

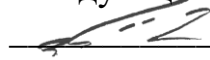
УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ  
«ВИТЕБСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ  
ИМЕНИ П.М. МАШЕРОВА»

Факультет юридический

Кафедра уголовного права и уголовного процесса


СОГЛАСОВАНО

Заведующий кафедрой

 А.В. Рыжик  
21.10.2021

СОГЛАСОВАНО

Декан факультета

 А.А. Бочков  
21.10.2021

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС  
ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

**УГОЛОВНО-ПРАВОВЫЕ,  
КРИМИНОЛОГИЧЕСКИЕ И КРИМИНАЛИСТИЧЕСКИЕ  
ПРОБЛЕМЫ РАССЛЕДОВАНИЯ И ПРЕДУПРЕЖДЕНИЯ  
КИБЕРПРЕСТУПЛЕНИЙ**

для специальности II ступени высшего образования (магистратура)

1-24 80 01 Юриспруденция

Составители: Т.Ф. Дмитриева, В.Г. Стаценко

Рассмотрено и утверждено

на заседании научно-методического совета 03.03.2022, протокол № 3

УДК [343.34+349+343.9]:004(075.8)  
ББК 67.408я73+67.51я73+67.52я73+16я73  
У26

Печатается по решению научно-методического совета учреждения образования «Витебский государственный университет имени П.М. Машерова». Протокол № 2 от 05.01.2022.

Составители: старший преподаватель кафедры уголовного права и уголовного процесса ВГУ имени П.М. Машерова **Т.Ф. Дмитриева**; доцент кафедры уголовного права и уголовного процесса ВГУ имени П.М. Машерова, кандидат исторических наук **В.Г. Стаценко**

**Р е ц е н з е н т ы :**  
кафедра правоведения  
и социально-гуманитарных дисциплин  
ВФ УО ФПБ «Международный университет “МИТСО”»;  
заведующий кафедрой истории и теории права  
ВГУ имени П.М. Машерова, кандидат педагогических наук,  
доцент *Е.Ф. Ивашкевич*

**У26 Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений для специальности II ступени высшего образования (магистратура) 1-24 80 01 Юриспруденция : учебно-методический комплекс по учебной дисциплине / сост.: Т.Ф. Дмитриева, В.Г. Стаценко. – Витебск : ВГУ имени П.М. Машерова, 2022. – 83 с.  
ISBN 978-985-517-876-8.**

Издание включает в себя учебные материалы по курсу «Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений».

Предназначено для магистрантов специальности 1-24 80 01 Юриспруденция.

УДК [343.34+349+343.9]:004(075.8)  
ББК 67.408я73+67.51я73+67.52я73+16я73

ISBN 978-985-517-876-8

© ВГУ имени П.М. Машерова, 2022

## СОДЕРЖАНИЕ

<b>ПОЯСНИТЕЛЬНАЯ ЗАПИСКА</b> .....	4
<b>ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ</b> .....	6
<i>Карта изучения дисциплины</i> .....	6
<i>Содержание учебного материала</i> .....	8
Тема 1 Информационно-коммуникационная безопасность .....	8
Тема 2 Преступность в сфере современных информационно-коммуникационных технологий (киберпреступность) .....	13
Тема 3 Киберпреступность в мире и в Республике Беларусь: особенности и тенденции .....	15
Тема 4 Уголовно-правовые проблемы охраны информационно-коммуникационной безопасности .....	18
Тема 5 Уголовное законодательство Республики Беларусь в сфере информационно-коммуникационной безопасности .....	23
Тема 6 Использование современных криминалистических технологий расследования преступлений в сфере информационно-коммуникационной безопасности .....	28
Тема 7 Цифровая криминалистика и ее значение для расследования преступлений в современном информационном обществе .....	45
<b>ПРАКТИЧЕСКИЙ РАЗДЕЛ</b> .....	58
<b>1. Учебный модуль 1</b> .....	58
1.1 Тематический план модуля .....	58
1.2 Темы и вопросы семинаров .....	58
1.3 Самостоятельная работа студентов .....	58
Темы рефератов .....	58
Задания коллоквиума по темам модуля 1 .....	59
1.4 Источники и литература для работы по модулю 1 .....	59
<b>2. Учебный модуль 2</b> .....	60
2.1 Тематический план модуля .....	60
2.2 Темы и вопросы семинаров .....	60
2.3 Самостоятельная работа студентов .....	60
Темы рефератов .....	60
Задания коллоквиума по темам модуля 2 .....	61
2.4 Источники и литература для работы по модулю 2 .....	63
<b>3. Учебный модуль 3</b> .....	64
3.1 Тематический план модуля .....	64
3.2 Темы и вопросы семинаров .....	64
3.3 Самостоятельная работа студентов .....	65
Темы рефератов .....	65
Задания коллоквиума по темам модуля 3 .....	65
3.4 Источники и литература для работы по модулю 3 .....	66
<b>САМОСТОЯТЕЛЬНАЯ РАБОТА МАГИСТРАНТОВ ПОД УПРАВЛЕНИЕМ ПРЕПОДАВАТЕЛЯ</b> .....	67
<b>РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ</b> .....	72
Контрольные вопросы к экзамену .....	72
Тематика рефератов по курсу .....	72
<b>ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ</b> .....	75
Литература .....	75

## ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Учебная дисциплина «Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений» предназначена для магистрантов юридического факультета ВГУ имени П.М. Машерова специальности 1-24 80 01 «Юриспруденция» второй ступени высшего образования (магистратура) профилизации «Судебно-прокурорско-следственная деятельность».

**Цель изучения дисциплины** – сформировать у магистрантов системные знания, умения и навыки по уголовно-правовому, криминологическому и криминалистическому анализу преступлений, совершенных с использованием компьютеров, информационно-коммуникационных технологий или сетей (киберпреступлений), их квалификации с учетом требований действующего законодательства, криминологических методов их выявления и расследования.

Достижение указанной цели предполагает решение следующих **задач**:

- расширить знания обучающихся в области основных понятий и категорий уголовно-правовой политики в области информационной и компьютерной безопасности;
- актуализировать знание международного и зарубежного законодательства, уголовно-правовых норм национального права, устанавливающих ответственность за преступления в сфере информационной и компьютерной безопасности;
- развить навыки криминологического анализа киберпреступности, ее показателей, состояния и динамики, причинного комплекса, особенностей личности преступников с сфере информационной безопасности, системы мер предупреждения данного вида преступлений;
- расширить знания современных криминалистических приемов исследования, фиксации и защиты электронной информации при расследовании компьютерных преступлений.

Общетеоретические уголовно-правовые, криминологические и криминалистические знания, которые студенты приобрели при изучении соответствующих юридических дисциплин на первой ступени образования, развиваются и уточняются на более высоком уровне.

В результате изучения учебной дисциплины обучающийся должен

**знать:**

- основные понятия, используемые международным и национальным уголовным законодательством в сфере борьбы с киберпреступностью;
- содержание действующих международных и национальных уголовно-правовых актов в сфере противодействия киберпреступности;
- понятие, задачи, методы, принципы, формы реализации уголовно-правовой политики в области противодействия преступлениям против информационно-коммуникационной безопасности;
- показатели, состояние и динамику киберпреступлений в мире и в Республике Беларусь, условия и причины киберпреступности, систему мер предупреждения киберпреступлений;
- современные криминалистические методики расследования преступной деятельности по воспрепятствованию нормальному функционированию информационных систем, их компонентов или деятельности, направленной на использование последних в качестве инструмента совершения преступлений;

**уметь:**

- характеризовать основные понятия, термины, институты в сфере уголовно-правового обеспечения информационно-коммуникационной безопасности, определять значение и место информационной безопасности в структуре национальной безопасности государства;

– ориентироваться в действующем международном, зарубежном и национальном уголовном законодательстве в сфере противодействия преступлениям против информационно-коммуникационной безопасности;

– анализировать качественно-количественные показатели киберпреступности и их динамику;

– оценивать эффективность и достаточность применения уголовно-правовых, криминологических и криминалистических средств противодействия и предупреждения киберпреступности;

**владеть:**

– приемами работы с актами законодательства, научной, учебной и справочной литературой, статистическими материалами;

– навыками криминологического анализа киберпреступности;

– способностью выработки мер и механизмов, направленных на предупреждение киберпреступности;

– методикой и алгоритмом криминалистических действия при расследовании преступлений в информационно-коммуникационной сфере;

– системным и сравнительным анализом противодействия киберпреступности в зарубежных странах с целью использования применимого для Республики Беларусь опыта;

– способностью к осуществлению полученных знаний и умений в правоприменительной деятельности.

В целях повышения эффективности обучения, повышения качества знаний, а также усиления мотивации в углубленном изучении предмета, курс «Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений» подразделяется на т.н. учебные модули или блоки, включающие в себя материал лекционных и семинарских занятий, а также комплекс заданий для самостоятельной работы по определенным разделам.

По каждому разделу (модулю), в соответствии с его целями и задачами по формированию и развитию у магистрантов конкретных компетенций, преподавателем реализуются определенные педагогические технологии, включая:

–методы проблемного и вариативного изложения, используемые на лекционных занятиях;

–метод анализа конкретных ситуаций;

–сравнительно-правовой метод исследования законодательства Республики Беларусь и зарубежных стран;

– инновационные коммуникативные и эвристические педагогические технологии (аудиторный диалог, исследовательский и творческий методы решения казусов, поиск версий правовых решений, дискуссия, учебные дебаты и другие активные формы и методы, используемые на практических занятиях).

– управляемой самостоятельной работы и использования элементов дистанционного обучения.

По каждому учебному модулю магистранты, изучающие курс, должны быть аттестованы. С этой целью изучение тем каждого учебного модуля завершается итоговым контрольным занятием в форме коллоквиума, контрольной работы, тестового контроля, либо в иной форме, предложенной преподавателем.

Основанием для аттестации по темам модуля является:

– способность магистранта ответить на проблемные вопросы по темам модуля;

– знание нормативно-правовых актов, относящихся к изучаемым темам;

– выполнение учебных заданий и задач.

При этом, магистрант, не прошедший аттестацию хотя бы по одному по учебному модулю, не допускается к курсовому экзамену, а условием допуска к сдаче экзамена является выполнение итоговой работы по всему курсу (в форме выполнения тестовой компьютерной программы).

## ТЕОРЕТИЧЕСКИЙ РАЗДЕЛ

### Карта изучения дисциплины «Уголовно-правовые, криминологические и криминалистические проблемы расследования и предупреждения киберпреступлений»

Название раздела, темы	Количество аудиторных часов				Формы контроля
	Лекции		Семинарские занятия		
	ДФО	ЗФО	ДФО	ЗФО	
<b>Учебный модуль 1</b> <b>Криминологический анализ киберпреступности</b>					
Тема 1. Информационно-коммуникационная безопасность	2	1	2		<i>Входной контроль:</i> Опрос, письменный контрольный срез знаний. <i>Текущий контроль:</i> решение теоретических и практических задач, разрешение юридических казусов, рефераты
Тема 2. Преступность в сфере современных информационно-коммуникационных технологий (киберпреступность)	2	1	1	1	<i>Формы текущего контроля:</i> решение теоретических и практических задач, разрешение юридических казусов, доклады на семинарских занятиях, деловая игра, рефераты
Тема 3. Киберпреступность в мире и в Республике Беларусь: особенности и тенденции	4	2	1	1	<i>Формы текущего контроля:</i> решение теоретических и практических задач, разрешение юридических казусов, доклады на семинарских занятиях, рефераты, подготовка компьютерных презентаций
<b>Выходной контроль по модулю</b>					Коллоквиум
<b>Учебный модуль 2</b> <b>Уголовное законодательство Республики Беларусь в сфере информационно-коммуникационной безопасности</b>					
Тема 4. Уголовно-правовые проблемы охраны информационно-коммуникационной безопасности	2	1	2	1	<i>Входной контроль:</i> опрос, письменный контрольный срез знаний. <i>Текущий контроль:</i> Решение теоретических и практических задач, доклады на семинарских занятиях, выполнение учебных заданий рефераты, подготовка компьютерных презентаций

Тема 5. Уголовное законодательство Республики Беларусь в сфере информационной и компьютерной безопасности	4	1	2	1	Формы <i>текущего контроля</i> : решение теоретических и практических задач, доклады на семинарских занятиях
<b>Выходной контроль по модулю</b>					Коллоквиум
<b>Учебный модуль 3</b> <b>Современные криминалистические технологии расследования преступлений в сфере ИКТ</b>					
Тема 6. Использование современных криминалистических технологий расследования преступлений в сфере информационно-коммуникационной безопасности	2	1	2	1	<i>Входной контроль</i> : опрос, письменный <i>контрольный срез знаний</i> . <i>Текущий контроль</i> : Решение теоретических и практических задач, доклады на семинарских занятиях, рефераты
Тема 7. Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе	2	1	2	1	Формы <i>текущего контроля</i> : решение теоретических и практических задач, практические задания, доклады на семинарских занятиях
<b>Выходной контроль по модулю</b>					Коллоквиум
Всего часов	18	8	12	6	
<b>Форма итогового контроля по курсу – экзамен</b>					

## СОДЕРЖАНИЕ УЧЕБНОГО МАТЕРИАЛА

### Тема 1

#### ИНФОРМАЦИОННО-КОММУНИКАЦИОННАЯ БЕЗОПАСНОСТЬ

1. Понятие, содержание и значение информационной безопасности.
2. Современное состояние и проблемы информационной безопасности.
3. Виды и источники угроз информационной безопасности, субъекты обеспечения информационной безопасности.
4. Законодательство Республики Беларусь в области обеспечения информационной безопасности.

##### **1. Понятие, содержание и значение информационной безопасности**

Вхождение человечества в эпоху цифрового информационного уклада, в котором компьютерные и телекоммуникационные системы определяют все области жизнедеятельности, всё более видоизменяет стороны и объекты социальных практик, включая и криминальную сферу.

Информационные технологии все глубже проникают в повседневную жизнедеятельность большинства граждан. В мире насчитывается сейчас почти 2 миллиарда сайтов. По прогнозам специалистов, к 2030 году число пользователей Интернета увеличится до 7,5 миллиарда (90 процентов прогнозируемого мирового населения в возрасте 6 лет и старше)<sup>1</sup>.

Важнейшей особенностью развитых стран является всеобщая связанность, интеграция личных девайсов (многофункциональных устройств), общественных сетей, корпоративных систем и правительственных инфраструктур в единое целое - цифровой взаимосвязанный мир. Это открывает невиданные возможности, но и возможности, риски и угрозы растут пропорционально и экспоненциально.

В Республике Беларусь по состоянию на 2021 год 98% населения в возрасте от 6 до 72 лет пользуется услугами сотовой связи; 85% - использует сеть Интернет, более 73% - пользуется персональным компьютером. Более 40% граждан делают покупки или оплачивают счета через интернет; насчитывается более 12 млн. мобильных абонентов (130% населения), широкополосный доступ в Интернет имеют более 60% абонентов. Количество выданных банковских платежных карточек на 2020 год по данным Национального банка Республики Беларусь превысило 15 млн., инфраструктура их обслуживания включает более 121 тыс. объектов торговли и сервиса, более 4200 банкоматов, 3100 инфокиосков<sup>2</sup>.

Результаты работы по созданию необходимой информационно-коммуникационной инфраструктуры позволяют активно развивать современные технологии электронного правительства и сервисы на их основе, а также осуществлять цифровую трансформацию процессов, протекающих в отраслях экономики.

Указанные темпы проникновения информационных технологий и безналичных платежей во все сферы жизнедеятельности человека наряду с имеющей место некачественностью и неосмотрительностью определенной части пользователей являются предпосылкой возрастающего количества компьютерных инцидентов.

---

<sup>1</sup> Official Annual Cybercrime Report 2019 [Электронный ресурс]. Режим доступа: <https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf>. – Дата доступа: 10.01.2022

<sup>2</sup> Информационное общество в Республике Беларусь. Статистический сборник [Электронный ресурс]. – Минск, 2021. – Режим доступа: <https://www.belstat.gov.by/upload/iblock/719/7199f71a6c5b80265d51141c9bbeaf39.pdf>. – Дата доступа: 26.01.2022.



Данный факт требует кардинального изменения подхода к национальной цифровой безопасности и кибербезопасности как несущей конструкции цифровой и информационной безопасности.

Единого подхода к определению информационной безопасности в настоящее время не определено. В Концепции национальной безопасности Республики Беларусь под информационной безопасностью понимается «состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере»<sup>3</sup>. Данное понятие является первичным и основным для определения компетенции государственных органов по обеспечению информационной безопасности, а также установлению государственной политики в информационной сфере.

Актуальность и значение обеспечения информационной безопасности обуславливаются следующими факторами<sup>4</sup>:

– повышением значимости формирования информационного общества в Республике Беларусь, его роли в социально-экономическом развитии Беларуси как суверенного и независимого государства, безопасности реализации национальных стратегий и планов создания цифровой экономики и научно-технического прогресса в целом;

– необходимостью предметной и всесторонне осознанной защиты национальных интересов в информационной сфере, определяемых Концепцией национальной безопасности Республики Беларусь, обобщения практически и научно обоснованных взглядов на обеспечение информационной безопасности, конкретизации и детализации подходов к данной деятельности;

– необходимостью рассмотрения информационной безопасности как обособленного феномена и нормативного института, а также правового закрепления основ государственной политики по защите национальных интересов в информационной сфере;

– важностью улучшения координации и управляемости деятельности субъектов, вовлеченных в развитие информационной сферы и обеспечение ее безопасности, устойчивого и последовательного функционирования механизмов реагирования на риски, вызовы и угрозы информационной безопасности;

– интеграцией Беларуси в систему международной информационной безопасности, важностью повышения концептуальной и технологической совместимости и синхронизации целей и задач национальной системы обеспечения информационной безопасности с корреспондирующими системами других государств и организаций.

## **2. Современное состояние и проблемы информационной безопасности**

В условиях обострения международных противоречий становится проблематичным выработать эффективные и общепринятые правила поведения мирового сообщества в информационном пространстве. Подходы различных стран к оценке угроз в информационной сфере и противодействию им не совпадают, а по отдельным направлениям поляризуются.

В связи с этим важнейшей целевой установкой обеспечения информационной безопасности является информационный суверенитет Республики Беларусь.

Информационный суверенитет достигается, прежде всего, путем формирования системы правового регулирования отношений в информационной сфере, обеспечива-

---

<sup>3</sup> Концепция национальной безопасности Республики Беларусь. Утверждена Указом Президента Республики Беларусь 09.11.2010 № 575 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информации Республики Беларусь. – Минск, 2022

<sup>4</sup> Концепция информационной безопасности Республики Беларусь. Утверждена Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информации Республики Беларусь. – Минск, 2022

ющей безопасное устойчивое развитие, социальную справедливость и согласие. Необходимо создание условий для построения и безопасного развития функциональной, технологически самодостаточной, надежной и устойчивой информационной инфраструктуры. Следует обеспечить защиту информационных ресурсов, в том числе государственных секретов, иной охраняемой информации, персональных данных, гарантировать политическую самостоятельность государства, защищенность жизненного пространства человека, сохранение духовных и культурных ценностей белорусского общества, научно-технологические преимущества и реализацию иных национальных интересов, т.н. принципа «суверенитета данных».

Государство осуществляет реагирование на риски и вызовы в информационной сфере в целях предупреждения их трансформации в угрозы национальной безопасности, развития и масштабирования вредоносного воздействия.

Государственное реагирование на риски, вызовы и угрозы в информационной сфере предполагает сбор информации об используемых технологиях, способах деструктивных информационных воздействий и совершения киберпреступлений, анализ, оценку и прогнозирование состояния безопасности данной сферы, выявление реализующихся вызовов и угроз, локализацию негативных последствий и восстановление нанесенного вреда (ущерба). Определяется защищенность и устойчивость объектов информационной безопасности, в том числе информационной инфраструктуры, информационных ресурсов, индивидуального, группового и массового сознания к действию угроз. Выявляются и исключаются условия возникновения и реализации рисков, вызовов и угроз информационной безопасности.

Подготавливаются и внедряются сценарии и планы кризисного реагирования на кибератаки, компьютерные инциденты, акты деструктивного информационного воздействия, иные угрозы информационной безопасности, а также проводятся учения и тренировки сил реагирования.

### **3. Виды и источники угроз информационной безопасности, субъекты обеспечения информационной безопасности**

Механизмы деструктивного информационно-психологического воздействия на личность, общество и государство постоянно совершенствуются, а масштабное манипулирование массовым сознанием принимает такую же остроту, как борьба за территории, ресурсы и рынки.

Неуклонно растет количество киберпреступлений. Информационные системы и ресурсы становятся как предметом преступлений, так и средством их совершения. Формируется тотальная зависимость финансового сектора и иных секторов от надежности электронных систем хранения, обработки и обмена данными.

Информационная безопасность направлена на:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению модификации, искажению, копированию, блокированию информации;
- предотвращение других форм незаконного вмешательства в информационные ресурсы и информационные системы, обеспечение правового режима документированной информации;
- защиту конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющих в информационных системах;
- сохранение государственной тайны, конфиденциальности документированной информации в соответствии с законодательством;

– обеспечение прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Государственная система защиты информации включает: органы законодательной, исполнительной и судебной властей; законодательство, регулирующее отношения в области защиты информации и информационных ресурсов; нормативную правовую базу по защите информации; службы (органы) защиты информации предприятий, организаций, учреждений.

К числу государственных органов исполнительной власти и иных учреждений Республики Беларусь, в наибольшей степени участвующих в выполнении координирующих функций в области обеспечения информационной безопасности, следует отнести Совет Безопасности, Совет Министров, Администрацию Президента Республики Беларусь, КГБ, ГЦБИ, НАНБ, Министерство информации, Министерство экономики Беларуси, Комитет по науке и технологии и МВК по вопросам информатизации при Совете Министров Республики Беларусь.

Важную роль в рассматриваемой сфере исполняет Оперативно-аналитический центр (ОАЦ) при Президенте Республики Беларусь, созданный в 2008 году. ОАЦ является государственным органом, осуществляющим регулирование деятельности по обеспечению защиты информации, содержащей сведения, составляющие государственные секреты Республики Беларусь или иные сведения, охраняемые в соответствии с законодательством, от утечки по техническим каналам, несанкционированных и непреднамеренных воздействий.

В 2002 году в МВД было создано самостоятельное управление, осуществляющее практическую деятельность по раскрытию преступлений в сфере высоких технологий (Управление «К»). Спустя два года, которые полностью подтвердили правильность принятого решения, во всех УВД облисполкомов возникли самостоятельные отделы криминальной милиции по раскрытию преступлений в сфере киберпреступности.

Управление определено головным подразделением в системе органов внутренних дел, отвечающим за организацию борьбы с преступлениями, предусмотренными статьями главы 31 УК, а также иными составами преступлений в информационной сфере. Управление координирует деятельность подразделений главного управления криминальной милиции МВД и органов внутренних дел при выявлении ими преступлений против информационной безопасности.

#### **4. Законодательство Республики Беларусь в области обеспечения информационной безопасности**

Правовое обеспечение информационной безопасности и в т.ч. защиты информации базируется на:

– Конституции Республики Беларусь, в соответствии с которой, гражданам Республики Беларусь гарантируется право на получение, хранение и распространение полной, достоверной и своевременной информации о деятельности государственных органов, общественных объединений, о политической, экономической, культурной и международной жизни, состоянии окружающей среды; и указывается, что пользование информацией может быть ограничено законодательством в целях защиты чести, достоинства, личной и семейной жизни граждан и полного осуществления ими своих прав;

– международных договорах в области информационной безопасности. К ним можно отнести: Концепцию сотрудничества государств – участников Содружества Независимых Государств в сфере обеспечения информационной безопасности от 10 октября 2008 года, Концепцию сотрудничества государств – участников Содружества Независимых Государств в борьбе с преступлениями, совершаемыми с использованием информационных технологий от 25 октября 2013 года; Соглашение о сотрудничестве

государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий от 28 сентября 2018, Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в области обеспечения информационной безопасности от 20 ноября 2013 года (для Беларуси вступило в силу 04.06.2015 г.), Соглашение между Правительством Республики Беларусь и Правительством Российской Федерации о сотрудничестве в области защиты информации и др.;

– кодифицированных нормативных правовых актах:

- Гражданский кодекс Республики Беларусь – содержит нормы, касающиеся служебной и коммерческой тайны, закрепляет такие формы отношений, как информационные услуги, электронную подпись признает как средство, подтверждающее подлинность сторон в сделках, предусматривает ответственность за незаконное использование информации (статья 140, часть 2 статьи 161, статья 1011 и др.).

- Кодекс Республики Беларусь об административных правонарушениях (далее — КоАП), в котором определяются административно-правовые санкции за правонарушения в информационной сфере. К таким правонарушениям относятся: отказ в предоставлении гражданину информации, посредственно затрагивающей его права, свободы и законные интересы (статья 10.5), несанкционированный доступ к компьютерной информации (статья 23.4), нарушение законодательства о защите персональных данных (статья 23.7), нарушение требований по использованию национального сегмента сети Интернет (статья 23.9) и др.

- Уголовный кодекс Республики Беларусь (далее — УК) закрепляет ответственность за преступления против информационной безопасности (Раздел XII «Преступления против компьютерной безопасности»), а также иные составы преступлений в информационной сфере (хищение имущества путем модификации компьютерной информации (статья 212) и др.

- Налоговый кодекс Республики Беларусь (общая часть) включает нормы, определяющие порядок защиты различных видов конфиденциальной информации;

– законах, среди которых следует отметить:

- Закон Республики Беларусь 21.06.2008 № 418-З «О регистре населения»;
- Закон Республики Беларусь от 10 ноября 2008 г. № 455-З «Об информации, информатизации и защите информации»;

- Закон Республики Беларусь от 28 декабря 2009 г. № 113-З «Об электронном документе и электронной цифровой подписи»;

- Закон Республики Беларусь 7 мая 2021 г. № 99-З «О защите персональных данных»;

– указах Президента Республики Беларусь и постановлениях Совета Министров Республики Беларусь. К таким законодательным актам можно отнести: указы Президента Республики Беларусь от 01 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет», от 25 октября 2011 г. № 486 «О некоторых мерах по обеспечению безопасности критически важных объектов информатизации», от 09.12.2019 № 449 «О совершенствовании государственного регулирования в области защиты информации»; постановление Совета Министров Республики Беларусь от 15 мая 2013 г. № 375 «Об утверждении технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР 2013/027/ВУ); приказах и постановлениях Оперативно-аналитического центра при Президенте Республики Беларусь и др.;

– государственных программах, утвержденных с целью формирования современных подходов к проектированию и созданию защищенных компьютерных систем, новых технологий и средств технической защиты информации, среди которых необходи-

мо отметить Государственную программу «Цифровое развитие Беларуси» на 2021–2025 годы, утвержденную постановлением Совета Министров Республики Беларусь от 2 февраля 2021 г. № 66.

