республик
КазССР	— Казахская советская социалистическая республика
фран.	— французский
англ.	— английский
т. п.	— тому подобное
т. д.	— так далее
т. е.	— то есть
т. к.	— так как
РФ	— Российская Федерация
США	— Соединенные Штаты Америки
пп.	— подпункт
п.	— пункт
ч.	— часть

НОРМАТИВНЫЕ ССЫЛКИ

Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V (с изменениями и дополнениями по состоянию на 02.01.2021 г.);

Закон Республики Казахстан от 1 января 2003 года N370 «Об электронном документе и электронной цифровой подписи

Постановление Правительства РК от 12 декабря 2017 года №827 «Об утверждении Государственной программы «Цифровой Казахстан»;

Указ Президента Республики Казахстан от 15 февраля 2018 года №636 «Об утверждении Стратегического плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан»

Закон Республики Казахстан «О ратификации Соглашения между Правительством Республики Казахстан и Организацией Объединенных Наций о целевом фонде технического сотрудничества» от 15 октября 2014 года № 242-V ЗРК.

Послание Президента Республики Казахстан от 05 октября 2018 года «рост благосостояния казахстанцев: повышение доходов и качества жизни».

Указ Президента Республики Казахстан от 9 февраля 2018 года №633 «О мерах по реализации Послания Главы государства народу Казахстана от 10 января 2018 года «Новые возможности развития в условиях четвертой промышленной революции».

Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстан»)».

Постановление Правительства Республики Казахстан от 29 января 2016 года №39 «О создании некоммерческого акционерного общества «Государственная корпорация «Правительство для граждан»

Введение

Актуальность темы диссертационного исследования. Использование Интернета растет по экспоненте: более 3,8 миллиардов пользователей по всему миру, что составляет почти 47% от всего населения планеты. Согласно расчетам, пользователи проводят пять лет жизни в социальных сетях. Считается, что более 80% киберпреступлений возникают в некоторой форме организованной преступности, связанной с «черными» онлайн-рынками, компьютерными вирусами сбором персональных и финансовых данных. [1]

За последнее десятилетие число и уровень сложности кибератак со стороны как прогосударственных хакерских групп, так и финансово мотивированных киберпреступников значительно возросли. Люди, компании и государственные организации больше не могут быть уверены в безопасности киберпространства, а также в целостности и защищенности своих данных. Кибератаки проводятся на международном уровне и разнообразны по своим направлениям: проведение открытых военных операций с использованием кибероружия; совершений кибератак направленных на нарушение стабильности интернета на государственном уровне; наличия скрытых угроз со стороны проправительственных группировок; целенаправленные атаки на банки, страховые, консалтинговые компании, энергетические и ядерные корпорации [2].

Указанные сведения о состоянии кибератак на мировой платформе заставляют задуматься о необходимости повышения потенциала страны, в частности правоохранительного блока, на изучение и повышения практики расследовании указанных фактов.

Согласно Уголовному Кодексу Республики Казахстан «транснациональная организованная группа - организованная группа, преследующая цель совершения одного или нескольких уголовных правонарушений на территории двух или более государств либо одного государства, при организации совершения деяния или руководстве его исполнением с территории другого государства, а равно при участии граждан другого государства» [3].

По мнению В.А. Номоконова **«Киберпреступность»** представляет собой широкую область криминализации, включая деяния, направленные против конфиденциальности, целостности и доступности компьютерных данных или систем; деяния, предполагающие использование компьютера в целях извлечения личной или финансовой прибыли, или причинения личного или финансового вреда; и деяния, связанные с содержанием компьютерных данных [4, с. 43.].

Технические методы киберпреступности коренным образом преобразовывают традиционные способы хищений денежных средств и преступлений, совершаемых в целях получения финансовой выгоды в отношении организаций частного сектора. Расширение возможностей преступной деятельности, позволяющих не только совершать хищения в отношении предприятий, но также получать посредством организации утечки данных хранящихся сведений личного и финансового характера, привели к

существенному повышению уровня восприятия частным сектором риска, связанного с киберпреступностью.

Указанные признаки латентности киберпреступлении в Республике Казахстан подтверждаются при сравнении сведении представленных ГУ «Управления комитета по правовой статистике и специальным учетам Генеральной Прокуратуры Республики Казахстан по городу Алматы» и АО «Государственная техническая служба».

По данным ГУ «Управления комитета по правовой статистике и специальным учетам Генеральной Прокуратуры Республики Казахстан по городу Алматы» за период с 2015 года по 2020 год в Республике зарегистрировано **23 747 уголовных правонарушении в сфере информатизации и связи**, в том числе иных преступлений с использованием информационных технологий. В разбивке по годам ситуация выглядит следующим образом: в **2015 году** зарегистрировано – **663** преступлений, в **2016 году** – **1705**, в **2017 году** – **2818**, в **2018 году** – **5101**, в **2019 году** – **9164,** в **2020 году – 4 296**[**7**].

Согласно сведениям АО «Государственная техническая служба» в **2015 году** в Республике зарегистрировано **17 621 инцидентов информационной безопасности**, в **2016 году** – **19 118**, в **2017 году** – **24 584**, в **2018 году - 19 335**, в **2019 году** – **20 458,** в **2020 году – 24 053**[**8**].

За **2020 год** из **24 053** инцидентов информационной безопасности: **4 885** в отношении Государственных органов страны, **2 365** в отношении местных исполнительных органов, **950** в отношении критически важных объектов информационно-коммуникационной инфраструктуры, **1038** в отношении квазигосударственного сектора, **489** в отношении финансового сектора, **14 326** в отношении частного сектора.

В **2015 году** в ГУ «Управления комитета по правовой статистике и специальным учетам Генеральной Прокуратуры Республики Казахстан» зарегистрировано ***663*** уголовных дел, а в АО «Государственная техническая служба» зарегистрировано ***17 621*** инцидентов информационной безопасности. Указанные сведения свидетельствуют, что **2015 году** лишь по ***3,8%***, от всех инцидентов информационной безопасности, проводились досудебные расследования. По годам картина выглядит следующим образом, а именно в **2016 году** – ***8,9%***, в **2017 году** – ***11,5%***, в **2018 году** – ***26,4%***, в **2019 году** – ***44,8%,*** в **2020 году – *17,9%***.

Вышеуказанная статистика, свидетельствует о низкой регистрация киберпреступлений в соотношении с зарегистрированными в АО «Государственная техническая служба» инцидентами информационной безопасности.

Если допустить, что какое-то количество инцидентов в АО «Государственная техническая служба» не регистрируются, что вполне реально, то цифра регистрации указанных фактов в Единый реестр досудебного расследования соответственно уменьшиться в разы.

Низкая регистрация киберпреступлений, это лишь одна сторона проблемы в нашей стране. Вторая сторона, которая показывает реальную

картину работы правоохранительных органов в раскрытии указанных преступлений, это количество дел, по которым виновные лица привлечены к уголовной ответственности.

Анализ соотношений уголовных дел по которым виновные лица привлечены к уголовной ответственности и зафиксированных инцидентов информационной безопасности, показывает: в **2015** году по ***152*** преступлениям виновные лица привлечены к уголовной ответственности, из них в суд направлено ***132***, прекращено по нереабилитирующим основаниям **20** уголовных дел**,** что эквивалентно ***0,8%*** от всех зарегистрированных инцидентов информационной безопасности за указанный период. По годам картина выглядит следующим образом, а именно в **2016** году – ***78*** дел (в суд – *38*; прекращено – *40*) эквивалентно - ***0,4%***, в **2017** году – ***207*** (в суд – *113*; прекращено – *94*) эквивалентно - ***1%***, в **2018** году – ***979*** (в суд – *379*; прекращено – *600*) эквивалентно - **5%**, в **2019** году – ***1488*** (в суд – *567*; прекращено – *921*) эквивалентно - ***7,3%***, в **2020** году – ***525*** (в суд - *234*; прекращено - *291*) эквивалентно – ***1%***.

Вышеуказанные сведения свидетельствуют, что правоохранительными органами не проводятся достаточные следственно-оперативные мероприятия, направленные на раскрытие киберпреступлений.

Одной из основных причин столь низких показателей в раскрытии и расследований киберпреступлений является низкий уровень подготовки сотрудников правоохранительных органов при расследовании уголовных правонарушений в сфере информатизации и связи.

Вышеуказанная проблема касается не только нашей страны, она существует во всем мире. В настоящее время ***невозможно контролировать киберпреступления, однако необходимо повысить качество расследования указанных преступлений***. В этой связи, органами уголовного преследования необходимо принять все меры, направленные на тщательное изучение и наращивания практики расследования киберпреступлений.

В 2019 году «кардинг» стал самым быстрорастущим сегментом в области угроз на клиентов банка. Рынок сбора данных банковских карт продолжает расти на протяжении нескольких лет. Его можно условно разделить на два сегмента: текстовые данные *(номер, дата истечения, имя держателя, адрес, CVV)* и дампы *(содержимое магнитных полос карт).* За 2019 год количество скомпрометированных карт выросло с **27,1** до **43,8** млн. по сравнению с 2018 годом. За 2019 год средняя цена на текстовые данные выросла с **9** до **14** долларов США, при этом снизилась средняя цена дампа – с **33** до **22** долларов США по сравнению с 2018 годом. В 2019 году общее количество скомпрометированных карт *по текстовым данным* составило **12 540 190** шт. (размер рынка **179 159 552** долларов США), общее количество скомпрометированных карт по *дампам* составило **41 213 941**шт. (размер рынка **700 520 520** долларов США) [2].

В 2020 г. общий рынок «кардинга» вырос с **880 млн.** долларов США до **1,9 млрд.** долларов США по сравнению с 2019 годом. Двойной рост касается как текстовых данных, так и дампов. Количество предлагаемых к продаже

текстовых данных выросло **с 12,5** до **38,3 млн.** карт, а дампов – **с 41** до **63,7 млн.**[13].

Социально-экономические факторы влияют на рост киберпреступности не только в развитых странах мира, но и в развивающихся странах.

Согласно сведениям АО «Государственная техническая служба» в Республике Казахстан зафиксирована активность определенных хакеров, которые занимаются атаками и попытками несанкционированных доступов к компьютерным данным или системам *(возможно промышленным шпионажем)*, ***в том числе в отношении государственных органов страны*** [7]. Указанные хакеры после кибер-атак оставляют свои псевдонимы или «почерк», согласно указанным сведениям можем предположить, что некоторые хакеры являются гражданами нашей страны. Указанные сведения свидетельствуют о наличии и даже процветаний хакеров в нашей стране. Конечно, при таком быстром развитии Интернета нельзя считать, что у нас в стране мало лиц, занимающихся или потенциально готовых совершать киберпреступления. Также немаловажную роль играет наличие слабой информационной защиты или её отсутствие у физических и юридических лиц, которые дополнительно привлекают иностранных киберпреступников, так как являются легкой наживой.

Неожиданным открытием 2019 года явилось деятельность группы **Golden Falcon** (или APT-C-34), которая проводила хакерские операции против частных компаний и государственных организаций Казахстана, вплоть до шпионажа. По предположению специалистов Group-IB за группой стоят спецслужбы Казахстана или лица, заинтересованные в мониторинге обстановки внутри государства. [13]

Согласно оценкам Организации Объединенных Наций, свыше 80 процентов киберпреступлений совершаются в рамках той или иной формы организованной деятельности, включая формирование черного рынка киберпреступности, основанного на цикле разработки вредоносного программного обеспечения, заражения компьютеров, управления бот-сетями, сбора данных личного и финансового характера, продажи данных и получения денег за финансовую информацию. В развитых странах доля киберпреступлений с транснациональным компонентом, выявляемых правоохранительными органами, как правило, велика, в то время как в развивающихся странах их доля значительно ниже и в некоторых случаях составляет менее 10 процентов. С одной стороны, это может указывать на то, что в развивающихся странах киберпреступления ориентированы больше на жертв внутри страны и, возможно, на отдельные национальные компьютерные системы. С другой стороны, вполне возможно, что ***в связи с недостаточным развитием потенциала правоохранительных органов развивающихся стран менее часто выявляют или работают с иностранными поставщиками услуг или иностранными жертвами преступлений, расследуемых внутри страны*** [5].

По словам Н.А. Марочкина, демографические особенности преступников зеркально отображают обычный уголовный мир, в том аспекте, что в этой среде

преобладают молодые люди мужского пола, хотя возрастной состав все в большей степени свидетельствует об увеличении числа пожилых лиц, в особенности, когда преступления связаны с детской порнографией [9, с. 46.].

Преступники, в том числе террористы, используют социальные сети, помимо прочего, для распространения пропаганды, сбора денежных средств, привлечения сторонников и обмена информацией. Такие электронные доказательства могут оказаться важными для определения того, где находился или находится подозреваемый, с кем он связан и поддерживает связь.

Исследование состояния и перспектив расследования и доказывания транснациональных киберпреступлений имеет важное практическое значение для органов уголовного преследования и суда, так как технические методы киберпреступности коренным образом преобразовывают традиционные способы преступлений, совершаемых в целях получения финансовой выгоды в отношении организаций частного сектора. Указанное исследование направлено на развитие потенциала правоохранительных органов по выявлению киберпреступлений и работы с иностранными поставщиками услуг или иностранными жертвами киберпреступлений.

Цели и задачи исследования.

Целью настоящего исследования является раскрытие организационно-процессуальных особенностей расследования и доказывания транснациональных киберпреступлений; определение основных организационно-процессуальных способов расследования и доказывания транснациональных киберпреступлений и их значение в процессе расследования;

Для реализации данной цели были определены следующие задачи:

– исследование порядка производства организационно-процессуальных особенностей расследования и доказывания транснациональных киберпреступлений и разработать рекомендации по его совершенствованию;

– раскрытие содержания терминов, используемых при расследовании и доказывании транснациональных киберпреступлений;

– на основе исследования теоритического, нормативного, эмпирического материала, его анализа разработать рекомендации, направленные на совершенствование практики реализации организационно-процессуальных особенностей расследования и доказывания транснациональных киберпреступлений.

– рассмотреть особенности собирания доказательств о совершении киберпреступлений.

Объект и предмет исследования. **Объектом** данного исследования является деятельность по применению норм при расследовании и доказывании транснациональных киберпреступлений.

Предметом данного исследования выступают нормы Конституции РК, уголовно-процессуального законодательства, других нормативно-правовых актов Республики Казахстан, регламентирующие вопросы расследования и доказывания транснациональных киберпреступлений, а также отношения, возникшие в процессе их реализации. Кроме того, предметом изучения явились

аналогичные нормы зарубежного права, имеющие значения для уголовно-процессуального законодательства, материалы практики следствия, прокуратуры, суда, экспертной деятельности по рассматриваемым вопросам.

Исследование в основном на материалах уголовных дел связанных с совершением уголовных правонарушений в сфере информационной безопасности и связи, расследовавших самим диссертантом, также будет дополнено другими материалами.

Теоретическую базу исследования составили труды таких ученных, как: Лоскутов И.Ю., Евдокимов К.Н., Оконенко Р.И., Пастухов П.С.

Методология и методика исследования. Методологическую базу исследования составили положения диалектико-материалистического метода, а также использование общенаучных и специальных методов научного исследования: аналогии, анализа, сравнения, синтеза, моделирования, системно-структурного, деятельностного подхода, исторического, сравнительно-правового, социологического и других.

Нормативной основой исследования являются: Конституция Республики Казахстан, Международные конвенции и договоры, Конституционные законы, Уголовный кодекс Республики Казахстан, Уголовно-процессуальный кодекс Республики Казахстан, законы и иные нормативные правовые акты Республики Казахстан, а также законы зарубежных государств, относящиеся к теме исследования.

Научная новизна диссертационного исследования. Стремительный рост использования Интернета в экономических, бытовых, социальных и других взаимоотношениях во всем мире, завлекает большое количество лиц, пытающих заработать путем предоставления услуг в различных направлениях по средствам Интернет ресурсов. С появлением «Виртуального мира» в обществе появились доступные и простые в использовании изменения, предоставляющие возможность заработать, получить необходимую информацию и услуги. Примерами использования Интернет ресурсов являются использование мобильных приложений, дающих возможность одним кликом узнать сумму на банковском счете, провести транзакцию, заказать такси, получить услуги «Электронного правительства», написать электронное заявление в государственные органы о совершении преступлений и получить массу других услуг. При таком истечении обстоятельств только ленивый не старается быть в гуще событии и получить что-то необходимое по средствам Интернет. Учитывая стремительное использование Интернета государства, холдинги, корпорации и обычные обыватели работают над упрощением использования Интернет ресурсов в свою пользу.

Развитие Интернет просторов и появление «Виртуального мира» привлекло преступников готовых совершать уголовные правонарушения – киберперступления. Наличие в просторах Интернета неограниченного количества инструментов, с помощью которых можно незаконно присвоить чужое имущество, проникнуть в частную жизнь, получить внутреннюю информацию и при этом остаться не замеченным слишком заманчиво для преступников. Тенденция развития преступлений показывает, что похищать

чужое имущество путем совершения разбойных нападений и грабежей не привлекательно, так как на месте совершения преступлений остаются слишком много следов совершений преступлений. С развитием государства, развиваются способы и разновидности преступлений, преступники не хотят оставлять доказательства совершения ими преступлений и тем более быть привлеченными к уголовной ответственности. В этой связи участились случая совершения преступниками мошенничеств, граничащих с гражданско-правовыми взаимоотношениями. Но совершение мошенничеств, все равно оставляет явные следы совершения преступлений и развитие «Виртуального мира» привлекло множество преступников готовых совершать преступления и не оставлять своих следов. Указанные киберпреступления в виду резкого скачка использования Интернета дают преступникам возможность замаскироваться и отправлять похищенные денежные средства в разные государства и в последующем легализовать их через электронную валюту и другие инструменты обильно пользуемые преступниками.

В уголовно-процессуальной науке Республики Казахстан отсутствуют исследования, посвященные самостоятельному изучению проблемы организационно-процессуальных особенностей расследования и доказывания транснациональных киберпреступлений. В этой связи, научная новизна исследования заключается в том, что на монографическом уровне впервые осуществлено комплексное изучение организационно-процессуальных особенностей расследования и доказывания транснациональных киберпреступлений.

Актуальной остается задача разработки и представления в распоряжение практикующих юристов теоретических основ процессуального порядка собирания информации с технических каналов связи и научно-обоснованных рекомендаций по организации и тактике получения и использования информации при расследовании и доказывании транснациональных киберпреступлений. Очевидно, что в такой проблемной ситуации требуется восполнить дефицит научных познаний, связанных с получением и использованием информации в цифровой форме, необходимой с целью подтверждения либо опровержения факта, который является предметом судебных разбирательств.

Диссертантом сформулированы новые теоретические положения, направленные на улучшение организационно-процессуальных особенностей расследования и доказывания транснациональных киберпреступлений, совершенствование законодательного регламентирования, а также практики его применения в стадиях досудебного производства, оптимизацию расследования уголовных дел.

Практические рекомендации, выносимые на защиту:

По всем предлагаемым изменениям разработана сравнительная таблица которая является приложением диссертации в связи с большим объемом (Приложение Б.);

1. В целях совершенствования понятия электронных доказательств предлагается внести изменения в Уголовно-процессуальный кодекс в части

«фактических данных» и дополнить часть 2 статьи 111 понятием «электронного доказательства», также добавить статью 118-1 с разъяснением понятия электронных доказательств;

2. В целях беспрепятственного получения служебной информации органами уголовного преследования и прокурорского надзора предлагается внести изменения в Закон Республики Казахстан «О связи» №567 и дополнить пункт 2 статьи 2, название статьи 15, пунктов 1, 3, 4 части 1 статьи 15, частей 3, 5 статьи 15, части 4 статьи 36 понятием «предоставлением служебной информации органам досудебного расследования и прокурорского надзора», а также ссылаться в качестве оснований на «Закон «О прокуратуре» и Уголовно-процессуальный Кодекс Республики Казахстан», предлагается внести изменения в Постановление Правительства «Об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года и дополнить статью 1, пункт 2 статьи 2 понятием «досудебного расследования, прокурорского надзора», а также ссылаться в качестве оснований на «Закон «О прокуратуре» и Уголовно-процессуальный Кодекс Республики Казахстан», предлагается внести изменения в Постановление Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» №358 от 19.06.2018 года и дополнить название постановления, статьи 1, пунктов 1, 3, 4 статьи 3, Главы 2, статей 4, 5, 6, 12, 13, 15, 18, 19, 22, 23, 24, 25, 26, 28, пунктов 1, 2, 4, 5, 6, 7, 10, статьи 5, первого абзаца статьи 10, пунктов 1,3,4 статьи 11, первого, второго, четвертого абзацев статьи 17, первого, второго, третьего абзацев статьи 20, добавить статью 6-1, добавить статью 13-1 понятиями «собирания доказательств в рамках досудебного расследования, прокурорского надзора» с целью расширения понятия служебной информации об абонентах и получения органами уголовного преследования и прокурорского надзора служебной информации у операторов связи для использования в служебных целях.

3. В целях повышения практики исследования инцидентов информационной безопасности органами уголовного преследования в уголовном праве предлагается внести изменения в Закон «Об информатизации» и дополнить пункт 12 в статью 7-4 понятием «предоставление Национальным координационным центром информационной безопасности компетентным специальным и правоохранительным органам Республики Казахстан развернутую информацию об инцидентах информационной безопасности» в части расширения функции Национального координационного центра информационной безопасности направленной на исследование всех зарегистрированных инцидентов информационной безопасности и передачи сведений в специализированные и

правоохранительные органы для дальнейшего исследования в плоскости уголовного права.

4. В целях повышения практики взаимоотношения при расследовании транснациональных киберпреступлений со странами ближнего зарубежья предлагается внести изменения в Положение «о Центральноазиатском региональном информационном координационном центре по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» являющимся неотъемлемой частью Закона Республики Казахстан «О ратификации Соглашения между Азербайджанской Республикой, Республикой Казахстан, Кыргызской Республикой, Российской Федерацией, Республикой Таджикистан, Туркменистаном и Республикой Узбекистан о создании Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» от 06 ноября 2008 года N 78-IV и дополнить в статье 1 понятие «киберпреступность», в части расширения функции ЦАРИКЦ на проведение международных операций по пресечению и раскрытию киберперстеплений;

5. Разработаны авторские примерные образцы процессуальных документов при расследовании уголовных дел в сфере информатизации и связи.

Апробация и внедрение результатов исследования. Диссертантом подготовлено две научных статьи, в которых излагаются результаты проведенного исследования, одно из которых опубликовано в XIV Международной научно-практической онлайн-конференции «Защита прав человека в современном мире: концепции механизмы и проблемы обеспечения», посвящённой 30-й годовщине провозглашения государственного суверенитета Республики Казахстан. Основные положения диссертации докладывались на семинаре организованном Институтом профессионального обучения Кафедры специальной подготовки по противодействию глобальным угрозам Академии правоохранительных органов при Генеральной Прокуратуре Республики Казахстан на тему «Особенности расследования уголовных дел о киберпреступлениях» проведенный с участием сотрудников органов прокуратуры и службы экономических расследований.

Теоретические положения и практические рекомендации работы используются в практической деятельности органов предварительного следствия и дознания ДП г.Алматы (Приложение А.).

Структура и объем диссертационного исследования. Структура работы определяется поставленными в диссертации целями, задачами и логикой исследования. Работа состоит из введения, двух разделов, включающих в себя семь подразделов, заключения, списка использованных источников, приложения. Диссертация соответствует требованиям, предъявляемым Инструкцией Комитета по надзору и аттестации науки и образования Министерство образовании и науки Республики Казахстан и ее объем составляет 80 страниц текста компьютерного набора (приложения в указанный объем диссертации не включаются).

1. ПРАВОВЫЕ ОСОБЕННОСТИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. Особенности правового регулирования взаимоотношении при использовании цифровых технологии

Нашим Государством приложены большие усилия для модернизации государственного сектора, включая информационно-коммуникационные технологии, позволившие преобразовать систему административного управления. Согласно результатам Исследования «электронного правительства» ООН 2012 года, Республика Казахстан является лидирующей страной среди стран Центрально-Азиатского региона. [18]

Постановлением Правительства Республики Казахстан от 29 января 2016 года №39 «О создании некоммерческого акционерного общества «Государственная корпорация «Правительство для граждан». Основными предметами деятельности общества являются оказание государственных услуг, услуг по выдаче технических условий на подключение к сетям субъектов естественных монополий и услуг субъектов квазигосударственного сектора в соответствии с законодательством Республики Казахстан, организация работы по приему заявлений на оказание государственных услуг, услуг по выдаче технических условий на подключение к сетям субъектов естественных монополий, услуг субъектов квазигосударственного сектора и выдаче их результатов услугополучателю по принципу "одного окна", обеспечение оказания государственных услуг ***в электронной форме***, а также осуществление государственной регистрации прав на недвижимое имущество по месту его нахождения, государственной регистрации юридических лиц, являющихся коммерческими организациями, и учетной регистрации их филиалов и представительств.[29]

Республика Казахстан значительно усовершенствовалась за последние несколько лет относительно предоставления онлайн услуг, позволяющих гражданам получить доступ к государственным услугам комплексным методом. Одним из интересных аспектов казахстанских онлайн услуг является блог Правительства. Граждане могут связаться с руководителями государственных органов путем комментариев и вопросов, которые способствуют прозрачности государственного управления и улучшают взаимодействие между гражданами и государственными служащими. Сайт также содержит статистическую информацию по вопросам и комментариям, полученным исполнителями учреждений, также количество ответов на них для обеспечения осуществления надлежащего контроля. [18]

15.10.2014 года Казахстаном ратифицировано Соглашение между Правительством Республики Казахстан и Организацией Объединенных Наций о целевом фонде технического сотрудничества. Проект направлен на содействие усилению стратегий электронного правительства, принципов и действий государств-членов посредством обмена опытом и передовыми методиками в

ходе Глобального форума «электронного правительства» Организации Объединенных Наций 2014. [18]

К цифровизации Казахстан шел с момента получения своей независимости, указанный вектор неоднократно определялся Посланиями Президента Республики Казахстан народу Казахстана и другими нормативными актами. В одном из своих послании Президент акцентировал, что «прежде всего, необходимо обеспечить развитие таких направлений «экономика будущего», как альтернативная энергетика, новые материалы, биомедицина, большие данные, интернет вещей, искусственный интеллект, блокчейн и другие». Как отмечал Президент «именно от них в будущем зависят место и роль страны в глобальном мире». [19]

Большим шагом в цифровизацию является принятый 7 января 2003 года Закон N307 «Об электронном документе и электронной цифровой подписи», который направлен на регулирование отношений, возникающих при создании и использовании электронных документов, удостоверенных посредством электронных цифровых подписей, предусматривающих установление, изменение или прекращение правоотношений, а также прав и обязанностей участников правоотношений, возникающих в сфере обращения электронных документов, включая совершение гражданско-правовых сделок. Согласно ч.1 ст.10 указанного Закона электронная цифровая подпись равнозначна собственноручной подписи подписывающего лица и влечет одинаковые юридические последствия. [14]

На основании Послании Президента Республики Казахстан «третья модернизация Казахстана: глобальная конкурентоспособность» от 31 января 2017 года Правительством принята комплексная Государственная программа «Цифровой Казахстан» - нацеленная на повышение уровня жизни каждого жителя страны за счет использования цифровых технологий. Основными целями Программы стали ускорение темпов развития экономики Республики Казахстан и улучшение качества жизни населения, а также создание условий для перехода экономики на принципиально новую траекторию – цифровую экономику будущего. Задачей указанной программы является цифровизация государственных направлений начиная промышленностью, электроэнергетикой, логистики, сельского хозяйства и других направлении[15].

Указом Президента Республики Казахстан от 9 февраля 2018 года №633 «О мерах по реализации Послания Главы государства народу Казахстана от 10 января 2018 года «Новые возможности развития в условиях четвертой промышленной революции» определен ряд мероприятии. Первоначальными мероприятиями указаны Совершенствование и разработка новых инструментов, направленных на модернизацию и цифровизацию отечественных предприятий с ориентацией на экспорт продукции и трансферт технологий; Реализация пилотного проекта по оцифровке ряда промышленных предприятий и дальнейшее широкое распространение полученного опыта; Разработка Дорожной карты по развитию экосистемы разработчиков цифровых и других инновационных решений в инновационных центрах Назарбаев Университет,

Международного финансового центра «Астана» и Международного технопарка IT-стартапов и другие направления. [20]

Согласно Указа Президента Республики Казахстан от 15 февраля 2018 №636 «Об утверждении Стратегического плана развития Республики Казахстан до 2025 года и признании утратившими, силу некоторых указов Президента Республики Казахстан» запланированы инициативы «Реализация концепции «Smart City», «Обеспечение гарантий личной безопасности». Инициативой «Smart City» запланировано внедрить цифровые технологии во все сферы жизнедеятельности городов, включая управление социальной, транспортной, инженерной, энергетической, жилищной и информационной инфраструктурами города, предоставление государственных услуг, градостроительное планирование, строительство «умных» зданий. Инициативой «Обеспечение гарантий личной безопасности» запланировано внедрение интеллектуальных систем видеонаблюдения и распознания на улицах и в местах массового пребывания граждан, контроля за дорожным движением. [16]

Вышеперечисленные и другие нормативные документы свидетельствуют, что Республика Казахстан, как и все развитые и развивающие страны, выбрал одним из стратегических направлении цифровизацию всех процессов в стране. К цифровой плоскости подвергнуты действия от подачи заявлении в портал «Электронного Правительства», проведение транзакции по банковским счетам с использованием мобильных приложении, оказания «онлайн услуг» во всех отраслях взаимоотношении, расследование уголовных дел в «Электронном формате» и другие функционалы.

Конечно, как отмечалось выше, преступники не упустят своего шанса обогатиться и совершить киберпреступление с использованием вычислительной техники или иной электронной аппаратуры, так как совершение преступлений посредством Глобальной сети Интернет дает преступникам уверенность того, что они не будут найдены или на их поимку уйдет большое время.

Изучен отправленный, в рамках международной правовой помощи, уполномоченными органами Российской Федерации архив электронных переписок зарегистрированных на сайте «Вконтакте» руководителя и участника ОПГ совершавших киберпреступления на территории Республики Казахстан. В своих переписках руководитель ***разъясняет*** участнику ОПГ о том, что ***их не смогут найти за совершение киберпреступлений и если даже найдут то только после 6-7 лет, если иностранные государства разрешат выдать ответ правоохранительным органам Казахстана***.[10] Из вышеуказанной переписки можем создать портрет киберпреступников, как очень высокоинформированных лиц, имеющих опыт работы не только в сфере информационных технологий, но и подкованных познаниями юриспруденции и международных взаимоотношении.

Первоначальными шагами в борьбе с преступностью, посягающей на информационную безопасность, стало создание универсального развитого и детального понятийного аппарата. Возникла необходимость четкого пояснения, основанного на осмыслении технических характеристик новых средств

обработки информации и сущности самой информации, хранящейся на машинном носителе, содержащейся в информационной системе или передаваемой по информационно-коммуникационной сети как новой уголовно-правовой категории. Без ясного понимания норм, регулирующих информационные правоотношения, государственные органы не смогут в дальнейшем правильно определить круг вопросов, подлежащих доказыванию, а затем и точно квалифицировать выявленные случаи преступлений.

Нашим Государством принимаются множество задач, направленных на обеспечение защиты электронных информационных ресурсов, информационных систем и сетей телекоммуникаций, обеспечение безопасного использования информационно-коммуникационных технологий.

С целью обеспечения защиты электронных информационных ресурсов Постановлением Правительства Республики Казахстан от 30 июня 2017 года №407 утверждена Концепция кибербезопасности «Киберщит Казахстан». Указанная Концепция разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная Конкурентно способность» с учетом подходов Стратегии «Казахстан-2050» по вхождению Казахстана в число 30-ти самых развитых государств мира.

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. [21]

Рост компьютерной преступности, включая преступления в сфере компьютерной информации, и необходимость согласованного подхода государств к выработке уголовно-правовых и уголовно-процессуальных процедур, направленных на борьбу с ней, привели к созданию в 1997 году Комитетом Министров Совета Европы Комитета экспертов по преступности в киберпространстве. По результатам этой работы в 2000 году разработан проект Конвенции Совета Европы по киберпреступности. Конвенция открыта к подписанию до 23 ноября 2001 года в Будапеште, и вступила в силу 18 марта 2004 года. По состоянию на 7 апреля 2007 года Конвенцию ратифицировали 19 государств. Европейская Конвенция по киберпреступности является комплексным документом, содержащим нормы различных отраслей права: уголовного, уголовно - процессуального, авторского, гражданского, информационного**.** В Конвенции не дается определения понятия «компьютерное преступление» или «преступление, связанное с использованием компьютерных технологий», которые использовались в принятых ранее международных документах. В документе используются понятие «киберпреступление», содержание которого раскрывается с помощью перечня, включающего в себя: 1) деяния, направленные против компьютерной информации *(как предмета преступного посягательства)*, 2) деяния, посягающие на иные охраняемые законом блага, при этом информация,

компьютеры и т.д. являются одним из элементов их объективной стороны, выступая в качестве, к примеру, орудия их совершения либо составной части способа их совершения или сокрытия. [23]

В целях урегулирования киберпреступлений Казахстан, как и другие развитые и развивающие страны принял новый Уголовный кодекс от 03.07.2014 года, в котором предусмотрена новая глава 7 «Уголовные правонарушения в сфере информатизации и связи».

Для уголовно-правовой науки и для законодательства появился новый предмет научных и политических обсуждений и разработок. А что же является предметом преступлений в сфере компьютерной информации по уголовному законодательству Казахстана. Это те позиции которые базируются в нормах Уголовного Кодекса Республики Казахстан регламентирующих отношения, связанные с использованием информации и информационных технологий, проведение анализа этих норм раскрывает всю обширность возможных преступных деяний в сфере новых коммуникационных технологий. Казалось бы, что компьютерную информацию каждый пользователь распространяет, также защищает на бытовом уровне, тем не менее, в соответствии с Уголовным Кодексом Республики Казахстан компьютерная информация подлежит уголовно – правовой защите, хотя в ограниченной форме. [22]

Общественная опасность уголовных правонарушений в сфере информатизации и связи заключается в нарушении права на конфиденциальность информации, ущемлении законных интересов собственников информационных систем и информационно – коммуникационных сетей по ограничению их доступности.

Объектом уголовных правонарушений в сфере информатизации и связи являются права и законные интересы граждан и организаций на конфиденциальность информации, информационных систем и информационно-коммуникационных сетей.

Предметом уголовных правонарушений в сфере информатизации и связи выступают: информация, охраняемая законом и содержащаяся на электронном носителе; информационная система, в том числе национальная информационная система; информационно-коммуникационная сеть; национальные электронные информационные ресурсы.

Объективная сторона уголовных правонарушений в сфере информатизации и связи выражается в умышленных неправомерных действиях с охраняемой законом информации, содержащейся на электронном носителе, в информационной системе или информационно-коммуникационных сетях, в результате которого существенно нарушаются права и законные интересы граждан или организаций либо охраняемые законом интересы общества или государства.

С ***субъективной стороны*** уголовных правонарушений в сфере информатизации и связи может быть совершен только умышленно *(прямой или косвенный умысел)*: виновный сознает, что он совершает неправомерный доступ к охраняемой законом информации, содержащейся на электронном носителе, в информационной системе или информационно-коммуникационных

сетях, предвидит возможность или неизбежность наступления общественно опасных последствий и желает их наступления.

По отношению к причинению существенного вреда в виде существенного нарушения прав и законных интересов граждан или организаций либо охраняемых законом интересов общества или государства возможен косвенный умысел, когда виновное лицо сознательно допускает эти последствия либо относится к их наступлению безразлично.

Мотивы и цели данных уголовных правонарушений в сфере информатизации и связи разнообразны и на квалификацию не влияют, но они должны учитываться при индивидуализации наказания. В большинстве случаев это корыстный мотив.

Субъектом является физическое вменяемое лицо, достигшее 16-летнего возраста.

Государством проводятся комплексные мероприятия и принимаются соответствующие законодательства, направленные на урегулирование взаимоотношении в сфере информатизации и связи, в том числе обеспечение охраны прав и свобод граждан на территории Республики Казахстан.

Развитие глобальной сети Интернет создает новый вид существования и взаимоотношении между гражданами, корпорациями, странами и международными организациями. Взаимоотношения, возникшие по средствам глобальной сети Интернет, по требованию времени и в связи с развитием информационно-коммуникационных сетей заставляют корпорации и государства на своем уровне стремиться регулировать указанные «цифровые» взаимоотношения. Республика Казахстан как его требуют общемировые стандарты принимает множество нормативно-правовых актов, направленных на регулирование взаимоотношении возникающих при использовании цифровых технологий. Соответственно цифровизация большого объема взаимоотношении порождает возникновение общественно опасных посягательств на охраняемые законом интересы общества и государства в сфере информатизации и связи. В этой связи, государством принимаются и апробируются нормативно-правовые акты, направленные на регулирование цифровых взаимоотношении и обеспечения информационной безопасности Республики Казахстан.

1.2. Состояние и перспективы совершенствования традиционных методов расследования при расследований киберпреступлений.

Технические методы киберпреступности коренным образом преобразовывают традиционные способы хищений денежных средств и преступлений, совершаемых в целях получения финансовой выгоды в отношении организаций частного сектора. Расширение возможностей преступной деятельности, позволяющих не только совершать хищения в отношении предприятий, но также получать посредством организации утечки данных хранящихся сведений личного и финансового характера, привели к существенному повышению уровня восприятия частным сектором риска, связанного с киберпреступностью.

Подключение к глобальной сети должно рассматриваться как центральный элемент современной киберпреступности и в особенности киберпреступности завтрашнего дня. По мере расширения киберпространства и IP-трафика, а также по мере опережения объема трафика беспроводных устройств, объемов трафика проводных устройств и роста интернет-трафика, генерируемого некомпьютерными устройствами, возможно, сложно будет представить себе «компьютерное» преступление при отсутствии IP-подключения к глобальной сети. Особый персонализированный характер мобильных устройств и появление подключенных к интернет-протоколу бытовых приборов или личных вещей ведут к тому, что электронные данные и их передача могут генерироваться или стать неотъемлемой частью практически каждого, будь то законного или незаконного, действия человека.

Быстрый и стремительный рост использования Интернет ресурсов порождает такой же рост киберпреступлений, что требует увеличения потенциала правоохранительных и специальных органов страны по работе с иностранными и отечественными поставщиками услуг в целях выявления и раскрытия киберпреступлений совершаемых на территории нашей страны и за ее пределами нашими гражданами.

Согласно оценкам Организации Объединенных Наций, свыше 80 процентов киберпреступлений совершаются в рамках той или иной формы организованной деятельности, включая формирование черного рынка киберпреступности, основанного на цикле разработки вредоносного программного обеспечения, заражения компьютеров, управления бот-сетями, сбора данных личного и финансового характера, продажи данных и получения денег за финансовую информацию. В развитых странах доля киберпреступлений с транснациональным компонентом, выявляемых правоохранительными органами, как правило, велика, в то время как в развивающихся странах их доля значительно ниже и в некоторых случаях составляет менее 10 процентов. С одной стороны, это может указывать на то, что в развивающихся странах киберпреступления ориентированы больше на жертв внутри страны и, возможно, на отдельные национальные компьютерные системы. С другой стороны, вполне возможно, что ***в связи с недостаточным развитием потенциала правоохранительных органов развивающихся стран менее часто выявляют или работают с иностранными поставщиками***

услуг или иностранными жертвами преступлений, расследуемых внутри страны [5].

Меры борьбы с киберпреступностью, принимаемые в порядке реагирования на совершенные преступления, должны сопровождаться целенаправленными и долгосрочными тактическими расследованиями в отношении рынков преступности и разработчиков преступных схем. Правоохранительные органы развитых стран работают в этой области, в том числе используя действующие под прикрытием подразделения по выявлению правонарушителей на сайтах социальных сетей, в чатах и при обмене мгновенными сообщениями и пользовании материалами совместного пользования («P2P»). Трудности при расследовании киберпреступлений связаны с использованием преступниками новаторских преступных методов, сложностями в получении доступа к электронным доказательствам и с внутренними ограничениями в отношении ресурсов, потенциала и материально – технических возможностей. Подозреваемые часто используют технологии анонимизации и запутывания следов, и новые технологии быстро получают распространение в преступном мире благодаря онлайновым преступным рынкам.

С одной стороны, деяние, предполагающее «просто незаконный доступ», может представлять собой сравнительно незначительное правонарушение. С другой стороны, незаконный доступ является отправной точкой многих серьезных киберпреступлений и может включать в себя преднамеренный неправомерный вход в компьютерные системы, например, в системы, используемые жизненно важными объектами национальной инфраструктуры.

Повсеместное распространение Интернета и персональных компьютерных устройств означает, что компьютерные системы или компьютерные данные могут использоваться для совершения практически любого уголовного правонарушения. Поэтому сфера электронных доказательств неразрывно связана с киберпреступностью, хотя и отличается от нее в концептуальном плане. Сбор и представление электронных доказательств являются неотъемлемой частью расследования и судебного преследования киберпреступлений. Кроме того, это все чаще касается традиционных преступлений, таких как грабеж, кража или кража с взломом, а также различных форм организованной преступности. Компьютерные записи телефонных разговоров, электронная почта, журналы IP-соединений, SMS-сообщения, адресные книги мобильных телефонов и компьютерные файлы могут содержать доказательства местонахождения, мотива, нахождения на месте преступления или вовлеченности подозреваемого в преступление в случае практически любого вида преступлений.

Для расследования киберпреступлений правоохранительным органам необходимо ***использовать как традиционные, так и новые методы*** следственно-оперативных мер. В то время как некоторые следственные действия могут быть осуществлены на основании традиционных полномочий, многие процессуальные положения, в основе которых лежит пространственный, ориентированный на предметы подход, трудно применять в

ситуациях, связанных с хранением электронных данных и потоками данных в режиме реального времени.

Хотелось бы акцентировать, что проведение лишь традиционных методов досудебного расследования не достаточно для раскрытия киберпреступлений, если конечно подозреваемые сами не признают вину.

В этой связи, в ходе досудебного расследования киберпреступлений необходимо применять новые методы следственно-оперативных мер с принятием компьютерно-ориентированных подходов. В их число могут входить просмотр, изъятие или копирование компьютерных данных, находящихся на принадлежащих подозреваемым лицам устройствах, получение компьютерных данных от третьих сторон, таких как поставщики услуг Интернета, и при необходимости перехват электронных сообщений.

Кроме того, необходимо учитывать такие проблемные аспекты, как неустойчивый характер электронных доказательств и применение злоумышленниками методов запутывания, включая шифрование, использование прокси-серверов, услуг облачного вычисления, «добросовестных» компьютерных систем, зараженных вредоносными программами, и многоадресную *(или «луковую»)* маршрутизацию интернет – соединений. Эти аспекты, в частности, представляют особые трудности в отношении традиционных полномочий.

Картина киберпреступности глазами правоохранительных органов, как и в случае любой иной преступности, является неизбежно неполной и воссоздается из отдельных расследованных дел в сочетании с более широкой оперативно-розыскной информацией.

Преступники, в том числе террористы, используют социальные сети, помимо прочего, для распространения пропаганды, сбора денежных средств, привлечения сторонников и обмена информацией. Такие электронные доказательства могут оказаться важными для определения того, где находился или находится подозреваемый, с кем он связан и поддерживает связь.

Исследование состояния и перспектив расследования и доказывания транснациональных киберпреступлений имеет важное практическое значение для органов уголовного преследования и суда, так как технические методы киберпреступности коренным образом преобразовывают традиционные способы преступлений, совершаемых в целях получения финансовой выгоды в отношении организаций частного сектора. Указанное исследование направлено на развитие потенциала правоохранительных органов по выявлению киберпреступлений и работы с иностранными поставщиками услуг или иностранными жертвами киберпреступлений.

1.3 Проблемы определения понятия электронных доказательств

Основной целью правоохранительных и специальных органов Республики Казахстан по выполнению своих задач и обязанностей, направленных на профилактику и раскрытие уголовных правонарушений в сфере информатизации и связи, являются законное и качественное собирание, исследование, оценка доказательств в цифровой форме. Ввиду цифровизации всех взаимоотношении, а не только при совершении киберпреступлений, собирание, исследование и оценка доказательств в цифровой форме проводятся по всем категориям и разновидностям уголовных правонарушений.

Пресечение, беспристрастное, быстрое и полное раскрытие, расследование уголовных правонарушений, изобличение и привлечение к уголовной ответственности лиц, их совершивших, справедливое судебное разбирательство и правильное применение уголовного закона, защита лиц, общества и государства от уголовных правонарушений являются задачами уголовного процесса. [6]

Собирание доказательств производится в процессе досудебного расследования и судебного разбирательства путем производства процессуальных действий, предусмотренных Уголовно-процессуальным Кодексом. Собирание доказательств включает их обнаружение, закрепление и изъятие. [6]

Основным доказательством совершения преступлении в киберпреступлениях является информация, хранящаяся в цифровой форме.

Доказательствами по уголовному делу являются законно полученные фактические данные, на основе которых в определенном Уголовно-процессуальным кодексом порядке орган дознания, дознаватель, следователь, прокурор, суд устанавливают наличие или отсутствие деяния, предусмотренного Уголовным кодексом, совершение или не совершение этого деяния подозреваемым, обвиняемым или подсудимым, его виновность либо невиновность, а также иные обстоятельства, имеющие значение для правильного разрешения дела. [6]

Однако в уголовно-процессуальном законодательстве Республики Казахстан отсутствует понятие «электронные доказательства». На практике участниками уголовного-процесса понятие «доказательство» охватывает понятие «электронное доказательство».