В 2019 году – утверждена Советом Безопасности Концепция информационной безопасности Республики Беларусь<sup>5</sup>. В ней определяются стратегические задачи и приоритеты в сфере информационной безопасности и борьбы с киберпреступностью. В основу Концепции положены геополитические интересы Беларуси и международные соглашения о сотрудничестве в области обеспечения международной информационной безопасности с учетом основных положений резолюций Генеральной Ассамблеи, а также рекомендаций Организации по безопасности и сотрудничеству в Европе.

## **Тема 2**

### **ПРЕСТУПНОСТЬ В СФЕРЕ СОВРЕМЕННЫХ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ (КИБЕРПРЕСТУПНОСТЬ)**

1. Киберпреступность как объект изучения: понятие, проблемы терминологии, основные концепции и подходы к изучению в современной доктрине.

2. Характеристика основных видов преступлений в сфере современных информационно-коммуникационных технологий.

#### **1. Киберпреступность как объект изучения: понятие, проблемы терминологии, основные концепции и подходы к изучению в современной доктрине**

Понятие «киберпреступность», хотя и утвердилось в последние десятилетия в качестве как доктринального, так и правового термина, тем не менее, имеет различающуюся содержательную трактовку. При этом, в русскоязычной литературе это понятие чаще всего употребляется наряду с такими понятиями, как «компьютерная преступность», «преступления в сфере компьютерной информации», «Интернет-преступность», «преступления в сфере высоких технологий», «преступления, сопряженные с компьютерными технологиями», причём, зачастую, эти понятия используются как синонимы

В праве Республики Беларусь, термин «киберпреступность» хотя и используется – примером может служить его применение в наименовании главы 19 «Противодействие киберпреступности» Концепции информационной безопасности Республики Беларусь от 18 марта 2019 г., тем не менее правового определения также не имеет. В белорусском уголовном законодательстве применяется понятие «преступления против компьютерной безопасности». Глава 31 Раздела 12 Уголовного Кодекса Республики Беларусь под этим наименованием включает в себя 5 видов преступлений, содержащихся в соответствующих статьях.

Следует исходить из того, что объединяющими признаками всех преступлений, входящих в состав киберпреступности, являются средства их совершения – киберпространство, информационно-телекоммуникационные сети и средства компьютерной техники. Соответственно, киберпреступность можно определить как совокупность преступлений, совершенных путём использования средств компьютерной техники и информационно-телекоммуникационных сетей.

---

<sup>5</sup> Концепция информационной безопасности Республики Беларусь. Утверждена Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1// Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информации Республики Беларусь. – Минск, 2022.

Исходя из данной трактовки киберпреступности, составляющие ее противоправные деяния можно – по объекту посягательства - классифицировать следующим образом:

- преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации (посягательства на собственность);

- преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т.д. (преступления против информационной безопасности;

- преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве средства совершения корыстного преступления (хищение путем использования компьютерной техники).

Термин «киберпреступность», таким образом, существенно шире понятия «компьютерные преступления».

Основными правовыми проблемами при расследовании киберпреступлений и судебном преследовании киберпреступников являются: разные правовые системы государств; различия национальных законодательств о киберпреступности; различия в нормах доказательственного права и уголовного судопроизводства (например, в процедурах получения доступа к цифровым доказательствам правоохранительными органами); различия в охвате и географической применимости региональных и многосторонних договоров о борьбе с киберпреступностью; различия в подходах к защите данных и соблюдению прав человека и др.

## **2. Характеристика основных видов преступлений в сфере современных информационно-коммуникационных технологий**

Наиболее развернутую классификацию киберпреступлений предложил в своем отчете Международный союз электросвязи (МСЭ).

А) Преступления против конфиденциальности, целостности и доступности компьютерных данных и систем.

Наиболее часто встречающиеся правонарушения, подпадающие под эту категорию:

- Незаконный доступ (хакерство, взлом шифра).
- Незаконное получение данных (информационный шпионаж).
- Незаконный перехват.
- Искажение информации
- Искажения системы.

Б) Преступления, связанные с контентом.

К этой категории относится контент, который считается незаконным, включая детскую порнографию, ксенофобские материалы или оскорбления в адрес религиозных символов. Разработка правовых инструментов для борьбы с этой категорией преступлений испытывает более сильное влияние со стороны национальных подходов, которые могут учитывать фундаментальные культурные и правовые принципы.

Основные на сегодняшний день преступления, связанные с контентом:

- эротические или порнографические материалы (за исключением детской порнографии);

- детская порнография;
- расизм, агрессивные высказывания, восхваление жестокости;
- религиозные преступления;
- незаконные азартные игры и онлайн-игры;
- клевета и фальшивая информация;

- спам и связанные с ним угрозы;
  - вымогательство;
  - другие формы незаконного контента. Интернет используется не только для прямых атак, но и как площадка для подстрекательства, предложений и побуждения к совершению преступлений, незаконной продажи продуктов, лекарств и предоставления информации и инструкций для незаконных действий, например по изготовлению взрывчатки.
- В) Преступления, связанные с правами собственности и товарными знаками
- Преступления, связанные с авторскими правами.
  - Преступления, связанные с товарными знаками.
- Г) Преступления, связанные с применением компьютеров.
- Мошенничество и компьютерное мошенничество, включая: мошенничество с онлайн-аукционами; мошенничество с предоплатой.
  - Подлог, связанный с применением компьютеров.
  - Кража идентичности.
  - Неправомерное использование устройств.
- Д) Комбинированные преступления
- Отмывание денег с использованием компьютерных технологий.
  - Фишинг.
- Е) Преступления, посягающие на общественную безопасность.
- К этой категории относятся такие деяния, как:
- кибертерроризм – использование киберпространства в террористических целях (например, вовлечение в совершение преступлений террористического характера или иное содействие их совершению);
  - социальные и политически мотивированные преступления: кибербуллинг, груминг, распространение оружия и наркотических средств с помощью даркнета и т.д.

### Тема 3

## **КИБЕРПРЕСТУПНОСТЬ В МИРЕ И В РЕСПУБЛИКЕ БЕЛАРУСЬ: ОСОБЕННОСТИ И ТЕНДЕНЦИИ**

1. Современные тенденции киберпреступности в мире.
2. Состояние, динамика и особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.

### **1. Современные тенденции киберпреступности в мире**

Киберпреступность превращается в один из самых крупных вызовов, с которыми человечество столкнется в ближайшие десятилетия.

В 2018 году исследование Центра стратегических и международных исследований (CSIS) показало, что ежегодно киберпреступность наносит ущерб около 600 миллиардов долларов, что составляет почти один процент мирового ВВП, а к 2022 году общий планетарный ущерб от киберпреступлений может достичь 8 триллионов долларов.

Огромной глобальной проблемой являются кибератаки, посягающие на национальную безопасность государств. Так, в период с мая 2006 года по июнь 2020 года США столкнулись с 156 такими инцидентами, объектами серьезных нападений за последние 14 лет стали также Германия, Индия, Австралия и Соединенное Королевство.

Эти нападения на разные страны включали нападения на оборонные ведомства, правительственные системы и известные технологические компании.

Европол разделяет киберпреступления на киберзависимые преступления (т.е. любое преступление, которое может быть совершено только с использованием компьютеров, компьютерных сетей или других форм информационно-коммуникационных технологий) и преступления, совершаемые посредством кибертехнологий (т.е. традиционные преступления, совершаемые с помощью Интернета и цифровых технологий). Ключевое различие между этими категориями киберпреступности заключается в роли информационно-коммуникационных технологий в совершении правонарушения – являются ли ИКТ целью преступления или неотъемлемой частью способа совершения преступления (*modus operandi* или метода действия), использованного преступником.

Киберпреступления могут совершаться физическими лицами, группами лиц, коммерческими организациями и государствами. Хотя эти субъекты могут применять схожие тактические методы (например, использовать вредоносное программное обеспечение) и атаковать схожие цели (например, компьютерную систему), они имеют разные мотивы и намерения при совершении киберпреступлений.

Киберпреступность становится все более серьезной проблемой для стран, в которых хорошо развита инфраструктура интернета и функционируют платежные системы. Согласно последним оценкам Интерпола угрозы киберпреступности, последняя становится все более агрессивной и конфронтационной. Это можно наблюдать в различных формах киберпреступности, включая высокотехнологичные преступления, утечку данных и сексуальное вымогательство.

В 2019 году Секретариат ООН предложил государствам-членам представить информацию о проблемах, с которыми они сталкиваются в борьбе с использованием информационно-коммуникационных технологий в преступных целях – для подготовки доклада Генерального секретаря ООН на ее семьдесят четвертой сессии.

Республика Беларусь предоставила такую информацию, где, в частности отмечалось: – «принимая во внимание модернизацию современной наркопреступности и использование даркнета и криптовалют в целях незаконного оборота наркотиков, Беларусь считает, что одним из приоритетных направлений деятельности государств-членов должна стать организация обмена информацией, касающейся средств совершения преступлений и методов обнаружения преступной деятельности в даркнете, на наднациональном уровне; подборка и изъятие электронных доказательств; а также разработка и использование конкретных методов расследования преступлений, совершенных в виртуальном пространстве...

– Одним из способов противодействия использованию информационно-коммуникационных технологий в преступных целях может стать разъяснение сотрудникам правоохранительных органов принципов работы даркнета и индустрии криптовалют.

– Беларусь подчеркнула важность разработки международно-правового механизма (рекомендаций) о порядке изъятия криминальных криптоактивов и их хранения до принятия решения судом.

– По мнению Беларуси, разработка и принятие универсального международного документа в рамках Организации Объединенных Наций будет содействовать развитию сотрудничества между компетентными органами государств-членов в борьбе с использованием информационно-коммуникационных технологий в преступных целях»<sup>6</sup>.

---

<sup>6</sup> Генеральная Ассамблея ООН. 74 сессия. Противодействие использованию информационно-коммуникационных технологий в преступных целях: Доклад Генерального секретаря [Электронный ресурс]. – Режим доступа: [https://www.unodc.org/documents/Cybercrime/SG\\_report/V1908184\\_R.pdf](https://www.unodc.org/documents/Cybercrime/SG_report/V1908184_R.pdf). -С.13-24. – Дата доступа: 25.10.2021.



## **2. Состояние, динамика и особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь**

Законодательство Республики Беларусь закрепляет следующие группы компьютерных преступлений:

преступления, направленные на незаконное завладение, изъятие, уничтожение либо повреждение средств компьютерной техники и носителей информации как таковых (такие действия рассматриваются как посягательства на собственность и квалифицируются по статьям гл. 24 УК);

преступления, направленные на получение несанкционированного доступа к компьютерной информации, ее модификации, связанные с неправомерным завладением компьютерной информацией, разработкой, использованием либо распространением вредоносных программ и т.д. (такие действия рассматриваются как преступления против компьютерной безопасности и квалифицируются по статьям гл. 31 УК);

преступления, в которых компьютеры и другие средства компьютерной техники используются в качестве средства совершения корыстного преступления, и умысел виновного лица направлен на завладение чужим имуществом путем изменения информации либо путем введения в компьютерную систему ложной информации (такие действия рассматриваются как хищение путем модификации компьютерной информации и квалифицируются по ст. 212 УК).

На протяжении последних лет в Республике Беларусь наблюдается устойчивый рост количества регистрируемых киберпреступлений: в 2015 году – 2 440 преступлений, в 2016 – 2 471, в 2017 – 3 099, в 2018 – 4 741, в 2019 – 10 539, в 2020 – 25 561<sup>7</sup>.

В 2021 году фиксируется существенное снижение объема киберпреступности в сравнении с 2020 годом – зарегистрировано 15 503 преступлений, что составляет 17,7% от общего числа зарегистрированных в стране преступлений<sup>8</sup>.

Атаки происходят в большинстве случаев с территории Украины и России.

подавляющее большинство преступлений как в предыдущие годы, так и в 2021 году (92% или 14.291), выявленных в сфере высоких технологий, относятся к хищениям путем модификации компьютерной информации (ст. 212 УК).

В результате проведенных оперативно-розыскных мероприятий сотрудниками подразделений РПСВТ в 2021 году выявлено 1.317 лиц (2020 г. – 2121) виновных в совершении киберпреступлений. 1282 или 97% из них – лица, обвиняемые в совершении хищений путем использования компьютерной техники. Из них: женщины – 366 (28,5%), не работающие и необучающиеся – 805 (63%); имеющие судимость – 399 (31%); несовершеннолетние – 59 (5%).

Сумма установленного материального ущерба от совершения квалифицированных преступлений составила в 2021 году 962,5 тыс. рублей, а ее возмещения – 404 тыс. рублей (42%).

Анализ основных факторов, а также причин и условий, оказывавших влияние на состояние криминогенной обстановки в сфере информационной безопасности дают основания полагать, что и в дальнейшем формирование криминологических параметров как в целом по республике, так и в ее регионах, будет осуществляться в условиях особенностей, отмечавшихся в течение предыдущего периода.

Специалисты Управления «К» МВД Республики Беларусь полагают, что динамичное развитие IT-отрасли в стране, функционирование объектов игорного бизнеса

---

<sup>7</sup> Сведения о совершенных правонарушениях на территории Республики Беларусь за январь–декабрь 2015 – 2020 г. / Информационный центр МВД Республики Беларусь. – Минск, 2016 – 2021.

<sup>8</sup> Сведения о совершенных правонарушениях на территории Республики Беларусь за январь–декабрь 2021 г. / Информационный центр МВД Республики Беларусь. – Минск, 2022.

и т.п., объективно и с неизбежностью будет способствовать увеличению числа киберпреступлений. По словам специалистов, если не повысить цифровую безопасность, то к 2025 число киберпреступлений достигнет уровня 100 тысяч в год.

При этом, если принимать во внимание общемировые тенденции, прежде всего следует ожидать дальнейшего роста хищений путем использования компьютерной техники и случаев несанкционированного доступа к компьютерной информации, совершаемых, в частности, мошенническими методами, посредством фишинга и взлома учетных записей пользователей в социальных сетях.

Предупреждение таких преступлений – задача не только правоохранительных органов. Эффективным способом профилактики данных видов преступлений будет расширение обозреваемой для широкого круга общественности правовой информации на данную тематику, а также гибкое и оперативное реагирование со стороны родителей и учреждений образования на проблемы, возникающие в подростковой и молодежной сфере.

В целом, системное противодействие киберпреступности можно обеспечить при комплексном решении задач, стоящих и перед судебной системой, и перед правоохранительными органами. При этом успех зависит от скоординированности действий всех заинтересованных сторон.

#### **Тема 4**

### **УГОЛОВНО-ПРАВОВЫЕ ПРОБЛЕМЫ ОХРАНЫ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТИ**

1. Международные стандарты уголовно-правовой борьбы с преступлениями против информационной безопасности.

2. Зарубежный опыт и борьбы с преступлениями в сфере современных информационно-коммуникационных технологий.

#### **1. Международные стандарты уголовно-правовой борьбы с преступлениями против информационной безопасности**

Проблема противодействия компьютерным преступлениям является объектом пристального внимания международных органов и учреждений в системе Организации Объединенных Наций, Интерпола, Европейского Союза, Организации по безопасности и сотрудничеству в Европе, Содружества Независимых Государств, а также прочих универсальных и региональных международных организаций.

Так, еще на 55-й сессии Генеральной Ассамблеи Организации Объединенных Наций в 2001 г. была принята Резолюция «Борьба с преступным использованием информационных технологий», которая подчеркнула необходимость принятия таких мер по борьбе с преступным использованием информационных технологий, как: противодействие «правовой гавани» для укрытия киберпреступников от наказания, обмен информацией, оснащение и обучение сотрудников правоохранительных органов, защита правовыми системами данных и компьютерных систем от несанкционированного вмешательства, своевременное обеспечение режимами взаимной помощи; расследование случаев преступного использования информационных технологий; предупреждение общественности о необходимости предупреждения преступного использования информационных технологий и борьбы с ним; техническая защита информации производителями программного обеспечения<sup>9</sup>.

---

<sup>9</sup> Борьба с преступным использованием информационных технологий. Резолюция, принятая Генеральной Ассамблеей ООН 22 января 2001 [Электронный ресурс]. – Режим доступа: <https://undocs.org/ru/A/RES/55/63>. – Дата доступа: 27.12.2021.

Кроме того, немаловажное значение в сфере борьбы с компьютерными преступлениями отводится принятой Резолюцией Генеральной Ассамблеи Организации Объединенных Наций N 55/25 Конвенции ООН «Против транснациональной организованной преступности» (заключена в г. Палермо 15.11.2000)<sup>10</sup>. Необходимость применения положений указанной Конвенции, особенно в части криминализации определенных преступных деяний и решения практических вопросов сотрудничества правоохранительных органов в данной сфере, объясняется тем, что около 60% компьютерных преступлений совершается в составе организованных групп.

К настоящему моменту ООН так и не выработала международную конвенцию по кибербезопасности.

#### *Региональные соглашения.*

Документом регионального международного характера, обязательным для его участников, является Соглашение Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.<sup>11</sup>

В этом документе акцент сделан на противостоянии террористическим угрозам в киберпространстве, угрозам международной безопасности. Соглашение содержит лишь общее определение информационной преступности, к которой данный документ также предлагает относить использование информационных технологий для совершения таких преступлений, как мошенничество, вымогательство, контрабанда, незаконная торговля наркотиками, распространение детской порнографии и др.

Наиболее актуальными для рассмотрения являются близкие Республике Беларусь правовые пространства: международные документы, принимаемые в Европейском правовом пространстве и СНГ. Изучение и последующая имплементация предложенных в международных актах составов компьютерных преступлений в отечественное законодательство будут способствовать облегчению преследования лиц, совершающих преступления с использованием компьютерных технологий, на межгосударственном уровне.

Исторически первым нормативным актом Совета Европы, посвященным вопросам регулирования киберпреступности, была Рекомендация № R 89 (9) Комитета Министров стран – членов Совета Европы о преступлениях, связанных с компьютерами, принятая 13 сентября 1989 г.

Самый значимый и известный из общеевропейских актов в рассматриваемой области – Конвенция о преступности в сфере компьютерной информации от 23.11.2001 (Будапешт)<sup>12</sup>.

Киберпреступления в Конвенции разделены на 5 групп:

– преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (противозаконный доступ, неправомерный перехват, воздействие на данные, воздействие на функционирование системы, противозаконное использование устройств);

– преступления, для совершения которых используется компьютер (подлог с использованием компьютерных технологий, мошенничество с использованием компьютерных технологий);

---

<sup>10</sup> Конвенция Организации Объединенных Наций против транснациональной организованной преступности. Принята резолюцией 55/25 Генеральной Ассамблеи от 15 ноября 2000 года [Электронный ресурс]. – Режим доступа: [https://www.un.org/ru/documents/decl\\_conv/conventions/orgcrime.shtml](https://www.un.org/ru/documents/decl_conv/conventions/orgcrime.shtml) – Дата доступа: 27.10.2021.

<sup>11</sup> Соглашение между правительствами государств – членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности (Екатеринбург, 16 июня 2009 г.) // Бюллетень международных договоров. – 2012. – N1.

<sup>12</sup> Конвенция о компьютерных преступлениях. Будапешт, 23 ноября 2001 года. [Электронный ресурс]. – Режим доступа: <https://tm.coe.int/1680081580>. – Дата доступа: 20.01.2022.

– преступления, связанные с содержанием данных (детская порнография);  
– преступления, связанные с нарушением авторского права и смежных прав;  
– преступления, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем (Дополнительный Протокол к Конвенции о преступлениях в сфере компьютерной информации относительно введения уголовной ответственности за правонарушения, связанные с проявлением расизма и ксенофобии, совершенные посредством компьютерных систем ETS N 189 (Страсбург, 28 января 2003 г.).

Совет Европы не ограничился разработкой и принятием Конвенции. Им создан Комитет по Конвенции о киберпреступности (Т-СУ), который представляет государства-участников, содействует эффективному использованию и реализации положений Конвенции, обмену информацией и рассмотрению поправок к ней. Кроме этого, помощь государствам в консолидации их возможностей в решении проблем, связанных с киберпреступностью, оказывает Управление Совета Европы по вопросам киберпреступности (С-PROC).

Особо следует отметить Закон о кибербезопасности ЕС 2019 г., принятый Постановлением 2019/881 Европейского парламента и Совета ЕС от 17 апреля 2019 г. о Европейском агентстве по кибербезопасности (ENISA) и о сертифицировании технологий в области информационной и коммуникационной безопасности<sup>13</sup>. Постановление вступило в силу 27 июня 2019 г.

В рамках СНГ наиболее важным является Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации<sup>14</sup> (заключено в г. Минске 01.06.2001), которое, в частности, устанавливает такие формы сотрудничества, как: обмен информацией; исполнение запросов; управление в области противодействия компьютерной преступности; сотрудничество в области осуществления кадровой политики; создание информационных систем; взаимная научно-исследовательская кооперация и др.<sup>15</sup>

В данный момент не существует общепризнанных определений «киберпространство» и «кибербезопасность». Отсутствие в международном праве консенсуса в отношении того, что понимать под подобными терминами, является негативным фактором при построении отношений между государствами. В этой связи крайне необходима выработка единой терминологии киберпространства и кибербезопасности, гармонизированной с существующей терминологией в области информационной безопасности, информационно-психологической безопасности и т.д.

## **2. Зарубежный опыт и борьбы с преступлениями в сфере современных информационно-коммуникационных технологий США.**

Американский законодатель значительное внимание уделяет вопросам обеспечения безопасности информации в государственных компьютерных системах. На современном этапе правовую основу для формирования и проведения государственной политики США в сфере информационной безопасности образуют более 500 федеральных

---

<sup>13</sup> Regulation (EU) 2019/881 of the European parliament and of the council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act) [Электронный ресурс]. – Режим доступа: <https://eur-lex.europa.eu/eli/reg/2019/881/oj>. – Дата доступа: 23.12.2021.

<sup>14</sup> Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации (Минск, 1 июня 2001 г.) // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Республики Беларусь. – Минск, 2021.

<sup>15</sup> Соглашение Республикой Беларусь не ратифицировано.

законов и значительное количество законов штатов. Прежде всего, это законы США «О компьютерной безопасности» и «Об усовершенствовании информационной безопасности», «О компьютерном мошенничестве и злоупотреблении компьютерами», «О свободе информации» и «Об освещении деятельности правительства», «Об охране персональных данных» и др.

В мае 2011 года США представили документ «Международная стратегия США в отношении киберпространства. Процветание, безопасность и открытость сетевого мира» (International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World)<sup>16</sup>. Этот документ можно рассматривать как первый политико-стратегический документ, в котором, во-первых, киберпространство было обозначено как самостоятельная предметная сфера регулирования, требующая международного сотрудничества, во-вторых, предложен комплексный подход регулирования по широкому спектру вопросов, относящихся к сфере киберпространства. В документе, который актуален и сегодня, определены взаимосвязанные стратегические направления, по каждому из которых Правительство США намеревается действовать сами и сотрудничать на международном, региональном и национальном уровне с частными и государственными структурами.

В мае 2018 г. была опубликована Стратегия кибербезопасности Министерства внутренней безопасности США, рассчитанная на пять лет и перечисляющая ключевые цели и задачи, стоящие перед ведомством до 2023 г.

В июле 2021 года Президент США Джо Байден подписал меморандум, предусматривающий создание стандартов в сфере кибербезопасности для ключевых инфраструктурных объектов - меморандум о национальной безопасности, повышении кибербезопасности для систем управления критически важной инфраструктурой<sup>17</sup>.

#### **КНР.**

В Китае действует несколько нормативно-правовых актов, сфера действия которых охватывает безопасность информационно-компьютерных систем и инфраструктуры: Закон об охране государственной тайны, «Положение о защите компьютерных информационных систем, об административных мерах для информационных служб Интернета»; утвержденные Министерством общественной безопасности «Административные меры по предотвращению заражения и лечению компьютерных вирусов» и «Административные меры по многоуровневой защите информационной безопасности», Закон о кибербезопасности Китайской Народной Республики<sup>18</sup>, принятый на 24-й сессии Постоянного комитета 12-й сессии Всекитайского собрания народных представителей Китайской Народной Республики 7 ноября 2016 года.

Особое место в Законе занимают положения об ответственности за нарушение требований и предписаний (глава VI). Предусмотрены административный, уголовный и гражданско-правовой виды ответственности, а формы ответственности включают предупреждения, штрафы, приостановление деятельности, запрет на занятие определенных должностей, конфискация незаконных доходов, административный арест, наложение ареста на имущество и возмещение причиненного ущерба.

---

<sup>16</sup> International Strategy for Cyberspace. Prosperity, Security and Openness in a Networked World [Электронный ресурс]. – Режим доступа: [http://www.whitehouse.gov/sites/default/files/rss\\_viewer/international\\_strategy\\_for\\_cyberspace.pdf](http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf). – Дата доступа: 31.01.2022.

<sup>17</sup> Овчинский, В., Жданов, Ю. Меморандум Байдена [Электронный ресурс]. – Режим доступа: [https://zavtra.ru/blogs/memorandum\\_bajdena](https://zavtra.ru/blogs/memorandum_bajdena). – Дата доступа: 31.10.2021.

<sup>18</sup> Cybersecurity Law of the People's Republic of China [Electronic resource]. – Режим доступа: [https://pkulaw.com/en\\_law/4dce14765f4265f1bdfb.html](https://pkulaw.com/en_law/4dce14765f4265f1bdfb.html). – Дата доступа: 21.12.2021.

## **Европейские страны<sup>19</sup>**

Позиции европейских законодателей в отношении криминализации несанкционированного доступа, полагаем, можно представить в виде трех групп.

К первой группе отнесем позицию законодателей Австрийской Республики, Королевства Бельгии, Королевства Дании, Французской Республики, Латвийской Республики, которые закрепили в УК самостоятельный состав несанкционированного доступа.

Ко второй группе отнесем позицию создателей УК Королевства Испании и Королевства Швеции, в которых несанкционированный доступ выступает в качестве способа совершения других преступлений.

В третью группу следует отнести УК Республики Польша, Королевства Нидерландов, Федеративной Республики Германии, где законодатели закрепили несанкционированный доступ не только в качестве самостоятельного состава, но и предусмотрели его в качестве способа совершения других преступлений.

Представляет интерес анализ объективных и субъективных признаков состава несанкционированного доступа.

В большинстве стран объектом выступают общественная безопасность и общественный порядок (Нидерланды, Латвия), неприкосновенность системы автоматизированной обработки информации (Бельгия, Франция), частная сфера и профессиональная тайна – Австрия, ФРГ и др. Таким образом, объектом несанкционированного доступа выступают различные группы общественных отношений, отсутствует единый законодательный подход к его определению.

## **Российская Федерация**

Бурное развитие нормативной и теоретической базы информационных отношений в Российской Федерации пришлось на конец XX в. Так, например, преступления в сфере компьютерной информации впервые были криминализованы в 1996 г. с принятием Уголовного кодекса Российской Федерации. Таким образом, Кодекс стал правовой основой в борьбе с компьютерными преступлениями в России.

Правовая база противодействия преступности с применением высоких технологий в Российской Федерации последовательно развивалась в дальнейшем, в частности, с принятием Доктрины информационной безопасности Российской Федерации (2000 г.), Указа Президента РФ от 17 марта 2008 г. № 351 «О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена», утверждении в 2013 г. «Основ государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 г.».

Еще одним примером государственной политики в рассматриваемой области служит утвержденная президентским указом от 5 декабря 2016 года Доктрина информационной безопасности, представляющая собой систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере.

Основы по обеспечению безопасности Российской Федерации в информационной сфере, заложенные в Доктрине информационной безопасности, получили развитие с принятием Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы, которая была введена в действие указом Президента РФ от 9 мая 2017 г. № 203 «О Стратегии развития информационного общества в Российской Федерации на 2017–2030 годы».

---

<sup>19</sup> Швед, Н.А. Сравнительный анализ уголовной ответственности за несанкционированный доступ к компьютерной информации в странах ЕС / Н.А. Швед // Вестник Нижегородского университета им. Н.И. Лобачевского. – 2016. – № 5. – С. 222–226.

Таким образом, несмотря на то что несанкционированный доступ нашел законодательное закрепление в уголовном законодательстве многих зарубежных государств, отсутствует унифицированный подход к описанию признаков состава данного преступления, что не способствует эффективному противодействию рассматриваемому преступлению. Тем не менее изучение накопленного в других странах законодательного опыта может быть использовано для выработки предложений по совершенствованию УК в части обеспечения безопасности компьютерной информации.

## Тема 5

### УГОЛОВНОЕ ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТИ

1. Уголовно-правовая характеристика и проблемы применения норм УК о преступлениях, предметом или средством совершения которых является информация.

2. Уголовно-правовая характеристика преступлений против компьютерной безопасности.

#### **1. Уголовно-правовая характеристика и проблемы применения норм УК о преступлениях, предметом или средством совершения которых является информация**

Согласно действующего законодательства Республики Беларусь, в содержание понятия «преступления против информационной безопасности» включаются:

1) *преступления против информационной безопасности, так или иначе связанные с использованием компьютерной техники*: изготовление и распространение порнографических материалов или предметов порнографического характера (ст.343УК), в том числе с изображением несовершеннолетнего (343<sup>1</sup>УК); разжигание расовой, национальной, религиозной либо иной социальной вражды или розни (ст.130 УК); вымогательство (ст. 208 УК); доведение до самоубийства через распространение каких-либо сведений (ст.145 УК); разглашение врачебной тайны (ст. 178 УК); клевета (ст.188 УК); оскорбление представителя власти (ст.369 УК); незаконные действия в отношении информации о частной жизни и персональных данных (ст.203.1 и 203.2); нарушение авторского права, смежных прав и права промышленной собственности (ст. 201 УК); распространение ложной информации о товарах и услугах (ст.250 УК); заведомо ложное сообщение об опасности (ст.340 УК); нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений (ст. 203 УК), коммерческий шпионаж (ст. 254 УК); мошенничество (ст.209 УК); шпионаж (ст. 358 УК); умышленное либо по неосторожности разглашение государственной тайны (ст.373-374 УК); умышленное разглашение служебной тайны (ст.375 УК) и др.

2) *преступления против компьютерной безопасности* (несанкционированный доступ к компьютерной информации, неправомерное завладение компьютерной информацией, разработка, использование либо распространение вредоносных программ, нарушение правил эксплуатации компьютерной системы или сети и др.);

3) *хищения путем модификации компьютерной информации* (ст.212УК).

Таким образом, к преступлениям против информационной безопасности относятся правонарушения, при совершении которых средства компьютерной техники выступают как орудия совершения преступления либо как предмет преступного посягательства.

#### **2. Уголовно-правовая характеристика преступлений против компьютерной безопасности**

В белорусском уголовном законодательстве применяется понятие «преступления против компьютерной безопасности». Глава 31 Раздела 12 Уголовного Кодекса Респуб-

лики Беларусь под этим наименованием включает в себя 5 видов преступлений, содержащихся в статьях 349, 350, 352, 354 и 355 УК.

Проведем более подробный уголовно-правовой анализ данных статей.

*1. Несанкционированный доступ к компьютерной информации как преступление против компьютерной безопасности (ст. 349 УК).*

Непосредственным *объектом* преступления, ответственность за совершение которого предусмотрена ст. 349 Уголовного кодекса Республики Беларусь является информационная безопасность, под которой следует понимать состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере<sup>20</sup>.

В части 1 ст. 349 УК Республики Беларусь в ее современной редакции установлена уголовная ответственность за «несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты (несанкционированный доступ к компьютерной информации), совершенный из корыстной заинтересованности либо повлекший по неосторожности причинение существенного вреда».

*Предметом преступления*, ответственность за совершение которого предусмотрена ст. 349 УК, является компьютерная информация.

*Объективная сторона* преступления характеризуется действием, которое выражается в несанкционированном доступе к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающемся нарушением системы защиты.

Преступление характеризуется сочетанием умысла и неосторожности (сложной виной) – умышленным совершением преступления («несанкционированный доступ к компьютерной информации, сопровождающийся нарушением системы защиты, совершенный из корыстной заинтересованности») и неосторожностью по отношению к наступившим в результате этого преступления последствиям («повлекший по неосторожности причинение существенного вреда»). В целом такое преступление признается совершенным *умышленно (ст.25 УК)* и имеет *материальный* состав: оно признается оконченным с момента наступления последствий от совершенного действия - «причинение существенного вреда».

Санкция ч.1 статьи 349 включает в себя наказания в виде штрафа, или лишения права занимать определенные должности или заниматься определенной деятельностью, или арест, или ограничение свободы на срок до двух лет, или лишение свободы на тот же срок.

В части 2 статьи 349 установлена уголовная ответственность за «несанкционированный доступ к компьютерной информации либо самовольное пользование компьютерной системой или сетью, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия».

Состав преступления, описанный в части 2 ст. 349 УК – *материальный*. Неправомерными признаются следующие действия: 1. несанкционированный доступ к компьютерной информации, что под этим понимается, рассмотрено выше; 2. самовольное пользование компьютерной системой или сетью, под которым следует понимать взаимодействие лица с перечисленными устройствами без разрешения на то со стороны собственника, владельца, уполномоченного ими лица или законного пользователя.

Преступление, описанное в части 2 ст. 349 УК, является неосторожным.

---

<sup>20</sup> Концепция информационной безопасности Республики Беларусь. Утверждена Постановлением Совета Безопасности Республики Беларусь 18.03.2019 № 1 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Республики Беларусь. – Минск, 2022.



Наказание по части 2 ст. 349 УК – ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет.

Субъект рассматриваемого преступления – общий, то есть любое вменяемое лицо, достигшее 16 лет, независимо от гражданства.

При анализе объективной стороны возникает и такой вопрос, касающийся места совершения преступления: как поступать в случае, если действие – несанкционированный доступ – было совершено на территории Республики Беларусь, а одно из перечисленных последствий наступило за пределами Беларуси, или такое же действие было совершено за границей, а последствия наступили в нашей республике, ведь глобальные компьютерные сети объединяют многие страны мира? Какое решение принять, если один из соучастников преступной группы, совершившей преступление против компьютерной безопасности, выполнил свои действия в Беларуси, а остальные – в других странах? При решении этого вопроса необходимо руководствоваться положениями ст. 5 УК, которая гласит: в части первой – что «лицо, совершившее преступление на территории Республики Беларусь, подлежит ответственности по настоящему Кодексу»; в части второй – что «преступление признается совершенным на территории Республики Беларусь, если оно начато, или продолжалось, или было окончено на ее территории, или совершено в пределах Республики Беларусь в соучастии с лицом, совершившим преступление на территории иностранного государства». Это правило распространяется и на другие составы преступлений против информационной безопасности.

2. *Уничтожение, блокирование или модификация компьютерной информации (ст.350 УК).*

Статьи 350–351 УК прежней редакции (модификация компьютерной информации и компьютерный саботаж) были объединены в одном альтернативном материальном составе преступления ввиду однородности характера противоправного поведения (например, изменение информации может повлечь ее блокирование), близкой степени общественной опасности деяний (изменение, уничтожение, блокирование информации влекут последствия в виде невозможности ее использования законным обладателем) и последовательным совершением на практике указанных действий с целью достижения единой цели.

Непосредственным *объектом* преступления являются общественные отношения, обеспечивающие целостность, подлинность, доступность и сохранность компьютерной информации.

*Предметом* преступления является компьютерная информация.

*Объективная сторона* выражается в деянии, которое характеризуется двумя альтернативными формами активного противоправного поведения, такими как:

а) уничтожение, блокирование информации, хранящейся в компьютерной системе, сети или на машинных носителях;

б) внесение заведомо ложной информации в компьютерную систему, сеть или на машинные носители.

Состав этого преступления материальный. В качестве последствия в диспозиции части 1 ст. 350 УК предусмотрено причинение существенного вреда. Что под ним следует понимать, рассмотрено выше при анализе части 1 ст. 349 УК.

Как указано в тексте анализируемой статьи, *модификация компьютерной информации* наказывается по ст. 350 УК только в том случае, когда отсутствуют признаки преступления против собственности. Данное преступление совершается *умышленно*, причем умысел может быть как прямым, так и косвенным.

Наказание по части 1 ст. 350 УК – штраф, или лишение права занимать определенные должности или заниматься определенной деятельностью, или арест, или ограничение свободы на срок до трех лет, или лишение свободы на тот же срок.

Часть 2 статьи 350 определяет квалифицированный состав: «те же деяния, совершенные повторно либо группой лиц по предварительному сговору, – наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения».

В части 3 ст. 350 УК предусмотрена ответственность за деяния, предусмотренные частями 1 или 2 статьи 350, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 Кодекса.

Наказание по части 3 ст. 350 УК – лишение свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения – самое строгое, установленное законодателем для преступлений против компьютерной безопасности.

Субъект преступления общий – лицо, достигшее возраста 16 лет.

### *3. Неправомерное завладение компьютерной информацией (статья 352 УК)*

Непосредственный объект преступления – общественные отношения, определяющие порядок получения и передачи компьютерной информации.

Предметом преступления является компьютерная информация, хранящаяся в компьютерной системе, сети или на машинных носителях либо передаваемая с использованием средств компьютерной связи.

Объективная сторона преступления, ответственность за совершение которого предусмотрена ст. 352 УК, выражается в деянии, которое характеризуется тремя альтернативными формами активного противоправного поведения, такими как:

а) умышленные несанкционированное копирование компьютерной информации, хранящейся в компьютерной системе, сети или на машинных носителях;

б) перехват компьютерной информации, передаваемой с использованием средств компьютерной связи;

в) иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, повлекшие причинение существенного вреда.

Состав рассматриваемого преступления материальный. По субъективной стороне неправомерное завладение компьютерной информацией – это умышленное преступление. Действие – несанкционированное копирование, иное неправомерное завладение компьютерной информацией либо ее перехват – совершается с прямым умыслом, при этом виновный относится к последствию – причинению существенного вреда – как с прямым, так и с косвенным умыслом.

Субъектом этого преступления может быть любое лицо, достигшее 16-летнего возраста.

Наказание – общественные работы, или штраф, или арест на срок до шести месяцев, или ограничение свободы на срок до двух лет, или лишение свободы на тот же срок.

Часть 2 статьи 352 определяет квалифицированный состав: «те же деяния, совершенные повторно либо группой лиц по предварительному сговору, – наказываются штрафом, или арестом, или ограничением свободы на срок до пяти лет, или лишением свободы на тот же срок с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения».

В части 3 ст. 352 УК предусмотрена ответственность за деяния, предусмотренные частями 1 или 2 статьи 352, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 Кодекса.

Наказание по части 3 ст. 350 УК – лишение свободы на срок от трех до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

*4. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (статья 354).*

Непосредственным объектом преступления являются общественные отношения, обеспечивающие конфиденциальность, целостность, подлинность, доступность и сохранность компьютерной информации.

Предметом этого преступления являются вредоносные компьютерные программы, специальные программные или аппаратные средства.

По объективной стороне состав рассматриваемого преступления – формальный.

Обязательным признаком субъективной стороны при совершении таких действий, как разработка компьютерных программ, является специальная цель – нарушения системы защиты, несанкционированного доступа к компьютерной системе, сети или машинному носителю, несанкционированного уничтожения, блокирования, модификации компьютерной информации или неправомерного завладения компьютерной информацией либо нарушения работы компьютерной системы, сети или машинного носителя. Следует отметить, что уголовно-наказуемым будет заведомое использование вредоносных программ как в том случае, когда они используются для заражения других компьютеров, так и тогда, когда они используются в целях защиты своего программного обеспечения, баз данных и другой информации от несанкционированного копирования. Мотивы преступления на квалификацию не влияют.

Субъект этого преступления – общий, лицо, достигшее 16-летнего возраста. Ответственность по ст. 354 УК несут не только разработчики вредоносных программ, но и другие пользователи, которые могут использовать или распространять эти программы.

Часть 2 ст. 354 УК предусматривает квалифицированный состав и устанавливает наказуемость за «те же действия, совершенные группой лиц по предварительному сговору».

В части 3 ст. 354 УК предусмотрена ответственность за деяния, предусмотренные частями 1 или 2 статьи, повлекшие по неосторожности последствия, указанные в части 2 статьи 349 Кодекса - крушение, авария, катастрофа, несчастные случаи с людьми, отрицательные изменения в окружающей среде. К тяжким также необходимо относить такие прямо не указанные в части 2 ст. 349 УК последствия, как причинение особо крупного материального ущерба, уничтожение, блокирование, модификация или копирование информации особой ценности и т.д.

Наказание по части 3 ст. 350 УК - лишение свободы на срок от трех до десяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

*5. Нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК).*

Непосредственным объектом преступления являются общественные отношения, обеспечивающие безопасность эксплуатации компьютерной информационной системы или сети. В качестве дополнительных объектов могут выступать конституционные права, свободы и законные интересы граждан, государственные и общественные интересы.

Статья предусматривает ответственность за «умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности причинение существенного вреда». Необходимо отметить, что предусмотренные ст. ст. 349 и 355 УК преступления имеют много схожего. Основное отличие между ними заключается в санкционированности или несанкционированности доступа, влекущего перечисленные последствия. В рассматриваемом составе, предусмотренном ст. 355 УК, предусмотрен именно правомерный (то есть санкционированный) доступ.

Состав этого преступления – *материальный*.

По субъективной стороне это преступление является *неосторожным*. Деяние – нарушение правил эксплуатации – совершается умышленно, о чем имеется прямое указание в диспозиции статьи, однако отношение к последствиям может быть только неосторожное. Соответственно, неосторожное нарушение правил, повлекшее причинение существенного вреда, не может быть признано преступным.

Субъект данного преступления, в отличие от состава, предусмотренного ст. 349 УК, специальный: это достигшее 16-летнего возраста лицо, имеющее доступ к компьютерной системе или сети, то есть законный пользователь.

Наказание по части 1 ст. 355 УК – штраф, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительные работы на срок до двух лет, или ограничение свободы на тот же срок.

В части 2 статьи предусмотрен материальный состав с неосторожной формой вины. В ней установлена ответственность за «деяния, повлекшее по неосторожности последствия, указанные в части 2 статьи 349...Кодекса». Содержание этих последствий было рассмотрено выше.

Наказание – ограничение свободы на срок до пяти лет или лишение свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

## Тема 6

### ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ КРИМИНАЛИСТИЧЕСКИХ ТЕХНОЛОГИЙ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТИ

1. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности; криминалистическая характеристика преступлений в сфере информационно-коммуникационной безопасности.

2. Использование современных криминалистических технологий при обнаружении, фиксации, изъятии следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

3. Современные возможности применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий.

#### **1. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности; криминалистическая характеристика преступлений в сфере информационно-коммуникационной безопасности**

Современный уровень развития цифровых криминалистических технологий расследования преступлений делает возможным, с одной стороны, существенное снижение латентности преступности, с другой – значительное повышение коэффициента раскрываемости преступлений, причем это относится как к традиционной уголовной преступности, так и к рассматриваемой в данной работе киберпреступности. Между тем, в проблемном поле криминалистики находится ряд актуальных дискуссионных аспектов, существенно влияющих на процесс раскрытия, расследования и предупреждения киберпреступлений, среди которых: 1) отсутствие единства толкования понятийного аппарата; 2) необходимость формирования теории информационно-компьютерного обеспечения криминалистической деятельности; 3) разработка адекватных современной криминогенной ситуации технико-криминалистических, тактических и методических

подходов к расследованию киберпреступлений, обновление учеными-криминалистами методик расследования компьютерных преступлений в современных условиях, совершенствование структуры методики расследований киберпреступлений, позволяющей поднять борьбу с киберпреступностью на соответствующий уровень; 4) дальнейшее совершенствование методологических основ криминалистики, разработка и применение технико-криминалистических цифровых источников информации, создание на этой основе новых действенных методических рекомендаций по расследованию киберпреступлений, новых и изменяющихся прежних составов преступлений, их унификация и адаптация к современной практике правоприменения; 5) решение других актуальных вопросов расследования киберпреступлений уголовно-процессуального, криминалистического и оперативно-розыскного характера, некоторые вопросы судебного разбирательства по таким уголовным делам.

Остановимся на трех первых основных проблемных направлениях криминалистики.

1. Киберпреступность, как международное явление, породило терминологическую множественность в криминалистике с различной понятийной трактовкой: 1) криминалистика программного обеспечения (Software Forensic)<sup>21</sup>; 2) компьютерная криминалистика<sup>22</sup>; 3) форензика<sup>23</sup>; 4) судебная дигитология<sup>24</sup>; 5) этиология информационных систем (Information systems etiology)<sup>25</sup>; 6) цифровая криминалистика, занимающаяся обнаружением, фиксацией и использованием следов «виртуального» мира<sup>26</sup>; 7) электронная цифровая криминалистика<sup>27</sup>; 8) электронная криминалистика и др. Большинство ученых считают, что все вышеприведенные термины являются неверными, т.к. априори такой криминалистики в природе не существует, поскольку «криминалистика – едина!»<sup>28</sup>, а толкование «электронной, компьютерной или цифровой криминалистики» как направленного исследования электронных доказательств с помощью специалистов и экспертов, ошибочно. Соответственно следует говорить только о криминалистическом исследовании носителей цифровой (электронной или компьютерной) информации<sup>29</sup>.

---

<sup>21</sup> Spafford, Eugene H. and Stephen A. Weeber. Software forensics: Can we track code to its authors? // *Computers & Security*. 12 (1993): pp. 585–595.

<sup>22</sup> Пастухов, П.С. О необходимости развития компьютерной криминалистики / П.С. Пастухов // *Пермский юридический альманах. Ежегодный научный журнал*. – 2018. – № 1. – С. 453; Мальцагов И.Д. Современные технологии в расследовании преступлений: компьютерная криминалистика / И. Д. Мальцагов // *Экономика. Бизнес. Право*. – 2018. – № 4–6(26). – С. 44–48.

<sup>23</sup> Медведев, И.В. Компьютерная криминалистика «Форензика» и киберпреступность в России / И.В. Медведев // *Пролог: журнал о праве*. – 2013. – № 3. – С. 66.

<sup>24</sup> Романенко, М.А. Судебная дигитология современный взгляд на содержание криминалистической техники / М.А. Романенко // *Вестник Омского университета. Серия «Право»*. – 2007. – № 1(10). – С. 148.

<sup>25</sup> Gregory, A. Hall, Wilbon P. Davis Toward Defining the Intersection of Forensics and Information Technology // *International Journal of Digital Evidence Spring*. – 2005. – Volume 4., Issue 1.

<sup>26</sup> Криминалистика: учебник / под ред. Т.А. Седовой, С.П. Кушниренко, В.Д. Пристанкова. – М.: ЮСТИЦИЯ, 2019. – С. 19.

<sup>27</sup> Смушкин, А.Б. К вопросу о наименовании теории «Электронная цифровая криминалистика» / А.Б. Смушкин // *Проблемы уголовного процесса, криминалистики и судебной экспертизы*. – 2019. – № 1(13). – С. 15–21.

<sup>28</sup> Россинская, Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е.Р. Россинская // *Вестник Восточно-сибирского института МВД России*. – 2019. – № 2 (89). – С. 196.

<sup>29</sup> Кучин, О.С. Электронная криминалистика: миф или реальность / О.С. Кучин // *Академическая мысль*. 2019. № 3 (8) [Электронный ресурс]. – Режим доступа: <https://cyberleninka.ru/article/n/elektronnaya-kriminalistika-mif-ili-realnost>. – Дата доступа: 07.10.2021.

2. В решении проблемы формирования теории информационно-компьютерного обеспечения криминалистической деятельности существует несколько подходов. Первый – обозначение частной теории «Криминалистическое исследование компьютерной информации, средств ее обработки и защиты» с выделением в ней трех направлений: криминалистическое учение о компьютерной информации, криминалистическое исследование компьютерных устройств, информационных систем и информационно-телекоммуникационных сетей, криминалистическое использование компьютерной информации, средств ее обработки и защиты<sup>30</sup>. Второй подход, поддерживаемый многими учеными-криминалистами, заключается в формировании системы теории информационно-компьютерного обеспечения криминалистической деятельности, включающей: концепцию теории информационно-компьютерного обеспечения криминалистической деятельности (предмет, задачи, объекты); «учение о способах компьютерных преступлений преступлений/правонарушений; учение о цифровых следах как источниках криминалистически значимой компьютерной информации; учение об информационно-компьютерных криминалистических моделях видов компьютерных преступлений; учение о криминалистическом исследовании компьютерных средств и систем, реализуемое в новом разделе криминалистической техники; учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий; учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений; учение о взаимосвязях и разграничениях цифровизации судебно-экспертной и криминалистической деятельности»<sup>31</sup>. Мы полностью солидарны с позицией Е.Р. Россинской, предложившей систему теории информационно-компьютерного обеспечения криминалистической деятельности, т.к. она отличается фундаментальностью решения общетеоретических проблем, способствующих совершенствованию всех разделов криминалистики и неразрывной связи со многими процессуальными науками.

3. В направлении обновления и разработки учеными-криминалистами современных методик расследования киберпреступлений, совершенствования их структуры, целесообразно конкретизировать важные элементы криминалистической характеристики этих преступлений. Новые информационные технологии усложнили не только такие понятия, как место и время совершения киберпреступлений, но и способы их совершения и следовую картину, круг предметов – вещественных доказательств<sup>32</sup>. В качестве характерных признаков криминалистической характеристики преступлений в сфере компьютерной информации выделяют: 1) информацию о предмете преступного посягательства; 2) информацию об обстановке или среде совершения преступления (вид информационного обеспечения, порядок его действия, схема обработки и защиты информации); 3) сведения о личности преступника; 4) типичные способы подготовки, орудия или средства совершения преступления; 5) обстоятельства совершения преступления (обстановка, время, место, вид технологической операции при обработке информации); 6) следы совершения преступления (виртуальные либо материальные)<sup>33</sup>.

---

<sup>30</sup> Вехов, В.Б. Электронная криминалистика: понятие и система / В.Б. Вехов // Криминалистика: актуальные вопросы теории и практики: сб. трудов участников междунар. науч.-практич. конф. – Ростов н/Д., 2017. – С. 41.

<sup>31</sup> Россинская, Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е.Р. Россинская // Вестник Восточно-сибирского института МВД России. – 2019. – № 2(89). – С. 200.

<sup>32</sup> Иванов, Н.А. Экспертиза электронных документов и машинограмм / Н.А. Иванов. – М: Юрлитинформ, 2009. – С. 8–135.

<sup>33</sup> Степаненко, Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко, В.В. Коломинов // ГлаголЪ правосудия. – 2018. – №3 (17). – С. 38–43.

Одним из важнейших элементов механизма преступления и криминалистической характеристики методики его расследования является способ преступления, под которым с современных позиций понимается детерминированная личностью, предметом и обстоятельствами преступного посягательства система действий субъекта, направленная на достижение преступной цели и объединенная единым преступным замыслом. Способы преступления делятся на полноструктурные, включающие подготовку, совершение и сокрытие, и неполноструктурные, когда один или два элемента отсутствуют<sup>34</sup>.

К основным способам киберпреступлений многие ученые относят следующие: 1) способы, направленные на сокрытие несанкционированного доступа к компьютерным средствам и системам, – использование VPN-сервисов (англ. Virtual Private Network – виртуальная частная сеть), многослойного шифрования с помощью системы прокси-серверов для анонимного сетевого подключения, технологии Bootkit, Rootkit и т.п.; 2) использование троянских программ различного назначения позволяет преступникам создавать бот-сеть из зараженных компьютеров и использовать ее для сокрытия своего IP-адреса, в криминалистическом плане такая программа является орудием совершения преступления; 3) заражение компьютерных систем вирусами; 4) использование аппаратно-программных комплексов для массовых кампаний распространения вредоносного программного обеспечения на мобильные устройства; 5) компьютерных атак на локальные корпоративные сети и др. Таким образом, появление новых программно-аппаратных средств, развитие телекоммуникационных технологий способствует распространению высокотехнологичных способов совершения киберпреступлений.