Р.И. Оконенко в диссертационном исследовании об электронных доказательствах приходит к выводу о том, что в настоящее время преждевременно говорить о понятии «электронного доказательства» как о состоявшейся категории позитивного права, а появление в Уголовно-процессуальный кодекс Российской Федерации термина «электронный носитель информации» следует рассматривать как промежуточный шаг на пути к возможному появлению в российском процессуальном праве термина «электронные доказательства». [24]

Авторы коллективной монографии «Основы теории электронных доказательств», соглашаясь с автором англоязычной статьи в сети Интернет,

считают, что электронным доказательством является любая электронно-хранимая информация (ESI), которая может быть использована в качестве доказательства в судебном процессе; к такому виду доказательств относятся любые документы, электронные письма или другие файлы, хранящиеся в электронном виде, а также электронные свидетельства, включающие записи, хранящиеся сетевыми или интернет-провайдерами. В этой же работе утверждается, что электронная информация может быть представлена в виде одного из традиционных доказательств — вещественного доказательства или иного документа. [25]

По мнению П.С. Пастухова, в Уголовно-процессуальном кодексе Российской Федерации не следует вводить новый вид доказательства («электронное доказательство») или новый источник («электронный носитель информации»), необходимо лишь уточнить понятие «доказательство», указав, что сведения могут быть в виде электронной информации, которая, в свою очередь, «вполне способна восприниматься в одном из традиционных доказательств — вещественном доказательстве или документе». [26]

Наличие электронных доказательств как самостоятельный термин в уголовно-процессуальном праве имеет разные точки зрении ученных правоведов.

Однако, при исследовании в рамках настоящей диссертационной работы я придерживаюсь необходимости принятия в уголовно-процессуальное право Республики Казахстан понятия – электронные доказательства.

Электронные доказательства – это любая накопленная, сохраненная или переданная в цифровой форме информация, необходимая подтверждения либо опровержения факта, который является предметом судебных разбирательств. [12]

Электронные доказательства во многом сходны с традиционными, но в то же время, они имеют ряд уникальных характеристик:

- ***Их не видно невооруженным глазом:*** Электронные доказательства зачастую спрятаны там, куда догадается заглянуть только специалист, либо там, куда можно добраться лишь с помощью специальных инструментов;
- ***Они очень неустойчивые:*** На некоторых устройствах или в определенных обстоятельствах во время обычной эксплуатации устройства информация в его памяти *(а значит, и доказательства, которые оно содержит)* может изменяться. Например, при разрядке устройства или нехватке памяти система накладывает *(записывает)* новую информацию поверх старой. Компьютерная память может быть повреждена или уничтожена под воздействием физических факторов *(большой влажности или высокой температуры)* и электромагнитных полей;
- ***Они могут быть изменены или уничтожены в процессе обычной эксплуатации устройства:*** Память компьютерных устройств постоянно изменяется по запросу пользователей *(«сохранить документ», «скопировать файл»)* либо операционной системы *(«выделить место для программы», «временно сохранить данные для обмена между устройствами»).* Последнее происходит автоматически;

- ***Их можно копировать без потери качества:*** Цифровые данные можно копировать неограниченное количество раз, и любая последующая копия ничем не будет отличаться от оригинала. Благодаря этой уникальной особенности разные специалисты могут параллельно и независимо друг от друга исследовать разные копии одного и того же электронного доказательства, не затрагивая при этом оригинал.

Исход дела во многом зависит от того, насколько правильно собраны и обработаны доказательства *(это в равной степени относится как к электронным, так и любым другим доказательствам).* Поэтому рекомендуется придерживаться следующих принципов работы с доказательствами:

- **Профессиональное обращение:** Каждое электронное устройство обладает своими уникальными характеристиками, поэтому при работе с ними нужно соблюдать соответствующие процедуры. Одним из наибольших рисков, связанных с электронными доказательствами, является их непреднамеренная модификация. Нарушение установленных процедур может привести к тому, что целостность данных будет оспорена в суде, а это, в свою очередь, может уменьшить и даже уничтожить их доказательную силу;

- Стремительная эволюция источников электронных доказательств: Новые технологии появляются и развиваются с невероятной скоростью, поэтому методы и процедуры по работе с электронными доказательствами нужно постоянно пересматривать и обновлять;

- Использование надлежащих процедур, методов и инструментов: Как и любые эксперты, специалисты в области компьютерной экспертизы используют в своей работе специальные методы и инструменты. Очень важно, чтобы в каждом конкретном случае эти методы и инструменты были выбраны правильно. Кроме того, чтобы полученная информация имела доказательную силу, процедуры должны быть составлены таким образом, чтобы другие специалисты могли воспроизвести и проверить описанные в них действия:

Приемлемость: Конечная цель использования электронных доказательств заключается в том, чтобы подтвердить или опровергнуть спорные факты. Поэтому чтобы суд принял электронные доказательства к рассмотрению, порядок их получения должен соответствовать действующему законодательству и существующим практикам. При получении тех или иных электронных доказательств все действия начиная с включения электронного носителя, использования какого-либо программного обеспечения для поиска и извлечения электронных доказательств, время проведения следственных действий должны фиксироваться в протоколе следственного действия в порядке ст.199 Уголовно-процессуального кодекса Республики Казахстан.

Согласно ст.199 Уголовно-процессуального кодекса Республики Казахстан протокол следственного действия составляется в ходе производства следственного действия или непосредственно после его окончания [6].

Согласно части 1 статьи 111 Уголовно-процессуального кодекса Республики Казахстан: «Доказательствами по уголовному делу являются законно полученные фактические данные, на основе которых в определенном настоящим Кодексом порядке орган дознания, дознаватель, следователь,

прокурор, суд устанавливают наличие или отсутствие деяния, предусмотренного Уголовным кодексом Республики Казахстан, совершение или несовершение этого деяния подозреваемым, обвиняемым или подсудимым, его виновность либо невиновность, а также иные обстоятельства, имеющие значение для правильного разрешения дела.». [6].

Согласно указанной части Уголовно-процессуального кодекса доказательствами признаются законно полученные **фактические данные**, в указанной статье также дано определение понятию **фактические данные**. Согласно части 2 статьи 111 Уголовно-процессуального кодекса Республики Казахстан: «Фактические данные, имеющие значение для правильного разрешения уголовного дела, устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля, имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста; **вещественными доказательствами;** протоколами процессуальных действий и иными документами.». [6].

Из всех фактических данных подходящих для исследования цифровой информации в плоскости Уголовно-процессуального кодекса рассматривается понятие вещественных доказательств.

Согласно части 1 статьи 118 Уголовно-процессуального кодекса Республики Казахстан: «Вещественными доказательствами признаются: 1.Предметы, если есть основания полагать, что они служили орудием или иным средством совершения уголовного правонарушения; 2.Предметы, которые сохранили или могли сохранить на себе следы уголовного правонарушения; 3.Предметы, которые были объектами общественно опасного посягательства; 4.Деньги, ценности и иное имущество, полученные в результате совершения уголовного правонарушения; 5.Деньги, ценности, иное имущество, предметы, документы, которые могут служить средствами к обнаружению уголовного правонарушения, установлению фактических обстоятельств дела, выявлению виновного лица либо опровержению его виновности или смягчению ответственности».

Из перечисленных вещественных доказательств для исследования цифровой информации по моему мнению ближе понятие «предметы, которые сохранили или могли сохранить на себе следы уголовного правонарушения».

Согласно сборнику словарей Ефремовой, Ожегова, Шведовой значение слова *предмет* в толковых словарях русского языка: ***предмет*** **–** *всякое материальное явление, вещь* (Пример: П. неопределенной формы; П. первой необходимости; П. домашнего обихода; П. народного потребления).[39]

Если буквально понимать закон, нами признаются не сведения, содержащие ту или иную информацию, а предметы содержащие указанную информацию. Но электронные доказательства подразумевает информацию в цифровой форме подтверждающую или опровергающую тот или иной факт.

Уголовно-процессуальным кодексом Республики Казахстан не охвачено понятие электронных доказательств в достаточной мере, что необходимо для идентификации в плоскости Уголовно-процессуального кодекса. Понятие

«электронных доказательств» – это притянутые за уши понятия «вещественных доказательств».

Цифровая реальность полностью участвует в жизни общества и государства, и стала средой и средством совершения преступлений. В этой связи, с целью доказывания тех или иных обстоятельств органу уголовного преследования и последующим суду необходимо изучать различные цифровые устройства, содержащие важную для расследования информацию. Действующее уголовно-процессуальное законодательство не в полной мере адаптировано к таким источникам информации. Сами по себе электронные доказательства могут охватываться понятием вещественных доказательств, предусмотренных Уголовно-процессуальным кодексом, однако порядок и специфика изъятия электронных доказательств принуждает орган уголовного преследования и суд иначе относиться к ним.

В этой связи, для четкого определения понятия электронных доказательств предлагаю внести в Уголовно-процессуальный кодекс Республики Казахстан дополнение, а именно:

1). Внести изменение в часть 2 статьи 111 Уголовно-процессуального кодекса Республики Казахстан от 04.07.2014 года №231-V ЗРК и изложить в следующей редакции: «Фактические данные, имеющие значение для правильного разрешения уголовного дела, устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста; вещественными доказательствами; **электронными доказательствами;** протоколами процессуальных действий и иными документами.»;

2). Добавить статью 118-1 Уголовно-процессуального кодекса Республики Казахстан от 04.07.2014 года №231-V ЗРК и изложить в следующей редакции: «Электронные доказательства – это любая накопленная, сохраненная или переданная в цифровой форме информация, необходимая подтверждения либо опровержения факта, который является предметом судебных разбирательств.».

2. СОВЕРШЕНСТВОВАНИЕ МЕТОДОВ ОБНАРУЖЕНИЯ И ЗАКРЕПЛЕНИЯ ЭЛЕКТРОННЫХ ДОКАЗАТЕЛЬСТВ.

2.1 Фиксация и изъятие электронных доказательств

Следователь должен иметь необходимые знания и опыт, которые помогут ему выбирать правильный алгоритм действия и применять методы, которые окажут минимальное влияние на систему. Очень важно все свои действия осуществлять с указанием времени их осуществления.

Сложно предложить универсальную схему обнаружения и изъятия компьютерных данных в режиме реального времени. Каждый случай по-своему уникален, и опытный следователь должен знать, как лучше поступить в той или иной ситуации.

Для криминалистического анализа компьютерных данных нужно иметь соответствующую подготовку, практический опыт, а также специальный набор утвержденных криминалистических инструментов. Если на месте обыска нет специалиста, который обладает вышеперечисленными навыками и инструментами, следует незамедлительно обратиться за помощью в специализированный отдел, в нашем случае в территориальные подразделения Управления «по борьбе с киберпреступлениями» Департамента Криминальной полиции Министерства Внутренних Дел, специалистам Департамента Экономических Расследовании, экспертам Института Судебных Экспертиз Министерства Юстиции Республики Казахстан.

В ходе проведения первоначальных следственных действии направленных на установление и сбор электронных доказательств нельзя вносить изменения в данные или устройства — как в само оборудование, так и в программное обеспечение. Лица, отвечающие за сохранность места преступления и сбор доказательств, обязаны обеспечить целостность отобранного материала и сохранность истории его передачи. Доступ к данным работающего устройства должен осуществляться квалифицированным специалистом, и это должно происходить таким образом, чтобы оказать минимальное влияние на сами данные.

В ходе составления соответствующего протокола следственного действия необходимо точно описать все действия лиц, чтобы при необходимости третья сторона могла воспроизвести эти действия. Нужно обеспечить подробное описание процесса поиска и выемки, условий хранения и порядка перемещения электронных данных и хранить эту информацию на случай проверки.

Интернет — это глобальная сеть, которая соединяет миллионы компьютеров во всем мире с помощью устройств и протоколов, и существуют несколько организаций, которые устанавливают правила и стандарты ее работы. В то же время, каждый отдельный узел глобальной паутины может работать как независимая подсеть, структура и содержание которой не зависят от других организаций. Существует множество технологий доступа в Интернет, что значительно расширяет диапазон онлайн-сервисов.

При работе с онлайн-доказательствами нужно четко различать виртуальный и физический мир и уметь переводить с одного языка на другой. На языке виртуального мира «местоположение» обычно называется URI/URL-адрес

(унифицированный идентификатор ресурса (Uniform Resource Identifier, сокр. URI) или унифицированный указатель ресурса (Uniform Resource Locator, сокр. URL) — это последовательность символов, которая функционирует как название или адрес места в сети Интренет), или IP-адрес.

Интернет-протокол — это устоявшийся набор стандартов и правил, которые используются для отправки или получения данных через сеть Интернет. IP-адрес — это самый базовый тип источника информации в Интернете. Он показывает, куда должны доставляться пакеты данных.

Процесс присвоения IP-адреса поставщикам интернет-услуг довольно прост. IANA сообщает региональной организации, какие IP-адреса доступны для заявителей в ее регионе. Затем поставщик интернет-услуг (Internet Service Providers, сокр. ISP) обращается к региональной организации для получения IP-адресов. После того как поставщик интернет-услуг получает определенный диапазон IP-адресов, он распределяет их между своими клиентами *(конечными пользователями)*, и выстраивает сеть, за которую несет ответственность.

Не бывает, чтобы к Интернету одновременно подключались два одинаковых общедоступных IP-адреса. Чтобы иметь возможность отправлять и получать письма *(данные),* каждый компьютер, подобно дому на городской улице, должен иметь свой уникальный адрес. При подключении домашнего компьютера к Интернету поставщик интернет-услуг предоставляет этому компьютеру во временное пользование уникальный IP-адрес. Это означает, что все действия в Интернете, которые осуществляются с этого компьютера в течение указанного времени, будут ассоциироваться с данным IP-адресом. После разъединения с Интернетом IP – адрес перераспределяется в пользу других компьютеров.

У каждого поставщика интернет-услуг есть определенный диапазон IP-адресов. Иногда количество клиентов поставщика интернет-услуг превышает количество его IP-адресов. Чтобы не терять клиентов из-за недостатка доступных адресов, разработаны специальные технологии и протоколы. Наиболее распространенным протоколом является протокол динамической настройки узла (Dynamic Host Configuration Protocol, сокр. DHCP).

DHCP — это протокол (*т.е. набор правил для устройств для осуществления связи друг с другом*), который используется для автоматического распределения диапазона IP-адресов среди группы устройств. Принцип работы этого протокола довольно простой. Когда устройство хочет подключиться к Интернету, оно запрашивает у своего поставщика интернет-услуг свободный IP-адрес; поставщик интернет-услуг проверяет свой список доступных IP-адресов *(т.е. смотрит, какие IP-адреса не присвоены в данный момент другим устройствам)* и выделяет запрашивающему клиенту *(устройству)* один из свободных IP – адресов. При этом поставщик интернет-услуг регистрирует дату, время и идентификаторы пользователя. Как только клиент отсоединяется от Интернета, используемый IP-адрес возвращается в список доступных IP – адресов для распределения между другими устройствами. Это означает, что при каждом подключении к Интернету пользователь или устройство могут

получать разные IP-адреса. Иногда IP-адрес меняется по несколько раз на протяжении одной сессии.

В реальном мире, если бы у вас постоянно менялся почтовый адрес, то писать вам письма было бы очень непросто, ведь почта не знала бы, куда их доставлять. В Интернете существуют определенные типы устройств, которые должны постоянно иметь один и тот же IP – адрес. В этих случаях используются статические IP-адреса, т.е. что поставщик интернет-услуг присваивает устройству *(клиенту)* определенный IP – адрес на весь период, пока он остается его клиентом.

Большинство поставщиков интернет-услуг имеют в своем диапазоне и статические, и динамические IP – адреса. И в первом, и во втором случае поставщики интернет-услуг знают, кто использовал конкретный IP – адрес в определенное время. Обратите внимание, хотя договора на предоставление услуг доступа в Интернет заключаются, как правило, с физическими или юридическими лицами, IP-адреса присваиваются устройствам, а не отдельным лицам.

Если во время интернет-расследования всплывает определенный IP-адрес, то у поставщика интернет-услуг можно узнать детали договора на предоставление доступа в Интернет и информацию об устройстве, которому был присвоен этот IP-адрес в определенное время. Как правило, доступ к такой информации можно получить на основании постановления о производстве выемки санкционированного следственным судом *(в отдельных случаях по требованию органа уголовного преследования)*. Обратите внимание, что вам необходимо максимально точно определить тот момент, когда соответствующий IP – адрес использовался в контексте расследуемых действий.

«UTC-10» указывает на часовой пояс, в данном случае — «всемирное координированное время минус 10 часов» (Гавайи). Направляя поставщику интернет-услуг запросы на предоставление информации об использовании IP – адресов, нужно обязательно указывать часовой пояс.

В рамках настоящего диссертационного исследования считаю нет необходимости останавливаться на порядке детального обнаружения электронных доказательств и последующего его изучения.

В настоящем исследовании акцент идет на проблемах с которыми орган уголовного преследования сталкивается при обнаружении и изъятии электронных доказательств.

При расследовании общеуголовных правонарушений основными следственными действиями в большинстве от которого зависит судьба уголовного дела являются осмотр, выемка и обыск. В указанных следственных действиях отражаются и описываются предметы на основании которых в последующем строится обвинение или принимаются решения о прекращении уголовного преследования. В ходе изъятия вещественных доказательств используется устойчивый алгоритм в котором описываются действия и фиксируются место обнаружения тех или иных доказательств.

Получение доказательств с электронных носителей информации многократно затрудняет получение и их изъятие. Учитывая, что целостность полученных электронных доказательств будет оспариваться в суде, органу уголовного преследования необходимо зафиксировать исходные данные электронных доказательств. Указанная фиксация необходима специалистам или экспертам, проводившим исследование электронных доказательств, для разъяснения где и каким образом получены те или иные электронные доказательства. Подсудимыми и их защитой выдвигаются разные версии о незаконности получения электронных доказательств, под сомнение ставятся обнаруженные электронные доказательства и их происхождение.

В ходе обнаружения и изъятии вещественных доказательств орган уголовного преследования полностью описывают предметы и документы, акцентируют внимание на отличительные признаки, описывают каждую деталь, упаковывают, прошнуровывают и оставляют разъяснительные пояснения на бирках. Однако, в ходе обнаружении и изъятии электронных носителей информации методы фиксаций применяемые к традиционным вещественным доказательствам, не достаточны. Объем памяти электронных носителей разный в зависимости от объемов информации, начиная с битов до петабайтов. Соответственно невозможно описывать свойства каждого из обнаруженных документов, находящихся в электронном носителе. Однако, чтобы убедить суд о законности получения электронных доказательств необходимо доказать, что электронный носитель информации не подвергался внешним и внутренним изменениям с момента его изъятия до обнаружения электронных доказательств.

При описании места обнаружения и изъятия электронных носителей информации необходимо зафиксировать следующую информацию *(на стадии сбора доказательств могут появиться дополнительные данные):*

➢ Физическое расположение объектов:

- Сделать зарисовку системы, т.е. расположения ее составных частей *(мыши, клавиатуры и т.д.);*
- Сделать фото- и видеосъемку помещения *(по возможности, круговую);*
- Обозначить местонахождение систем и электронных компонентов/устройств/оборудования и описать, каким образом они связаны между собой;

➢ Зафиксировать:

- Подробную информацию обо всех обнаруженных устройствах, которые имеют отношение к расследованию. Указать их марку, модель и серийный номер;
- Данные о состоянии и расположении всех компьютерных систем, которые содержат или представляют собой электронные доказательства, включая информацию о том, в каком состоянии находится компьютер (*включен, выключен, в спящем режиме);*
- Информацию о кабельном и беспроводном подключении компьютерных систем и прочих устройств;

• Обозначить все порты и кабели, а также соединения с периферийными устройствами: в дальнейшем это поможет восстановить точную конфигурацию системы. Пометить неиспользуемые порты;
• Для определения носителей данных найти стыковочные узлы ноутбука;
• Указать характеристики монитора;
• Сфотографировать переднюю часть компьютера, монитор и другие комплектующие;
• Описать, изображение экрана монитора;
• Снять включенные программы на видео или сделать подробное описание изображения на экране;
• Описать электронные устройства и компоненты, имеющие отношение к расследованию, но не подлежащие выемке;
➢ Информацию о лицах, находящихся в месте проведения обыска, выемки, осмотра;
➢ Опросить лиц, находящихся в месте проведения обыска, и внести их ответы в соответствующие формы;
➢ Задокументировать:
• Персональные данные всех лиц, находящихся в месте обнаружения и изъятия электронных носителей информации;
• Персональные данные всех лиц, использовавших компьютерные системы и оборудование;
• Информацию и комментарии, предоставленные свидетелями и пользователями/владельцами компьютерных устройств;
• Описание всех действий, осуществленных на месте проведения обыска;
• Сделать протокол соответствующего следственного действия с описанием всех действий и времени их осуществления;

Электронные *(впрочем, как и любые другие)* доказательства требуют бережного отношения — иначе они могут утратить доказательную силу. А значит, следователь должен обеспечить сохранность не только самих предметов и устройств, но и электронных данных, которые они содержат. Для некоторых видов электронных доказательств необходим специальный порядок изъятия, упаковки и транспортировки. Электронные доказательства могут повредиться или измениться под воздействием электромагнитных полей *(статического электричества, магнитов, радиопередатчиков и т.д.),* поэтому нужно предпринять необходимые меры для их защиты.

Традиционные неэлектронные доказательства могут также иметь больше значение для расследования дела, поэтому их необходимо изъять и обеспечить их сохранность. Объекты, которые представляют интерес для следствия, зачастую находятся прямо возле компьютера и других электронных устройств и тоже подлежат изъятию. По общему правилу, любые доказательства должны быть идентифицированы, изъяты, упакованы и отправлены на хранение в соответствии с ведомственными инструкциями и действующим законодательством.

Упаковка, транспортировка и хранение обнаруженных и изъятых электронных носителей информации:

Компьютеры и компьютерное оборудование — это хрупкие устройства, чувствительные к воздействию температур, влаги, механических повреждений, статического электричества, магнитного излучения и даже операционных команд *(например, включению/выключению).* Поэтому при их упаковке, транспортировке и хранении следует соблюдать соответствующие меры предосторожности. Необходимо документировать процесс упаковки, транспортировки и хранения доказательств, а также любые изменения, связанные с их местонахождением и условиями хранения: это - дает возможность отследить, в чьем распоряжении находились доказательства в тот или иной момент.

Нарушение правил работы с источниками электронных доказательств может привести к потере данных. Во избежание подобных ситуаций следует соблюдать такие рекомендации.