Еще одним важным элементом криминалистической характеристики киберпреступлений являются следы и вещественные доказательства преступлений, а соответственно и особенности слеодообразования в киберпространстве, применения специальных технических средств, позволяющих выявлять и закреплять в нем доказательственную и иную криминалистически значимую информацию<sup>35</sup>. Следы могут быть как пассивные (техническая информация использования электронных устройств и др.), так и активные (следы действий, совершенных непосредственным пользователем: фото, записи)<sup>36</sup>. Особенности поиска, обнаружения, фиксации и изъятия цифровой информации в ходе следственных действий обуславливаются спецификой электронно-цифровых следов (наличие новой среды отражения преступления – цифрового виртуального пространства, носителя цифровой информации – специального технического устройства, передача по каналам связи и др.). Появилась группа таких доказательств – носителей виртуальной информации – электронные документы, элементы интернет-порталов, цифровые объекты – виртуальные машины и торрент-трекеры<sup>37</sup>. Обеспечение результативности и эффективности работы с такими следами и объектами возможно путем

---

<sup>34</sup> Россинская, Е.Р., Рядовский, И.А. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский // Московский государственный юридический университет имени О.Е. Кутафина (МГЮА) «Lex russica (Русский закон)» – 2019. № 3(148). – С. 87.

<sup>35</sup> Ищенко, Е.П. Криминалистические аспекты расследования киберпреступлений / Е.П. Ищенко // Уголовное производство: процессуальная теория и криминалистическая практика: материалы V Международной научно-практической конференции, 27–29 апреля 2017 года, г. Симферополь-Алушта / отв. Ред. М.А. Михайлов, Т.В. Омельченко ; Крымский федеральный университет имени В.И. Вернадского. – Симферополь: ИТ «АРИАЛ», 2017. – С. 62–64.

<sup>36</sup> Криминалистика: учебник / под ред. Т.А. Седовой, С.П. Кушниренко, В.Д. Пристанкова. – М.: ЮСТИЦИЯ, 2019. – С. 19.

<sup>37</sup> Ищенко, Е.П. К вопросу об экспертном и криминалистическом обеспечении расследования киберпреступности / Е.П. Ищенко // Вестник Московского университета МВД России, – 2013. – № 3. – С. 15–17.

применения современной криминалистической техники, позволяющей извлекать криминалистически значимую информацию с любых мобильных устройств, планшетов, навигаторов и т.д.

Таким образом, решение рассмотренных актуальных криминалистических проблем будет способствовать: совершенствованию методологических основ криминалистики в сфере раскрытия, расследования и предупреждения киберпреступлений; разработке современных методов, криминалистических средств и технологий их применения при осуществлении указанной деятельности; созданию новых действенных методических рекомендаций по расследованию киберпреступлений; решению других актуальных вопросов уголовно-процессуального, криминалистического, оперативно-розыскного характера, судебного разбирательства по таким уголовным делам.

Многие ученые считают, что необходима систематизация всех достижений криминалистики, переоценка с учетом реалий сегодняшнего дня, выделение ценного и ожидающего своего дальнейшего поступательного развития знания. «Особую актуальность эти задачи приобретают в деле имплементации в научные ресурсы отечественной криминалистики новых сведений, основанных на использовании современных компьютерных и сетевых технологий»<sup>38</sup>.

## **2. Использование современных криминалистических технологий при обнаружении, фиксации, изъятии следовой информации преступлений в сфере современных информационно-коммуникационных технологий**

Качественное и результативное применение криминалистических технологий при расследовании преступлений в сфере информационно-коммуникационной безопасности позволяет осуществить предусмотренные уголовно-процессуальным кодексом задачи уголовного процесса в Республике Беларусь: собрать доказательства, как уличающие, так и оправдывающие обвиняемого; установить обстоятельства, имеющие значение для правильного разрешения дела, защиты прав и законных интересов участвующих в уголовном деле лиц, а также выдвинуть версии, избрать пути их проверки и реализации, а иногда и вынести суждение о самом характере происшедшего события.

Собирание доказательств – это понятие комплексное, включающее действия по обнаружению, фиксации, изъятию и сохранению доказательств. Следы – важное средство установления объективной истины по делу, поэтому работа с материальными следами на месте происшествия – исходный и наиболее важный момент раскрытия и расследования преступлений<sup>39</sup>. При этом качество и полнота извлечения криминалистически значимой информации при проведении следственных действий находится в прямой зависимости, во-первых, от выбора криминалистических технологий, применяемых для выявления, фиксации и изъятия следов преступления и вещественных доказательств; и, во-вторых, от уровня квалификации лица, их использующего. Несмотря на большое разнообразие криминалистических технологий, имеющихся на вооружении правоохранительных органов Беларуси, существование теоретических знаний и практических рекомендаций относительно их использования для обнаружения, фиксации и изъятия следов и объектов преступления, на практике иногда возникают проблемы с их применением, что препятствует достижению эффективности следственного действия. По нашему мнению, указанный факт является значительным пробелом, поскольку четкое

---

<sup>38</sup> Шаталов, А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции / А.С. Шаталов // Вестник Сибирского юридического института МВД России. – 2018. – № 3(32). – С. 7–15.

<sup>39</sup> Карлов, В.Я. Использование криминалистической техники в расследовании преступлений: науч.-практ. пособие / В.Я. Карлов; Моск. акад. экономики и права. – М.: Экзамен, 2006. – С. 112, 119.



понимание технологий позволит обеспечить достижения главной цели – оказание помощи в раскрытии и расследовании преступлений.

В криминалистической литературе отсутствует единообразие в определении понятия «криминалистическая технология» расследования преступлений в целом и осмотра места происшествия в частности. У ученых существуют различные мнения относительно понятия «технология»: одни авторы под технологией понимают какой-либо способ действия (Р.С. Белкин, В.Г. Болычев), др. – процесс использования средств, методов и приемов (А.М. Зинин, Н.П. Майлис), третьи – систему определенных элементов (А.А. Калмыков). Так, по мнению Р.С. Белкина, технология – это наиболее целесообразный и эффективный *способ* осуществления неких трудовых операций в должной последовательности, когда исполнителю не оказывается противодействия. Поэтому в учебнике 1999 г. он включил в название двух разделов – техники и тактики – указание на технологию: «Криминалистическая техника и технология» и «Криминалистическая тактика и технология» с соответствующими изменениями и в названия некоторых глав<sup>40</sup>. В.Г. Болычев отмечает, что понятие «технология» отражает специфику способа применения именно технических средств и в него обоснованно трансформируется универсальная категория, применяемая во всех отраслях научно-технического знания, – метод<sup>41</sup>. А.М. Зинин, Н.П. Майлис под экспертной технологией понимают совокупность операций, действий, осуществляемых в определенной последовательности на основе специальных знаний<sup>42</sup>, представляющих конкретный процесс. А.А. Калмыков определяет технологию как социальную систему, ориентированную на достижение цели гарантированного производства стандартной продукции<sup>43</sup>. В.А. Юматов, являясь представителем криминалистическо-технологического подхода, отмечает, что криминалистическая технология есть, прежде всего, система инструктивных предписаний выражения знаний и опыта, позволяющая рационально организовать получение проектного результата. Соглашаясь с М. Марковым, он подчеркивает, что технология – это процесс, осуществляемый людьми путем разделения его на систему последовательных взаимосвязанных процедур и операций. При этом под процессом В.А. Юматов понимает последовательность действий, согласованных с условиями выполнения технологических операций с использованием соответствующих средств, направленных на получение запланированного результата. Криминалистическая технология, по его мнению, представляет собой неразрывно связанный комплекс последовательных процедур, которые выполняются нормативно зафиксированными способами действий с целью достижения запланированной эффективности деятельности по выявлению и расследованию преступлений. В.А. Юматов обоснованно структурирует криминалистическую технологию в виде системы элементов, состоящей из этапов, операций и действий<sup>44</sup>. Таким образом, соглашаясь с суждением указанных авторов, можно сделать вывод о том, что вышеприведенные определения технологии объединяют в единый механизм

---

<sup>40</sup> Белкин, Р.С. Криминалистика: проблемы сегодняшнего дня. Злободневные вопросы российской криминалистики / Р.С. Белкин. – М.: Норма: Инфра-М, 2001. – С. 85.

<sup>41</sup> Болычев, В.Г. Применение научно-технических средств в процессуально-тактической деятельности следователя: автореф. дис. ... канд. юрид. наук: 12.00.09 / В.Г. Болычев ; Воронеж. гос. ун-т. – Воронеж, 2012. – С. 14.

<sup>42</sup> Зинин, А.М., Майлис Н.П. Судебная экспертиза / А.М. Зинин, Н.П. Майлис. – М., 2002. – С. 126.

<sup>43</sup> Калмыков, А.А. Системный анализ образовательных технологий / А.А. Калмыков. – Пермь : изд-во ПермГУ, 2002. – С. 16–21.

<sup>44</sup> Юматов, В.А. Технологические и организационные аспекты оптимизации деятельности специалистов и экспертов в уголовном судопроизводстве: дис. ... канд. юрид. наук: 12.00.09 / В.А. Юматов. – Н. Новгород, 2006. – Л. 27, 28.

существующие термины «метод», «способ», «прием», «методика». Представляется, что в аспекте данной темы следует использовать системный подход и следующие *исходные ориентиры* для формирования криминалистической технологии осмотра места происшествия: *во-первых*, технология – это наиболее целесообразный и эффективный *способ* осуществления неких трудовых операций в должной последовательности (Р.С. Белкин); *во-вторых*, технология – это специфичность способа (метода) применения именно технических средств (В.Г. Большев); *в-третьих*, технология – это совокупность операций, действий, осуществляемых в определенной последовательности на основе специальных знаний (А.М. Зинин, Н.П. Майлис), т.е. процесс; *в-четвертых*, технология – это система, ориентированная на достижение цели (А.А. Калмыков); *в-пятых*, неразрывно связанный комплекс последовательных процедур, которые выполняются нормативно зафиксированными способами действий с целью достижения запланированной эффективности деятельности (В.А. Юматов).

Однако выявленные исходные ориентиры для определения криминалистической технологии расследования киберпреступлений имеют ярко выраженный *технический акцент* и не включают тактических положений использования технологий. Заслуживает внимания точка зрения Ф.Г. Аминева, который считает, что криминалистические технологии в осмотре места происшествия – это непрерывный *процесс* использования комплекса современных технико-криминалистических средств и методов, тактико-криминалистических приемов в условиях дефицита времени, необходимости решения значительного числа сложных мыслительных задач при крайней недостаточности информации о событии преступления<sup>45</sup>. На основе анализа и обобщения всех приведенных точек зрения, с учетом выявленных исходных ориентиров предлагается следующее определение понятия криминалистических технологий осмотра места происшествия. *Криминалистические технологии осмотра места происшествия – это непрерывный процесс использования субъектами его криминалистического обеспечения комплекса современных технико-криминалистических средств; целесообразных, эффективных способов и методов, тактико-криминалистических приемов их применения в должной последовательности, в условиях дефицита времени, необходимости решения значительного числа сложных мыслительных задач при крайней недостаточности информации о событии преступления в целях получения максимально полной и необходимой информации по расследуемому преступному событию, от применения которого зависит эффективность следственного действия и расследования в целом.* Представляется, что данное определение криминалистических технологий наиболее точно отражает сущность технологического компонента криминалистического обеспечения осмотра места происшествия во взаимосвязи с технико-тактическими аспектами.

В структуре системы технико-криминалистического обеспечения следственных действий, по нашему мнению, криминалистические технологии отражают механизм деятельности субъекта данной системы по использованию конкретных методов, способов, приемов и средств в определенной последовательности. С учетом предложенной нами систематизации технико-криминалистических средств осмотра места происшествия<sup>46</sup> можно сказать, что технологии их использования включают применение средств для: 1) обнаружения следов преступления, 2) их фиксации, 3) изъятия следов преступления.

---

<sup>45</sup> Аминева, Ф.Г. Об использовании криминалистических технологий при осмотре места происшествия / Ф.Г. Аминева // Российский следователь. – 2009. – № 20. – С. 3.

<sup>46</sup> Дмитриева, Т.Ф. Система технико-криминалистических средств, используемых при осмотре места происшествия / Т.Ф. Дмитриева // Вестн. Акад. МВД Респ. Беларусь. – 2013. – № 1. – С. 42–45.

1. *Криминалистические технологии обнаружения следов и объектов преступления*, по нашему мнению, включают пять групп технологий применения средств для обнаружения: 1) следов папиллярных узоров (рук и ног); 2) микрообъектов; 3) металлических предметов; 4) неметаллических следов и объектов (трупов или их частей); следов биологического происхождения; пылевидных частиц от обуви на текстильных изделиях; взрывчатых, наркотических и химических веществ; человека; тайников); 5) аудио-, видеозаписей или фотоизображений<sup>47</sup>. Наибольший интерес в контексте темы представляет группа *криминалистической технологии обнаружения неметаллических следов и объектов*, которая среди многих<sup>48</sup> включает применение средств для отыскания цифровых следов; аудио-, видео-изображений или фотоизображений. *Технологии обнаружения цифровых следов, аудио-, видеозаписей или фотоизображений* включают методы работы с такими элементами материальной обстановки места его совершения, как электронные приборы с функцией памяти (телефонные аппараты, смартфоны, планшеты и иные), обладающие свойством сохранять в электронной памяти вводимую владельцем информацию личного характера, а также сведения об обстоятельствах их эксплуатации. При ОМП можно обнаружить объекты, содержащие уголовно релевантные записи, созданные различными электронными цифровыми средствами, к которым относятся цифровые регистраторы речи и камеры видеонаблюдения (том числе различные web-камеры), а также мобильные телефоны, системы IP- и Интернет-телефонии и иные средства пакетной передачи оцифрованной речи.

2. *Криминалистические технологии фиксации следов и объектов преступления* представляют систему действий субъектов поисково-познавательной деятельности, направленной на процессуальное, криминалистическое и оперативное запечатление информации в установленной законом и подзаконными актами форме. Криминалистическая фиксация осуществляется в четырех формах: вербальной, графической, наглядно-образной и предметной. *Вербальная форма* фиксации объединяет протоколирование и звукозапись. *Описание в протоколе* является методом комплексным, в результате использования которого воспроизводится и запечатлевается информация, воспринимаемая всеми рецепторами человека – зрительным, слуховым, обонятельным, осязательным и вкусовым. Протокол ОМП является источником доказательства по делу, поэтому в нем полно и объективно отражаются ход и результаты осмотра с соблюдением соответствующих правил<sup>49</sup>. Сущность *фоноскопического* метода (звукозаписи) состоит в том, что специальное электронно-механическое устройства (магнитофон, диктофон и др.) преобразует физические свойства устной речи в составляющие ее фонемы, в систему электромагнитных колебаний – фонограмму, а фонограмму – обратно в устную речь. *Графическая форма* проявляется в измерении, составлении *планов, схем, чертежей и зарисовок*. *Наглядно-образная форма* фиксации заключается в фото- и видеосъемке, осуществляемой в ходе ОМП по правилам судебной фотографии, с использованием различных технических средств, в том числе цифровых устройств и возможностей голографии. Интересным и перспективным является предложение Э.А. Ли о создании с помощью специализированной компьютерной программы панорамной, трехмерной и масштабной модели, максимально воссоздающей материальную обстановку места происшествия, которая сможет восприниматься с разных ракурсов, визуализироваться в изменяющемся масштабе. Такая программа предполагает применение цифро-

---

<sup>47</sup> Дмитриева, Т.Ф. Криминалистическое обеспечение осмотра места происшествия: монография / Т.Ф. Дмитриева; под науч. ред. Е.И. Климовой. – Витебск: ВГУ имени П.М. Машерова, 2016. – С. 131–136.

<sup>48</sup> Там же. – С. 136–138.

<sup>49</sup> Там же. – С. 142.

вой фото- и видеосъемки, а также лазерного сканирования места происшествия<sup>50</sup>. Предметная фиксация обнаруженных при ОМП следов и объектов осуществляется путем изъятия самого предмета – носителя следа, способом консервирования объекта или моделирования его свойств и качеств.

3. *Криминалистическая технология изъятия следов и объектов преступления.* Целью изъятия, также как и фиксации, является сохранение определенных свойств и качеств обнаруженных при ОМП объектов. Отличие изъятия от фиксации заключается в различии путей решения стоящей перед ними общей задачи – сохранения определенных качеств, свойств и признаков объектов, имеющих значение для установления истины по делу. При проведении ОМП возникает необходимость в изъятии самых разнообразных следов и объектов, находящихся в твердом, полутвердом, жидком, газообразном состоянии. Выбор ТКСр для изъятия обнаруженных при ОМП следов и объектов зависит от их природы, свойств, качеств и преследуемых целей. Их делят на средства, предназначенные для изъятия твердых объектов (отвертки, стеклорезы и т.п.), жидкостей (медицинская аппаратура, сосуды, марля и т.д.), сыпучих (совки, ситечки и др.), газообразных веществ (путем консервации – с помощью шприца и иглы, путем адсорбции – с помощью фрагмента ткани, фольги, банки), микрообъектов (специальные пленки, пинцеты, пробирки и пр.). Упаковка – один из окончательных этапов собирания следов или объектов, от которого, порой, зависит сохранение результатов всех предыдущих этапов собирания (обнаружения, фиксации, изъятия) и характер исходных данных. Она выполняется с соблюдением определенных требований и гарантирует защиту изъятых следов (объектов) от изменений и возможной подмены.

Новизна представленных криминалистических технологий для обнаружения, фиксации и изъятия следов и объектов преступления заключается, во-первых, в группировке криминалистических знаний с учетом исследуемого вопроса соответственно предложенной ранее системе технико-криминалистических средств; во-вторых, в использовании знаний о современных направлениях развития и возможностях их использования при проведении следственных действий с целью достижения их результативности. Используя предложенные технологии обнаружения, фиксации и изъятия следов и объектов преступления, субъект его криминалистического обеспечения становится более подготовленным для дифференцированного подхода к выбору совокупности конкретных технологий и последовательности применения средств, требующих владения значительными объемами теоретических знаний и практических навыков для получения качественно более полной и содержательной информации о преступнике, механизме совершения преступления в каждом конкретном случае.

### **3. Современные возможности применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий**

Ход и результаты расследования преступлений в сфере информационно-коммуникационной безопасности в значительной степени зависят от полноты и качества полученной в ходе осмотра места происшествия криминалистически значимой информации о преступнике и преступлении, на основе которой строится информационная модель расследуемого события, а эффективность деятельности в этом направлении определяется объемом и достоверностью имеющейся информации<sup>51</sup>.

---

<sup>50</sup> Ли, Э.А. Совершенствование использования компьютерных технологий в расследовании преступлений: автореф. дис. ... канд. юрид. наук: 12.00.09 / Э.А. Ли; Кыргыз. гос. юрид. акад. при Правительстве Кыргыз. Респ. – Бишкек, 2011. – С. 19.

<sup>51</sup> Карлов, В.Я. Современное состояние и перспективы совершенствования организации и правового регулирования использования криминалистической техники в расследовании преступлений: дис. ... канд. юрид. наук: 12.00.09 / В.Я. Карлов. – М., 2004. – Л. 147.

Организация деятельности по собиранию доказательств при проведении следственного действия с участием специалиста – одна из основных функций управления следственными и экспертными органами, заключающаяся в упорядочении, планировании этой деятельности, придании согласованности ее взаимодействующим элементам. К отдельным методам осуществления данной деятельности В. А. Снетков относит контроль качества изымаемых доказательств (полноту собирания доказательств; их относимость к событию преступления; сохранность объектов в неизменном состоянии; соблюдение правил их обнаружения, фиксации, исследования, изъятия и упаковки) и анализ деятельности по доказыванию<sup>52</sup>.

В соответствии со ст. 11 Закона «О Государственном комитете судебных экспертиз Республики Беларусь» одним из направлений деятельности данного ведомства является криминалистическое обеспечение расследования преступлений, включающее в себя контроль за реализацией мероприятий по поддержанию на надлежащем уровне эффективности использования технических средств; определение критериев оценки эффективности судебно-экспертной деятельности; анализ форм, методов, результативности участия сотрудников (лиц гражданского персонала из числа судебных экспертов) в следственных, других процессуальных действиях и оперативно-розыскных мероприятиях, результативности использования криминалистических учетов и коллекций, технических средств и криминалистических методов; организация и реализация мероприятий по повышению эффективности данной работы. Контроль качества этой деятельности заключается в собирании, систематизации, анализе, хранении и использовании информации об эффективности применения технико-криминалистических средств субъектами системы криминалистического обеспечения осмотра места происшествия.

Технологии реализации механизма контроля качества данной системы в криминалистике уделяется недостаточно внимания, хотя ее значение в современных условиях все более возрастает. Весь огромный массив информации по криминалистическому обеспечению осмотра места происшествия нуждается в переработке, вычленении из него криминалистически значимой информации. Это позволит осуществить оценку полноты, качества, эффективности и результативности применения криминалистических технологий; проконтролировать своевременность и полноту исследования изъятых материальных следов преступления, обеспечить использование полученной информации в расследовании противоправных деяний. Такие непростые задачи не могут быть решены без хорошо поставленной информационно-аналитической работы, для чего необходима разработка единой республиканской автоматизированной информационно-поисковой системы (далее – АИПС), способствующей осуществлению всех этих действий.

Задачи технологизации следственных действий, расследования преступлений в целом, экспертных исследований в форме реализации механизмов новаций и развития решаются на протяжении всего существования криминалистики. Тем или иным проблемам, сопряженным с математизацией и автоматизацией решения криминалистических задач, посвящены работы Л.Е. Ароцкера, Р.С. Белкина, А.И. Винберга, Г.Л. Грановского, Г.Г. Зуйкова, З.И. Кирсанова, В.Н. Кудрявцева, И.Д. Кучерова, И.М. Лузгина, Р.М. Ланцмана, В.С. Митричева, Н.С. Полевого, В.А. Пошквичуса, В.А. Снеткова, А.Р. Шляхова, Л.Г. Эджубова, А.А. Эйсмана и др. авторов. Вместе с тем ряд вопросов, связанных с внедрением в деятельность по расследованию преступлений информаци-

---

<sup>52</sup> Деятельность экспертно-криминалистических подразделений органов внутренних дел по применению экспертно-криминалистических методов и средств в раскрытии и расследовании преступлении: учеб. пособие / В.А. Ивашков [и др.]; Эксперт.-криминалист. центр МВД Рос. Федерации. – М.: ЭКЦ МВД РФ, 1996. – С. 25–26.

онных систем, не нашел достаточно полного отражения в научных исследованиях. Это произошло вследствие того, что в литературе сложилось два подхода к изучению АИПС. С одной стороны, в работах, посвященных общим вопросам применения правоохранительными органами средств и методов кибернетики и информатики, данная проблема не является объектом детального самостоятельного анализа. В основном подобные исследования ведутся в рамках общетеоретического раздела криминалистической кибернетики. С другой стороны, информационные системы исследуются применительно к отдельным видам деятельности (например, к экспертизе)<sup>53</sup>. Из-за недостаточной технической оснащенности деятельности следователей и экспертов ранее преобладали устаревшие приемы и методы информационной работы, не предпринимались необходимые меры по широкому внедрению в практику передовых форм и методов, мало использовались сведения, хранящиеся в различных информационных системах. Сложившаяся практика формирования и накопления криминалистической информации в виде журнального учета не способствует ее эффективному применению в расследовании преступлений; влечет за собой принятие не всегда обоснованных решений, отсутствие должной мобильности в реагировании на изменения оперативной обстановки, эффективного контроля и т.п.

Во всех развитых странах на основе современных информационных технологий создаются специальные АИПС, в том числе криминалистического назначения, в развитии которых наблюдается ряд общих тенденций. Это возрастающие темпы роста объемов информационных банков данных; расширение перечня источников криминалистически значимой информации, сосредотачиваемых в них; интеграция различных банков данных в единую информационную систему; развитие территориальных, ведомственных и централизованных АИПС; разработка средств и методов ограничения доступа к информации, исключающих несанкционированное ее использование.

В условиях компьютеризации всех государственных структур существует реальная необходимость создания современной технологии реализации механизма контроля качества криминалистического обеспечения расследования киберпреступлений. Одним из решений данной проблемы может быть формирование единой АИПС республиканского масштаба, способной стать методико-криминалистическим средством повышения эффективности расследования преступлений. Она должна иметь вид современной информационной модели, правильно определить пути и механизмы реализации основных направлений повышения эффективности расследования. Собранная в АИПС криминалистическая информация может и в дальнейшем использоваться как экспертами, следователями, так и сотрудниками других структур правоохранительной системы для обеспечения расследования преступлений. В свете реализации требований ведомственных нормативных правовых актов по сокращению документооборота в государственных органах использование АИПС на современном этапе приобретает еще большую актуальность.

Стремительно возросшие сегодня возможности автоматизации, появление новых компьютерных технологий и гаджетов требуют создания принципиально нового программного продукта республиканского масштаба, позволяющего оперативно, мобильно и продуктивно осуществлять контроль качества реализации криминалистического обеспечения расследования киберпреступлений следующим образом: 1) рационализировать процесс получения, обработки, анализа информации и выявления пред-

---

<sup>53</sup> Пацкевич, А.П. Перспективы создания автоматизированных информационно-поисковых систем криминалистического назначения в Беларуси / А.П. Пацкевич // Проблемы криминалистики: сб. науч. тр. / Акад. МВД Респ. Беларусь; редкол.: Г.И. Грамович [и др.]; отв. ред. Г.Н. Мухин. – Минск, 2007. – Вып. 5. – С. 105–114.

ставляющих интерес преступлений, по которым осмотр места происшествия проводился без сотрудника (работника) ГКСЭ; 2) оптимизировать механизм контроля соблюдения учетно-регистрационной дисциплины путем обработки информации об обнаруженных и изъятых в ходе осмотра места происшествия следах преступления и иных объектах; 3) обеспечить процесс получения и обработки информационного потока о полноте, всесторонности, эффективности и результативности применения криминалистических технологий при осмотре; 4) реально осуществить распознавание и систематизацию значимого для расследования информационного массива, минимизировав временные затраты; 5) значительно облегчить процесс аналитической обработки полученных данных, выдвижения версий и планирования; 6) осуществить контроль своевременности назначения и проведения экспертных исследований каждого из изъятых с места происшествия материальных следов преступления; 7) обеспечить контроль результативности использования информационного блока криминалистических учетов и коллекций Государственного комитета в выявлении и расследовании преступлений; 8) внедрить принцип взаимообмена информацией о криминалистическом обеспечении осмотра места происшествия между ГКСЭ, Следственным комитетом, органами внутренних дел Республики Беларусь. На наш взгляд, современная АИПС по реализации механизма контроля качества использования криминалистических технологий при расследовании преступлений должна включать следующее: во-первых, создание возможности просмотра фото- и видеоизображений осмотра места происшествия, что обеспечит наглядность и позволит увеличить диапазон механизма контроля качества работы на местах происшествий; во-вторых, изучение и ведомственное правовое закрепление возможности замены данным автоматизированным технологическим ресурсом существующего сегодня журнального учета участия экспертов в качестве специалистов в осмотре места происшествия, что, несомненно, обеспечит существенную экономию времени и денежных средств; в-третьих, создание условий и возможности внедрения соответствующего программного продукта во все заинтересованные в данном информационном массиве подразделения Следственного комитета и правоохранительных органов Республики Беларусь; в-четвертых, изучение возможностей объединения АИПС с Единым Банком данных о правонарушениях и преступлениях в Республике Беларусь на платформе ее Единого информационного пространства с целью предоставления доступа к информационному банку данных о криминалистическом обеспечении осмотра места происшествия любого из преступлений. При расследовании киберпреступления субъект криминалистического обеспечения заполняет технологическую карточку, содержащую информацию как о следственном действии, так и о результатах применения криминалистических технологий. К основным ее сведениям целесообразно отнести: 1) номер карточки и дату ее заполнения; 2) орган и дату поступления заявления о совершенном преступлении; 3) период, способ совершения и вид преступления; 4) дату, время, адрес проведения осмотра места происшествия, краткие данные о потерпевшем; 5) персональные данные субъекта криминалистического обеспечения осмотра места происшествия; 6) результаты изъятия при осмотре места происшествия всех видов следов и объектов; 7) использование криминалистических учетов (АДИС, АСПИ «Портрет-2005» и др.); 8) исследование изъятых при осмотре места происшествия следов преступления и иных объектов; 9) факт установления подозреваемого (обвиняемого) лица<sup>54</sup>. Одним из важных условий при выборе программного обеспечения для создания АИПС должна быть простота ввода информации, ее поиска, обработки, внесения изме-

---

<sup>54</sup> Дмитриева, Т.Ф. Криминалистическое обеспечение осмотра места происшествия: монография / Т.Ф. Дмитриева ; под науч. ред. Е.И. Климовой. – Витебск: ВГУ имени П.М. Машерова», 2016. – С. 162.

нений, формирования вывода и возможности использования результатов на любом современном гаджете без применения специальных знаний в области программирования.

Следовательно, постоянная доступность актуальной информации об эффективности применения криминалистических технологий даст возможность оценить текущее положение дел, получить полную информацию о каждом конкретном осмотре в статике и динамике, принять грамотное решение по осуществлению мер регулирования, своевременному устранению недоработок и повышению качества применения криминалистических средств. Внедрение в практику Государственного комитета, Следственного комитета и правоохранительных органов Республики Беларусь компьютерных технологий несомненно позволит сократить временные затраты сотрудников данных подразделений, сроки расследования уголовных дел, повысить уровень криминалистического обеспечения расследования преступлений.

*Перспективы использования современных криминалистических технологий расследования преступлений в сфере информационно-коммуникационной безопасности* указывают на следующие пути данной деятельности: во-первых, совершенствование уголовно-процессуального законодательства Республики Беларусь в части законодательного закрепления ответственности специалистов за некачественную и нерезультативную криминалистическую работу на месте происшествия; во-вторых, создание Единого государственного информационно-программного продукта в виде реестра экспертов, техников-криминалистов, допущенных к самостоятельному участию в проведении осмотра места происшествия для оптимизации процесса ситуационного поиска нужного специалиста соответствующего профиля; в-третьих, создание в Республике Беларусь современного автоматизированного компьютерного продукта в виде системного комплекса объемно материализованных криминалистических знаний по применению криминалистических технологий расследования преступлений в сфере информационно-коммуникационной безопасности; в-четвертых, разработку инструктивных и рекомендательных документов по применению криминалистических технологий расследования преступлений в сфере информационно-коммуникационной безопасности сотрудниками (работниками) следственных, экспертных и других правоохранительных органов.

1. Основной целью использования специальных знаний специалиста в следственных действиях является содействие следователю в обнаружении, закреплении и изъятии доказательств, которое осуществляется путем применения технических средств и использования научно обоснованных способов. Между тем, ответственность за нерезультативную криминалистическую работу в ходе осмотра места происшествия в законодательстве Республики Беларусь не предусмотрена, что, на наш взгляд, требует совершенствования. Из УПК Республики Беларусь закон от 5 января 2008 года исключил ст. 133, ранее предусматривавшую для специалиста, эксперта и других участников денежное взыскание за неисполнение без уважительных причин процессуальных обязанностей и неподчинение законным распоряжениям органа, ведущего уголовный процесс<sup>55</sup>. Таким образом, в настоящее время в Республике Беларусь законодателем не предусмотрена никакая норма об ответственности за невыполнение своих процессуальных обязанностей или за их некачественное выполнение, а тем более норма об ответственности специалиста за отказ или уклонение от выполнения своих обязанностей, а также за дачу ложных пояснений и за заведомо неправильные действия, которые повлекли или могли повлечь утрату доказательств. Между тем, представляется верным

---

<sup>55</sup> Уголовно-процессуальный кодекс Республики Беларусь от 16 июля 1999 года № 295-3 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информации Республики Беларусь. – Минск, 2022.



мнение В.Н. Махова о том, что, участвуя в осмотре места происшествия, имея непосредственное отношение к обнаружению, фиксации и изъятию следов преступления и вещественных доказательств, специалист может безвозвратно причинить большой ущерб расследованию, если недобросовестно отнесется к исполнению своих обязанностей, даст заведомо неправильные пояснения по поводу выполняемых им действий, совершит повреждение или уничтожение доказательств, с учетом чего предлагается в УК предусмотреть норму об уголовной ответственности за данные действия<sup>56</sup>. В литературе имеются различные предложения о возможности привлечения специалиста к уголовной ответственности. Так, А.А. Новиков с целью фиксации процессуального положения специалиста в уголовном судопроизводстве и обеспечения возможности применения к нему мер процессуального принуждения, предлагал внести дополнение в УПК Российской Федерации о предупреждении специалиста об уголовной ответственности за дачу заведомо ложного заключения или ложных показаний<sup>57</sup>. И.Н. Сорокотягин для получения дополнительных гарантий добросовестного и объективного выполнения специалистом возложенных на него обязанностей предлагал ввести в УПК РСФСР статью, предусматривающую ответственность специалиста за умышленное уничтожение вещественных доказательств, а также за заведомо неправильные ответы на вопросы следователя и суда<sup>58</sup>. На наш взгляд, целесообразно в УК Республики Беларусь предусмотреть норму «об уголовной ответственности специалиста за отказ или уклонение от выполнения своих обязанностей, а также за предоставление заведомо ложных сведений и за заведомо неправильные действия, которые повлекли или могли повлечь утрату следов преступления и вещественных доказательств». Данная норма будет служить дополнительной гарантией добросовестности специалиста и в значительной степени способствовать как повышению результативности криминалистической работы по обеспечению качественной доказательственной информацией процесса расследования преступлений.

2. Анализ практики свидетельствует о том, что если в областных центрах следователи (лица, производящие дознание) способны оперативно выяснить сведения об интересующем их специалисте, то в районных звеньях такую информацию им зачастую взять неоткуда. Особенностью районных подразделений является малочисленность экспертов-криминалистов (специалистов). В случае отсутствия одного из них или сразу двух по причине некомплекта, отпуска, болезни, учебы и т.д. следователь (лицо, производящее дознание) не располагает оперативными сведениями, в каком регионе и какой компетенции имеются специалисты. С учетом результатов проведенного исследования и потребностей практики возможно предложить вариант решения обозначенной проблемы. Для повышения эффективности криминалистического обеспечения следственных действий в целом предлагаем оптимизировать использование специальных знаний на платформе Единого информационного пространства Республики Беларусь. Для этого следует снять информационную блокаду следователей и других сотрудников правоохранительных органов относительно оперативного получения информации об интересующем их специалисте и его компетенции.

---

<sup>56</sup> Махов, В.Н. Теория и практика использования знаний сведущих лиц при расследовании преступлений: дис. ... д-ра юрид. наук: 12.00.09 / В.Н. Махов. – М., 1993. – Л. 291.

<sup>57</sup> Новиков, А.А. Институт специалиста в уголовном судопроизводстве России: автореф. дис. ... канд. юрид. наук : 12.00.09 / А.А. Новиков; Калинингр. юрид. ин-т МВД России. – Калининград, 2007. – С. 7.

<sup>58</sup> Сорокотягин, И.Н. Криминалистические проблемы использования специальных познаний в расследовании преступлений: дис. ... д-ра юрид. наук: 12.00.09 / И.Н. Сорокотягин. – Екатеринбург, 1992. – Л. 9.

Наряду с решением вопроса о целесообразности привлечения специалиста к следственным действиям также будет способствовать созданию Единого государственного информационно-программного продукта в виде реестра экспертов, техников-криминалистов, допущенных к самостоятельному участию в проведении осмотра места происшествия для оптимизации процесса ситуационного поиска нужного специалиста соответствующего профиля. Аналоги названного реестра, существующие в других сферах деятельности, значительно облегчают работу, например, реестр врачей-специалистов, реестр аттестованных специалистов недвижимости, Белорусский реестр специалистов в области спортивного ориентирования. В реестр в качестве ключевых полей поиска специалистов целесообразно включить следующие составляющие: 1) специализацию (квалификацию по диплому и свидетельствам на право проведения экспертиз); 2) фамилию, имя, отчество; 3) наименование подразделения, учреждения, организации; 4) стаж работы; 5) номера всех свидетельств и дату их выдачи; 6) даты и темы прохождения стажировок и курсов повышения квалификации; 7) наличие ученой степени; 8) темы публикаций и прочее<sup>59</sup>. Форма этого реестра может представлять собой единый программный продукт с доступом к нему сотрудников правоохранительных органов, Следственного комитета всех регионов республики, организованной по аналогу успешно функционирующей единой государственной системы регистрации и учета правонарушений<sup>60</sup>. При этом ответственными за формирование и ведение реестра могут являться руководители подразделений и секретари квалификационных и экзаменационных комиссий, имеющие право выдавать допуски на проведение экспертиз и участие в осмотре. Предоставлять право на проведение экспертиз могут Государственный комитет судебных экспертиз Республики Беларусь (далее – ГКСЭ) и Академия МВД, а также другие государственные судебно-экспертные учреждения иностранных государств в соответствии с международными и межгосударственными договорами (соглашениями). Выдавать допуск к самостоятельному участию в качестве специалистов в осмотре места происшествия и иных следственных действиях может ГКСЭ. Предложенный реестр создаст оптимальные условия для принятия решений следователем (лицом, производящим дознание) и любым сотрудником правоохранительных органов о привлечении необходимого специалиста к участию в осмотре места происшествия и, несомненно, позволит повысить качество, эффективность и результативность его криминалистического обеспечения. К положительной стороне такого решения проблемы можно отнести экономию времени на организационные моменты, гарантию применения квалифицированных специальных знаний, участие компетентных лиц в данной работе.

3. Современный этап научно-технического прогресса выступает важнейшим источником совершенствования криминалистических технологий расследования преступлений. Повышение эффективности криминалистического обеспечения расследования преступлений во многом связано с отысканием средств устранения разрыва между высоким уровнем имеющихся научных разработок и объемом знаний, реально используемых в

---

<sup>59</sup> Дмитриева, Т.Ф. Криминалистическое обеспечение осмотра места происшествия : монография / Т.Ф. Дмитриева ; под науч. ред. Е.И. Климовой. – Витебск: ВГУ имени П.М. Машерова, 2016. – С. 168.

<sup>60</sup> О единой государственной системе регистрации и учета правонарушений: Закон Респ. Беларусь, 9 янв. 2006 г., № 94-З:// КонсультантПлюс. Беларусь [Электронный ресурс]: СПС «Беларусь» / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022; Об утверждении Положения о порядке функционирования единой государственной системы регистрации и учета правонарушений : Постановление Совета Министров Респ. Беларусь, 20 июля 2006 г., № 909 // КонсультантПлюс. Беларусь [Электронный ресурс]: СПС «Беларусь» / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

процессе этих действий. Выход из сложившейся ситуации может быть обеспечен в определенной мере посредством технологизации расследования преступлений, в частности посредством реализации на практике современных информационных технологий.

Под информационным обеспечением в криминалистике понимаются действия по выявлению и предоставлению (передаче) криминалистически значимой информации ее непосредственному пользователю, в том числе лицу, осуществляющему оперативно-розыскную, следственную, экспертную и иные виды деятельности для использования данной информации в целях расследования и предупреждения преступлений<sup>61</sup>. При этом для расследования преступлений необходимы фактически все виды информации, которыми являются: прогнозируемая информация, которая имеет вспомогательный характер и позволяет моделировать действия; обучающая, необходимая следователям, специалистам для закрепления их знаний, умений, навыков проведения следственных действий; справочная, содержащая важные для расследования преступления сведения; директивная, использование которой позволяет следователю решать организационные проблемы, связанные с расследованием; осуществлять должное взаимодействие со специалистом и другими участниками следственного действия; методическая, необходимая для эффективного проведения осмотра места происшествия, поскольку в ней содержатся сведения, касающиеся методики проведения данного следственного действия, а также рекомендации по осуществлению конкретных стадий осмотра места происшествия; аналитическая, которая предусматривает наличие и степень влияния криминогенных факторов, оказывающих отрицательное воздействие на процесс расследования преступлений; оперативно-служебная, включающая текущую документацию, жалобы и заявления граждан, в жилых квартирах которых проводится осмотр места происшествия; иную информацию, имеющую отношение к данному следственному действию; нормативно-правовая, использование которой необходимо для законного расследования преступления<sup>62</sup>.

Первые попытки разработать и применить программы расследования преступлений, предпринятые И.Н. Якимовым, не имели успеха ввиду отсутствия в то время средств реализации данных программ и возможностей машинной обработки большого объема информации относительно многовариантности следственных ситуаций. На различных временных этапах к проблемам алгоритмизации расследования преступлений обращались в своих работах Р.С. Белкин, М.Б. Вандер, Л.Г. Видонов, И.А. Возгрин, В.К. Гавло, Г.А. Густов, Л.Я. Драпкин, П.П. Ищенко, А.А. Леви, И.М. Лузгин, В.П. Лавров, В.А. Образцов, Н.С. Полевой, Н.А. Селиванов, Л.А. Соя-Серко, А.Г. Филиппов, А.С. Шаталов и многие другие ученые. Именно на первоначальном этапе расследования, когда неизвестны обстоятельства совершения преступления, необходимо применять заранее подготовленные алгоритмы и так называемые «сертифицированные методики», которые охватывают все типичные ситуации. Сегодня уже многие авторы говорят о новейших технических и технологических разработках, например: об осмотре места происшествия как об активной образовательной технологии применения имитационных обучающих методов в рамках общего курса криминалистики<sup>63</sup>; об интерактивном осмотре места происшествия с аутсенсуальными участниками следственного действия как о новейшей криминалистической технологии современного периода<sup>64</sup>; о вир-

---

<sup>61</sup> Белов, О.А. Информационное обеспечение раскрытия и расследования преступлений: монография / О.А. Белов. – М.: Юрлитинформ, 2009. – С. 36.

<sup>62</sup> Бульбачева, А.А. Информационное обеспечение осмотра места происшествия / А.А. Бульбачева // Публичное и частное право. – 2015. – № III. – С. 173.

<sup>63</sup> Телегина, Т.Д. «Осмотр места происшествия» как активная образовательная технология / Т.Д. Телегина // Вестн. Моск. ун-та. Сер. 11, Право. – 2014. – № 4. – С. 103–111.

<sup>64</sup> Королева, Д.В. Интерактивный осмотр места происшествия с аутсенсуальными участниками следственного действия как новейшая криминалистическая технология современного периода / Д.В. Королева // Законность и правопорядок в современном обществе. – 2014. – № 21. – С. 51–55.

туальном осмотре места происшествия как инновационном методе повышения профессионального мастерства следователей<sup>65</sup> и т.д.

На современном этапе в Республике Беларусь для обеспечения эффективности криминалистического обеспечения осмотра места происшествия, являющегося многогранным сложным следственным действием, жизненно необходимы разработка и использование аналогичной автоматизированной программы. Такой компьютерный продукт может представлять системный комплекс материализованных криминалистических знаний проведенного исследования, включающий организационный, технологический и оценочно-контрольный компоненты криминалистического обеспечения осмотра места происшествия. При моделировании различных мест происшествий (квартира, лестничная площадка, двор, улица в населенном пункте, поле, лес, парковая зона, железнодорожный вокзал и др.) и создании библиотеки различных объектов и следов моделируемого преступления (предметов интерьера, различных следов, орудий преступления, трупов и т.п.) целесообразно использовать технологическую карту работы специалиста на месте происшествия, предложенную В.А. Юматовым. Данная технологическая карта позволяет структурировать, придавать строгую логическую форму исходным сведениям и выступает как средство обобщения разнородных данных, как способ решения познавательной задачи по материальным следам преступления<sup>66</sup>. Таким образом, создание в Республике Беларусь предложенного программного продукта поможет не только моделировать следственную ситуацию и следовую информацию, но и составлять подробную схему прямо на реальном месте происшествия и реконструировать совершенное преступление, создавая видеoversию произошедшего, что естественно будет способствовать повышению эффективности криминалистического обеспечения не только осмотра места происшествия, но и расследования преступления в целом. В качестве примера материализации полученных результатов исследования можно предложить технологию формирования 3-D автоматизировано-прикладного интерактивного тренажера (ИПИТ) «Криминалистическое обеспечение осмотра места происшествия»<sup>67</sup>.

4. Разработка инструктивных и рекомендательных документов по применению криминалистических технологий расследования киберпреступлений для практического использования сотрудниками (работниками) следственных, экспертных и других правоохранительных органов, является важной информационной составляющей методического компонента системы криминалистического обеспечения расследования. К подобным рекомендательным документам следует отнести методические рекомендации по совершенствованию практики привлечения специалистов к участию в осмотре места происшествия киберпреступления; по совершенствованию практики применения криминалистических технологий; по совершенствованию криминалистического обеспечения расследования киберпреступлений.

---

<sup>65</sup> Елинский, В.И. Виртуальный осмотр места происшествия – инновационный метод повышения профессионального мастерства следователей / В.И. Елинский, Ф.М. Ашимов // Российский следователь. – 2013. – № 4. – С. 6–8; Муранов, М.Г. Компьютерная программа «Виртуальный осмотр места происшествия : учебно-методический комплекс / М.Г. Муранов // Криминалистика – прошлое, настоящее, будущее : достижения и перспективы развития : материалы Международной научно-практической конференции, приуроченной к 60-летию образования службы криминалистики (Москва, 16 октября 2014 года). – М.: Академия Следственного комитета Российской Федерации, 2014. – С. 80–83.

<sup>66</sup> Юматов, В.А. Технологические и организационные аспекты оптимизации деятельности специалистов и экспертов в уголовном судопроизводстве: дис. ... канд. юрид. наук: 12.00.09 / В.А. Юматов. – Н. Новгород, 2006. –Л. 54.

<sup>67</sup> Дмитриева, Т.Ф. Криминалистическое обеспечение осмотра места происшествия: монография / Т.Ф. Дмитриева; под науч. ред. Е.И. Климовой. – Витебск: ВГУ имени П.М. Машерова», 2016. – С. 172, 283–305.

Следовательно, для повышения эффективности применения криминалистических технологий расследования киберпреступлений необходимы:

1) совершенствование уголовного законодательства Республики Беларусь в части законодательного закрепления ответственности специалистов за некачественную и безрезультатную работу;

2) создание Единого государственного информационно-программного продукта в виде реестра экспертов, техников-криминалистов, допущенных к самостоятельному участию в проведении следственного действия, для оптимизации процесса ситуационного поиска нужного специалиста соответствующего профиля;

3) разработка в Республике Беларусь современного автоматизированного компьютерного продукта, представляющего системный комплекс объемно материализованных криминалистических знаний по криминалистическому обеспечению осмотра места происшествия, включающий организационный, технологический и оценочно-контрольный компоненты криминалистического обеспечения осмотра места происшествия, с возможностью моделирования различных мест происшествий и следовой информации, составления схемы на месте происшествия и создания видеoversии произошедшего;

4) создание инструктивных и рекомендательных документов по применению криминалистических технологий расследования киберпреступлений для практического использования сотрудниками (работниками) следственных, экспертных и других правоохранительных органов.

#### Тема 7

### ЦИФРОВАЯ КРИМИНАЛИСТИКА И ЕЕ ЗНАЧЕНИЕ ДЛЯ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СОВРЕМЕННОМ ИНФОРМАЦИОННОМ ОБЩЕСТВЕ

1. Понятие, проблемы терминологии, цели, задачи, функции электронной цифровой криминалистики.

2. Современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений.

3. Передовые практические методы расследования преступлений в области цифровой криминалистики.

#### **1. Понятие, проблемы терминологии, цели, задачи, функции электронной цифровой криминалистики**

*Цифровая криминалистика* – новый термин, который не является устоявшимся, и уже имеет синонимы, указанные ранее («электронная криминалистика», «компьютерная криминалистика» и т.д.). Вместе с тем, это настолько серьезная и перспективная адаптация подходов традиционной криминалистики к реалиям развития современного информационного общества, что правоохранительная практика требует как можно быстрее пройти путь научного становления этого направления и перейти к массовой практической реализации её положений при расследовании преступлений<sup>68</sup>.

Современные преступления совершаются де-факто в двух мирах, один из которых привычный нам мир материальных объектов, а другой – виртуальный. Мы погружены в этот виртуальный мир различными способами. Например, опосредованно – попадая в

---

<sup>68</sup> Яковлев, А.Н. Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе / А.Н. Яковлев // В сб. Совершенствование следственной деятельности в условиях информатизации: сб. материалов междунар. науч.-практ. конф. (Минск, 12–13 апреля 2018 г.) / Следственный комитет Республики Беларусь; редкол.: С.Я. Аземша [и др.]. – Минск: Редакция журнала «Промышленно-торговое право», 2018. – С. 357–362.

объективы систем видеонаблюдения, перенося мобильные телефоны, регистрируемые базовыми станциями сетей сотовой связи, используя карты накопления бонусных баллов в магазинах или устанавливая в автомобиль систему сигнализации с GSM-модулем и функцией трекинга маршрута. Также мы непосредственно взаимодействуем с объектами этого мира, потому что используем сеть Интернет как источник получения информации (сетевые СМИ), разнообразное программное обеспечение как инструмент для социальных связей, социальные сети «ВКонтакте», «Фейсбук» и др., инструмент для общения (мессенджеры WhatsApp, Telegram и т.п.), инструмент для решения профессиональных задач (офисные программы с поддержкой облачного хранения информации и другие). Подавляющее большинство современных устройств, используемых человеком, от мобильных телефонов до смарт-телевизоров, также хранят на своих электронных носителях и на внешних хранилищах информации следы использования человеком.

Безусловно, сегодня необходимо использовать цифровые следы в интересах раскрытия и расследования преступлений и установления истины по делу. Однако такое желание, возможность и конкретная реализация этой возможности – разные составляющие различающейся практики расследования преступлений правоохранительными органами. Еще 15 лет назад преступления в сфере высоких технологий (такowymi считались любые преступления, при подготовке и совершении которых использовались компьютеризированные устройства и цифровая информация) объявлялись латентными, и в это слово вкладывался негативный смысл, сводящийся к тому, что ожидать быстрого расследования преступления, выявления совершивших его лиц и надежного доказывания их вины объективно не приходится. Эта констатация учитывала отсутствие экспертно-криминалистического инструментария обнаружения, фиксации и исследования цифровых следов, отсутствие методик выполнения таких действий, гарантий обеспечения сохранности и относимости цифровых доказательств, отсутствие системы применения специальных знаний, закрепленной на уровне структуры правоохранительного органа (наличие специализированных подразделений и подготовленных специалистов в них). Но более важным было отсутствие ключевого звена расследования – следователя, подготовка которого позволяла бы использовать в доказывании процессуально правильно полученные разнообразные сведения в цифровой форме о подготовке и совершении преступления.

Сегодня же расследование преступлений, в которых фигурируют цифровые следы, не сложнее, а нередко легче традиционных (в прежнем смысле этого слова) преступлений, потому что специалистам известен механизм слеодообразования в различных информационных системах, на различных носителях информации, при действиях с файлами различных форматов в разнообразных операционных системах. Имеется необходимое для поиска, фиксации, интерпретации цифровых следов специализированное оборудование и программное обеспечение. Специалисты обучены и умеют правильно применять криминалистическую технику нового поколения. Накоплен опыт сопоставления получаемых результатов действиям подозреваемых лиц в обычной «вещной» обстановке.

Необходимо определиться с сутью и природой электронной цифровой криминалистики (и иных аналогичных теорий, предлагаемых авторами) и ее местом в системе криминалистики. По этому поводу до сих пор прослеживается дискуссия в криминалистических публикациях.