➢ Упаковка:

- Описать и промаркировать электронные доказательства перед тем, как их упаковывать;
- Перевезти изъятые доказательства в оригинальной упаковке;
- Если оригинальная упаковка не сохранилась, использовать антистатические материалы *(т.е. бумажные или антистатические полиэтиленовые пакеты).* Не использовать материалы, которые могут создавать статическое электричество *(т.е. **обычные полиэтиленовые пакеты**);*
- Не складывать, не сгибать и не царапать носители информации *(компакт-диски);*
- Ничего не наклеивать на поверхность носителей информации. По возможности упаковывать их в конверты или коробки;
- Подписывать все коробки и конверты с доказательствами;
- Если изъято несколько компьютерных систем, сделать соответствующие пометки, чтобы в дальнейшем можно было воссоздать исходную конфигурацию.

➢ Смартфоны, сотовые мобильные телефоны должны оставаться в том режиме (вкл./выкл.), в котором они были обнаружены:

- Для упаковки смартфонов и мобильных телефонов необходимо использовать изоляционные пакеты Фарадея *(они блокируют сигналы),* радиоизоляционные материалы или алюминиевую фольгу: это позволит предотвратить отправку и получение сообщений. Если устройство упаковано неправильно или его достали из защитной упаковки, то оно может отправлять и получать сообщения. Необходимо обратить внимание: в изоляционной упаковке устройство может разрядиться гораздо быстрее. Если заряд батареи заканчивается, можно перевести устройство ***в «режим полета»***.

➢ Транспортировка:

- Держать электронные доказательства вдали от источников магнитного излучения. Радиопередатчики, микрофоны и нагретые сиденья могут повредить электронные данные;
- Защитить изъятое оборудование от воздействия физических факторов *(ударов, влажности и высокой температуры);*
- Компьютеры и устройства, которые не были упакованы в коробки, во время транспортировки должны быть хорошо закреплены для защиты от повреждений и излишней вибрации. В частности, компьютеры размещаются на полу, а мониторы — на сиденье транспортного средства экраном вниз. Мониторы пристегиваются ремнями безопасности;
- Не класть большие тяжелые предметы на маленькие;
- По возможности не держать оборудование и устройства в машине дольше, чем необходимо.

➢ Хранение:

- Провести опись собранных доказательств в соответствии с Уголовно-процессуальным кодексом Республики Казахстан от 4 июля 2014 года №231-V ЗРК и Постановления Правительства Республики Казахстан №1291 «Об утверждении Правил изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, изъятых документов, денег в национальной и иностранной валюте, наркотических средств, психотропных веществ по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы» от 9 декабря 2014 года;
- Хранить доказательства в надежном месте, вдали от источников влаги и высоких температур в соответствии правил, указанных в Постановлении Правительства Республики Казахстан №1291 «Об утверждении Правил изъятия, учета, хранения, передачи и уничтожения вещественных доказательств, изъятых документов, денег в национальной и иностранной валюте, наркотических средств, психотропных веществ по уголовным делам судом, органами прокуратуры, уголовного преследования и судебной экспертизы» от 9 декабря 2014 года;
- Обеспечить защиту доказательств от магнитного излучения, влаги, пыли и других, вредоносных частиц и веществ;
- Для хранения доказательств использовать безопасные помещения с достаточным уровнем:
  - контроля доступа;
  - пожарной безопасности *(сигнализация, огнетушители, запрет на курение в зоне хранения и в прилежащих зонах);*
  - контроля температуры и влажности;
  - защиты от магнитных полей *(изоляция от направленного воздействия радиоустройств).*

➢ **Не хранить** в одном помещении с электронными доказательствами легковоспламеняющиеся вещества и предметы *(например, моющие средства или бумагу)*;

- Не хранить доказательства в помещениях с напольным покрытием, которое создает статическое электричество;
- Не хранить электронные доказательства в помещениях, где пролегают водопроводные трубы, особенно если трубы идут вдоль потолка;
- *Обратить внимание: со временем такие потенциальные доказательства как дата, время и конфигурация системы могут быть утеряны. Кроме того, информация может исчезнуть, если разрядится батарея. Проинструктируйте своих коллег, что в первую очередь следует обратить внимание на устройства, которые работают от батареи (ПК/CMOS). (CMOS-батарея, или батарея на основе технологии комплементарного металло-оксидного полупроводника (Mmplementary metal-oxide-semiconductor, сокр. CMOS) используется для запуска BIOS (basic input output system - базовая система ввода-вывода), которая, в свою, очередь, запускает компьютерную систему).*

Из опыта расследования уголовных дел с использованием электронных носителей информации предлагается в практике для удостоверения целостности и неизменности данных на носителе использовать однонаправленные хэш-функции.

Хеш использует алгоритм, применяемый к данным, который приводит к некоторому типу математического значения. Когда хеш применяется к двум точным наборам данных, ожидаемым результатом будет одно и то же значение хеш-функции. Если один набор данных немного отличается или отличается от другого набора данных, ожидаемым результатом будет другое значение хеш-функции

Хэш-функция обеспечивает шифрование с использованием алгоритма и без ключа. Они называются «односторонними хэш-функциями», потому что отменить шифрование не возможно. Открытый текст переменной длины «хешируется» в *(обычно)* хэш-значение фиксированной длины (часто называемое «*дайджестом сообщения*» или просто «*хешем*»). Хеш-функции в основном используются для обеспечения целостности: если хэш-код открытого текста изменяется, изменяется и сам открытый текст. Общие старые хэш-функции включают алгоритмы безопасного хеширования.

Например, при снятии специалистом образа диска на месте происшествия подсчитывается хэш-функция, значение которой заносится в протокол. Эксперт, получив на исследование копию, подсчитывает с нее хэш-функцию. Если ее значение совпадает со значением, внесенным в протокол, эксперт и иные лица получают уверенность, что исследуемая копия совпадает с оригиналом с точностью до бита. Аналогично хэш-функция используется для контроля целостности отдельных файлов. Например, при изъятии логов. Подсчитывается хэш-функция от лог-файла, она заносится в протокол. Значение хэш-функции в протоколе обеспечивает неизменность файла при копировании и последующем хранении. Совпадение значений хэш-функции гарантирует полное совпадение файлов.

В уголовно-процессуальном законодательстве содержатся порядок сбора доказательств и их допустимость. Что касается доказательств в электронном

виде, компьютерные данные легко можно изменить. Поэтому при сборе и обращении с электронными доказательствами необходимо обеспечить целостность, подлинность и непрерывность доказательства в течение всего периода времени с момента его выемки до приговора суда или вынесения окончательного решения органом уголовного преследования.

В качестве примера хотелось бы остановиться на опыте Соединенных Штатов Америки, которые в августе 2015 года приняли на Федеральном уровне «Стандарты безопасного хеширования» (SHS) (FIPS PUB 180-4) разработанный Департаментом Коммерции США. Этот стандарт определяет хэш-алгоритмы, которые могут использоваться для генерации дайджестов сообщений. Дайджесты используются с целью определения были ли сообщения изменены с момента создания дайджестов. [40]

В указанном под разделе описываются особенности обнаружения и изъятия электронных носителей информации, учитывая специфику электронных доказательств необходимо четко придерживаться всех выше описанных рекомендации. Так как электронные доказательства являются хрупкими, чувствительными к воздействию температур, влаги, механических повреждений, статического электричества, магнитного излучения и даже операционных команд при их упаковке, транспортировке и хранении следует соблюдать соответствующие меры предосторожности. Помимо специфичности изъятия и хранения электронных доказательств органу уголовного преследования и суду необходимо доказать исходные данные электронных доказательств. Для удостоверения целостности и неизменности данных электронных носителей информации с момента изъятия рекомендуется на примере Соединенных Штатов Америки определить «стандарт безопасного хеширования», которые могут использоваться для определения были ли сообщения изменены с момента создания дайджестов.

2.2. Особенности сбора данных, находящихся в распоряжении третьих лиц, в том числе расположенных за границей

Поскольку террористы и представители организованной преступности все активнее используют Интернет, социальные сети и системы мгновенного обмена сообщениями с функцией шифрования для совершения своих преступных деяний, получение доказательств от поставщиков таких услуг имеет первостепенное значение. [1]

Электронные доказательства, хранящиеся у поставщиков услуг, могут быть использованы для подтверждения того, что преступление было совершено, раскрытия сведений об обличающих связях и определения местонахождения правонарушителей. Получение таких электронных доказательств поможет обеспечить судебное преследование конкретного виновного лица, а также привлечение к ответственности лиц, совершающих серьезное преступление. [1]

Иногда у следователя нет возможности получить прямой или удаленный доступ к устройству, на котором хранятся данные и произвести необходимые следственные действия. А если данные хранятся на большом сложном оборудовании *(например, на оборудовании крупного поставщика интернет-услуг)*, то доступ к ним иногда и вовсе не возможен без содействия и помощи со стороны его владельцев. В таких случаях рекомендуется установить сотрудничество с третьими лицами, например, с компанией-поставщиком хостинговых услуг, которая может иметь в своем распоряжении системные журналы и регистрационные данные.

Кроме того, третьи лица могут собирать и некоторое время **сохранять** электронные доказательства, которые указывают на совершение преступления и являются основанием для регистрации уголовного дела. Учитывая необъятный размер Интернета и количество транзакций, которые совершаются в сети каждую минуту, правоохранительные органы с их ограниченными ресурсами просто не в состоянии охватить все веб-пространство. В то время как одни данные в сети Интернет являются общедоступными, доступ к другим данным ограничен, и для его получения необходимо знать регистрационные данные. Если для совершения преступления используются закрытые каналы связи *(например, электронная почта)*, то пока лицо, имеющее доступ к такому каналу, не обратится в правоохранительные органы, у них практически нет никаких шансов отследить эти действия или получить необходимые доказательства.

Иногда очень непросто установить лицо, совершившее компьютерное преступление через Интернет. Зачастую все, что известно о подозреваемом, — это его IP-адрес, MAC-адрес *(Адрес управления доступом к среде (Media Access Control address) — это уникальное число, которое идентифицирует устройство в сети)*, адрес электронной почты, доменное имя или интернет-псевдоним (*«ник»*). Чтобы идентифицировать физическое лицо по IP-адресу, специалисту нужны данные, которые находятся в распоряжении поставщика интернет-услуг. Поставщики интернет-услуг *(электронной почты, хостинговых услуг)* зачастую являются единственным источником информации,

которая помогает установить связь между виртуальной личностью правонарушителя и конкретным физическим лицом. Поэтому независимые владельцы данных часто оказываются ключевым звеном в расследовании.

Использование базы данных для идентификации преступников — стандартная процедура в рамках уголовного процесса. Базы данных отпечатков пальцев и ДНК во многих странах являются одним из основных пунктов, обеспечивающих успех расследования. В то же время, базы данных, которые могут использоваться в качестве электронных доказательств, принадлежат скорее не правоохранительным органам или государственным организациям, а множеству частных компаний, обеспечивающих работу сети Интернет. Это означает, что необычайно важно поддерживать сотрудничество с такими компаниями. В то же время, из-за отсутствия централизованной информации об идентификационных данных пользователей поставщикам интернет-услуг довольно сложно выработать единые стандарты обмена данными. Каждый использует свои собственные методы фиксации запрашиваемых данных, определения приоритетности запросов на предоставление данных и борьбы с правонарушителями в сети.

Если между правоохранительными органами и независимым владельцем данных налажен регулярный диалог, то это помогает избежать недоразумений, дает возможность определить приоритетность запросов на предоставление данных и способствует укреплению культуры сотрудничества. Кроме того, поставщики услуг, у которых налажены доверительные отношения с правоохранительными органами, гораздо охотнее идут на контакт и сообщают о выявленных нарушениях.

Правоохранительным органам рекомендуется проводить регулярные встречи с поставщиками интернет-услуг и другими лицами, которые владеют данными о пользователях сети Интернет. Эти встречи можно использовать не только для обсуждения насущных проблем сотрудничества, но и для стратегического анализа возможных тенденций и угроз. Кроме того, можно проводить совместные тренинги для представителей правоохранительных органов и частных компаний: это поможет сторонам избавиться от взаимных предубеждений и будет способствовать созданию доверительной атмосферы.

Согласно пункта 18 статьи 2 Закона Республики Казахстан «О связи»: «оператор связи – физическое или юридическое лицо, зарегистрированное на территории Республики Казахстан, оказывающее услуги связи и (или) эксплуатирующее сети связи. [30]

Согласно ответа №28-1-28/2734 от 06.12.2019 года Республиканского государственного учреждения «Комитет Телекоммуникации» Министерства цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан оператор связи с момента начала деятельности по оказанию услуг связи в порядке ст.16-1 Закона «О связи» направляет уведомление в уполномоченный орган. Согласно приложенной таблицы указанного Комитета в Казахстане зарегистрировано **119** операторов связи. [28]

В соответствии со ст.5 постановления Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной

информации об абонентах» № 246 от 30 марта 2010 года оператор обеспечивает сбор и хранение служебной информации об абонентах ***в течение двух лет***, по истечении которых информация уничтожается. Оператор несет ответственность, предусмотренную законами Республики Казахстан, за нарушение обязанности по сбору и хранению служебной информации об абонентах. [32]

Однако, у нас в стране орган уголовного преследования во время обращения к операторам связи на законодательном уровне имеет большую преграду, а именно операторами связи игнарируются законные требования органа уголовного преследования и органа надзора в выдаче служебной информации.

Закон Республики Казахстан «О связи» от 05 июля 2004 года №567 устанавливает правовые основы деятельности в области связи на территории Республики Казахстан, определяет полномочия государственных органов по регулированию данной деятельности, права и обязанности физических и юридических лиц, оказывающих или пользующихся услугами связи. [30]

В соответствии с ч.1 ст.15 Закона Республики Казахстан «О связи» №567 операторы связи, осуществляющие свою деятельность на территории Республики, обязаны в соответствии с законодательством Республики Казахстан обеспечивать органам, осуществляющим оперативно-розыскную деятельность, контрразведывательную деятельность на сетях связи, организационные и технические возможности проведения оперативно-розыскных, контрразведывательных мероприятий на всех сетях связи, доступ к служебной информации об абонентах. [30]

Согласно статьи 15 Закона РК «О связи» законодатель предоставляет на сетях связи организационные и технические возможности проведения оперативно-розыскных и контрразведывательных мероприятий лишь органам, осуществляющим оперативно-розыскную и контрразведывательную деятельность. [30]

Согласно пункта 2 статьи 2 Закона РК «О связи» служебная информация об абонентах – сведения об абонентах, предназначенные исключительно для целей проведения контрразведывательной деятельности и оперативно-розыскных мероприятий на сетях связи и включающие в себя: 1). Информацию об абонентских номерах, включая сведения об индивидуальных идентификационных номерах *(для физических лиц)* или бизнес-идентификационных номерах *(для юридических лиц)* владельцев абонентских номеров; 2). Информацию об идентификационных кодах абонентских устройств сотовой связи включая сведения об индивидуальных идентификационных номерах *(для физических лиц)* или бизнес-идентификационных номерах *(для юридических лиц)* владельцев абонентских устройств сотовой связи; 3). Биллинговые сведения *(сведения о полученных абонентам услугах)*; 4). Местоположение абонентского устройства в сети в соответствии с требованиями технического регламента; 5). Адреса в сети передачи данных; 6). Адреса обращения к интернет-ресурсам в сети передачи

данных; 7). Идентификаторы интернет-ресурса; 8). Протоколы сети передачи данных. [30]

В законе «О связи» отсутствуют права лиц, осуществляющих досудебное расследование или прокурорский надзор. Отсутствие в законе «О связи» лиц, осуществляющих досудебное расследование и прокурорский надзор, является основанием необоснованного отказа операторами связи в предоставлении законно требуемой служебной информации об абонентах. В мотивировочной части операторы связи указывают, что поскольку требование лиц, осуществляющих досудебное расследование и прокурорский надзор не связаны с проведением оперативно-розыскных мероприятий и контрразведывательной деятельности, оператор связи вынужден отказать в исполнении требовании.

Согласно, ч.5 ст. 34 Уголовно-процессуального кодекса Республики Казахстан «требования органа уголовного преследования, предъявленные в соответствии с законом, обязательны для исполнения всеми государственными органами, организациями, должностными лицами и гражданами и должны быть исполнены в установленный им срок, но не позднее трех суток. Невыполнение указанных требований без уважительных причин влечет установленную законом ответственность». [6]

Согласно, пункту 10 части 1 статьи 44 Закона Республики Казахстан «О прокуратуре» от 30.06.2017 года №81-VI «прокурор в соответствии со своей компетенцией вправе в установленном законодательством порядке получать доступ к документам и материалам, связанным с проведением проверок». [31]

Согласно, части 6 ст.45 Закона Республики Казахстан «О прокуратуре» от 30.06.2017 года №81-VI «неисполнение законных требований прокурора либо неявка по требованию прокурора без уважительных причин влечет ответственность, установленную законом». [31]

В этой связи, возникает необходимость во внесении изменении в Закон Республики Казахстан «О связи» с четким указаниям прав органов уголовного преследования и органа надзора на получения служебной информации об абонентах.

Согласно ответам АО «Кселл», ТОО «Сеть Казахстан», ТОО «BTcom infocommunications», АО «ASTEL» и еще некоторых операторов связи доступ к системам сбора и хранения служебной информации об абонентах переданы в КНБ РК, в этой связи, представить служебную информацию об абонентах, не могут так как не имеют доступа. [28]

Согласно ответу уполномоченного Департамента Комитета национальной безопасности Республики Казахстан от 23.02.2021 года за исх. №5/1/7473 получена информация в отношении абонентов АО «Кселл», осуществлявших соединения с интересующим IP-адресом. На сети оператора связи АО «Инженерно-технический центр» средства сбора и хранения служебной информации на сети передачи данных отсутствуют. В этой связи для получения запрашиваемой информации необходимо обратиться в адрес указанного оператора. [28]

Согласно ответов операторов связи на основании подпункта 5 пункта 8 Постановления Правительства Республики Казахстан «Об утверждении Правил

обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 Компании предоставляют доступ к служебной информации об абонентах уполномоченному подразделению органа национальной безопасности *(при размещении владельца оборудования на объектах оперативного обеспечения Службы государственной охраны Республики Казахстан соглашение согласовывается со Службой государственной охраны Республики Казахстан)*. [33]

Также операторы связи ссылаются на пункт 7 вышеуказанного Правила поясняют, что в целях обеспечения функции телекоммуникационного оборудования для технического проведения ОРМ, КРМ в интересах решения задач всеми органами, осуществляющими ОРД, КРД, между владельцем оборудования и уполномоченным подразделением органов национальной безопасности заключается двустороннее соглашение о взаимодействии на объектах связи. [33]

Согласно 3 абзаца подпункта 2 пункта 4 статьи 12 Закона Республики Казахстан «Об оперативно-розыскной деятельности» от 15 сентября 1994 года №154-XIII «Специальные оперативно-розыскные мероприятия, связанные с использованием сети связи в интересах решения задач всеми органами, технически осуществляются органами национальной безопасности Республики Казахстан, для чего им выделяются необходимые силы и средства». [34]

В Законе Республики Казахстан «О связи» №567 от 05.07.2004 года и в Постановлениях Правительства №246 от 30.03.2010 года и №358 от 19.06.2018 года законодатель ссылаясь на Закон РК «Об оперативно-розыскной деятельности» от 15.09.1994 г. №154-XIII определил выдачу служебной информации об абонентах лишь в рамках Специальных оперативно-розыскных мероприятиях.

Кроме того, операторы связи ссылаясь на подпункт 5 пункта 8 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 *предоставляют лишь доступ к служебной информации подразделению Комитета национальной безопасности и на этом свою деятельность в предоставлении служебной информации замораживают, формулируя что им доступ к служебной информации запрещен*. В основном операторы связи покупают оборудование, которое не всегда соответствует требованию, и предоставляют доступ сотрудникам Комитета национальной безопасности, для проведения СОРМ,

однако на требования и постановления органов уголовного преследования не отвечают ссылаясь, что не имеют доступа к служебной информации. Тем самым, операторы связи не хотят взаимодействовать с правоохранительными органами с целью раскрытия и пресечения преступлений путем предоставления служебной информации об абонентах.

Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и надзорному органу в соответствии их деятельности.

В этой связи в рамках настоящего диссертационного исследования предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года, Постановление Правительства Республики Казахстан «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года, Постановление Правительства Республики Казахстан «Правила обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» №358 от 19.06.2018 года.

В рамках настоящего диссертационного исследования предлагается внести следующие поправки ***в закон Республики Казахстан «О связи» №567 от 05.07.2004 года***:

1). Изменить пункт 2 статьи 2 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «служебная информация об абонентах – сведения об абонентах, предназначенные исключительно для целей проведения контрразведывательной деятельности, оперативно-розыскных мероприятий, **досудебного расследования, прокурорского надзора** на сетях связи и включающие в себя:»;

2). Изменить название статьи 15 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «Взаимодействие операторов связи, оператора централизованной базы данных абонентских номеров, оператора базы данных идентификационных кодов абонентских устройств сотовой связи с органами, осуществляющими оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор**»;

3). Изменить пункт 1 части 1 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «обеспечивать органам, осуществляющим оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор** на сетях связи, организационные и технические возможности проведения оперативно-розыскных, контрразведывательных мероприятий, **досудебное расследование, прокурорский надзор** на всех сетях связи, а также принимать меры по

недопущению раскрытия форм и методов проведения указанных мероприятий»;

4). Изменить пункт 3 части 1 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «обеспечить органам, осуществляющим оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор** на сетях связи, доступ к служебной информации, а также принимать меры по недопущению раскрытия форм и методов проведения указанных мероприятий»;

5). Изменить пункт 4 части 1 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «обеспечить за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **досудебного расследования, прокурорского надзора** в соответствии с требованиями к сетям и средствам связи и порядком, которые определены Правительством Республики Казахстан»;

6). Изменить часть 3 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «операторы связи, оператор централизованной базы данных абонентских номеров и оператор базы данных идентификационных кодов абонентских устройств сотовой связи обязаны безвозмездно обеспечить доступ к сведениям, содержащимся в базах данных абонентских номеров и идентификационных кодов абонентских устройств сотовой связи, органам, осуществляющим оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор** на сетях связи, в соответствии с настоящим Законом и законами Республики Казахстан «Об оперативно-розыскной деятельности», «О контрразведывательной деятельности», «О персональных данных и их защите», **«О прокуратуре» и Уголовно-процессуальным Кодексом Республики Казахстан»**;

7). Изменить часть 5 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «Взаимоотношения операторов связи, оператора централизованной базы данных абонентских номеров, оператора базы данных идентификационных кодов абонентских устройств сотовой связи с органами, осуществляющими оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор,** регулируются в соответствии с настоящим Законом и законами Республики Казахстан «Об оперативно-розыскной деятельности», «О контрразведывательной деятельности», **«О прокуратуре» и Уголовно-процессуальным кодексом Республики Казахстан»;**

8). Изменить часть 4 статьи 36 Закона РК «О связи» №567 от 05.07.2004 года и изложить в следующей редакции: «Получение от оператора связи служебной информации допускается только с согласия абонента и в случаях, предусмотренных настоящим Законом и законами Республики Казахстан "Об оперативно-розыскной деятельности", "О контрразведывательной

деятельности", "О персональных данных и их защите", **“О прокуратуре” и «Уголовно-процессуального кодекса Республики Казахстан».**

В рамках настоящего диссертационного исследования предлагается внести следующие поправки в ***Постановление Правительства Республики Казахстан «Об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года:***

1). Изменить статью 1 Постановления Правительства «Об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года и изложить в следующей редакции: «настоящие Правила осуществления операторами связи сбора и хранения служебной информации об абонентах (далее – Правила) разработаны в соответствии с законами Республики Казахстан от 15 сентября 1994 года "Об оперативно-розыскной деятельности", от 5 июля 2004 года "О связи", от 6 января 2012 года "О национальной безопасности Республики Казахстан", от 24 ноября 2015 года "Об информатизации", от 28 декабря 2016 года "О контрразведывательной деятельности", от 30 июня 2017 года **«О прокуратуре» и от 3 июля 2014 года «Уголовно-процессуального кодекса Республики Казахстан»** и определяют порядок осуществления операторами связи Республики Казахстан сбора и хранения служебной информации об абонентах;

2). Изменить пункт 2 статьи 2 Постановления Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года и изложить в следующей редакции: «служебная информация об абонентах – сведения об абонентах, предназначенные исключительно для целей проведения контрразведывательной деятельности, оперативно-розыскных мероприятий, **досудебного расследования, прокурорского надзора** на сетях связи и включающие в себя:».

В рамках настоящего диссертационного исследования предлагается внести следующие поправки в ***Постановление Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358:***

1). Изменить название Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в

следующей редакции: «Постановление Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** и требований к сетям и средствам связи» от 19.06.2018 года №358»;

2). Изменить статью 1 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Настоящие Правила обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функций своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** (далее – Правила) определяют порядок обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств, функций своего телекоммуникационного оборудования для технического проведения оперативно-розыскных мероприятий (далее – ОРМ), контрразведывательных мероприятий (далее – КРМ), **собирания доказательств в рамках досудебного расследования, прокурорского надзора»;**

3). Изменить пункт 1 статьи 3 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «средства проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** – аппаратные и (или) программные средства, входящие в состав телекоммуникационного оборудования для обеспечения функций технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**;»;

4). Изменить пункт 3 статьи 3 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории

Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «владельцы телекоммуникационного оборудования (далее – владельцы оборудования) – операторы связи и (или) владельцы сетей связи, телекоммуникационное оборудование которых обеспечивает функции технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**;»;

5). Изменить пункт 4 статьи 3 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «тестовое подключение – подключение к сети телекоммуникаций оператора связи или сервиса в целях проверки корректности работы функций телекоммуникационного оборудования для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**;»;

6). Изменить Главу 2. Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: **«**Порядок обеспечения операторами связи и (или) владельцами сетей связи функций своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **собирания доказательств в рамках досудебного расследования, прокурорского надзора;**»;

7). Изменить статью 4 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Функционирование и сохранность телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** включая техническое обслуживание и ремонт, применение систем охранной сигнализации и видеонаблюдения,

обеспечиваются владельцами оборудования за счет собственных и (или) привлеченных средств.»;

8). Изменить статью 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «При обеспечении функций телекоммуникационного оборудования для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** владельцы оборудования за счет собственных и (или) привлеченных средств обеспечивают:»;

9). Изменить пункт 1 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «необходимые канальные и технические ресурсы сети телекоммуникаций для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**;»;

10). Изменить пункт 2 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «доступ органов, осуществляющих оперативно-розыскную деятельность (далее – ОРД), контрразведывательную деятельность (далее – КРД), **досудебное расследование, прокурорский надзор к служебной информации об абонентах;**»;

11). Изменить пункт 4 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «сохранность и безопасность телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания**

доказательств в рамках досудебного расследования, прокурорского надзора, размещенного на объектах связи;»;

12). Изменить пункт 5 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «необходимые условия для бесперебойного функционирования оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** включая электроснабжение, заземление, климатические условия, пожарную безопасность;»;

13). Изменить пункт 6 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «организационные и технические возможности проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** на всех сетях связи;»;

14). Изменить пункт 7 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «принятие мер по недопущению раскрытия форм и методов проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора;**»;

15). Изменить пункт 10 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «незамедлительное устранение неисправностей, возникших в работе телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора;**»;

16). Изменить статью 6 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «ОПС по обращению уполномоченного подразделения органов национальной безопасности представляют информацию о выданных сертификатах на телекоммуникационное оборудование с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора.**»;

17). **Добавить статью 6-1** в Постановление Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «**В целях обеспечения функции телекоммуникационного оборудования для технического собирания доказательств в рамках досудебного расследования, прокурорского надзора в интересах решения задач всеми органами, осуществляющими досудебное расследование, прокурорский надзор владельцы оборудовании самостоятельно осуществляют выдачу информации на основании мотивированного постановления вынесенного в соответствии с Уголовно-процессуальным кодексом Республики Казахстан и Закон Республики Казахстан «О прокуратуре»**;

18). Изменить первый абзац статьи 10 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Ввод в эксплуатацию нового и вывод из эксплуатации или модернизация устаревшего телекоммуникационного оборудования, изменение действующих схем связи производятся в соответствии с разработанным и утвержденным владельцем оборудования по согласованию с уполномоченным подразделением органов национальной безопасности планом мероприятий по обеспечению функций телекоммуникационного оборудования для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** на сети телекоммуникаций владельца оборудования»;

19). Изменить пункт 1 статьи 11 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «обеспечение технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** на сети телекоммуникаций оператора связи»;

20). Изменить пункт 3 статьи 11 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «реализация новых проектов, приобретение и установка телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** (место установки телекоммуникационного оборудования согласовывается с органами национальной безопасности);»;

21). Изменить пункт 4 статьи 11 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «ввод в постоянную эксплуатацию нового оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** проведение опытной эксплуатации, устранение недостатков, выявленных органами национальной безопасности;»;

22). Изменить статью 12 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Проведение внеплановых работ на телекоммуникационном оборудовании с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного**

расследования, прокурорского надзора, осуществляется по согласованию с уполномоченными подразделениями органов национальной безопасности.»;

23). Изменить статью 13 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Владельцы оборудования принимают меры по ограничению круга лиц, привлекаемых к обеспечению функций для технического проведения ОРМ, КРМ, установке средств проведения ОРМ, КРМ, а также недопущению раскрытия организационных и технических приемов проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**»;

24). **Добавить статью 13-1** Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Владельцы оборудования принимают меры по организации и определения лиц, работающих у них, имеющих соответствующие допуска к секретным материалам, к обеспечению функций для технического собирания доказательств в рамках досудебного расследования, прокурорского надзора, установке средств собирания доказательств в рамках досудебного расследования, прокурорского надзора, а также недопущению раскрытия организационных и технических приемов собирания доказательств в рамках досудебного расследования, прокурорского надзора.»;

25). Изменить статью 15 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Испытания при подтверждении соответствия телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** проводятся ОПС в присутствии представителя уполномоченного подразделения органа национальной безопасности в срок, не превышающий 30 календарных дней с момента начала испытания.»;

26). Изменить первый абзац статьи 17 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Ввод оборудования в опытную эксплуатацию подтверждается актом ввода в опытную эксплуатацию телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** составляемым по форме согласно приложению 1 к настоящим Правилам, утверждаемым руководителем уполномоченного подразделения органов национальной безопасности и владельца оборудования. Продолжительность опытной эксплуатации определяется уполномоченным подразделением органов национальной безопасности, но не более 60 календарных дней с момента подписания акта ввода в опытную эксплуатации.»

27). Изменить второй абзац статьи 17 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Положительные результаты опытной эксплуатации оформляются заключением, составляемым по форме согласно приложению 2 к настоящим Правилам, в котором отражаются наименование владельца оборудования, предмет испытаний, тип сети связи, продолжительность, результаты испытаний и выводы о соответствии требованиям технических регламентов и национальных стандартов в области обеспечения проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**.»;

28). Изменить четвертый абзац статьи 17 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Ввод в постоянную эксплуатацию оформляется актом ввода в эксплуатацию телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** составляемым по форме согласно приложению 3 к настоящим Правилам.»;

29). Изменить статью 18 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «При авариях, сбоях, повреждении телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** владельцы оборудования незамедлительно уведомляют об этом уполномоченное подразделение органов национальной безопасности и предпринимают меры по устранению неисправностей и восстановлению работоспособности оборудования.»;

30). Изменить статью 19 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «При систематических авариях, сбоях или продолжительном нефункционировании телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** уполномоченным подразделением органов национальной безопасности инициируется аннулирование акта ввода в эксплуатацию с последующим обращением в уполномоченный орган на предмет приостановления действия сертификата соответствия.»;

31). Изменить первый абзац статьи 20 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Вывод из эксплуатации телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** и их повторное использование, а также утилизация устройств накопления и хранения информации владельцами оборудования осуществляются по согласованию с уполномоченным подразделением органов национальной безопасности.»;

32). Изменить второй абзац статьи 20 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами

связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Вывод из эксплуатации оформляется актом вывода из эксплуатации телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** составляемым по форме согласно приложению 4 к настоящим Правилам.»;

33). Изменить третий абзац статьи 20 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «По итогам утилизации средств накопления и хранения информации владельцами оборудования составляется акт утилизации средств накопления и хранения информации телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** по форме согласно приложению 5 к настоящим Правилам. Акт утилизации составляется в двух экземплярах, первый экземпляр представляется владельцем оборудования в уполномоченное подразделение органов национальной безопасности, второй хранится у владельца оборудования.»;

34). Изменить статью 22 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «На телекоммуникационном оборудовании с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** должны предусматриваться меры физического и аппаратно-программного ограничения несанкционированного доступа к оборудованию.»;

35). Изменить статью 23 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и

требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Телекоммуникационное оборудование с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** подключается владельцами оборудования к каналам и линиям связи органов национальной безопасности через точки подключения.»;

36). Изменить статью 24 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Владельцы оборудования обеспечивают соблюдение требований по качеству телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** и длительному сроку его непрерывного бесперебойного функционирования в круглосуточном режиме с наименьшим количеством отказов.»;

37). Изменить статью 25 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Техническое обслуживание и ремонт телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** обеспечивают владельцы оборудования за счет собственных и/или привлеченных средств.»;

38). Изменить статью 26 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «Владельцы оборудования в целях своевременного устранения неисправностей и восстановления работоспособности оборудования обеспечивают наличие резервных узлов и (или) комплектующих телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**.»;

39). Изменить статью 28 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 и изложить в следующей редакции: «При изменениях сетей телекоммуникаций, вводе нового оборудования, увеличении емкости каналов связи владельцы оборудования производят необходимые изменения телекоммуникационного оборудования для обеспечения функций технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** с последующим проведением сертификационных испытаний.».

Еще одной проблемой с которой сталкиваются органы уголовного преследования является очень большое количество операторов связи.

Согласно ответа №28-1-28/2734 от 06.12.2019 года Республиканского государственного учреждения «Комитет Телекоммуникации» Министерства цифрового развития, оборонной и аэрокосмической промышленности Республики Казахстан оператор связи с момента начала деятельности по оказанию услуг связи в порядке ст.16-1 Закона «О связи» направляет уведомление в уполномоченный орган. Согласно приложенной таблицы указанного Комитета в Казахстане зарегистрировано **119** операторов связи. [28]

В ходе анализа ответов операторов связи, зарегистрированных в Комитете Телекоммуникации, получены ответы, которые показали отсутствие контроля со стороны уполномоченного органа.

Согласно ответу ИП «AZIZA», ГУ «отдел ветеринарии уйгурского района» подали в портале Государственных закупок ценовое предложение «Услуги, направленные на предоставление доступа к Интернету широкополосному по сетям проводным» на общую сумму 170 000 тенге. 28.01.2019 года составил договор с последним, купил модем и СИМ карту АО «Altel» и подключил без лимитный интернет трафик со скоростью 40 мб/с. [28]

Согласно ответам ИП «IT Service Group», ТОО «Eurasian Telecom» и многих других компании они предоставляют услуги доступа к сети интернет арендуя канал связи у операторов на основании договоров (последняя миля – last mile), не имеют возможности предоставить информацию по IP-адресам. [28]

Согласно ответу Дивизиона по корпоративному бизнесу – филиал АО «Казахтелеком» от 23.02.2021 за №03-04-14/909 «четко не определен порядок или правила аренды интернет каналов (последней мили). Отдельный документ, утвержденный на уровне Правительства РК регламентирующий данный спектр услуг также не утвержден. Таким образом, предоставление в аренду интернет каналов (последней мили) осуществляется на договорной основе по соглашению сторон». [28]

Согласно ответу РГУ «Комитет Телекоммуникаций» Министерства цифрового развития, инноваций и аэрокосмической промышленности

Республики Казахстан от 24.02.2021 года за исх.№ 28-1-1-28/324 *«Юридические лица, арендующие каналы связи у операторов на основании договоров (последняя миля – last mile) – **являются операторами связи** по предоставлению нелицензируемых услуг связи. Данные операторы получают трафик у междугородних и международных операторов связи в рамках заключенного договора. Договор заключается согласно гражданскому законодательству Республики Казахстан. Условия договора определяются по усмотрению сторон».*

Согласно ответам ТОО «ТТК», АО «Казахтелепорт» и еще нескольких операторов связи предоставление служебной информации об абонентах не представилось возможным по тем или иным причинам. [28]

Учитывая, что согласно ст.5 постановления Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года оператор обеспечивает сбор и хранение служебной информации об абонентах ***в течение двух лет,*** предлагается включить деятельность операторов связи сбора и хранения служебной информации об абонентах в лицензируемую деятельность. Лицензию и разрешение на оказание услуг связи операторам связи предлагается выдавать после эксплуатации сертифицированной системы сбора и хранения служебной информации об абонентах.

При наличии вышеуказанных проблем, возникших на основании узкого применения Закона Республики «О связи» и вытекающих с указанного закона нормативных постановлении Правительства у органа уголовного преследования возникают иные проблемы, связанные не сохранением служебной информации иными государственными органами.

Специальными прокурорами в ходе досудебного расследования выявлены недостатки, связанные с электронными доказательствами, а именно:

1). В ИС «Судебный кабинет» отследить IP-адрес сервера, с которого осуществлено подписание документа 2017 года не представляется возможным, так как логирование IP-адресов осуществляется лишь с 15.06.2020г.

2). АО «Центр электронных финансов» на сайте goszakup.gov.kz логирование имени и MAC адреса компьютера по договорам о государственном закупе, логирование имени и MAC адреса компьютера, IP-адреса сервера при составлении актов приема-передачи по заключенному договору посредством веб-портала «Государственные закупки» не проводится.

Указанные недостатки дают преступникам, в том числе расхищающим государственные средства лазейку на избежание от уголовной ответственности за совершенные преступления, так как затрудняется идентификация совершения такого или иного действия конкретными человеком на конкретном компьютере.

Вышеуказанные инициативы об изменении Законодательств в области предоставления служебной информации об абонентах уполномоченными частными организациями повлекут проведение качественного и всестороннего расследования органами уголовного преследования. В этой связи, органам уголовного преследования необходимо развивать свой потенциал в

обнаружении и изучении необходимых электронных доказательств полученных у Поставщиков Услуг.

Еще одним и очень важным инструментом в ходе расследования являются данные, находящиеся в распоряжении третьих лиц, расположенных за границей. Указанные сведения являются большим аспектом исследования в области добывания электронных доказательств.

Чрезвычайно важно учитывать на раннем этапе возможность запроса доказательств у иностранного Поставщика услуг, поскольку такие расследования могут потребовать много времени, оказаться сложными и дорогостоящими. Зачастую это означает обращение за Взаимной правовой помощью, и означенный механизм становится все более перезагруженным, что приводит к значительным задержкам. Это никак не сочетается со стремительным характером терроризма или организованной преступности, для которых в Интернете нет границ. [1]

Практикующим специалистам в запрашивающем Государстве (а именно – сотрудникам правоохранительных органов, прокуратуры и судебных органов) необходимо понимать, как сохранить электронные доказательства, получить данные, чтобы предотвратить чрезвычайную ситуацию, как и когда использовать альтернативы Взаимной правовой помощи в отношении электронных доказательств. Аспект развития компетенций в этих сферах сохраняет свою важность, поскольку отдельные правительства и региональные органы начинают разрабатывать новые, дополнительные структуры для получения электронной записи. [1]

В ходе досудебного расследования уголовного дела в отношении участников транснациональной киберпреступной группы «Карбанак/Кобальт» направлено 44 международных поручении в страны дальнего и ближнего зарубежья, из которых исполнено или частично исполнено поручения, направленные в Российскую Федерацию, на Украину, Республику Болгария, Румынию. Остальные международные поручения свыше одного года остаются не исполненными.

Поручения, направленные в Российскую Федерацию исполняются в течении четырех, пяти месяцев или больше в зависимости от исполнителя, качество исполнения также зависит от исполнителя.

К примеру, в ходе расследования уголовного дела в отношении преступной группы **О.** и **Д.** по результатам мониторинга установлены их логины в социальной сети «ВКонтакте». После чего, в уполномоченные органы Российской Федерации направлено международное поручение об оказании правовой помощи. Через свыше четырех месяцев уполномоченными органами Российской Федерации направлены изъятые в ООО «ВКонтакте» архивные данные логинов участников ОПГ в социальной сети «ВКонтакте», согласно которым полностью подтвердилась причастность указанных лиц к совершенным ими преступлениям.

Процессуальные документы *(постановления о выемки сведений, охраняемых законом тайну адресованные поставщикам интернет-услуг)*, выданные компетентными органами одного государства, не имеют обязательной

юридической силы для органов другого государства. Чтобы истребовать данные у поставщика интернет-услуг, который находится в другой юрисдикции, необходимо пройти установленную процедуру предоставления международной правовой помощи. Это занимает определенное время, и есть риск, что пока будет готовиться ответ, данные, которые находятся в распоряжении третьей стороны, уже будут недоступны: обычно поставщики коммуникационных услуг хранят данные о трафике не бессрочно, а ровно столько, сколько необходимо для выставления счетов абонентам.

При проведении онлайн-расследований данные о потоках информации могут оказаться единственной зацепкой, подтверждающей наличие связи между электронными сообщениями и конкретным физическим лицом. Если данные будут удалены раньше, чем следователь сможет их запросить, то возможность установить эту связь будет утрачена навсегда. К сожалению, прежде чем правоохранительные органы могут приступить к расследованию и уж, тем более установить, какие веб-ресурсы использовал злоумышленник *(который, вероятно, скрыл свои следы),* зачастую проходит слишком много времени. Использование традиционных дипломатических каналов международной правовой помощи точно также отнимает много времени и не всегда позволяет предоставить своевременный запрос соответствующему поставщику услуг.

Поэтому статья 16 Будапештской конвенции позволяет сторонам добиваться оперативного обеспечения сохранности компьютерных данных до получения разрешения суда. Статья 17, регулирующая вопросы потоков информации и процедуру оперативного обеспечения сохранности данных, позволяет компетентному органу «оперативно» раскрывать необходимые данные потоков информации, «чтобы Сторона могла идентифицировать поставщиков услуг и маршрут, по которому производилась передача сообщения». Одна Сторона Конвенции может направлять другой Стороне запросы об обеспечении сохранности данных трафика и содержимого через круглосуточный контакт-центр, созданный в соответствии со статьей 35 Будапештской конвенции.

В запросе об обеспечении сохранности данных рекомендуется ходатайствовать о подтверждении того, что данные были сохранены, а также о предоставлении соответствующего регистрационного номера.

Стороны Будапештской конвенции не обязаны направлять запросы исключительно через контакт-центры. На практике прямое сотрудничество между поставщиками интернет-услуг и правоохранительными органами может оказаться гораздо более выгодным и поможет сторонам лучше осознать взаимные потребности и ограничения.

Использование Интернета, социальных сетей и систем мгновенного обмена сообщениями (мессенджеров) постоянно развивается. Преступники хотят обеспечить сохранение своей анонимности и используют любую технологию, которая помогает этого достичь. Обязанности практикующих специалистов – всегда оставаться в курсе соответствующих изменений, реформ национального законодательства, а также процедур поставщиков услуг, чтобы иметь возможность получить необходимые им электронные доказательства. [1]

Террористы используют социальные сети, помимо прочего, для распространения пропаганды, сбора денежных средств, привлечения сторонников и обмена информацией. Такие электронные доказательства могут оказаться важными для определения того, где находится подозреваемый, с кем он связан и с кем он связывает связь. Результаты последнего исследования в Европейском союзе подтвердили, что:

- в рамках более половины расследований направляется запрос на получение трансграничного доступа к электронным доказательствам;
- электронные доказательства в любой форме имеют большое значение для приблизительно 85% от общего числа (уголовных) расследовании;
- почти в двух третях (65%) расследований, в рамках которых важно получить электронные доказательства, необходимо направить запрос Поставщикам Услуг, располагающимся в другой юрисдикции.

Существующая система Взаимной правовой помощи может быть сложной, а в некоторых Государствах – бюрократической, что за частую приводит к большим задержкам в получении электронных доказательств. Это никак не сочетается со стремительным характером киберпреступности и трансграничной преступности, для которых в Интернете нет границ.

Кроме того, облачные вычисления создают проблемы, связанные с определением юрисдикции, что подразумевает особое внимание к тому, куда направлять запросы на оказание Взаимной правовой помощи (Запрос об оказании взаимной правовой помощи) для исполнения. Недавние террористические атаки продемонстрировали необходимость в немедленной реакции на чрезвычайные происшествия, в обеспечении сохранности данных, а также в срочных запросах в отношении международного сотрудничества. Электронные доказательства быстро перемещаются через границы, а получение соответствующих сведений посредством Взаимной правовой помощи зачастую происходит медленно и предоставляет собой трудоемкую задачу, особенно если практикующий специалист не имеет опыта в осуществлении процедуры Взаимной правовой помощи. Учитывая, что число трансграничных преступлений растет, а электронные доказательства нередко располагаются за границей, «Практическое Руководство по порядку запроса электронных доказательств из других стран». Выпущенное ООН в январе 2019 года снабдит сотрудников правоохранительных органов и прокуратуры инструментами, которые помогут запрашивать эти важные доказательства. [1]

«Практическое Руководство по порядку запроса электронных доказательств из других стран». Выпущенное ООН в январе 2019 года прилагается к настоящей диссертационной работе в целях использования сотрудниками правоохранительных и специальных органов в поиске электронных доказательств, находящихся у заграничных Поставщиков услуг.

У Поставщиков услуг имеется большой объем служебной информации об абонентах, который может быть единственным доказательством причастности конкретного лица к совершению тех или иных действии в Глобальной сети Интернет. В этой связи, в настоящем диссертационном исследовании предлагается усилить и развить взаимоотношение между органами досудебного

расследования/прокурорского надзора и Поставщиками услуг с целью увеличения практики получения служебной информации об абонентах. В настоящем исследовании предлагается законодательно конкретизировать обязанности отечественных Поставщиков Услуг по предоставлению органам досудебного расследования и прокурорского надзора служебной информации об абонентах. Также, в указанном разделе для получения электронных доказательств у заграничных Провайдеров Услуг предлагается использовать «Практическое Руководство по порядку запроса электронных доказательств из других стран». Выпущенное ООН в январе 2019 года.