По мнению Яковлева А.Н., *цифровая криминалистика* – это те новые знания в криминалистике, которые базируются на понимании особенностей функционирования современных информационно-коммуникационных технологий и используются для выявления уголовно-релевантных закономерностей: 1) преступной деятельности, направленной на воспрепятствование нормальному функционированию информационных систем, их компонентов или деятельности, направленной на использование последних в

качестве инструмента совершения иных преступлений; 2) создания, изменения, передачи, удаления информации на электронных носителях, в информационно-телекоммуникационных сетях, виртуальном пространстве, связанной с подготовкой, совершением, сокрытием преступлений; 3) собирания цифровой информации с выполнением технических процедур обеспечения ее юридической значимости; 4) исследования цифровой информации, сохраненной в отдельных информационных объектах, а также в информационной среде электронного носителя информации; 5) оценки полученных результатов, соотнесения их с действиями субъекта и использования для квалификации преступного деяния; 6) интеграции цифровых доказательств в систему существующих доказательств с соблюдением процессуальной формы их получения<sup>69</sup>.

Смушкин А.Б. также в своих публикациях указал на необходимость ограничить теорию в области комплексного противодействия киберпреступлениям, их расследования и раскрытия, а также применения соответствующих электронных технологий в процессуальной деятельности, от остальных информационно-коммуникативных технологий сочетанием категорий «электронная» и «цифровая» и использованием наименования «Электронная цифровая криминалистика»<sup>70</sup>. При этом основным содержанием данной концепции он видит собирание, исследование и использование электронной цифровой информации и информационно-технологических устройств.

Н.Н. Федотов предлагает форензику и рассматривает её в качестве прикладной науки, основным направлением которой является раскрытие преступлений, связанных с компьютерной информацией, цифровыми доказательствами, их поиску, получению, закреплению и исследованию. Н.В. Шухова и А.Л. Снигирев понимают под форензикой, или криминалистической информатикой, подраздел криминалистики<sup>71</sup>. Смушкин А.Б. подчеркивает, что не совсем понятно место, которое данные авторы выделяют форензике в отечественной криминалистике, что дидактически неверным представляется даже выделение подразделов в рамках криминалистической техники, т.к. традиционно элементами разделов криминалистики являются отрасли, а не подразделы. Автору представляется, что криминалистическое исследование электронных носителей информации и цифровых следов с электронной цифровой криминалистикой сочетается как часть и целое, где целое — это электронная цифровая криминалистика<sup>72</sup>. Многие ученые рассматривают частные теории, отрасли вне зависимости от их наименования и структурной характеристики, однако имеются и другие взгляды. Так, М.А. Романенко дифференцировал исследования в интересующем нас направлении на три группы<sup>73</sup>: 1) разработка конкретных частных методик расследования преступлений в сфере компьютерной информации (Л.Н. Соловьев, В.Б. Вехов, В.А. Мещеряков); 2) разработка тактических аспектов отдельных следственных действий, направленных на обнаруже-

---

<sup>69</sup> Там же.

<sup>70</sup> Смушкин, А.Б. О природе электронной цифровой криминалистики / А.Б. Смушкин // *Lex russica*. – 2020. – Т. 73. – № 6. – С. 110–121; Смушкин, А.Б. К вопросу о наименовании теории «Электронная цифровая криминалистика» / А.Б. Смушкин // *Проблемы уголовного процесса, криминалистики и судебной экспертизы*. – 2019. – № 1(13). – С. 15–21.

<sup>71</sup> Шухова, Н.В., Снигирев, А.Л. О роли форензики в криминалистическом обеспечении расследования преступлений / Н.В. Шухова // *XX Международная научная конференция «Информатизация и информационная безопасность правоохранительных органов»*, Москва, 24–25 мая 2011 г. – М., – 2011. – С. 331.

<sup>72</sup> Смушкин, А.Б. О природе электронной цифровой криминалистики / А.Б. Смушкин // *Lex russica*. – 2020. – Т. 73. – № 6. – С. 110–121.

<sup>73</sup> Романенко, М.А. Новый подход к содержанию системы криминалистической техники / М.А. Романенко // *Вестник Пермского университета. Юридические науки*. – 2008. – Вып. 2(2). – С. 116–117.

ние, фиксацию и изъятие электронно-цифровой техники и программных средств в качестве вещественных, электронных доказательств или «иных документов» (О.Я. Баев); 3) экспертологические исследования в области судебной компьютерно-технической экспертизы (Е.Р. Россинская).

Большинство авторов считают, что по своей сути электронная цифровая криминалистика является частной теорией. Р.С. Белкин отмечал, что отдельные закономерности предмета могут быть рассмотрены и в рамках отдельных изолированных теоретических положений, но лишь в рамках частной криминалистической теории можно получить знания более глубокой сущности — объективной связи этих закономерностей<sup>74</sup>. Согласно такому подходу, частные теории должны отвечать практическим потребностям борьбы с преступностью, способствовать появлению нового знания, знания нового уровня. Частные теории должны отличаться внутренней упорядоченностью. Их положения должны быть взаимно обусловлены. В.П. Лавров предложил следующие требования, позволяющие отнести определенную идею, сумму знаний к частной криминалистической теории: 1) соответствие предполагаемых теоретических конструкций закономерностям, составляющим предмет криминалистики; 2) значение теорий для остальных разделов криминалистической науки; 3) целевую направленность (выявление и решение наиболее важных проблем уголовного судопроизводства); 4) высокий уровень общности теоретических положений; 5) динамичность, а также возможность служить предпосылкой для появления новых учений; 6) системный подход при объединении разрозненных положений в единую частную теорию; активное внедрение в научный оборот теоретических построений на различных уровнях<sup>75</sup>.

Большинство авторов подчеркивают, что в настоящий момент потребность в частной теории, изучающей обнаружение, собирание, исследование и использование электронной информации, ее носителей, велика как никогда. Четвертая промышленная революция, активная цифровизация всех сфер человеческой деятельности, включая судопроизводство, необходимость обеспечения правоохранительных органов эффективными инструментами для работы с указанными объектами, а также выход вопросов, органически объединяющихся в теорию электронной цифровой криминалистики требует разработки единой частной теории<sup>76</sup>.

Становление частной теории электронной цифровой криминалистики (обнаружения, фиксации, изъятия, исследования и использования электронной информации и информационно-технологических устройств) способствует развитию общей теории криминалистики и ее частных теорий, поскольку отражает определенный взгляд на некоторую часть закономерностей, составляющих предмет криминалистики, применительно к электронной цифровой криминалистике как ее части. К таким *закономерностям* Смушкин А.Б. относит: 1) закономерности возникновения, движения, трансформации криминалистически значимой электронной информации; 2) закономерности криминальной деятельности субъектов, совершаемой с использованием компьютерной техники и иных информационно-технологических устройств; 3) закономерности собирания, изъятия и исследования электронных цифровых следов; 4) закономерности оценки и использования криминалистически значимой электронной цифровой информации; 5) закономерности криминалистического обеспечения деятельности при производстве

---

<sup>74</sup> Белкин, Р.С. Криминалистика: проблемы, тенденции, перспективы. Общая и частные теории / Р.С. Белкин. – М., 1987. С. – 139–140.

<sup>75</sup> Лавров, В.П. Частные криминалистические теории: современное состояние и тенденции развития / В.П. Лавров // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3–2. – С. 89.

<sup>76</sup> Смушкин, А.Б. О природе электронной цифровой криминалистики / А.Б. Смушкин // Lex russica. – 2020. – Т. 73. – № 6. – С. 110–121.



следственных действий с электронными устройствами; б) закономерности информационного и иного криминалистического обеспечения методик расследования преступлений, совершенных с использованием компьютерной техники и иных информационно-технологических устройств. Кроме того, в настоящее время на подходе уже иная, не цифровая и не электронная техника<sup>77</sup>.

В частной теории электронной цифровой криминалистики (обнаружения, фиксации, изъятия, исследования электронной информации и информационно-технологических устройств) учитываются и получают развитие основные положения общей теории криминалистики. В рамках предлагаемой частной теории предполагается рассматривать тактику отдельных процессуальных действий в цифровой среде, элементы аппаратно-программного обеспечения научной организации труда следователя и информационного обеспечения, программные комплексы, направленные на содействие следствию в построении версий, планировании расследования и иных организационных мероприятиях. На информации частной теории должны основываться методики расследования киберпреступлений. Системность построения частной теории электронной цифровой криминалистики (обнаружения, фиксации, изъятия, исследования электронной информации и информационно-технологических устройств) обуславливает выделение в ней 4 внутренне упорядоченных и взаимно обусловленных разделов: 1) концептуальные основы частной теории собирания, исследования и использования электронной цифровой информации и ее носителей; 2) концептуальные основы отдельных разделов частной теории; 3) концептуальные основы использования правоохранительными органами электронной цифровой среды; 4) концептуальные основы расследования киберпреступлений.

Таким образом, предлагаемая Смушкиным А.Б. частная теория электронной цифровой криминалистики (обнаружения, фиксации, изъятия, исследования и использования электронной информации и информационно-технологических устройств) удовлетворяет требованиям общности, системности, взаимообусловленности и внутренней упорядоченности ее разделов. При этом считается, что электронная цифровая криминалистика является именно частной теорией, а не учением.

Рассмотрим место частной теории электронной цифровой криминалистики (частной теории собирания и исследования электронной цифровой информации и информационно-технологических устройств) в системе криминалистики. Так, Е.Р. Россинская указывает, что частная теория информационно-компьютерного обеспечения криминалистической деятельности должна содержать в себе элементы, входящие в различные разделы криминалистики, а в совокупности – служить основой для подготовки соответствующих методик расследования компьютерных преступлений<sup>78</sup>. Многие ученые сходятся во мнении, что концептуальные вопросы частной теории электронной цифровой криминалистики (собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств) должны рассматриваться в рамках раздела «Общая теория криминалистики».

Многими авторами поддерживается мнение Е.Р. Россинской<sup>79</sup> о возможности выделения в рамках рассматриваемой частной теории учений, содержащих элементы,

---

<sup>77</sup> Там же.

<sup>78</sup> Россинская, Е.Р. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности / Е.Р. Россинская // Известия Тульского государственного университета. Экономические и юридические науки. – 2016. – № 3–2. – С. 110.

<sup>79</sup> Россинская, Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е.Р. Россинская // Вестник Восточно-Сибирского института МВД России. – 2019. – № 2(89). – С. 193–202; Она же. К вопросу о частной теории информационно-компьютерного обеспечения криминалистической деятельности. – С. 109–117.

входящие и в иные разделы криминалистики – криминалистическую технику, следственную тактику, а также методику. Теория собирания, исследования и использования электронной цифровой информации и информационно-технологических устройств является частной теорией более высокого уровня общности, чем входящие в ее структуру элементы. Положения данной частной криминалистической теории взаимосвязаны с иными частными теориями: криминалистической идентификации, механизма слеодооб-разования и др. Кроме того, отмечается тесная связь данной частной теории с иными науками и активное использование их достижений. Прежде всего – достижений кибер-нетики и информатики (особенно разделов криптографии и стеганографии, защиты ин-формации, искусственного интеллекта, прикладной информатики, компьютерного мо-делирования и др.), уголовного права (в области закрепления диспозиции конкретных видов преступлений) и процесса (в области закрепления понятия доказательств, их ви-дов и источников, порядка производства процессуальных действий и их фиксации и т.д.), информационного права (разработки в области понятия информации, информаци-онных технологий и информационных правоотношений), основ оперативно-розыскной деятельности (в области применения информационных баз и отдельных образцов тех-ники при производстве оперативно-розыскных мероприятий), теории доказательств (в области рассмотрения отдельных вопросов процесса доказывания и отдельных видов доказательств), судебной экспертологии (методик производства соответствующих ви-дов экспертиз), общей, юридической и кибернетической лингвистики и т.д. Таким об-разом, представляется, что на настоящий момент электронная цифровая криминалисти-ка достигла глубины разработки, позволяющей именовать ее частной теорией, и отве-чает основным требованиям к частным теориям, предложенным ранее в криминалисти-ке. Положения данной частной теории основаны на других естественных, гуманитар-ных и технических науках и тесно связаны с ними<sup>80</sup>.

*Структуры* частной теории электронной цифровой криминалистики (обнаруже-ния, фиксации, изъятия, исследования и использования электронной информации и ин-формационно-технологических устройств) представлены учеными в сильно различаю-щихся видах. Так, А.Б. Максимович считает, что структура большинства частных кри-миналистических учений (теорий) состоит из двух частей – общей и частной, но их со-держание определяется областью изучения. В.Б. Вехов разделил криминалистическое компьютероведение на общую и особенную часть. К.Е. Домин, рассматривая матери-альную, программную, информационную и сетевую сторону объектов предлагаемой им теории, выделял следующую систему криминалистического исследования электронных носителей информации: 1) криминалистические аппаратно-компьютерные исследова-ния; 2) криминалистические программно-компьютерные исследования; 3) кримина-листические информационно-компьютерные исследования; 4) криминалистические компьютерно-сетевые исследования. Очевидно, что содержание частной теории кри-миналистического обеспечения собирания, исследования и использования электронной цифровой информации и её носителей (электронная цифровая криминалистика) не мо-жет ограничиваться рамками одного раздела. Для более полного решения задач данной частной теории, а также изучения закономерностей, составляющих её предмет, насущ-но необходимо использовать знания, явно относящиеся как криминалистической тех-нике, так и к организационным основам расследования, криминалистической тактике и методике расследования отдельных видов преступлений. Е.Р. Россинская в качестве элементов структуры частной теории называет: 1) концепцию теории информационно-компьютерного обеспечения криминалистической деятельности, включая предмет тео-рии, её задачи и объекты; 2) учение о способах компьютерных преступлений ( правона-

---

<sup>80</sup> Смушкин, А.Б. О природе электронной цифровой криминалистики / А.Б. Смушкин // Lex russica. – 2020. – Т. 73. – № 6. – С. 110–121.

рушений); 3) учение о цифровых следах как источниках криминалистически значимой компьютерной информации; 4) учение об информационно-компьютерных криминалистических моделях видов компьютерных преступлений; 5) учение о криминалистическом исследовании компьютерных средств и систем, реализуемое в новом разделе криминалистической техники; 6) учение об информационно-компьютерном криминалистическом обеспечении тактики следственных и судебных действий; 7) учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений; 8) учение о взаимосвязях и разграничениях цифровизации судебно-экспертной и криминалистической деятельности. Однако представляется, что в подобной структуре смешиваются разноуровневые понятия: отдельные элементы частной методики расследования (способы совершения компьютерных преступлений, информационно-компьютерные криминалистические модели видов компьютерных преступлений и т.д.) и учение об информационно-компьютерном криминалистическом обеспечении методик расследования компьютерных преступлений (в целом)<sup>81</sup>.

В.А. Мещеряков в рамках содержания цифровой криминалистики выделяет следующие элементы: I. Введение в цифровую криминалистику. 1. Цифровая криминалистика: предпосылки возникновения, современное состояние и перспективы развития. 2. Криминалистическая онтология преступлений в сфере информационно-коммуникационных технологий. II. Техника и технология цифровой криминалистики. 3. Виртуальные следы и механизм слеодообразования при совершении преступлений в сфере информационно-коммуникационных технологий. 4. Криминалистические методы и средства исследования цифровой информации. III. Тактика цифровой криминалистики. 5. Особенности производства отдельных следственных и иных действий при расследовании преступлений в сфере информационно-коммуникационных технологий. 6. Использование научно-технических средств и специальных знаний при расследовании преступлений в сфере информационно-коммуникационных технологий. IV. Методики расследования отдельных видов и групп преступлений в сфере информационно-коммуникационных технологий. 7. Особенности расследования преступлений, связанных с неправомерным доступом к компьютерной информации. 8. Особенности расследования преступлений, связанных с созданием, использованием и распространением вредоносных компьютерных программ. 9. Особенности расследования преступлений, связанных с нарушением правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. 10. Особенности расследования преступлений в сфере электронных финансовых технологий. 11. Особенности расследования преступлений в сфере мобильных телекоммуникаций. 12. Особенности расследования мошенничества с использованием платежных карт и в сфере компьютерной информации. 13. Особенности расследования преступлений, связанных с незаконным оборотом специальных технических средств, предназначенных для негласного получения информации. 14. Особенности расследования преступлений, связанных с нарушением авторских и смежных прав в сфере оборота объектов интеллектуальной собственности, представленных в электронной цифровой форме.

Проанализировав основные мнения ученых, в рамках предлагаемой частной теории собирания, исследования и использования электронной цифровой информации и электронно-технологических устройств мы солидарны со А.Б. Смушкиным, который предлагает выделять следующие разделы:

1. Концептуальные основы частной теории собирания, исследования и использования электронной цифровой информации и её носителей. В рамках данного раздела автор выделяет такие учения и теории, как: А. Теоретические и методологические ос-

---

<sup>81</sup> Смушкин, А.Б. О структуре электронной цифровой криминалистики / А.Б. Смушкин // Криминалистика: вчера, сегодня, завтра. – 2020. – № 3(15). – С. 140–148.

новы частной теории Электронной цифровой криминалистики. Б. Частная теория электронной цифровой информации. В. Частная теория электронных цифровых следов и доказательств.

2. Концептуальные основы отдельных разделов частной теории. А. Частная теория криминалистического исследования компьютеров и их систем. Б. Частная теория исследования и использования компьютерных сетей (сетевая криминалистика). В. Частная теория криминалистического исследования облачных сервисов и сервисов распределенного хранения электронных данных. Г. Частная теория криминалистического исследования мобильных устройств (мобильная криминалистика). Д. Частная теория криминалистического исследования иных портативных электронных устройств, снабженных микропроцессорами, автомобильных электронных датчиков и «Интернета вещей».

3. Концептуальные основы использования правоохранительными органами электронной цифровой среды. В рамках данного раздела А.Б. Смушкин предлагает выделять следующие учения и теории: А. Криминалистическое учение об использовании отдельных электронных цифровых технологий в правоохранительной деятельности. Б. Криминалистическое учение об использовании компьютерных сетей в целях борьбы с преступностью. В. Теория криминалистического обеспечения тактики следственных действий, проводимых с электронными устройствами, их системами и сетями.

4. Концептуальные основы расследования киберпреступлений. А. Криминалистическая онтология киберпреступлений (преступлений в электронной цифровой среде). Б. Теория криминалистического обеспечения методик расследования компьютерных преступлений. В. Особенности расследования преступлений в сфере мобильных телекоммуникаций. Г. Основы расследования хищений, совершённых с использованием компьютерных устройств. Д. Основы расследования иных преступлений, совершённых с использованием информационно-технологических устройств.

Подводя итог, необходимо отметить, что научные разработки в области систематизации теории, предназначенной для работы с электронной информацией и информационно-технологическими устройствами, будут способствовать повышению эффективности работы с информационно-коммуникативными технологиями.

## **2. Современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений**

Актуальными направлениями развития современной отечественной криминалистики являются: дальнейшее совершенствование ее методологических основ, разработка и применение технико-криминалистических источников информации (электронные следы, компьютерные системы наблюдения, цифровые носители информации, компьютерные экспертизы и т. п.), создание на этой основе новых методических рекомендаций по расследованию новых и изменяющихся прежних составов преступлений, их унификация и адаптация к современной практике правоприменения. Техничко-криминалистические методы и средства собирания и исследования материальных носителей информации, их оценки и использования, находят все более широкое применение в уголовном судопроизводстве. В практику расследования уголовных дел, в частности, для фиксации вербальной криминалистически значимой информации, активно внедряются средства аудио- и видеотехники, а также электронные способы передачи данной информации. Цифровые и компьютерные технологии в настоящее время прочно заняли ведущее место в развитии криминалистической техники. В связи с развитием технического прогресса и IT-технологий в различных сферах правоприменительной деятельности, в настоящее время в теории науки криминалистики активно рассматривается вопрос о проведении в ходе расследования уголовных дел онлайн-допроса (интернет-допроса, web-допроса, допроса с помощью видеоконференцсвязи), который представ-

ляет собой специальный метод получения криминалистически значимой и доказательственной информации, осуществляемый на основе использования интернет-технологий<sup>82</sup>. Правоохранительными органами успешно используется разветвленная система криминалистических учетов, действующая на основе компьютерной техники. Научно-технические средства криминалистического учета, розыска преступников и похищенного имущества включают средства, используемые для накопления и переработки криминалистической информации путем ведения различных учетных систем и облегчения поиска необходимых материалов.

Рассмотрим три наиболее освещаемые в криминалистике **новые технологии**: 1) электронная технология, 2) компьютерная технология, 3) цифровая технология.

*Электронная технология* или электроника – это область науки и техники, занимающаяся созданием и практическим использованием различных устройств и приборов, работа которых основана на изменении концентрации и перемещении заряженных частиц (электронов) в вакууме, газе или твердых кристаллических телах, и других физических явлениях. Данная технология является составной частью электронной аппаратуры.

*Компьютерные технологии или информационные технологии (ИТ)* – это обобщенное название технологий, отвечающих за хранение, передачу, обработку, защиту и воспроизведение информации с использованием компьютеров.

*Цифровые технологии* основаны на представлении сигналов дискретными полосами аналоговых уровней, а не в виде непрерывного спектра. Все уровни в пределах полосы представляют собой одинаковое состояние сигнала. Эта технология работает, в отличие от аналоговой, с дискретными, а не непрерывными сигналами. Цифровые технологии главным образом используются в вычислительной цифровой электронике, прежде всего в компьютерах, в различных областях электротехники, таких как игровые автоматы, робототехника, автоматизация, измерительные приборы, радио- и телекоммуникационные устройства, и во многих других цифровых устройствах.

Анализируя вышеизложенное, очевидно, что обобщающим термином является *электронная технология*, в которую входит компьютерная, а составной частью последней является цифровая технология. Во всем мире вещественным доказательством является именно носитель цифровой информации (флэш-карта, диск, телефон, смартфон, айфон, планшет, компьютер и т.п.), а полученная из него цифровая информация становится доказательством только после исследования самого носителя специалистом или посредством заключения соответствующей экспертизы. Поэтому цифровая информация становится доказательством только после ее специальной обработки и исследования<sup>83</sup>.

В этом ее особенность и отличие, например, от письменного документа, который сам по себе, а также изложенная в нем информация являются самостоятельным и самостоятельным доказательством, не требующим обязательного экспертного исследования.

В процессе осмотра места происшествия данной группы преступлений могут быть обнаружены и зафиксированы важные документы, которые в дальнейшем станут вещественными доказательствами по делу:

1. Документы, которые сохраняют в себе следы совершенного преступления, различные рукописные тексты, записи, пароли или коды, телефонные счета, номера телефонов и банковских счетов, которые могут выявить связь с другими участниками, сведения о совершенных процедурах на компьютере или в сети Интернет и др.

---

<sup>82</sup> Кучин, О.С. Электронная криминалистика: миф или реальность / О.С. Кучин // Сетевое издание «Академическая мысль». – № 3 (8). – 2019. – С.67–70.

<sup>83</sup> Там же.

2. Документы со следами печати, которые необходимо искать в периферийных устройствах, например в принтерах, сканерах, факсах. Также необходимо обратить внимание на бумажные носители информации, которые могли остаться внутри этих устройств.

3. Личные документы (информация о подозреваемом).

4. Правила пользования компьютером, нормативные правовые акты, инструкции, которые регламентируют правила работы с компьютером, сетью, доказывающие, что преступник умышленно совершил преступление.

5. Документы, которые содержат в себе инструкцию либо описание аппаратуры или какого-либо устройства, доказывают нелегальное приобретение<sup>84</sup>.

При неработающем компьютере информация может находиться в ящиках электронной почты, на других электронных носителях и технических устройствах либо в компьютерной сети. Более детальному осмотру они подлежат в лаборатории либо на рабочем месте следователя при участии специалиста. Лучше всего изучать копии, изъятые из электронных устройств, которые изготовлены с помощью данных операций, а не сам подлинник. Для того чтобы получить более точную информацию, необходимо обращать внимание на скрытые файлы (папки), в которых может храниться важная информация, зашифрованная паролями и кодами; если такие имеются, то их нужно отправлять специалистам на декодирование и расшифровку.

Деятельность специалиста при осмотре складывается из следующих последовательных действий: 1) установление наличия и выполнения соответствующей компьютерной программы (при включенном компьютере); 2) подробное изучение изображения на мониторе компьютера и его описание; 3) фото- либо видеофиксация изображения, фиксация всех действий специалиста при производстве следственного действия; 4) завершение работы компьютерной программы. Письменное закрепление хода и результатов осмотра в протоколе; 5) фиксация наличия у компьютера внешних и периферийных устройств (магнитные и виртуальные диски, флеш-накопители и иное); б) по окончании процессуальных действий разъединение сетевого кабеля при включенном сетевом питании; 7) копирование всей информации, которая необходима для расследования преступления, со всех файлов, хранящихся на виртуальных дисках и магнитных носителях; 8) упаковывание каждого устройства, а также соединительных проводов и кабелей, обеспечивающих их сохранность<sup>85</sup>.

После проведения осмотра и фиксации его в необходимых процессуальных документах следователь назначает необходимую экспертизу, определяет, какие виды исследований необходимо провести, выбирает экспертное учреждение и эксперта, выделяет необходимые объекты, которые предоставляются на экспертизу, а также формулирует вопросы эксперту. Объекты, отправленные на компьютерную экспертизу, могут быть в виде текста (текстов), который сохранен на электронном носителе либо предоставлен на бумаге. Не стоит забывать о том, что носителем информации является ПК, локальная сеть и само место происшествия.

В ходе расследования компьютерных преступлений определяющей экспертизой является компьютерная, в рамках которой проводятся следующие виды исследований: в целях исследования технических (аппаратных) средств компьютерной системы, а именно исследования закономерностей эксплуатации аппаратных средств компьютерной системы, назначается и проводится судебная аппаратно-компьютерная экспертиза; в рамках исследования функционального предназначения программного обеспечения

---

<sup>84</sup> Лантух, Э.В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э.В. Лантух, В.С. Ишигеев, О.П. Грибунов // Всероссийский криминологический журнал. – 2020. – Т. 14, – № 6. – С. 882–890.

<sup>85</sup> Там же.

компьютерной системы, его характеристик и реализуемых к нему требований, его алгоритма и структурных особенностей, текущего состояния – судебная программно-компьютерная экспертиза; в целях поиска, обнаружения, анализа и оценки информации, подготовленной пользователем или порожденной (созданной) программами для организации информационных процессов в компьютерной системе, – судебная информационно-компьютерная экспертиза (данных); в рамках исследования функционального предназначения компьютерных средств, реализующих какую-либо сетевую информационную технологию, – судебная компьютерно-сетевая экспертиза.

Таким образом, цифровая криминалистика представляет собой сложную систему, включающую совокупность постоянно работающих программных обеспечений (программ) для исследования цифрового пространства в целях предотвращения и выявления преступлений, анализ цифрового материала, а также направленного исследования конкретных носителей цифровых данных или самих данных (например, логов) для выявления следов конкретного преступления. При этом ведущую роль в цифровой криминалистике, в отличие от науки криминалистики «традиционного» типа, играет именно специализированное программное обеспечение (ПО) и широта его возможностей, а не специалист или эксперт, – проще сказать, не человек. Объясняется это тем, что сложность и многослойность цифровых устройств, их технические характеристики, а также действия преступников в цифровом пространстве настолько ускорены и усовершенствованы возможностями этого пространства, что человеческий мозг не в силах противостоять им в одиночку<sup>86</sup>.

На основании изложенного следует констатировать, что не только проведение экспертизы экспертами, имеющими специальные знания в сфере высоких технологий, по уголовным делам, связанным с преступлениями в сфере компьютерных технологий, является серьезной поддержкой, оказываемой правоохранительным органам в борьбе как с данными преступлениями, так и с целым спектром преступлений, в которых информационные технологии выступают частью базы преступной деятельности, но и участие специалиста на всех этапах расследования данных преступлений, а также при проведении всех следственных действий становится залогом успешного раскрытия, расследования и предупреждения данного вида преступлений.

### **3. Передовые практические методы расследования преступлений в области цифровой криминалистики**

Расследование киберпреступлений вызывает у практических работников определенные трудности, что обусловлено спецификой источников доказательственной информации, представленной в виде электронных сообщений, страниц, сайтов и др. Следует отметить, что и в зарубежной практике выделяют самостоятельный класс цифровых доказательств, обусловленных особенностями компьютерных средств и систем<sup>87</sup>.

Низкая раскрываемость преступлений в сфере компьютерной информации обуславливает возникновение в следственной практике необходимости дополнительного комплексного исследования тактики производства отдельных следственных действий, изучения особенностей назначения и производства специальных экспертиз, разработки новых методов работы с цифровыми объектами с учетом современных достижений техники и различных наук. При расследовании данного вида преступлений исследование компьютерной информации и компьютерной техники возможно в следующих след-

---

<sup>86</sup> Лантух, Э.В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э.В. Лантух, В.С. Ишигеев, О.П. Грибунов // Всероссийский криминологический журнал. – 2020. – Т. 14, – № 6. – С. 882–890.

<sup>87</sup> Guidelines for Best Practice in the Forensic Examination of Digital Technology // IOCE. 2002. May. [Электронный ресурс]. – Режим доступа: <https://ru.scribd.com/document/183506063/Guidelines-for-BestPractices-in-Examination-of-Digital-Evid>. – Дата доступа: 11.02.2022

ственно-экспертных ситуациях: 1) наличие объектов преступных посягательств в виде фальсифицированных данных бухгалтерского или иного учета, наличие защитных программных средств с признаками взлома, скорректированных либо измененных персональных данных и др.; 2) компьютерная информация и техника являются средствами совершения преступления либо средствами связи; 3) компьютерная информация (или техника) характеризует определенный объект по уголовному делу, при этом не являясь объектом преступного воздействия или средством совершения преступления (данные с видеорекамера наблюдения, информация о деятельности предприятия и др.).<sup>88</sup>

Достигнутый уровень развития составляющих цифровой криминалистики позволяет уже сейчас обеспечить раскрытие и расследование особо сложных преступлений, ранее справедливо считавшихся латентными. Доля преступлений, совершаемых с использованием сети Интернет, с каждым годом увеличивается. В то же время в Уголовно-процессуальном кодексе Республики Беларусь (далее – УПК) и Законе Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» понятие «интернет» не встречается. Полагаем, что это является одним из условий низкой раскрываемости преступлений указанной категории. Основным направлением установления лиц, удаленно совершающих преступления, является получение информации у провайдеров, хостеров, владельцев интернет-ресурсов, банковских учреждений, эмитентов электронных валют, операторов мобильной связи. Данное направление расследования мы называем пассивным сбором информации. Однако имеется большое разнообразие приемов активного, наступательного сбора данных о преступнике, которые практически не применяются из-за неосведомленности о них сотрудников, а также в связи с отсутствием правовой регламентации процессуальной и оперативно-розыскной деятельности в сети Интернет. Приведем отдельные приемы и методы активного расследования, разработанные Кобринским районным отделом Следственного комитета Республики Беларусь и уже апробированные во взаимодействии с оперативными подразделениями<sup>89</sup>.

*Активный мониторинг.* Сотрудники размещают в сети Интернет информацию, ожидая определенную реакцию преступника, которая может его выдать. Метод успешно применен при раскрытии резонансного убийства в Кобрине, когда за неделю до установления преступника была выявлена его страница в социальной сети «ВКонтакте».

*Web-капкан* – система получения данных о пользователе, осуществившем переход по специальной гиперссылке. В случае перехода сотрудник на свой email получает электронный отчет с информацией о времени перехода, IP-адресе лица, кликнувшего ссылку, а также данные об используемой им операционной системе, браузере, языках, часовом поясе, а при определенных обстоятельствах – даже о модели мобильного телефона. Исключительно с применением этого метода уже раскрыто одно преступление, установлено местонахождение без вести пропавшей несовершеннолетней.

*Click-капкан* – усовершенствованный вариант предыдущего метода, позволяющий при определенных обстоятельствах устанавливать также аккаунт социальной сети «ВКонтакте», который используется искомым пользователем.

*Наступательный осмотр.* Так, в ходе расследования одного из уголовных дел следователями получена информация об электронном почтовом ящике, длительное

---

<sup>88</sup> Лантух, Э.В. Использование специальных знаний при расследовании преступлений в сфере компьютерной информации / Э.В. Лантух, В.С. Ишигеев, О.П. Грибунов // Всероссийский криминологический журнал. – 2020. – Т. 14, – № 6. – С. 882–890.

<sup>89</sup> Зарецкий, П.П. Направление совершенствования деятельности по раскрытию преступлений, совершаемых с использованием интернета / П.П. Зарецкий // Противодействие киберпреступности: современное состояние и пути повышения эффективности: сборник статей / Следств. ком. Респ. Беларусь; редкол.: С.Я. Аземша (гл. ред.) [и др.]. – Минск: ЮрСпектр, 2020. – С. 106–108.



время используемом преступником. Получив санкцию прокурора на производство осмотра, следователи осуществили подбор контрольного слова для смены пароля к данному ящику, вошли в него и получили данные, позволившие установить лицо, совершившее сотни хищений денежных средств с карт-счетов граждан.

*Fish-капкан* – система получения активационных данных искомого пользователя путем инициирования перехода его на контролируруемую сотрудником страницу, визуально схожую с каким-либо сервисом. Данная система сейчас используется только в учебных целях – для разъяснения следователям принципов работы фишинговых сайтов. Но принятие ее на вооружение в оперативно-розыскной деятельности, несомненно, повысило бы эффективность раскрытия интернет-преступлений. Это лишь некоторые из огромного числа возможных активных методов раскрытия преступлений. Их разработка – это процесс заимствования и приспособления для нужд правоохранителей современных особенностей функционирования интернет-узлов, наработок в области интернет-рекламы и веб-коммерции, а также инструментария, который используют хакеры<sup>90</sup>.

Методы и средства, входящие в арсенал цифровой криминалистики, активно востребованы при проведении следственных действий, сопряженных с осмотром и изъятием компьютеров, мобильных устройств, электронных носителей информации. Организуются как незамедлительный осмотр изъятого оборудования в целях быстрого обнаружения ориентирующей и доказательственной информации на его электронных носителях, которая может быть использована для раскрытия преступления по горячим следам, так и проведение компьютерно-технических, информационно-аналитических, видеотехнических экспертиз, позволяющих максимально тщательно изучить уголовно-релевантную цифровую информацию. Организуется обучение следователей особенностям использования цифровой информации в доказывании, а также целевое обучение специалистов со специализацией в области исследования цифровой. Все это является гарантией того, что достижения цифровой криминалистики будут и далее эффективно использоваться следственным органом в расследовании преступлений.

---

<sup>90</sup> Там же.

# ПРАКТИЧЕСКИЙ РАЗДЕЛ

## УЧЕБНЫЙ МОДУЛЬ 1

### КРИМИНОЛОГИЧЕСКИЙ АНАЛИЗ КИБЕРПРЕСТУПНОСТИ

#### 1.1. Тематический план модуля

	Темы	Лекции		Семинарские занятия	
		ДФО	ЗФО	ДФО	ЗФО
	Информационно-коммуникационная безопасность.	2	1	2	
	Преступность в сфере современных информационно-коммуникационных технологий (киберпреступность).	2	1	1	1
	Киберпреступность в мире и в Республике Беларусь: особенности и тенденции	4	2	1	1
	Итоговый контроль по модулю	Коллоквиум			

#### 1.2. Темы и вопросы семинаров

##### **Занятие 1. Понятие информационной безопасности как составляющей национальной безопасности и объекта уголовно-правовой охраны (2 ч.)**

###### *Вопросы для обсуждения*

1. Понятие, содержание и значение информационной безопасности.
2. Политика государства в сфере информационной безопасности, современное состояние и проблемы информационной безопасности.
3. Виды и источники угроз информационной безопасности, субъекты обеспечения информационной безопасности.
4. Законодательство Республики Беларусь в области обеспечения информационной безопасности.

##### **Занятие 2. Преступность в сфере современных информационно-коммуникационных технологий (киберпреступность) (2 ч.)**

###### *Вопросы для обсуждения*

1. Киберпреступность как объект изучения киберкриминологии: понятие, проблемы терминологии, основные концепции и подходы к изучению в современной доктрине.
2. Классификация киберпреступлений. Характеристика основных видов преступлений в сфере современных информационно-коммуникационных технологий.
3. Современные тенденции киберпреступности в мире.
4. Состояние, динамика и особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.

#### 1.3. Самостоятельная работа студентов

##### **Темы рефератов**

Понятие, содержание и значение информационной безопасности современного цифрового (информационного) общества.

Современное состояние и проблемы информационной безопасности. Историко-правовой анализ развития законодательства Республики Беларусь в области обеспечения информационной безопасности.

Концепция информационной безопасности Республики Беларусь и субъекты ее реализации.

Акты ООН и Совета Европы о борьбе с киберпреступлениями как инструмент международного сотрудничества.

Криминогенные факторы современного цифрового мира.

Виды и источники угроз информационной безопасности Республики Беларусь.

### **Задания коллоквиума по темам модуля 1**

#### *Задание 1*

1. Информационно-коммуникационная безопасность: определение и содержание понятия

2. Назовите основные криминогенные факторы современного цифрового мира и охарактеризуйте их.

3. Назовите основные источники права Республики Беларусь в области обеспечения информационной безопасности.

4. Определите понятие киберпреступности

5. Определите современные тенденции киберпреступности в мире

#### *Задание 2*

1. Охарактеризуйте современные проблемы информационной безопасности

2. Определите предмет киберкриминологии

3. Дайте характеристику основных видов преступлений в сфере современных информационно-коммуникационных технологий.

4. Охарактеризуйте состояние, динамику и особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.

#### *Задание 3*

Проведите правовой анализ Концепции национальной безопасности Республики Беларусь с позиций обеспечения информационной безопасности

#### *Задание 4*

Проведите сравнительный анализ Концепции информационной безопасности Республики Беларусь и Конвенции Совета Европы «О преступности в сфере компьютерной информации» (ЕСТ № 185).

### **Источники и литература для работы по модулю 1**

#### *Источники*

№ по Списку источников и литературы: 1–4, 11, 14, 15–26

#### **Литература**

№ по Списку источников и литературы: 27, 30, 32–33, 39–50, 55–57, 67–74, 77–82, 84, 89–90, 105.

## УЧЕБНЫЙ МОДУЛЬ 2

### УГОЛОВНОЕ ЗАКОНОДАТЕЛЬСТВО РЕСПУБЛИКИ БЕЛАРУСЬ В СФЕРЕ ИНФОРМАЦИОННО-КОММУНИКАЦИОННОЙ БЕЗОПАСНОСТИ

#### 2.1. Тематический план модуля

	Темы	Лекции		Семинарские занятия	
		ДФО	ЗФО	ДФО	ЗФО
1	Уголовно-правовые проблемы охраны информационно-коммуникационной безопасности	2	1	2	1
2.	Уголовное законодательство Республики Беларусь в сфере информационно-коммуникационной безопасности.	4	1	2	1
	Итоговый контроль по модулю	Коллоквиум			

#### 2.2. Темы и вопросы семинаров

##### **Занятие 1. Уголовно-правовые проблемы охраны информационно-коммуникационной безопасности (2 ч.)**

###### *Вопросы для обсуждения*

1. Терминологический аппарат уголовно-правовых норм о преступлениях против информационной безопасности.
2. Уголовно-правовая характеристика объективных признаков преступлений против информационной безопасности.
3. Уголовно-правовая характеристика субъективных признаков преступлений против информационной безопасности.
4. Зарубежный опыт и международные стандарты уголовно-правовой борьбы с преступлениями против информационной безопасности.

##### **Занятие 2. Уголовное законодательство Республики Беларусь в сфере информационно-коммуникационной безопасности (2 ч.)**

###### *Вопросы для обсуждения*

1. Статьи уголовного закона о преступлениях, предметом или средством совершения которых является информация, их уголовно-правовая характеристика
2. Применение статей о незаконном сборении либо распространении информации о частной жизни, нарушении тайны переписки, телефонных переговоров, телеграфных или иных сообщений в условиях цифровизации общества.
3. Уголовно-правовая характеристика преступлений против компьютерной безопасности.

#### 2.3. Самостоятельная работа студентов

##### **Темы рефератов**

- Киберпреступность: понятие, основные концепции
- Международно-правовая классификация киберпреступлений.
- Современные тенденции киберпреступности в мире.
- Кибертерроризм и киберэкстремизм
- Использование искусственного интеллекта криминальными сообществами

Современные биотехнологии и преступность  
Хакеры: криминологическая характеристика  
Сетевые «тролли» и иные группы травли в Интернете  
Организованная преступность цифрового мира  
Особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.

Уголовно-правовая характеристика объективных и субъективных признаков преступлений против компьютерной безопасности.

Хищение имущества путем модификации компьютерной информации (ст. 212 УК): уголовно-правовая характеристика

Несанкционированный доступ к компьютерной информации как преступление против информационной безопасности (ст. 349 УК): уголовно-правовая характеристика

Уничтожение, блокирование или модификация компьютерной информации (ст. 350 УК): уголовно-правовая характеристика.

Уголовная ответственность за неправомерное завладение компьютерной информацией (ст. 352 УК).

Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354 УК): уголовно-правовая характеристика.

Нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК): уголовно-правовая характеристика

Проблемы правоприменительной практики статей гл. 31 УК в деятельности органов, ведущих уголовный процесс.

Зарубежный опыт и международные стандарты уголовно-правовой борьбы с преступлениями в сфере современных информационно-коммуникационных технологий.

Уголовно-правовая характеристика и проблемы применения норм УК о преступлениях, предметом или средством совершения которых является информация.

Незаконное собирание либо распространение информации о частной жизни и нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений.

Нарушение авторского права, смежных прав и права промышленной собственности (ст. 201 УК): проблемы применения и пути совершенствования.

Незаконные действия в отношении информации о частной жизни и персональных данных (ст. 203.1)

Уголовная ответственность за коммерческий шпионаж.

Судебная практика по уголовным делам о преступлениях против информационной безопасности.

Использование новейших технологий цифрового мира в предупреждении преступлений

## **Задания коллоквиума по темам модуля 2**

### *Задание 1*

1. Дайте уголовно-правовую характеристику объективных и субъективных признаков преступлений против компьютерной безопасности.

2. Охарактеризуйте виды преступлений против компьютерной безопасности и их составы в соответствии с Уголовным кодексом Республики Беларусь.

3. Дайте уголовно-правовую характеристику ст. 349 УК «Несанкционированный доступ к компьютерной информации» как преступление против информационной безопасности».

4. Дайте уголовно-правовую характеристику ст. 350 УК «Уничтожение, блокирование или модификация компьютерной информации»

5. Дайте уголовно-правовую характеристику ст. 352 УК «Неправомерное завладение компьютерной информацией»

6. Дайте уголовно-правовую характеристику ст. 354 «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»

7. Дайте уголовно-правовую характеристику ст. 355 «Нарушение правил эксплуатации компьютерной системы или сети»

8. Дайте уголовно-правовую характеристику статей 203, 203.1, 203.2 УК, определяющих незаконные действия в отношении информации о частной жизни и персональных данных.

9. Дайте уголовно-правовую характеристику ст. 212 «Хищение имущества путем модификации компьютерной информации»

#### *Задание 2*

1. Охарактеризуйте международные стандарты уголовно-правовой борьбы с преступлениями против информационной безопасности.

2. Определите преимущества и недостатки уголовно-правовой охраны информационной безопасности в Республике Беларусь

#### *Задачи*

1. Серегин взломал компьютерную базу данных потерпевшей Ахтямовой, проникнув на ее страничку в сайте «В контакте», обидевшись на то, что девушка не желала продолжить с ним виртуальную переписку. Решив отомстить, он украл и поменял пароли от ее электронного почтового ящика и анкеты на сайте. В результате девушка не могла попасть на свою страницу. Серегин вступал от ее имени в эротическую переписку с мужчинами, а также разместил фотографии порнографического содержания.

*Есть ли в действиях Серегина признаки какого-либо состава преступления?*

2. Директора АО Бульдогова заинтересовали банковские счета конкурента. Он нанял специалиста, который, преодолев защиту, проник в компьютерную сеть банка, отыскал информацию об операциях по нужному счету и вывел ее на экран монитора. Бульдогов просмотрел информацию и сделал выписки в блокнот о заинтересовавших его операциях по счету.

*Квалифицируйте содеянное.*

3. Логунов написал и распространил с помощью электронной почты программу, которая активизировалась при попытке открыть почтовое сообщение и производила несанкционированные изменения в операционной системе. 31 декабря на мониторах всех компьютеров с измененным программным обеспечением отобразилось: «С новым годом!».

*Квалифицируйте содеянное Логуновым.*

4. Боков сконструировал прибор – сканер, с помощью которого перехватывал идентификационные коды мобильных телефонов пользователей и, вводя их в память своего устройства, осуществлял звонки, счета на оплату которых приходили законным абонентам. Общая сумма в счетах пользователям сотовых телефонов превысила базовую величину более чем в 250 раз.

В ходе предварительного расследования было установлено, что идентификационный код, перехватываемый Боковым, является компьютерной информацией.

*Решите вопрос об ответственности Бокова.*

5. Шевцов и Трусов, продолжительное время работая на одном предприятии – ООО «Виктория», вступили в сговор, направленный на хищение ликероводочной продукции. Они обговорили условия, по которым Шевцов создает на фирме условия для получения продукции без предоплаты, а Трусов обеспечивает вывоз и сбыт.

Будучи главным специалистом службы сбыта и маркетинга и зная порядок ввода информации в локальную компьютерную сеть для последующего получения продукции предприятия с отсрочкой платежа, Шевцов с помощью компьютера проник в локально-вычислительную сеть ООО «Виктория», где, уничтожив в списке клиентов фирмы запись «300» - номер договора с ЗАО «Лотос», ввел в указанный реестр заведомо ложную информацию о фирме «Победа», что послужило основанием для отгрузки последней ликероводочной продукции.

Трусов подыскал для исполнения роли экспедитора своего знакомого Котова, о чем уведомил Шевцова, который на имеющемся у него типовом бланке оформил доверенность от фирмы «Победа» на получение 200 ящиков ликероводочной продукции на имя экспедитора Котова и поставил на нее оттиск печати фирмы «Победа».

На следующий день Котов, используя доверенность фирмы «Победа», вывез со склада ООО «Виктория» 4 тыс. бутылок водки «Столичная». Трусов реализовал водку за наличный расчет, полученные деньги поделил со Швецовым и Котовым.

*Дайте юридическую оценку действиям указанных лиц.*

### **Источники и литература для работы по модулю 2**

#### *Источники*

№ по Списку источников и литературы: 5–10, 16

#### *Литература*

№ по Списку источников и литературы: 31, 34–35, 38, 47, 51, 54, 66–70, 76–80, 87–89, 93–98, 101, 104, 106, 108, 111

### УЧЕБНЫЙ МОДУЛЬ 3

## СОВРЕМЕННЫЕ КРИМИНАЛИСТИЧЕСКИЕ ТЕХНОЛОГИИ РАССЛЕДОВАНИЯ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИКТ

### 3.1. Тематический план модуля

	Темы	Лекции		Семинарские занятия	
		ДФО	ЗФО	ДФО	ЗФО
1	Использование современных криминалистических технологий расследования преступлений в сфере информационно-коммуникационных технологий	2	1	2	1
2.	Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе	2	1	2	1
	Итоговый контроль по модулю				

### 3.2. Темы и вопросы семинаров

#### **Занятие 1. Использование современных криминалистических технологий расследования преступлений в сфере информационно-коммуникационных технологий (2 ч.)**

##### *Вопросы для обсуждения*

1. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности.
2. Характеристика инструментальных модулей, необходимых для обнаружения следов преступлений в сфере современных информационно-коммуникационных технологий.
3. Современные возможности применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий.
4. Современные технологии криминалистического исследования компьютерных систем, их сетей и периферийного оборудования.
5. Использование современных криминалистических технологий при обнаружении, фиксации, изъятии следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

#### **Занятие 2. Цифровая криминалистика и её значение для расследования преступлений в современном информационном обществе (2 ч.)**

##### *Вопросы для обсуждения*

1. Понятие, проблемы терминологии, цели, задачи, функции электронной цифровой криминалистики.
2. Современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений.
3. Передовые практические методы расследования преступлений в области цифровой криминалистики.



4. Современные возможности цифровой криминалистики при производстве судебных экспертиз.
5. Криминалистическая экспертиза Интернета вещей.

### **3.3. Самостоятельная работа студентов**

#### **Темы рефератов**

Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности.

Характеристика инструментальных модулей, необходимых для обнаружения следов преступлений в сфере современных информационно-коммуникационных технологий.

Современные возможности применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий.

Современные технологии криминалистического исследования компьютерных систем, их сетей и периферийного оборудования.

Использование современных криминалистических технологий при обнаружении, фиксации, изъятии следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

Понятие, проблемы терминологии, цели, задачи, функции электронной цифровой криминалистики.

Современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений.

Передовые практические методы расследования преступлений в области цифровой криминалистики.

Современные возможности цифровой криминалистики при производстве судебных экспертиз.

Криминалистическая экспертиза Интернета вещей.

#### **Задания коллоквиума по темам модуля 3**

##### *Задание 1*

1. Особенности концепции теории информационно-компьютерного обеспечения криминалистической деятельности.

2. Элементы системы концепции теории информационно-компьютерного обеспечения криминалистической деятельности.

3. Основные закономерности концепции теории информационно-компьютерного обеспечения криминалистической деятельности.

4. Понятие и проблемы терминологии электронной цифровой криминалистики.

5. Цели, задачи, функции электронной цифровой криминалистики.

##### *Задание 2*

1. Охарактеризуйте инструментальные модули, необходимые для обнаружения следов преступлений в сфере современных информационно-коммуникационных технологий.

2. Охарактеризуйте современные технологии криминалистического исследования компьютерных систем, их сетей и периферийного оборудования.

3. Охарактеризуйте современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений.

4. Охарактеризуйте современные возможности цифровой криминалистики при производстве судебных экспертиз.

### *Задание 3*

1. Приведите примеры современного применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий.

2. Приведите примеры современного применения криминалистических технологий при обнаружения следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

3. Приведите примеры современного применения криминалистических технологий при фиксации следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

4. Приведите примеры современного применения криминалистических технологий при изъятия следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

5. Приведите примеры передовых практических методов расследования преступлений в области цифровой криминалистики.

6. Сформулируйте вопросы экспертам при назначении криминалистической экспертизы Интернета вещей.

### **Источники и литература для работы по модулю 3**

#### *Источники*

№ по Списку источников и литературы: 6–9, 14, 16, 20, 23–25

#### *Литература*

№ по Списку источников и литературы: 28–29, 34, 36–37, 40–44, 46, 52, 56, 58–63, 65, 71–73, 75, 83, 85, 91–93, 99–100, 102–104, 107, 109–110

## САМОСТОЯТЕЛЬНАЯ РАБОТА МАГИСТРАНТОВ ПОД УПРАВЛЕНИЕМ ПРЕПОДАВАТЕЛЯ

Самостоятельная работа предусмотрена учебным планом для развития способностей магистрантов к самостоятельной научной исследовательской деятельности.

Такая форма приобретения магистрантами знаний, навыков, умений служит

– углубленному изучению определенной темы, ее отдельных вопросов, теоретико-правовых проблем и, тем самым, росту знаний магистранта;

– формированию умений использования правовых и научных литературных источников – поиска, отбора и изучения информации; критического обзора литературы, осуществлению полного и последовательного анализа источников;

– овладению отдельными методами и методологией научного исследования, анализом нормативных правовых актов, относящихся к используемым источникам;

– формированию собственной позиции магистранта по правовым вопросам и возможности ее выражения, в том числе изложения собственных теоретических и экспериментальных результатов, оценка достоверности полученных данных.

Самостоятельная работа предполагает автономное освоение магистрантами поставленных целей и задач в пределах учебного материала. Данная форма подготовки должна носить логически последовательный, системный, комплексный характер и предполагает использование всех доступных рекомендуемых форм и методов подготовки.

Непременным условием усвоения содержания учебной дисциплины является углубленное изучение рекомендуемой научной литературы и правовых источников.

### **Вопросы и задания для самостоятельной работы студентов и промежуточного контроля знаний**

#### **1. Тема: «Криминологический анализ киберпреступности»**

##### *1.1 Задания формирующие знания на уровне узнавания*

*Проблемы для изучения (темы рефератов) в рамках КУСР*

1. Информационно-коммуникационная безопасность: определение и содержание понятия

2. Основные криминогенные факторы современного цифрового мира и охарактеризуйте их.