2.3. Практика информирования о киберпреступлениях уполномоченными организациями

Зачастую жертва интернет-мошенничества не знает, что злоумышленники получили доступ к ее данным, пока эти данные не начинают использоваться в реальной жизни. Более того, потерпевший может так никогда и не узнать, что его данные были скомпроментированы. Если он об этом не узнает, то не обратится в правоохранительные органы, которые, в свою очередь, не зарегистрируют уголовное дело, и преступление не появится в официальной статистике. *Считается, что показатели компьютерных преступлений очень занижены.*

Еще одним препятствием для правоохранительных органов является то, что общедоступное интернет-пространство, которое можно эффективно отслеживать, относительно небольшое. Как и в реальном мире, большинство коммуникаций в сети Интернет происходит между индивидами в конфиденциальном пространстве, которое считается частной собственностью. Не имея санкции суда, правоохранительные органы могут отслеживать лишь ту небольшую часть Интернета, который отображается в общедоступном пространстве.

Поскольку преступления, совершенные с помощью сети Интернет, практически незаметны, то правоохранительные органы намного больше зависят от сообщений третьих лиц о подозрительной деятельности в сети. Когда в распоряжение правоохранительных органов поступает достоверная, подтвержденная электронными доказательствами информация о компьютерных преступлениях, это помогает им стратегически взглянуть на явление киберпреступности, выявить новейшие тенденции и потенциальные угрозы в этой сфере и сконцентрироваться на тех методах работы злоумышленников, которые наносят наибольший ущерб общественным отношениям. Сообщения третьих лиц важны и для частных компаний, которые могут даже не догадываться о том, что в их сети произошел взлом и утечка данных. Например, при использовании бот- сетей многие пользователи даже не думают, что их устройства поражены вирусом и используются злоумышленниками, пока третье лицо, например, компания по IT-безопасности не передаст поставщику интернет-услуг список зараженных IP-адресов. *Понятие «бот-сеть» (botnet) образовано из слов «робот» (roBOT) и «сеть» (NETwork). Оно означает сеть, где все компьютеры заражены определенным вирусом, благодаря чему их можно использовать удаленно для осуществления противоправных действий через Интернет. Как правило, владельцы компьютеров об этом не догадываются.*

Как правило, жертвы компьютерных преступлений обращаются в правоохранительные органы только в том случае, если им был нанесен ущерб или они лично ощутили какие-то негативные последствия. В то же время, многие не хотят подавать заявление, потому что считают ущерб незначительным, не желают оказаться втянутыми в расследование, боятся судебной волокиты и/или не уверены, что правоохранительные органы смогут найти и наказать преступника.

Примером того, что, казалось бы, незначительное неудобство говорит о более масштабной противоправной деятельности, является спам. В мире не существует универсального запрета на рассылку спам-сообщений, но даже в тех юрисдикциях, где спам запрещен, пользователь, увидев такое сообщение, скорее всего, отправит его в папку для нежелательной почты и тут же о нем забудет. Пользователь не думает о том, что ежедневно рассылаются миллионы таких сообщений, которые используются для целей организованной преступности. Или же другой пример: когда на компьютер попадает вирус, то хакер получает доступ ко всем данным пользователя на этом устройстве, но потерпевший, очистив компьютер при помощи антивирусной программы, уже не видит необходимости обращаться в полицию. Но даже в этом случае потерпевший мог бы предоставить правоохранительным органам важную информацию, если бы существовал простой порядок ее подачи.

В 2002 году Федеральная торговая комиссия США обратилась к пользователям с просьбой пересылать любой полученный ими спам на электронный адрес spam@uce.gov, чтобы иметь возможность анализировать тенденции и повышать эффективность борьбы с нежелательными сообщениями.

Правоохранительные органы некоторых стран внедрили удобные процедуры для информирования об интернет-преступлениях, в частности:

- Федеральная полиция Бельгии: http://e-cops.be
- Французская национальная полиция: https://www.internet-signalement.gouv.fr/
- Французские неправительственные организации: http://www.signal-spam.fr/
- Великобритания: http://www.actionfraud.police.uk/
- Центр по работе с сообщениями об интернет-преступлениях ФБР США: http://www.ic3.gov/ [12]

Следует отметить, что такие центры не принимают экстренные вызовы.

Как уже говорилось, ущерб, нанесенный отдельно взятому лицу, может быть незначительным, и эти дробные суммы не отображают ни общую прибыль, полученную злоумышленниками, ни ущерб, нанесенный обществу в целом. Если объединить нескольких случаев в одно дело, то это оправдает и ресурсы, и время, потраченные на их расследование, чего не скажешь об отдельно взятом случае. Кроме того, при получении запросов на предоставление международной правовой помощи некоторые страны требуют, чтобы обращение удовлетворяло минимальные критерии приемлемости, а это значительно легче обеспечить, если расследовать несколько малозначимых случаев в совокупности.

При сборе и обработке сообщений о компьютерных преступлениях не стоит забывать о международном сотрудничестве, поскольку злоумышленники, как правило, не ограничиваются одной юрисдикцией и могут выбрать жертву в любой стране мира. В Европе существует база расследований Европол, доступ к которой имеют правоохранительные органы Европейского Союза. Организация Inhope Foundation *(www.inhope.org)* ведет глобальную базу

адресов веб-ресурсов, на которых размещена детская порнография, и сотрудничает с горячими линиями для выявления материалов, которые могут использоваться правоохранительными органами как доказательства при обращении к владельцам ресурсов с требованием удалить содержимое и для проведения дальнейшего расследования. Правоохранительные органы любой страны мира могут обратиться в Интерпол *(www.interpol.int)*. Штаб-квартира организации Интерпол в Лионе ведет базу данных материалов с изображением сексуального насилия над детьми, и эти материалы могут использоваться в качестве доказательств. Связь с Интерполом осуществляется через национальные бюро соответствующей юрисдикции. [12]

Существуют контакт-центры в форме государственно-частного партнерства. Хорошим примером такого партнерства является французская ассоциация Signal Spam *(www.signal- spam.fr),* которая собирает и обрабатывает сообщения граждан о рассылке спама, после чего передает данные не только правоохранительным органам, но и поставщикам почтовых услуг. Благодаря этому поставщики могут заблокировать пользователей, которые злоупотребляют их услугами. [12]

В ходе мониторинга сети ее операторы могут обнаружить сетевые атаки. Поставщики почтовых услуг могут заметить необычно большое количество писем, отправленных или полученных определенным пользователем. Проанализировав новый вирус, производитель антивирусного программного обеспечения может идентифицировать сервер и поставщиков хостинговых услуг, которые использовались для управления бот-сетью. Все они являются свидетелями компьютерных преступлений, но могут не знать, куда можно сообщить о выявленных правонарушениях.

Для приема свидетельских сообщений можно использовать специализированный контакт- центр *(его можно объединить с контакт-центром для пострадавших, о котором говорилось в разделе)*. Такой центр должен быть централизованным и доступным, и общественность должна знать о его существовании.

В США для сообщения информации о взломанных кредитных картах был создан Центр информирования об интернет-мошенничестве *(http://www.ifraudalert.org)*. Этот центр является совместным проектом правоохранительных органов и частного сектора, представленного поставщиками интернет-услуг и компаниями-эмитентами кредитных карт. Центр сравнивает номера кредитных карт, которые оказались в публичном доступе, с номерами карт, которые уже заблокированы финансовыми учреждениями, чтобы выявить случаи мошенничества и определить необходимость новых блокировок. [12]

Еще одним примером источника электронных доказательств и свидетельской информации является веб-сайт *malwareurl.com,* куда свидетели могут сообщать о веб-страницах с вредоносной активностью.

Контакт-центр может быть, как общедоступным, так и с ограниченным доступом *(например, веб-сайт ops-trust.net)*. Государственные и частные контакт-центры могут предоставить правоохранительным органам большие

объемы данных, которые помогут им если не на оперативном, то на стратегическом уровне. [12]

Наконец, обратите внимание, что в определенных случаях контакт-центры должны поощрять пользователей, чтобы те оставляли сообщения, но отговаривать их от проведения собственных расследований или активного поиска противозаконных материалов. Например, в случае с материалами с изображением сексуального насилия над детьми, сам поиск таких материалов может быть квалифицирован как правонарушение.

В Республике Казахстан АО «Государственная техническая служба» является центром информационной безопасности, указанные функции регламентированы Законом Республики Казахстан «Об Информатизации». Заказчиком услуг АО «Государственная техническая служба» является Комитет национальной безопасности, в этой связи ГТС занимается исполнением целями и задачами, определенными Комитетом национальной безопасности Республики Казахстан.

Согласно подпункта 15 пункта 1 статьи 14 Закона Республики Казахстан «Об информатизации» Государственная техническая служба в сфере информатизации, отнесенные к государственной монополии реализует задачи и функции Национального координационного центра информационной безопасности.

Согласно статьи 7-4 Закона Республики Казахстан «Об информатизации» Национальный координационный центр информационной безопасности:

1. Содействует собственникам, владельцам и пользователям объектов информатизации в вопросах безопасного использования информационно-коммуникационных технологий;
2. Обеспечивает взаимодействие оперативных и отраслевого центров информационной безопасности финансового рынка и финансовых организаций;
3. Осуществляет сбор, анализ и обобщение информации оперативных центров информационной безопасности об инцидентах информационной безопасности на объектах информационно-коммуникационной инфраструктуры "электронного правительства" и других критически важных объектах информационно-коммуникационной инфраструктуры;
4. Обеспечивает функционирование объектов информационно-коммуникационной инфраструктуры Национального координационного центра информационной безопасности;
5. Осуществляет межотраслевую координацию по вопросам мониторинга обеспечения информационной безопасности, защиты и безопасного функционирования объектов информатизации "электронного правительства", казахстанского сегмента Интернета, а также критически важных объектов информационно-коммуникационной инфраструктуры, реагирования на инциденты информационной безопасности с проведением совместных мероприятий по обеспечению информационной безопасности в порядке, определяемом законодательством Республики Казахстан;

6. Осуществляет мониторинг обеспечения информационной безопасности объектов информатизации "электронного правительства" посредством системы мониторинга обеспечения информационной безопасности Национального координационного центра информационной безопасности;

7. Осуществляет мониторинг событий информационной безопасности объектов информатизации государственных органов;

8. Обеспечивает функционирование единой национальной резервной платформы хранения электронных информационных ресурсов, устанавливает периодичность резервного копирования электронных информационных ресурсов критически важных объектов информационно-коммуникационной инфраструктуры в порядке, определяемом уполномоченным органом в сфере обеспечения информационной безопасности;

9. Осуществляет организационное и техническое сопровождение системы мониторинга обеспечения информационной безопасности Национального координационного центра информационной безопасности;

10. Осуществляет мероприятия по выявлению, пресечению и исследованию угроз и инцидентов информационной безопасности на объектах информатизации "электронного правительства" и формирует рекомендации по их устранению или предотвращению;

11. Осуществляет координацию мероприятий по обеспечению информационной безопасности объектов информатизации "электронного правительства" и критически важных объектов информационно-коммуникационной инфраструктуры, а также реагированию на инциденты информационной безопасности.

В большинстве случаев Национальные службы реагирования на компьютерные инциденты (далее - CERT) участвуют только в сборе и анализе информации об инцидентах информационной безопасности, а также их устранении. Расследование киберпреступлений во многих государствах, в основном, относится к зоне ответственности специальных уполномоченных органов или специальных подразделений по борьбе с киберпреступностью.

Силами CERT проводятся мероприятия в части обнаружения, анализа и устранения компьютерных инцидентов. При выявлении факта киберпреступления направляется запрос в специальные подразделения по борьбе с киберпреступностью, где осуществляется анализ полученной информации в части нарушения законодательства государства. При подтверждении состава преступления заводится дело. Специальные подразделения по борьбе с киберпреступностью организуют сбор доказательств, поиск злоумышленников, а также их задержание.

Мировым сообществом выработаны и применяются эффективные механизмы противодействия киберпреступности. Так, между странами-участницами Европейского Союза действует упрощенный механизм получения сведений на их территории - Европейская конвенция о компьютерных преступлениях (о киберпреступности), подписанная 23 ноября 2001 г. в Будапеште (далее – Конвенция). На территории стран Центральной Азии международные поручения подлежат выполнению посредством Минской и

Кишиневской конвенций. В Конвенции отмечена необходимость решения вышеперечисленных проблем противодействия киберпреступности и выделены следующие основные три рекомендации:

1) вопросы уголовно-правовой характеристики преступлений в сфере компьютерной информации (криминализации).

2) уголовно-процессуальные аспекты борьбы с преступностью, направленные на собирание доказательств при расследовании компьютерных преступлений.

3) вопросы международного сотрудничества: оказание правовой помощи, экстрадиция, наложение ареста и конфискация имущества и т.д.

Региональная Европейская Конвенция стала одной из наиболее масштабных международных актов, решающих многие проблемы международного сотрудничества. Помимо присоединившихся стран Европы, Конвенцию ратифицировали США, Япония, ЮАР, Грузия, Канада и др.

Однако Казахстан, как и Российская Федерация, не ратифицировал Конвенцию до настоящего времени. Основной темой для дискуссии и несогласия явилось требование статьи 32 Конвенции, которая предусматривает право любой из Сторон без согласия другой Стороны посредством компьютерной системы на своей территории получать доступ к компьютерным данным, расположенным на территории другой Стороны.

Еще одной проблемой является низкий уровень компьютерной грамотности населения, юридических лиц. Хакеры обманным путем, используя отсутствие знаний по обеспечению элементарной информационной безопасности, получают доступ к личной, коммерческой информации физических и юридических лиц, что становится инструментом вымогательства денежных средств.

Государственными органами на недостаточном уровне проводится профилактическая работа по предупреждению преступлений в сфере информатизации и связи, не освещаются наиболее распространенные способы взлома средств безопасности компьютеров, смарт-телефонов и т.д., не пропагандируются элементарные способы обеспечения информационной безопасности.

В этой связи согласно Указу Президента Республики Казахстан от 15 февраля 2018 года № 636 «Об утверждении Стратегического плана развития Республики Казахстан до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан», выдвинута инициатива 2.11, которая предусматривает повышение осведомленности граждан по вопросам информационной безопасности, а также внедрение обучения основам безопасного использования информационно-коммуникационных технологий в школах.

Изучив мировой опыт и деятельность АО «Государственная техническая служба», занимающееся регистрацией инцидентов информационной безопасности, возникает предложение не ограничиваться лишь регистрацией инцидентов информационной безопасности, но и проведение АО «Государственной технической службой» исследовании, анализа всех

зарегистрированных инцидентов информационной безопасности и передачи всех сведений в специализированные и правоохранительные органы для дальнейшего исследования в плоскости уголовного права.

Если мы не начнем глубже изучать инциденты информационной безопасности, на первый взгляд являющиеся простыми, безобидными и не повлекшими какие-либо последствия, то мы не сможем изучать иные инциденты информационной безопасности повлекшие значительный ущерб в плоть до промышленного шпионажа и террористических атак. В этой связи необходимо укреплять функции Национального координационного центра информационной безопасности.

В качестве результата диссертационного исследования предлагаю добавить в редакцию Закона «Об Информатизации» изменение.

Добавить пункт 12 в статью 7-4 Закона Республики Казахстан «Об Информатизации» от 24.11.2015 года №418-V и изложить в следующей редакции: «Осуществлять исследование, анализ инцидентов информационной безопасности с последующим предоставлением компетентным специальным и правоохранительным органам Республики Казахстан развернутую информацию об источниках, функциях, целях, задач, назначениях инцидентов информационной безопасности для проведения соответствующего расследования по каждому выявленному факту».

В реальном времени киберпреступления соприкасаются со всеми видами преступлении начиная от хищении денежных средств, заканчивая незаконным оборотом наркотических средств, финансированием терроризма, промышленным шпионажом, распространением детской порнографии и д.р.

Согласно положению «о Центральноазиатском региональном информационном координационном центре по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» целями и задачами Центра являются: 1. Координация на региональном уровне усилий государств-участников по борьбе с незаконным оборотом наркотиков; 2. Создание механизмов взаимодействия компетентных органов государств-участников; 3. Содействие укреплению сотрудничества между компетентными органами государств-участников в борьбе с трансграничной организованной преступностью, связанной с незаконным оборотом наркотиков; 4. Содействие в организации и проведении согласованных совместных операций и оперативно-розыскных мероприятий, в том числе контролируемых поставок; 5. Сбор, хранение, анализ и организация обмена оперативно-розыскной и справочной информацией в области борьбы с незаконным оборотом наркотиков; 5. Содействие в реализации мер по унификации информационных систем, в том числе баз данных компетентных органов Сторон; 6. Разработка процедур по системному накоплению информации, формирование и пополнение банка данных Центра; 7. Введение стандартизированных форм и систем обмена информацией; 8. Внедрение новейших программ анализа оперативной информации; Анализ наркоситуации и выработка соответствующих рекомендаций; 9.Оказание помощи компетентным органам Сторон, а также других государств, территория которых используется для

незаконного производства и транспортировки наркотиков, в реализации антинаркотических программ по их просьбе; 10. Оказание содействия в гармонизации нормативной правовой базы государств-участников в сфере контроля за оборотом наркотиков; 11. Проведение конференций, тренингов, семинаров по вопросам совершенствования методов борьбы с незаконным оборотом наркотиков и укрепления международного сотрудничества в этой сфере.

В целях повышения практики взаимоотношения при расследовании транснациональных киберпреступлений со странами ближнего зарубежья предлагается внести изменения в Положение «о Центральноазиатском региональном информационном координационном центре по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» являющимся неотъемлемой частью Закона Республики Казахстан «О ратификации Соглашения между Азербайджанской Республикой, Республикой Казахстан, Кыргызской Республикой, Российской Федерацией, Республикой Таджикистан, Туркменистаном и Республикой Узбекистан о создании Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» от 06 ноября 2008 года N 78-IV и дополнить в статье 1 понятия «1. Координация на региональном уровне усилий государств-участников по борьбе с незаконным оборотом наркотиков **и с киберпреступностью**; 2. Создание механизмов взаимодействия компетентных органов государств-участников; 3. Содействие укреплению сотрудничества между компетентными органами государств-участников в борьбе с трансграничной организованной преступностью, связанной с незаконным оборотом наркотиков **и с киберпреступностью**; 4. Содействие в организации и проведении согласованных совместных операций и оперативно-розыскных мероприятий, в том числе контролируемых поставок **и киберперступлений**; 5. Сбор, хранение, анализ и организация обмена оперативно-розыскной и справочной информацией в области борьбы с незаконным оборотом наркотиков **и с киберпреступностью**; 5. Содействие в реализации мер по унификации информационных систем, в том числе баз данных компетентных органов Сторон; 6. Разработка процедур по системному накоплению информации, формирование и пополнение банка данных Центра; 7. Введение стандартизированных форм и систем обмена информацией; 8. Внедрение новейших программ анализа оперативной информации; Анализ нарко **и кибер** ситуации и выработка соответствующих рекомендаций; 9.Оказание помощи компетентным органам Сторон, а также других государств, территория которых используется для незаконного производства и транспортировки наркотиков **и совершения киберпреступлений**, в реализации антинаркотических и **антихакерских** программ по их просьбе; 10. Оказание содействия в гармонизации нормативной правовой базы государств-участников в сфере контроля за оборотом наркотиков и **киберпреступлений;** 11. Проведение конференций, тренингов, семинаров по вопросам совершенствования методов борьбы с незаконным оборотом наркотиков,

киберпреступлениями и укрепления международного сотрудничества в этой сфере.», в части расширения функции ЦАРИКЦ на содействие в организации, проведении и координации, согласованных совместных международных операций по киберперстеплениям.[38]

Учитывая опыт Европейского Союза об информировании о киберпреступлениях предлагаю увеличить потенциал существующего АО «Государственная техническая служба» и обязать осуществлять исследование, анализ инцидентов информационной безопасности с последующим предоставлением компетентным органам развернутую информацию об источниках, функциях, целях, задач, назначениях инцидентов информационной безопасности для проведения соответствующего расследования по каждому выявленному факту. Указанный функционал АО «Государственной технической службы» несомненно улучшит потенциал пресечения и расследования киберперступлении в Республике Казахстан. В этой связи предлагается добавить пункт 12 в статью 7-4 Закона Республики Казахстан «Об Информатизации» от 24.11.2015 года №418-V акцентирования работы в указанном направлении Национальный координационный центр информационной безопасности.

Учитывая функционал Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров созданного в рамках Соглашения о создании ЦАРИКЦ предлагаю изменить цели и задачи указанной организации. Определить целями и задачами ЦАРИКЦ: 1). Содействие в организации, проведении и координации, согласованных совместных международных операций по киберперстеплениям; 2). Сбор, хранение, защита, анализ и обмен информацией по трансграничной киберпреступности.

2.4 Особенности составления процессуальных документов при обнаружении преступлений, совершенных с использованием электронных носителей информации

После получения информации о совершенном преступлении правоохранительным органам необходимо провести одно из основных следственных действий, а именно осмотр места происшествия. Осмотр местности, помещений, предметов, документов, живых лиц, трупов, животных производится, лицом, осуществляющим досудебное расследование, с целью обнаружения и выявления следов уголовного правонарушения и иных материальных объектов, выяснения обстановки происшествия и установления обстоятельств, имеющих значение для дела. [17]

Сотрудники органа уголовного преследования обязаны вынести постановление о привлечении специалиста, обладающего специальными знаниями и опытом работы в области информационных технологий для процедуры обнаружения и изъятия электронных носителей информации. В постановлении разъясняются права и обязанности специалиста.

В качестве специалиста для участия в производстве по уголовному делу привлекается не заинтересованное в деле лицо, обладающее специальными знаниями, необходимыми для оказания содействия в собирании, исследовании и оценке доказательств путем разъяснения участникам уголовного процесса вопросов, входящих в его специальную компетенцию, а также применения научно-технических средств. [17]

Если у органа уголовного преследования отсутствует возможность привлечь специалиста, то необходимо привлечь сотрудника, обладающего необходимыми знаниями для выявления и сбора электронных носителей информации.

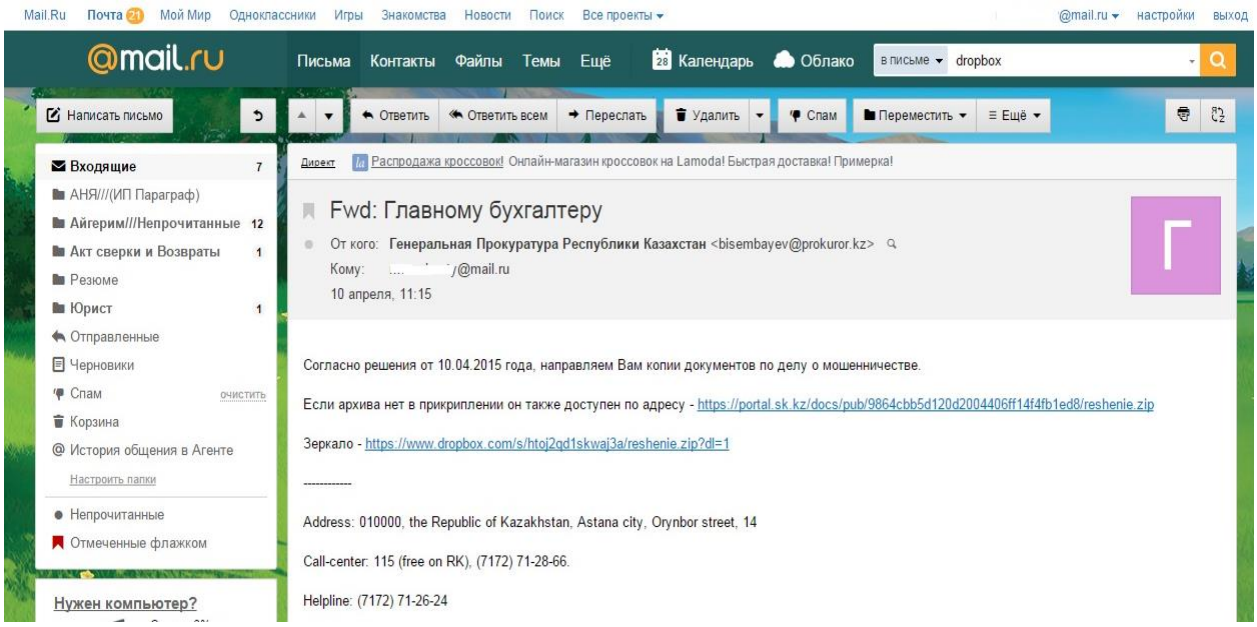
При совершении киберпреступлений необходимо изъять и осмотреть электронные устройство потерпевшего *(компьютеры, периферийные устройства, компьютерные сети, мобильные телефоны и другие портативные устройства для хранения информации, а также сети Интернет).* В этой связи необходимо вынести постановление о производстве выемки электронного устройства потерпевшего, так как они содержат сведения, имеющие значение для дела.

Органом уголовного преследования составляется протокол производства выемки на основании соответствующего постановления. В протоколе указываются обстоятельства и описывается весь ход производства выемки. В качестве примера ниже указан детальный порядок производства выемки.

«В последующем производился осмотр изъятого у потерпевших системного блока. В ходе осмотра установлено, что в истории скаченных файлов браузера Google Chrome обнаружена информация о том, что 27.03.2015г. скачен по ссылке document_po_delu.zip. В папке «пользователя» обнаружено вредоносное программное обеспечение, обеспечивающее удаленное управление данным компьютером и имеющее возможность перехвата данных с клавиатуры, а также журналы записи данных ввода с клавиатуры вредоносного ПО за период с 27.03.2015г. – 01.04.2015г. Установлено, что один

из процессов тестового компьютера осуществляет непрерывный обмен данными с сервером, имеющим IP адрес 178.32.144.104.

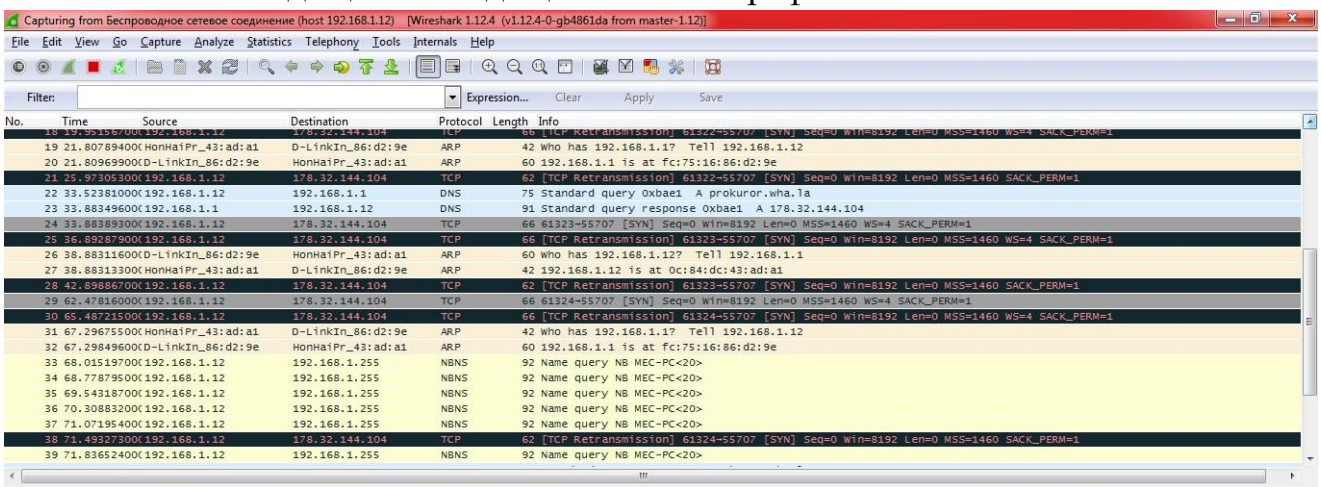
В почтовом ящике пользователя ***Firma_M...@mail.ru*** *обнаружены письма, содержащие ссылку на файл вредоносным ПО, который при запуске устанавливает вышеуказанное вредоносное ПО. Указаны фиктивные адреса отправителей через сервер host-2.ahost.org.ua, который позволяет указывать в качестве адреса отправителя любой произвольный адрес.»*



Скриншот электронного письма с вредоносным ПО.

С помощью вредоносной программы используя компьютер жертвы и через Интернет-Банкинг БТА-Online в *(логин пароль найден с помощью вредоносной программы)* выполнен перевод денежных средств на заранее подготовленные банковские карты.

В последующем органом уголовного преследования производился дополнительный осмотр обнаруженного у потерпевшего ТОО «Фирма М…» в системном блоке вредоносного ПО. При осмотре извлеченное вредоносное ПО размещено на тестовые компьютеры, где предварительно установлено специализированное программное обеспечение WireShark, позволяющее отслеживать исходящий и входящий сетевой трафик.



Таким образом установлено, что само заражение компьютера производится путем установки соединения с вспомогательным сервером и скачиванием, с последующей установкой, специализированного ПО, позволяющего добывать конфиденциальную информацию *(отслеживать пароли, запускаемые программы, посещаемые страницы в интернете)*. Кроме того, установленное вредоносное ПО позволяет производить удаленное управление компьютером *(выполнять набор на клавиатуре, перемещать мышь, видеть содержание рабочего стола и т.д.)*.

В данном случае для заражения использовался файл ***dokumenty_po_delu.zip*** *и для управления используется вспомогательный сервер, размещенный по динамическому адресу* ***prokuror.wha.la,*** *который на момент осмотра присвоен IP-адрес* ***178.32.144.104****. Использование динамической адресации позволяет размещать физические сервера в любом удобном месте, с последующим указанием фактического размещения при помощи сервиса dyndns или no-ip.*

Дальнейший анализ приложения **dokument.exe**, позволяет утверждать, что обнаружена клиентская часть системы Nanocore RAT.

Система Nanocore RAT позиционируется продавцами данного ПО как система удаленного администрирования. Но большинством антивирусных систем распознается как вредоносное программное обеспечение.

Система Nanocore RAT состоит из двух частей: серверной и клиентской. Серверная часть системы представляет собой программный модуль, устанавливаемый на управляющем компьютере. Серверная часть позволяет выполнять и настраивать сборки клиентских модулей, подключать различные функции и задавать варианты скрытого запуска в заражаемой системе. При подключении к серверу через сеть Интернет, созданного таким образом клиентского модуля, серверная часть программы позволяет получить полное управление над подключенным удаленным компьютером.

Клиентская часть системы предназначена для установки на заражаемом *(удаленном)* компьютере и имеет набор специальных функций для получения контроля над этим компьютером в частности:

- Передача содержимого экрана на серверный компьютер;
- Доступ к дискам, файлам, папкам;
- Передача сохраненных паролей для доступа к различным интернет ресурсам;
- Просмотр и передача вводимых с клавиатуры данных;
- Получение команд с серверной части и имитация перемещения и нажатия клавиш манипулятора «мышь» и клавиатуры;
- Блокировка работы экрана;
- Включение и передача данных от ВЕБ камеры *(при ее наличии)*.

Для скрытой установки клиентской части Nanacore RAT, данный модуль был модифицирован *(перепакован)*. В результате переупаковки, модуль стал трудно заметен антивирусным программам и мог достаточно долго выполнять

свои функции, оставаясь незамеченным пользователями зараженного компьютера.

После обнаружения IP-адреса злоумышленников, через которые проводились рассылка вредоносного программного обеспечения, принимаются меры по установлению местонахождения IP-адреса и лиц, администрировавших указанным сервером.

Как описывалось ранее, по средствам Интернет необходимо получить максимальную информацию по IP-адресам Соответственно после установления страны нахождения IP-адреса сервера администратора, распространяющего вредоносное программное обеспечение направляется запрос об оказании международной правовой помощи в указанную страну.

В целях установления злоумышленников на территории Республики Казахстан, всем провайдерам связи направляются постановления о выемки сведений о соединениях с сервером IP-адреса **178.32.144.104** по портам **3389** *(по умолчанию TCP 3389 используется для обеспечения удалённой работы пользователя с сервером)***.**

Если в ходе досудебного расследования провайдерами связи будет представлена информация о соединениях с интересующим следствие сервером, то сотрудникам необходимо направить постановление о производстве выемки сведений о детализациях IP соединении установленных абонентских номеров за интересующее следствие время.

В целях раскрытия вышеуказанных преступлений необходимо провести следующие следственно-оперативные действия:

1). Изъять с банков второго уровня сведения, интересующие следствие, по расчетным счетам, на которые незаконно перечислены похищенные денежные средства;

2). При наличии сведений о перечислении похищенных денежных средств на электронный кошелек в платежной системе WOOPPAY, необходимо изъять в ТОО «WOOPPAY» сведения по интересующему следствие логину;

3). При наличии сведений о перечислении похищенных денежных средств на электронный кошелек в платежной системе ТОО «OLIMP KZ», необходимо изъять в ТОО «OLIMP KZ» сведения по интересующее следствие логину;

4). При изучении информации, полученных в ТОО «WOOPPAY» и ТОО «OLIMP KZ» необходимо запросить у провайдеров связи полные данные владельцев, контакты и месторасположение интересующих следствие IP-адресов, посещавших сайты www.Olimp.kz, www. WOOPPAY.com;

5). При изучении информации, полученных в ТОО «WOOPPAY» и ТОО «OLIMP KZ» и обнаружения взаимоотношении с ТОО «QIWI Kazakhstan» необходимо произвести выемку сведений у эмитента системы электронных денег ТОО «QIWI Kazakhstan» - АО ДБ «Альфа-Банк» по интересующим следствие логину;

3. – ЗАКЛЮЧЕНИЕ

В работе на основе исследования и анализа нормативного, теоретического материала освещены проблемы законодательной регламентации и практической реализации организационно-процессуальных особенностей расследования и доказывания транснациональных киберпреступлений, сформированы конкретные выводы и предложения.

1. Анализ практики реализации норм о фактических данных, а также теоретическое и правовое исследование позволили диссертанту разработать рекомендации по совершенствованию законодательной регламентации применениями понятия «электронное доказательство» в уголовно-процессуальном праве Республики Казахстан. Предлагается внести изменения в понятие фактических данных и законодательно закрепить определение «электронных доказательств». В частности, предлагается внести изменения в Уголовно-процессуальный кодекс Республики Казахстан от 04.07.2014 года №231-V ЗРК в редакции предложенной в подпункте 1.3. «Проблемы определения понятия электронных доказательств» настоящего диссертационного исследования;

2. Для удостоверения целостности и неизменности данных электронных носителей информации с момента изъятия рекомендуется на примере Соединенных Штатов Америки определить «стандарт безопасного хеширования», который может использоваться для определения были ли сообщения изменены с момента создания дайджестов.

3. Анализ практики реализации норм о деятельности операторов связи, а также теоретическое, правовое и практическое исследование позволили диссертанту разработать рекомендации по совершенствованию законодательной регламентации расширения обязанностей операторов связи по предоставлению органам уголовного преследования и прокурорского надзора служебной информации об абонентах. В частности, предлагается внести изменения в Закон РК «О связи» №567 от 05.07.2004 года, Постановление Правительства «Об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» №246 от 30 марта 2010 года, Постановление Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» №358 от 19.06.2018 года в редакции предложенной в подпункте 2.2. «Особенности сбора данных, находящихся в распоряжении третьих лиц, в том числе расположенных за границей» настоящего диссертационного исследования;

4. Для получения электронных доказательств у заграничных Провайдеров Услуг органам уголовного преследования, прокурорам и судам

предлагается использовать в работе «Практическое Руководство по порядку запроса электронных доказательств из других стран». Выпущенное ООН в январе 2019 года *(прилагается к диссертации)*.

5. В целях повышения практики исследования инцидентов информационной безопасности органами уголовного преследования в уголовном праве диссертантом предлагается внести изменения в Закон «Об информатизации» в части расширения функции Национального координационного центра информационной безопасности направленных на исследование всех зарегистрированных инцидентов информационной безопасности и передачи сведений в специализированные и правоохранительные органы для дальнейшего исследования в плоскости уголовного права. В частности, предлагается добавить пункт 12 в статью 7-4 Закона Республики Казахстан «Об Информатизации» от 24.11.2015 года №418-V в редакции предложенной в подпункте 2.3. «Практика информирования о киберпреступлениях уполномоченными организациями» настоящего диссертационного исследования;

5. Анализ практики работы Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров созданного в рамках Соглашения о создании ЦАРИКЦ, а также теоритическое и правовое исследование позволило диссертанту разработать рекомендации по внесению изменении в Положение «о Центральноазиатском региональном информационном координационном центре по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» являющимся неотъемлемой частью Закона Республики Казахстан «О ратификации Соглашения между Азербайджанской Республикой, Республикой Казахстан, Кыргызской Республикой, Российской Федерацией, Республикой Таджикистан, Туркменистаном и Республикой Узбекистан о создании Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» от 06 ноября 2008 года N 78-IV в целях развития международного опыта на содействие в организации, проведении и координации, согласованных совместных международных операций по раскрытию и расследованию киберперстеплений;

1. В рамках настоящего диссертационного исследования диссертантом разработан авторский примерный образец процессуальных документов при досудебном расследовании преступлений совершенных с использованием электронных носителей информации.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Руководство Организации Объединенных Наций «Практическое руководство по порядку запроса электронных доказательств из других стран (для использования только правоохранительными и судебными органами)» - www.drive.google.com;

2. Отчет Group-IB “HI-TECHCRIMETRENDS 2019/2020” - www.group-ib.com;

3. Уголовный кодекс Республики Казахстан от 3 июля 2014 года № 226-V *(с изменениями и дополнениями по состоянию на 06.10.2020 г.)* - www.adilet.kz;

4. Номоконов В.А. Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. - 2012. - № 1 (24). - С. 45-55.

5. Доклад Управления Организации Объединённых Наций по Наркотикам и Преступности «Всестороннее исследование проблемы киберпреступности» - www.drive.google.com;

6. Уголовно-процессуальный кодекс Республики Казахстан от 4 июля 2014 года № 231-V *(с изменениями и дополнениями по состоянию на 16.11.2020 г.)* - www.adilet.kz;

7. Ответ ГУ «Управление комитета по правовой статистике и специальным учетам Генеральной Прокуратуры РК по г.Алматы» за исх.№2-21603-20-00146 от 10.01.2020г. – 50 с.

8. Ответ зарегистрированные инциденты информационной безопасности Службой реагирования на компьютерные инциденты KZ-CERTc 2015 по 2019 год за исх.№36/08-1/01-1-2057 от 11.10.2019 г. – 2 с.

9. Марочкин Н.А. Алгоритмизация -эффективный метод оптимизации расследования преступлений // Известия Алтайского государственного университета. - №2. - 2001. - С. 45-49.

10. Приговор районного суда №2 Бостандыкского района города Алматы от 24.01.2017г. (7550-16-00-1/362).

11. Россинская Е.Р. Современные способы компьютерных преступлений и закономерности их реализации // Lex Russica. 2019. № 3. С. 87-99.

12. «Руководство по работе с электронными доказательствами» Базовое руководство для сотрудников полиции, прокуратуры и судов для служебного пользования Версия 2.0» - www.drive.google.com;

13. Отчет Group-IB «HI-TECH CRIME TRENDS 2020/2021» - www.group-ib.com;

14. Закон Республики Казахстан от 1 января 2003 года N370 «Об электронном документе и электронной цифровой подписи» - www.adilet.kz;

15. Постановление Правительства РК от 12 декабря 2017 года №827 «Об утверждении Государственной программы «Цифровой Казахстан» - www.adilet.kz;

16. Указ Президента Республики Казахстан от 15 февраля 2018 года №636 «Об утверждении Стратегического плана развития Республики Казахстан

до 2025 года и признании утратившими силу некоторых указов Президента Республики Казахстан» - www.adilet.kz;

17. Уголовно-процессуальный кодекс Республики Казахстан от 04 июля 2014 года №231-V ЗРК - www.adilet.kz;

18. Закон Республики Казахстан «О ратификации Соглашения между Правительством Республики Казахстан и Организацией Объединенных Наций о целевом фонде технического сотрудничества» от 15 октября 2014 года № 242-V ЗРК - www.adilet.kz;

19. Послание Президента Республики Казахстан от 05 октября 2018 года «Рост благосостояния Казахстанцев: повышение доходов и качества жизни» www.adilet.kz;

20. Указ Президента Республики Казахстан от 9 февраля 2018 года №633 «О мерах по реализации Послания Главы государства народу Казахстана от 10 января 2018 года «Новые возможности развития в условиях четвертой промышленной революции» - www.adilet.kz;

21. Постановление Правительства Республики Казахстан от 30 июня 2017 года №407 «Об утверждении Концепции кибербезопасности («Киберщит Казахстан»)» - www.adilet.kz;

22. Лоскутов И.Ю. Преступления в сфере информационных технологий в проекте новой редакции Уголовного кодекса Республики Казахстан// Международно-практическая конференция «Актуальные вопросы развития уголовного законодательства в рамках разработки нового уголовного кодекса РК» (Алматы, 20 сентября 2012 года).

23. Евдокимов К. Н. Актуальные вопросы уголовно-правовой квалификации преступлений в сфере компьютерной информации//Российский следователь. – 2015-№10.

24. Окоменко Р. И. «Электронные доказательства» и проблемы обеспечения прав граждан на защиту тайны личной жизни в уголовном процессе: сравнительный анализ законодательства Соединенных Штатов Америки и Российской Федерации : дис. ... канд. юрид. наук. М., 2016.

25. Основы теории электронных доказательств : монография / под ред. д-ра юрид. наук С. В. Зуева. М. : Юрлитинформ, 2019. С. 253, 254;

26. Пастухов П. С. О развитии уголовно-процессуального доказывания с использованием электронных доказательств // СПС «КонсультантПлюс»;

27. ВикипедиЯ – https://ru.m.wikipedia.org;

28. Уголовное дело №167500031001620 в отношении участников транснациональной киберпреступной группы «Карбанак/Кобальт»;

29. Постановление Правительства Республики Казахстан от 29 января 2016 года №39 «О создании некоммерческого акционерного общества «Государственная корпорация «Правительство для граждан» - www.adilet.kz;

30. Закон Республики Казахстан «О связи» от 05 июля 2004 года №567. - www.adilet.kz;

31. Закон Республики Казахстан «О прокуратуре» от 30.06.2017 года №81-VI - www.adilet.kz;

32. Постановление Правительства «Об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года - www.adilet.kz;

33. Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358 - www.adilet.kz;

34. Закон Республики Казахстан «Об оперативно-розыскной деятельности» от 15 сентября 1994 года №154-XIII - www.adilet.kz;

35. Ответ Комитета национальной безопасности за исх. №5/1/7473 от 23.02.2021 г. – 5 с.;

36. Ответ Республиканского государственного учреждения «Комитет телекоммуникаций» Министерство цифрового развития, инновации и аэрокосмической промышленности Республики Казахстан за исх. №28-1-1-28/324 от 24.02.2021г. – 2 с.;

37. Ответ зарегистрированные инциденты информационной безопасности Службой реагирования на компьютерные инциденты KZ-CERT за 2020 год за исх.№36/9/262 от 05.02.2021 г. – 2 с.

38. Закон Республики Казахстан «О ратификации Соглашения между Азербайджанской Республикой, Республикой Казахстан, Кыргызской Республикой, Российской Федерацией, Республикой Таджикистан, Туркменистаном и Республикой Узбекистан о создании Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» от 06 ноября 2008 года N 78-IV - www.adilet.kz;

39. Сборник словарей Ефремовой, Ожегова, Шведовой – http://*что-означает.рф/*;

40. «Стандарты безопасного хеширования» (SHS) (FIPS PUB 180-4) разработанный Департаментом Коммерции США – http://dx.doi.org/10/6028/NIST.FIPS.180-4.

ПРИЛОЖЕНИЕ А

«УТВЕРЖДАЮ»
Заместитель начальника
Департамента полиции г.Алматы
подполковник полиции
Р.Абдрахменов
«26» 2021 г.

АКТ

внедрения результатов диссертационного исследования магистранта Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан Күнғожинова Қ.Ә. в практическую деятельность

Комиссия в составе:
Председатель – и.о. начальника Следственного Управления ДП г.Алматы майор полиции Сейсенұлы М.

Члены комиссии:
Начальник Управления дознания ДП г.Алматы майор полиции Шарипов О.М.

Начальник отдела расследования преступлений против собственности Следственного Управления ДП г.Алматы подполковник полиции КасымбаевК.Б.

Начальник отдела расследования преступлений против личности Следственного Управления ДП г.Алматы подполковник полиции Ержанова Т.А.

Начальник отдела расследования преступлений против общественной безопасности и общественного порядка майор полиции Салаев А.Б.

Составили настоящий акт о том, что выводы и предложения магистранта Академии правоохранительных органов при Генеральной прокуратуре Республики Казахстан Күнғожинова Қаната Әуелбекұлы по теме диссертационного исследования: «Организационно-процессуальные особенности расследования и доказывания транснациональных киберпреступлений» приняты к сведению и использованию в ходе досудебного расследования киберпреступлений.

Председатель комиссии

Члены комиссии

Члены комиссии

Члены комиссии

Члены комиссии

ПРИЛОЖЕНИЕ Б

Приложение
К приказу Генерального Прокурора
Республики Казахстан
от 12.07.2011 года № 61

Реестр предложений по совершенствованию законодательства
В рамках магистерского проекта на соискание степени магистра национальной безопасности и военного дела на тему «Организационно-процессуальные особенности расследования и доказывания транснациональных киберпреступлений»

№	Название нормативного правового акта, структурного элемента НПА	Предлагаемая редакция нормы	Обоснование предлагаемых изменений и/или дополнений
1	часть 2 статьи 111 Уголовно-процессуального кодекса Республики Казахстан от 04.07.2014 года №231-V ЗРК	Предложено внести соответствующее дополнение в Уголовно-процессуальный кодекс, изложив в следующей редакции: - «Фактические данные, имеющие значение для правильного разрешения уголовного дела, устанавливаются: показаниями подозреваемого, обвиняемого, потерпевшего, свидетеля, свидетеля имеющего право на защиту, эксперта, специалиста; заключением эксперта, специалиста; вещественными доказательствами; **электронными доказательствами;** протоколами процессуальных действий	Уголовно-процессуальным кодексом Республики Казахстан не охвачено понятие электронных доказательств в достаточной мере, что необходимо для идентификации в плоскости Уголовно-процессуального кодекса. С целью доказывания тех или иных обстоятельств органу уголовного преследования и последующим суду необходимо изучать различные цифровые устройства, содержащие важную для расследования информацию. Действующее уголовно-процессуальное законодательство не в полной мере адаптировано к таким

		и иными документами.».	источникам информации. Сами по себе электронные доказательства могут охватываться понятием вещественных доказательств, предусмотренных Уголовно-процессуальным кодексом, однако порядок и специфика изъятия электронных доказательств принуждает орган уголовного преследования и суд иначе относиться к ним.
2	Добавить статью 118-1 в Уголовно-процессуальный кодекс Республики Казахстан от 04.07.2014 года №231-V ЗРК	Предложено внести соответствующее дополнение в Уголовно-процессуальный кодекс, изложив в следующей редакции: - «Электронные доказательства – это любая накопленная, сохраненная или переданная в цифровой форме информация, необходимая подтверждения либо опровержения факта, который является предметом судебных разбирательств.».	Уголовно-процессуальным кодексом Республики Казахстан не охвачено понятие электронных доказательств в достаточной мере, что необходимо для идентификации в плоскости Уголовно-процессуального кодекса. С целью доказывания тех или иных обстоятельств органу уголовного преследования и последующим суду необходимо изучать различные цифровые устройства, содержащие важную для расследования информацию. Действующее уголовно-процессуальное законодательство не в полной мере адаптировано к таким источникам информации. Сами по себе электронные доказательства могут охватываться понятием вещественных доказательств, предусмотренных Уголовно-процессуальным кодексом, однако порядок и специфика изъятия электронных доказательств принуждает орган уголовного преследования и суд иначе относиться к ним.

3	пункт 2 статьи 2 Закона РК «О связи» №567 от 05.07.2004 года	Предложено внести соответствующее дополнение в Закон РК «О связи», изложив в следующей редакции: - «служебная информация об абонентах – сведения об абонентах, предназначенные исключительно для целей проведения контрразведывательной деятельности, оперативно-розыскных мероприятий, **досудебного расследования, прокурорского надзора** на сетях связи и включающие в себя:»	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.
4	название статьи 15 Закона РК «О связи» №567 от 05.07.2004 года	Предложено внести соответствующее дополнение в Закон РК «О связи», изложив в следующей редакции: - «Взаимодействие операторов связи, оператора централизованной базы данных абонентских номеров, оператора базы данных идентификационных кодов абонентских устройств сотовой связи с органами, осуществляющими оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор**»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.
5	пункт 1 части 1 статьи 15 Закона РК «О связи» №567 от	Предложено внести соответствующее дополнение в Закон	Учитывая широкое распространение Глобальной сети Интернет в жизни

	05.07.2004 года	РК «О связи», изложив в следующей редакции: - «обеспечивать органам, осуществляющим оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор** на сетях связи, организационные и технические возможности проведения оперативно-розыскных, контрразведывательных мероприятий, **досудебное расследование, прокурорский надзор** на всех сетях связи, а также принимать меры по недопущению раскрытия форм и методов проведения указанных мероприятий»;	человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.
6	пункт 3 части 1 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года	Предложено внести соответствующее дополнение в Закон РК «О связи», изложив в следующей редакции: - «обеспечить органам, осуществляющим оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор** на сетях связи, доступ к служебной информации, а также принимать меры по недопущению раскрытия форм и методов проведения указанных мероприятий»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.
7	пункт 4 части 1 статьи 15	Предложено внести соответствующее дополнение в Закон	Учитывая широкое распространение Глобальной сети Интернет в жизни

	Закона РК «О связи» №567 от 05.07.2004 года	РК «О связи», изложив в следующей редакции: - «обеспечить за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **досудебного расследования, прокурорского надзора** в соответствии с требованиями к сетям и средствам связи и порядком, которые определены Правительством Республики Казахстан»;	человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.
8	часть 3 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года	Предложено внести соответствующее дополнение в Закон РК «О связи», изложив в следующей редакции: - «операторы связи, оператор централизованной базы данных абонентских номеров и оператор базы данных идентификационных кодов абонентских устройств сотовой связи обязаны безвозмездно обеспечить доступ к сведениям, содержащимся в базах данных абонентских номеров и идентификационных кодов абонентских устройств сотовой связи, органам, осуществляющим оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор** на сетях связи, в соответствии с настоящим Законом и законами Республики Казахстан «Об оперативно-розыскной деятельности», «О контрразведывательной деятельности», «О персональных данных и их защите», **«О прокуратуре» и Уголовно-процессуальным Кодексом Республики Казахстан»**;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.

9	часть 5 статьи 15 Закона РК «О связи» №567 от 05.07.2004 года	Предложено внести соответствующее дополнение в Закон РК «О связи», изложив в следующей редакции: - «Взаимоотношения операторов связи, оператора централизованной базы данных абонентских номеров, оператора базы данных идентификационных кодов абонентских устройств сотовой связи с органами, осуществляющими оперативно-розыскную, контрразведывательную деятельность, **досудебное расследование, прокурорский надзор,** регулируются в соответствии с настоящим Законом и законами Республики Казахстан «Об оперативно-розыскной деятельности», «О контрразведывательной деятельности», **«О прокуратуре» и Уголовно-процессуальным кодексом Республики Казахстан»;**	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.
10	- часть 4 статьи 36 Закона РК «О связи» №567 от 05.07.2004 года	Предложено внести соответствующее дополнение в Закон РК «О связи», изложив в следующей редакции: - «Получение от оператора связи служебной информации допускается только с согласия абонента и в случаях, предусмотренных настоящим Законом и законами Республики Казахстан "Об оперативно-розыскной деятельности", "О контрразведывательной деятельности", "О персональных данных и их защите", **“О прокуратуре” и «Уголовно-процессуального кодекса Республики Казахстан».**	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Закон Республики Казахстан «О связи» №567 от 05.07.2004 года.

11	- статью 1 Постановления Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» №246 от 30 марта 2010 года	Предложено внести соответствующее дополнение в Постановление Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах», изложив в следующей редакции: - «настоящие Правила осуществления операторами связи сбора и хранения служебной информации об абонентах (далее – Правила) разработаны в соответствии с законами Республики Казахстан от 15 сентября 1994 года "Об оперативно-розыскной деятельности", от 5 июля 2004 года "О связи", от 6 января 2012 года "О национальной безопасности Республики Казахстан", от 24 ноября 2015 года "Об информатизации", от 28 декабря 2016 года "О контрразведывательной деятельности", от 30 июня 2017 года **«О прокуратуре» и от 3 июля 2014 года «Уголовно-процессуального кодекса Республики Казахстан»** и определяют порядок осуществления операторами связи Республики Казахстан сбора и хранения служебной информации об абонентах;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» №246 от 30 марта 2010 года.
12	пункт 2 статьи 2 Постановления Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» № 246 от 30 марта 2010 года	Предложено внести соответствующее дополнение в Постановление Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах», изложив в следующей редакции: - «служебная информация об абонентах – сведения об абонентах, предназначенные исключительно для целей проведения контрразведывательной деятельности, оперативно-розыскных мероприятий, **досудебного расследования, прокурорского надзора** на сетях связи и	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их

		включающие в себя:».	деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «об утверждении Правил осуществления операторами связи сбора и хранения служебной информации об абонентах» №246 от 30 марта 2010 года.
13	название Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Постановление Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** и требований к сетям и средствам связи» от 19.06.2018 года №358».	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и

			средствам связи» от 19.06.2018 года №358
14	статью 1 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Настоящие Правила обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функций своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** (далее – Правила) определяют порядок обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств, функций своего телекоммуникационного оборудования для технического проведения оперативно-розыскных мероприятий (далее – ОРМ), контрразведывательных мероприятий (далее – КРМ), **собирания доказательств в рамках досудебного расследования, прокурорского надзора**»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
15	пункт 1 статьи 3 Постановления Правительства	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил	Учитывая широкое распространение Глобальной сети Интернет в жизни

	Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «средства проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** – аппаратные и (или) программные средства, входящие в состав телекоммуникационного оборудования для обеспечения функций технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**;»;	человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
16	пункт 3 статьи 3 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи,	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации

	осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «владельцы телекоммуникационного оборудования (далее – владельцы оборудования) – операторы связи и (или) владельцы сетей связи, телекоммуникационное оборудование которых обеспечивает функции технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**;»;	органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
17	пункт 4 статьи 3 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «тестовое подключение – подключение к сети телекоммуникаций оператора связи или сервиса в целях проверки корректности работы функций телекоммуникационного оборудования для технического	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление

	функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**;»;	Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
18	Главу 2. Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных,	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: «Порядок обеспечения операторами связи и (или) владельцами сетей связи функций своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий, **собирания доказательств в рамках досудебного расследования, прокурорского надзора;»;**	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего

	контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358		телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
19	статью 4 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: «Функционирование и сохранность телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** включая техническое обслуживание и ремонт, применение систем охранной сигнализации и видеонаблюдения, обеспечиваются владельцами оборудования за счет собственных и (или) привлеченных средств.»	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
20	статью 5 Постановления Правительства Республики	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил	Учитывая широкое распространение Глобальной сети Интернет в жизни

	Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: **- «При обеспечении функций телекоммуникационного оборудования для технического проведения ОРМ, КРМ, собирания доказательств в рамках досудебного расследования, прокурорского надзора владельцы оборудования за счет собственных и (или) привлеченных средств обеспечивают:»;**	человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
21	пункт 1 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции:	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их

	Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	- «необходимые канальные и технические ресурсы сети телекоммуникаций для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора;**»;	деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
22	пункт 2 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - **«доступ органов, осуществляющих оперативно-розыскную деятельность (далее – ОРД), контрразведывательную деятельность (далее – КРД), досудебное расследование, прокурорский надзор к служебной информации об абонентах;»;**	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или

	технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358		привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
23	пункт 4 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - **«сохранность и безопасность телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, собирания доказательств в рамках досудебного расследования, прокурорского надзора, размещенного на объектах связи;»;**	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358

24	пункт 5 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: «необходимые условия для бесперебойного функционирования оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** включая электроснабжение, заземление, климатические условия, пожарную безопасность;»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
25	пункт 6 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить

	сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «организационные и технические возможности проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** на всех сетях связи;»;	порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
26	пункт 7 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «принятие мер по недопущению раскрытия форм и методов проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора;**»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил

	функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358		обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
27	пункт 10 статьи 5 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «незамедлительное устранение неисправностей, возникших в работе телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора;**»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-

	мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358		розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
28	статью 6 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «ОПС по обращению уполномоченного подразделения органов национальной безопасности представляют информацию о выданных сертификатах на телекоммуникационное оборудование с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора.**»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
29	**Добавить статью 6-1** в Постановление Правительства Республики Казахстан «Об	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам

	утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «**В целях обеспечения функции телекоммуникационного оборудования для технического собирания доказательств в рамках досудебного расследования, прокурорского надзора в интересах решения задач всеми органами, осуществляющими досудебное расследование, прокурорский надзор владельцы оборудовании самостоятельно осуществляют выдачу информации на основании мотивированного постановления вынесенного в соответствии с Уголовно-процессуальным кодексом Республики Казахстан и Закон Республики Казахстан «О прокуратуре»**;	исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
30	Изменить первый абзац статьи 10 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Ввод в эксплуатацию нового и вывод из	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности.

	Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	эксплуатации или модернизация устаревшего телекоммуникационного оборудования, изменение действующих схем связи производятся в соответствии с разработанным и утвержденным владельцем оборудования по согласованию с уполномоченным подразделением органов национальной безопасности планом мероприятий по обеспечению функций телекоммуникационного оборудования для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** на сети телекоммуникаций владельца оборудования»;	В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
31	Изменить пункт 1 статьи 11 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «обеспечение технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** на сети телекоммуникаций оператора связи»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или

	технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358		привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
32	пункт 3 статьи 11 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «реализация новых проектов, приобретение и установка телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** (место установки телекоммуникационного оборудования согласовывается с органами национальной безопасности);»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358

33	пункт 4 статьи 11 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «ввод в постоянную эксплуатацию нового оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** проведение опытной эксплуатации, устранение недостатков, выявленных органами национальной безопасности;»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
34	статью 12 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи,	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить

	осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Проведение внеплановых работ на телекоммуникационном оборудовании с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора,** осуществляется по согласованию с уполномоченными подразделениями органов национальной безопасности.»;	порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
35	статью 13 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Владельцы оборудования принимают меры по ограничению круга лиц, привлекаемых к обеспечению функций для технического проведения ОРМ, КРМ, установке средств проведения ОРМ, КРМ, а также недопущению раскрытия организационных и технических	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или)

	оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	приемов проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**»;	владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
36	**Добавить статью 13-1** Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «**Владельцы оборудования принимают меры по организации и определения лиц, работающих у них, имеющих соответствующие допуска к секретным материалам, к обеспечению функций для технического собирания доказательств в рамках досудебного расследования, прокурорского надзора, установке средств собирания доказательств в рамках досудебного расследования, прокурорского надзора, а также недопущению раскрытия организационных и технических приемов собирания доказательств в рамках досудебного расследования, прокурорского надзора.**»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и

	19.06.2018 года №358		средствам связи» от 19.06.2018 года №358
37	статью 15 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Испытания при подтверждении соответствия телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** проводятся ОПС в присутствии представителя уполномоченного подразделения органа национальной безопасности в срок, не превышающий 30 календарных дней с момента начала испытания.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
38	первый абзац статьи 17 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи

	связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Ввод оборудования в опытную эксплуатацию подтверждается актом ввода в опытную эксплуатацию телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** составляемым по форме согласно приложению 1 к настоящим Правилам, утверждаемым руководителем уполномоченного подразделения органов национальной безопасности и владельца оборудования. Продолжительность опытной эксплуатации определяется уполномоченным подразделением органов национальной безопасности, но не более 60 календарных дней с момента подписания акта ввода в опытную эксплуатации.»	необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
39	второй абзац статьи 17 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: «Положительные результаты опытной эксплуатации оформляются заключением, составляемым по форме согласно приложению 2 к настоящим Правилам, в котором	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление

	привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	отражаются наименование владельца оборудования, предмет испытаний, тип сети связи, продолжительность, результаты испытаний и выводы о соответствии требованиям технических регламентов и национальных стандартов в области обеспечения проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**.»;	Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
40	четвертый абзац статьи 17 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных,	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Ввод в постоянную эксплуатацию оформляется актом ввода в эксплуатацию телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** составляемым по форме согласно приложению 3 к настоящим Правилам.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для

	контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358		технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
41	статью 18 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «При авариях, сбоях, повреждении телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** владельцы оборудования незамедлительно уведомляют об этом уполномоченное подразделение органов национальной безопасности и предпринимают меры по устранению неисправностей и восстановлению работоспособности оборудования.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
42	статью 19 Постановления Правительства Республики	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об

	Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «При систематических авариях, сбоях или продолжительном нефункционировании телекоммуникационного оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** уполномоченным подразделением органов национальной безопасности инициируется аннулирование акта ввода в эксплуатацию с последующим обращением в уполномоченный орган на предмет приостановления действия сертификата соответствия.»;	абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
43	первый абзац статьи 20 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Вывод из эксплуатации телекоммуникационного	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности.

	Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	оборудования с функциями технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** и их повторное использование, а также утилизация устройств накопления и хранения информации владельцами оборудования осуществляются по согласованию с уполномоченным подразделением органов национальной безопасности.»;	В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
44	второй абзац статьи 20 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Вывод из эксплуатации оформляется актом вывода из эксплуатации телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** составляемым по форме согласно приложению 4 к настоящим Правилам.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или

	технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358		привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
45	третий абзац статьи 20 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «По итогам утилизации средств накопления и хранения информации владельцами оборудования составляется акт утилизации средств накопления и хранения информации телекоммуникационного оборудования с функциями проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** по форме согласно приложению 5 к настоящим Правилам. Акт утилизации составляется в двух экземплярах, первый экземпляр представляется владельцем оборудования в уполномоченное подразделение органов национальной безопасности, второй хранится у владельца оборудования.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358

46	статью 22 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «На телекоммуникационном оборудовании с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** должны предусматриваться меры физического и аппаратно-программного ограничения несанкционированного доступа к оборудованию.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
47	статью 23 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации

	деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: -«Телекоммуникационное оборудование с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** подключается владельцами оборудования к каналам и линиям связи органов национальной безопасности через точки подключения.»;	органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
48	статью 24 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Владельцы оборудования обеспечивают соблюдение требований по качеству телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** и длительному сроку его	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими

	технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	непрерывного бесперебойного функционирования в круглосуточном режиме с наименьшим количеством отказов.»;	деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
49	статью 25 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «Техническое обслуживание и ремонт телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** обеспечивают владельцы оборудования за счет собственных и/или привлеченных средств.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358

50	статью 26 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: -«Владельцы оборудования в целях своевременного устранения неисправностей и восстановления работоспособности оборудования обеспечивают наличие резервных узлов и (или) комплектующих телекоммуникационного оборудования с функциями для технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора**.»;	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
51	статью 28 Постановления Правительства Республики Казахстан «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими	Предложено внести соответствующее дополнение в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных	Учитывая широкое распространение Глобальной сети Интернет в жизни человечества, служебная информация об абонентах становится основным объектам исследования в ходе добычи доказательств преступлений. В этой связи операторам связи необходимо законодательно разъяснить порядок выдачи служебной информации

	деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358	мероприятий и требований к сетям и средствам связи», изложив в следующей редакции: - «При изменениях сетей телекоммуникаций, вводе нового оборудования, увеличении емкости каналов связи владельцы оборудования производят необходимые изменения телекоммуникационного оборудования для обеспечения функций технического проведения ОРМ, КРМ, **собирания доказательств в рамках досудебного расследования, прокурорского надзора** с последующим проведением сертификационных испытаний.».	органам уголовного преследования и прокурорского надзора в соответствии их деятельности. В этой связи предлагается внести соответствующие поправки в Постановление Правительства «Об утверждении Правил обеспечения операторами связи и (или) владельцами сетей связи, осуществляющими деятельность на территории Республики Казахстан, за счет собственных или привлеченных средств функции своего телекоммуникационного оборудования для технического проведения оперативно-розыскных, контрразведывательных мероприятий и требований к сетям и средствам связи» от 19.06.2018 года №358
52	Добавить пункт 12 в статью 7-4 Закона Республики Казахстан «Об Информатизации» от 24.11.2015 года №418-V	Предложено внести соответствующее дополнение в Закона Республики Казахстан «Об Информатизации» от 24.11.2015 года №418-V, изложив в следующей редакции: - «Осуществлять исследование, анализ инцидентов информационной безопасности с последующим предоставлением компетентным специальным и правоохранительным органам Республики Казахстан развернутую информацию об источниках, функциях, целях, задач, назначениях инцидентов информационной безопасности для проведения соответствующего расследования по каждому выявленному факту».	Изучив мировой опыт и деятельность АО «Государственная техническая служба», занимающееся регистрацией инцидентов информационной безопасности, возникает предложение не ограничиваться лишь регистрацией инцидентов информационной безопасности, но и проведение АО «Государственной технической службой» исследовании, анализа всех зарегистрированных инцидентов информационной безопасности и передачи всех сведений в специализированные и правоохранительные органы для дальнейшего исследования в плоскости

			уголовного права.
53	статью 1 Положения «о Центральноазиатском региональном информационном координационном центре по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» являющимся неотъемлемой частью Закона Республики Казахстан «О ратификации Соглашения между Азербайджанской Республикой, Республикой Казахстан, Кыргызской Республикой, Российской Федерацией, Республикой Таджикистан, Туркменистаном и Республикой Узбекистан о создании Центральноазиатского регионального информационного координационного центра по	Предложено внести соответствующее дополнение в Положение «о Центральноазиатском региональном информационном координационном центре по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» являющимся неотъемлемой частью Закона Республики Казахстан «О ратификации Соглашения между Азербайджанской Республикой, Республикой Казахстан, Кыргызской Республикой, Российской Федерацией, Республикой Таджикистан, Туркменистаном и Республикой Узбекистан о создании Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» от 06 ноября 2008 года N 78-IV, изложив в следующей редакции: «1. Координация на региональном уровне усилий государств-участников по борьбе с незаконным оборотом наркотиков **и с киберпреступностью**; 2. Создание механизмов взаимодействия компетентных органов государств-участников; 3. Содействие укреплению сотрудничества между компетентными органами государств-участников в борьбе с трансграничной организованной преступностью, связанной с незаконным оборотом наркотиков **и с киберпреступностью**; 4. Содействие в организации и проведении согласованных совместных операций и оперативно-розыскных мероприятий, в том числе контролируемых поставок **и киберперступлений**; 5. Сбор, хранение, анализ и организация обмена оперативно-розыскной и справочной информацией в области борьбы с незаконным оборотом	В целях повышения практики взаимоотношения при расследовании транснациональных киберпреступлений со странами ближнего зарубежья являющимися участниками Центральноазиатского регионального информационного координационного центра по борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров.

	борьбе с незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров» от 06 ноября 2008 года N 78-IV	наркотиков **и с киберпреступностью**; 5. Содействие в реализации мер по унификации информационных систем, в том числе баз данных компетентных органов Сторон; 6. Разработка процедур по системному накоплению информации, формирование и пополнение банка данных Центра; 7. Введение стандартизированных форм и систем обмена информацией; 8. Внедрение новейших программ анализа оперативной информации; Анализ нарко **и кибер** ситуации и выработка соответствующих рекомендаций; 9.Оказание помощи компетентным органам Сторон, а также других государств, территория которых используется для незаконного производства и транспортировки наркотиков **и совершения киберпреступлений**, в реализации антинаркотических и **антихакерских** программ по их просьбе; 10. Оказание содействия в гармонизации нормативной правовой базы государств-участников в сфере контроля за оборотом наркотиков и **киберпреступлений;** 11. Проведение конференций, тренингов, семинаров по вопросам совершенствования методов борьбы с незаконным оборотом наркотиков, киберпреступлениями и укрепления международного сотрудничества в этой сфере.».	