3. Основные источники права Республики Беларусь в области обеспечения информационной безопасности.

4. Понятие и содержание киберпреступности

5. Современные тенденции киберпреступности в мире

##### *1.2 Задания, формирующие знания на уровне воспроизведения:*

1. Охарактеризуйте современные проблемы информационной безопасности

2. Определите предмет киберкриминологии

3. Дайте характеристику основных видов преступлений в сфере современных информационно-коммуникационных технологий.

4. Охарактеризуйте состояние, динамику и особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.

##### *1.3. Задания, формирующие знания на уровне применения*

1. Проведите правовой анализ Концепции национальной безопасности Республики Беларусь с позиций обеспечения информационной безопасности

2. Проведите сравнительный анализ Концепции информационной безопасности Республики Беларусь и Конвенции Совета Европы «О преступности в сфере компьютерной информации» (EST № 185).

***Источники и литература:***

1. Концепция национальной безопасности Республики Беларусь: утв. Указом Президента Республики Беларусь, 09.11.2010 № 575/ / Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». Минск, 2022.

2. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]: утверждена постановлением Совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». Минск, 2022.

3. Конвенция о преступности в сфере компьютерной информации (ETS№ 185) [Электронный ресурс]. – Режим доступа: [http://www.alpp.ru/law\\_pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii-185rus-angl.html](http://www.alpp.ru/law_pravosudie/46/konvencija-o-prestupnosti-v-sfere-kompyuternoj-informacii-185rus-angl.html).

4. Семькина, О.И. Противодействие киберпреступности за рубежом / О.И. Семькина // Журнал зарубежного законодательства и сравнительного правоведения. – 2016. – № 6(61) – С. 104–113.

5. Стаценко, В.Г. Киберкриминология как область криминологического знания: объект исследования и перспективы развития / В.Г.Стаценко // Право. Экономика. Психология. – 2020. – № 3(19). – С. 29–34

6. Шидловский, А.В. Некоторые аспекты противодействия кибертерроризму и кибердиверсиям / А.В. Шидловский // Право.by. – 2018. – № 1. – С. 86–91.

**2. Тема: Уголовное законодательство Республики Беларусь в сфере информационно-коммуникационной безопасности**

***2.1 Задания формирующие знания на уровне узнавания***

***Проблемы для изучения (темы рефератов) в рамках КУСР***

10. Уголовно-правовая характеристика объективных и субъективных признаков преступлений против информационной безопасности

11. Виды преступлений против информационной безопасности и их составы в соответствие с Уголовным кодексом Республики Беларусь

12. Уголовно-правовая характеристика ст. 349 УК «Несанкционированный доступ к компьютерной информации»

13. Уголовно-правовая характеристика ст. 350 УК «Уничтожение, блокирование или модификация компьютерной информации»

14. Уголовно-правовая характеристика ст. 352 УК «Неправомерное завладение компьютерной информацией»

15. Уголовно-правовая характеристика ст.354 УК «Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств»

16. Уголовно-правовая характеристика ст. 355 УК «Нарушение правил эксплуатации компьютерной системы или сети»

17. Уголовно-правовая характеристика ст. 203<sup>1</sup> УК «Незаконные действия в отношении информации о частной жизни и персональных данных» и 203<sup>2</sup> УК «Несоблюдение мер обеспечения защиты персональных данных»

***2.2 Задания формирующие знания на уровне воспроизведения:***

1. Охарактеризуйте международные стандарты уголовно-правовой борьбы с преступлениями против информационной безопасности.

2. Определите преимущества и недостатки уголовно-правовой охраны информационной безопасности в Республике Беларусь

### 2.3 Задания формирующие знания на уровне применения:

*Решите задачи:*

1. Серегин взломал компьютерную базу данных потерпевшей Ахтямовой, проникнув на ее страничку в сайте «В контакте», обидевшись на то, что девушка не желала продолжить с ним виртуальную переписку. Решив отомстить, он украл и поменял пароли от ее электронного почтового ящика и анкеты на сайте. В результате девушка не могла попасть на свою страницу. Серегин вступал от ее имени в эротическую переписку с мужчинами, а также разместил фотографии порнографического содержания.

*Есть ли в действиях Серегина признаки какого-либо состава преступления?*

2. Директора А.О. Бульдогова заинтересовали банковские счета конкурента. Он нанял специалиста, который, преодолев защиту, проник в компьютерную сеть банка, отыскал информацию об операциях по нужному счету и вывел ее на экран монитора. Бульдогов просмотрел информацию и сделал выписки в блокнот о заинтересовавших его операциях по счету.

*Квалифицируйте содеянное.*

3. Логунов написал и распространил с помощью электронной почты программу, которая активизировалась при попытке открыть почтовое сообщение и производила несанкционированные изменения в операционной системе. 31 декабря на мониторах всех компьютеров с измененным программным обеспечением отобразилось: «С новым годом!».

*Квалифицируйте содеянное Логуновым.*

4. Боков сконструировал прибор – сканер, с помощью которого перехватывал идентификационные коды мобильных телефонов пользователей и, вводя их в память своего устройства, осуществлял звонки, счета на оплату которых приходили законным абонентам. Общая сумма в счетах пользователям сотовых телефонов превысила базовую величину более чем в 250 раз.

В ходе предварительного расследования было установлено, что идентификационный код, перехватываемый Боковым, является компьютерной информацией.

*Решите вопрос об ответственности Бокова.*

5. Шевцов и Трусов, продолжительное время работая на одном предприятии - ООО "Виктория", вступили в сговор, направленный на хищение ликероводочной продукции. Они обговорили условия, по которым Шевцов создает на фирме условия для получения продукции без предоплаты, а Трусов обеспечивает вывоз и сбыт.

Будучи главным специалистом службы сбыта и маркетинга и зная порядок ввода информации в локальную компьютерную сеть для последующего получения продукции предприятия с отсрочкой платежа, Шевцов с помощью компьютера проник в локально-вычислительную сеть ООО «Виктория», где, уничтожив в списке клиентов фирмы запись «300» – номер договора с ЗАО «Лотос», ввел в указанный реестр заведомо ложную информацию о фирме «Победа», что послужило основанием для отгрузки последней ликероводочной продукции.

Трусов подыскал для исполнения роли экспедитора своего знакомого Котова, о чем уведомил Шевцова, который на имеющемся у него типовом бланке оформил доверенность от фирмы «Победа» на получение 200 ящиков ликероводочной продукции на имя экспедитора Котова и поставил на нее оттиск печати фирмы «Победа».

На следующий день Котов, используя доверенность фирмы «Победа», вывез со склада ООО «Виктория» 4 тыс. бутылок водки «Столичная». Трусов реализовал водку за наличный расчет, полученные деньги поделил со Швецовым и Котовым.

*Дайте юридическую оценку действиям указанных лиц.*

### ***Источники и литература:***

1. Уголовный кодекс Республики Беларусь [Электронный ресурс]: 9 июля 1999 г., № 275-З: принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

2. Швед, Н.А. Несанкционированный доступ к компьютерной информации: анализ состава преступления [Электронный ресурс] / Н.А. Швед // КонсультантПлюс: Беларусь. Технология 3000 / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

### **3. Тема: Современные криминалистические технологии расследования преступлений в сфере ИКТ**

#### ***3.1 Задания формирующие знания на уровне узнавания.***

##### ***Проблемы для изучения (темы рефератов) в рамках КУСР***

1. Особенности концепции теории информационно-компьютерного обеспечения криминалистической деятельности.

2. Элементы системы концепции теории информационно-компьютерного обеспечения криминалистической деятельности.

3. Основные закономерности концепции теории информационно-компьютерного обеспечения криминалистической деятельности.

4. Понятие и проблемы терминологии электронной цифровой криминалистики.

5. Цели, задачи, функции электронной цифровой криминалистики.

#### ***3.2 Задания формирующие знания на уровне воспроизведения:***

1. Охарактеризуйте инструментальные модули, необходимые для обнаружения следов преступлений в сфере современных информационно-коммуникационных технологий.

2. Охарактеризуйте современные технологии криминалистического исследования компьютерных систем, их сетей и периферийного оборудования.

3. Охарактеризуйте современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений.

4. Охарактеризуйте современные возможности цифровой криминалистики при производстве судебных экспертиз.

#### ***3.3 Задания формирующие знания на уровне применения:***

1. Приведите примеры современного применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий.

2. Приведите примеры современного применения криминалистических технологий при обнаружения следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

3. Приведите примеры современного применения криминалистических технологий при фиксации следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

4. Приведите примеры современного применения криминалистических технологий при изъятия следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

5. Приведите примеры передовых практических методов расследования преступлений в области цифровой криминалистики.

6. Сформулируйте вопросы экспертам при назначении криминалистической экспертизы Интернета вещей.

### Источники и литература

1. Вехов В.Б. Электронная криминалистика: понятие и система // Криминалистика: актуальные вопросы теории и практики: сб. трудов участников междунар. науч.-практич. конф. – Ростов н/Д., 2017. – С. 40–46.
2. Иванов, Н.А. Экспертиза электронных документов и машинограмм / Н.А. Иванов. – М: Юрлитинформ, 2009. – 144 с.
3. Ищенко, Е.П. К вопросу об экспертном и криминалистическом обеспечении расследования киберпреступности / Е.П. Ищенко // Вестник Московского университета МВД России, – 2013. – №3. – С. 15–17.
4. Ищенко, Е.П. Криминалистические аспекты расследования киберпреступлений / Е.П. Ищенко // Уголовное производство: процессуальная теория и криминалистическая практика: материалы V Международной научно-практической конференции, 27–29 апреля 2017 года, г. Симферополь-Алушта / отв. ред. М.А. Михайлов, Т.В. Омельченко; Крымский федеральный университет имени В.И. Вернадского. – Симферополь: ИТ «АРИАЛ», 2017. – с. 62–64.
5. Криминалистика XXI века: стратегия и тактика развития: коллективная монография. – Москва: Проспект, 2016. – 208 с.
6. Мальцагов И.Д. Современные технологии в расследовании преступлений: компьютерная криминалистика / И.Д. Мальцагов // Экономика. Бизнес. Право. – 2018. – № 4–6(26). – С. 44–48.
7. Медведев И.В. Компьютерная криминалистика «Форензика» и киберпреступность в России / И.В. Медведев // Пролог: журнал о праве. – 2013. – № 3. – С. 66–69.
8. Побегайло, А.Э. Борьба с киберпреступностью: учеб. пособие / А.Э. Побегайло; Ун-т прокуратуры Рос. Федерации. – М., 2018. – 184 с.
9. Россинская Е.Р., Рядовский И.А. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский // Московский государственный юридический университет имени О.Е. Кутафина (МГЮА) «Lex russica (Русский закон)» – 2019. № 3(148). – С. 87–99.
10. Россинская, Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е.Р. Россинская // Вестник Восточно-сибирского института МВД России. – 2019. – № 2 (89). – С. 193–202.
11. Смушкин А.Б. К вопросу о наименовании теории «Электронная цифровая криминалистика» / А.Б. Смушкин // Проблемы уголовного процесса, криминалистики и судебной экспертизы. – 2019. – № 1(13). – С. 15–21.
12. Степаненко Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко, В.В. Коломинов // ГлаголЪ правосудия. – 2018. – № 3(17). – С. 38–43.
13. Харина, Э.Н. Киберпреступления: уголовно-правовой и криминалистический аспект / Э.Н. Харина // Вестник университета имени О.Е. Кутафина (МГЮА). – 2017. – № 5. – С.164–171. DOI: 10.17803/2311-5998.2017.33.5.164–171.
14. Шаталов, А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции / А.С. Шаталов // Вестник Сибирского юридического института МВД России. – 2018. – № 3(32). – С. 7–15.

## РАЗДЕЛ КОНТРОЛЯ ЗНАНИЙ

### ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ К ЭКЗАМЕНУ

1. Понятие информационно-коммуникационной безопасности как составляющей национальной безопасности
2. Понятие, содержание и значение информационной безопасности человека, общества и государства в современных социально-экономических условиях.
3. Политика государства в сфере информационной безопасности, современное состояние и проблемы информационной безопасности.
4. Криминогенные факторы современного цифрового мира.
5. Законодательство Республики Беларусь в области обеспечения информационной безопасности.
6. Концепция информационной безопасности Республики Беларусь.
7. Киберпреступность как объект изучения киберкриминологии: понятие, проблемы терминологии, основные концепции и подходы к изучению в современной доктрине.
8. Киберкриминология как формирующаяся область научного знания.
9. Международно-правовое определение киберпреступности. Классификация киберпреступлений.
10. Характеристика основных видов преступлений в сфере современных информационно-коммуникационных технологий.
11. Современные тенденции киберпреступности в мире.
12. Состояние, динамика и особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.
13. Проблемы противодействия киберпреступности и предупреждения киберпреступлений.
14. Международные стандарты уголовно-правовой борьбы с преступлениями против информационной безопасности.
15. Зарубежный опыт и борьбы с преступлениями в сфере современных информационно-коммуникационных технологий.
16. Уголовно-правовая характеристика объективных и субъективных признаков преступлений против информационной безопасности
17. Несанкционированный доступ к компьютерной информации как преступление против информационной безопасности (ст. 349 УК).
18. Уничтожение, блокирование или модификация компьютерной информации (ст. 350 УК).
19. Неправомерное завладение компьютерной (ст. 352 УК).
20. Разработка, использование, распространение либо сбыт вредоносных компьютерных программ или специальных программных или аппаратных средств (ст. 354 УК).
21. Нарушение правил эксплуатации компьютерной системы или сети (ст. 355 УК).
22. Уголовно-правовая характеристика норм УК о преступлениях, предметом или средством совершения которых является информация.
23. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности.
24. Характеристика инструментальных модулей, необходимых для обнаружения следов преступлений в сфере современных информационно-коммуникационных технологий.



25. Современные возможности применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий.

26. Современные технологии криминалистического исследования компьютерных систем, их сетей и периферийного оборудования.

27. Использование современных криминалистических технологий при обнаружении, фиксации, изъятии следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

28. Понятие, проблемы терминологии, цели, задачи, функции электронной цифровой криминалистики.

29. Современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений.

30. Передовые практические методы расследования преступлений в области цифровой криминалистики.

31. Современные возможности цифровой криминалистики при производстве судебных экспертиз.

32. Криминалистическая экспертиза Интернета вещей.

## **ТЕМАТИКА ДОКЛАДОВ, РЕФЕРАТОВ, ПРЕЗЕНТАЦИЙ, ЭССЕ**

1. Понятие, содержание и значение информационной безопасности современного цифрового (информационного) общества.

2. Современное состояние и проблемы информационной безопасности.

3. Историко-правовой анализ развития законодательства Республики Беларусь в области обеспечения информационной безопасности.

4. Концепция информационной безопасности Республики Беларусь и субъекты ее реализации.

5. Акты ООН и Совета Европы о борьбе с киберпреступлениями как инструмент международного сотрудничества.

6. Криминогенные факторы современного цифрового мира.

7. Виды и источники угроз информационной безопасности Республики Беларусь.

8. Киберпреступность: понятие, основные концепции.

9. Международно-правовая классификация киберпреступлений.

10. Современные тенденции киберпреступности в мире.

11. Кибертерроризм и киберэкстремизм.

12. Использование искусственного интеллекта криминальными сообществами.

13. Современные биотехнологии и преступность.

14. Хакеры: криминологическая характеристика.

15. Сетевые «тролли» и иные группы травли в Интернете.

16. Организованная преступность цифрового мира.

17. Особенности преступности в сфере современных информационно-коммуникационных технологий в Республике Беларусь.

18. Уголовно-правовая характеристика объективных и субъективных признаков преступлений против информационной безопасности.

19. Несанкционированный доступ к компьютерной информации как преступление против информационной безопасности.

20. Модификация компьютерной информации и компьютерный саботаж (ст. 350-351 УК): характеристика и отграничение составов.

21. Проблемы правоприменительной практики статей гл. 31 УК в деятельности органов, ведущих уголовный процесс.

22. Зарубежный опыт и международные стандарты уголовно-правовой борьбы с преступлениями в сфере современных информационно-коммуникационных технологий.

23. Уголовно-правовая характеристика и проблемы применения норм УК о преступлениях, предметом или средством совершения которых является информация.

24. Незаконное соби́рание либо распространение информации о частной жизни и нарушение тайны переписки, телефонных переговоров, телеграфных или иных сообщений.

25. Нарушение авторского права, смежных прав и права промышленной собственности (ст. 201 УК): проблемы применения и пути совершенствования.

26. Уголовная ответственность за коммерческий шпионаж.

27. Судебная практика по уголовным делам о преступлениях против информационной безопасности.

28. Использование новейших технологий цифрового мира в предупреждении преступлений.

29. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности.

30. Характеристика инструментальных модулей, необходимых для обнаружения следов преступлений в сфере современных информационно-коммуникационных технологий.

31. Современные возможности применения специальных знаний при расследовании преступлений в сфере современных информационно-коммуникационных технологий.

32. Современные технологии криминалистического исследования компьютерных систем, их сетей и периферийного оборудования.

33. Использование современных криминалистических технологий при обнаружении, фиксации, изъятии следовой информации преступлений в сфере современных информационно-коммуникационных технологий.

34. Понятие, проблемы терминологии, цели, задачи, функции электронной цифровой криминалистики.

35. Современные криминалистические возможности работы с цифровыми доказательствами при расследовании преступлений.

36. Передовые практические методы расследования преступлений в области цифровой криминалистики.

37. Современные возможности цифровой криминалистики при производстве судебных экспертиз.

38. Криминалистическая экспертиза Интернета вещей.

## ВСПОМОГАТЕЛЬНЫЙ РАЗДЕЛ

### ЛИТЕРАТУРА

#### *Нормативные правовые акты:*

1. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в области обеспечения информационной безопасности [Электронный ресурс]: [Заключено в г. Санкт-Петербурге 20.11.2013] // Консультант Плюс: Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
2. Соглашение о сотрудничестве государств – участников Содружества Независимых Государств в борьбе с преступлениями в сфере информационных технологий [Заключено в г. Душанбе 28 сентября 2018] // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
3. Convention on Cybercrime. The Council of Europe. Hungary. –2001. [Электронный ресурс]. –Режим доступа: [http:// cyber-crime.com/legislative](http://cyber-crime.com/legislative). – Дата доступа: 21.09.2022
4. Соглашение между Правительством Российской Федерации и Правительством Республики Беларусь о сотрудничестве в области обеспечения международной информационной безопасности (Заключено в г. Москве 25 декабря 2013) // Консультант Плюс: Беларусь / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022
5. Кодекс Республики Беларусь об административных правонарушениях [Электронный ресурс]: 6 января 2021 г. № 91-3; принят Палатой представителей 18 декабря 2020 г.: одобр. Советом Респ. 18 декабря 2020 г. // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
6. Уголовный кодекс Республики Беларусь [Электронный ресурс]: 9 июля 1999 г., № 275-3; принят Палатой представителей 2 июня 1999 г.: одобр. Советом Респ. 24 июня 1999 г.// ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
7. Уголовно-процессуальный кодекс Республики Беларусь, 16 июля 1999 г. // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
8. О единой государственной системе регистрации и учета правонарушений: Закон Респ. Беларусь, 9 янв. 2006 г., № 94-3 [Электронный ресурс] // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
9. Об органах внутренних дел Республики Беларусь [Электронный ресурс]: Закон Респ. Беларусь, 17 июля 2007 г., № 263-3 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
10. Об основах деятельности по профилактике правонарушений [Электронный ресурс]: Закон Республики Беларусь, 4 янв. 2014 г., № 122-3 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
11. О регистре населения [Электронный ресурс]: Закон Респ. Беларусь от 21 июля 2008 г., № 418-3 // Эталон-Беларусь [Электронный ресурс] / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
12. О государственных секретах: Закон Республики Беларусь, 29 нояб. 1994 г., № 3410-ХП // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». – Минск, 2022.
13. Об авторском праве и смежных правах [Электронный ресурс] Закон Респ. Беларусь, 17 мая 2011 г., № 262-3 // Консультант Плюс: Беларусь.Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

14. Об электронном документе и электронной цифровой подписи [Электронный ресурс]: Закон Респ. Беларусь, 28 дек. 2009 г., № 113-3 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

15. Об информации, информатизации и защите информации [Электронный ресурс]: Закон Респ. Беларусь, 10 ноября 2008 г., № 455-3: в ред. Закона Респ. Беларусь от 1 июля 2017 г. // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

16. О защите персональных данных: Закон Республики Беларусь 7 мая 2021 г. № 99-3 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информ. Республики Беларусь. – Минск, 2022.

17. О развитии цифровой экономики [Электронный ресурс]: Декрет Президента Респ. Беларусь, 21 дек. 2017 г., № 8 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

18. Об утверждении Концепции национальной безопасности Республики Беларусь [Электронный ресурс]: Указ Президента Респ. Беларусь, 9 нояб. 2010 г., № 575 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

19. О мерах по совершенствованию использования национального сегмента сети Интернет Указ Президента Республики Беларусь от 01.02.2010 N 60 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

20. О некоторых мерах по совершенствованию защиты информации (вместе с «Положением о технической и криптографической защите информации в Республике Беларусь» [Электронный ресурс]: Указ Президента Респ. Беларусь, 16 апр. 2013 г., № 196 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.

21. Концепция информационной безопасности Республики Беларусь [Электронный ресурс]: утверждена постановлением Совета Безопасности Республики Беларусь, 18 марта 2019 г., № 1 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». Минск, 2022.

22. О Государственной программе «Цифровое развитие Беларуси» на 2021–2025 годы: Постановление Совета Министров Республики Беларусь 2 февраля 2021 г. № 66 // Эталон – Беларусь [Электронный ресурс] / Нац. центр правовой информации Республики Беларусь. - Минск, 2022

23. Об утверждении Инструкции о порядке ведения электронного журнала регистрации административных правонарушений: приказ МВД Республики Беларусь, 12 сен. 2016 г., № 246 // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». Минск, 2022.

24. Об утверждении Инструкции о порядке предоставления доступа к автоматизированной информационной системе «ГАИ-Центр» и некоторых вопросах ее функционирования: приказ МВД Республики Беларусь от 23 августа 2016 года № 223// Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». Минск, 2022.

25. Об утверждении Инструкции о порядке предоставления удаленного доступа к базам данных, администрируемым информационным центром Министерства внутренних дел Республики Беларусь: приказ МВД Республики Беларусь от 29 июня 2015 года № 200// Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». Минск, 2022.

26. Верховенство права в Интернете и в остальном цифровом мире: тематический доклад Совета Европы. 2014. [Электронный ресурс]. – Режим доступа: <https://docviewer.yandex.by/view/173172177/?page>. – Дата доступа: 21.02.2022

#### ***Основная литература***

27. Абламейко, М.С. Правовые проблемы построения информационного общества в Республике Беларусь: теория и практика: диссертация на соискание ученой степени кандидата юридических наук: 12.00.14 / М.С. Абламейко. – Белорусский государственный университет. – Минск, 2012. – 129, [4] л.

28. Дмитриева, Т.Ф. Криминалистика: курс лекций / М-во образования Республики Беларусь, Учреждение образования «Витебский государственный университет имени П.М. Машерова», каф. уголовного права и уголовного процесса. – 2-е изд., с изм. и доп. – Витебск: ВГУ имени П.М. Машерова, 2018. – 340, [1] с.

29. Криминалистика: пособие для студентов учреждений высшего образования, обучающихся по специальности 1-24 01 02 «Правоведение» / [под ред. В.Б. Шабанова, В.Л. Григоровича]; Белорусский государственный университет. – Минск: БГУ, 2019. – 550, [2] с.

30. Нестеров, С.А. Информационная безопасность: учебник и практикум для академического бакалавриата / Санкт-Петербургский политехнический университет Петра Великого. – Москва: Юрайт, 2018. – 321 с.

31. Пантелеева, Н.В. Уголовное право (особенная часть): теория и практик: учеб.-метод. пособие для студентов учреждений высшего образования, обучающихся по специальности 1-24 01 02 «Правоведение» / М-во образования Республики Беларусь, Учреждение образования «Могилевский государственный университет имени А.А. Кулешова». – Могилев: МГУ имени А.А. Кулешова, 2020. – 505 с.

#### ***Дополнительная литература***

32. Абламейко М.С. Правовые проблемы построения информационного общества в Республике Беларусь: теория и практика: автореф. дис. на соиск. учен. степ. канд. юрид. наук: по спец. 12.00.14 - административное право, финансовое право, информационное право / БГУ. – Минск., 2012. – 25 с

33. Арчаков, В.Ю. Нормативное регулирование информационной безопасности в Республике Беларусь (в условиях становления и развития цифровой экономики) // В.Ю. Арчаков, О.С. Макаров, А.Л. Баньковский // Право.by. – 2018. – № 6. – С. 53–58.

34. Амброс, Ю. Предупреждение, выявление и раскрытие в сфере высоких технологий - актуальное направление деятельности правоохранительных органов Беларуси / Ю. Амброс // Законность и правопорядок. – 2018. – № 3. – С. 29–35.

35. Боричевская, В.В. Уголовно-правовые аспекты обеспечения информационной безопасности в Республике Беларусь / В.В. Боричевская // Гуманітарна-эканамічны Веснік. – 2010. – № 2. – С. 56–65.

36. Вехов, В.Б. Тактические особенности расследования преступлений в сфере компьютерной информации: научно-практ. пособие / В.Б. Вехов. / Изд. 2-е, доп. и испр. – М.: ЛексЭст, 2004. – 157 с.

37. Вехов, В.Б. Электронная криминалистика: понятие и система / В.Б. Вехов // Криминалистика: актуальные вопросы теории и практики: сб. трудов участников междунар. науч.-практ. конф. – Ростов н/Д., 2017. – С. 40–46.

38. Воронцова, С.В. Киберпреступность: проблемы квалификации преступных деяний / С.В. Воронцова // Российская юстиция. – 2011. – N 2. – С. 14–15.

39. Вус, М.А. Понятийный аппарат сферы информационной безопасности в нормативно-правовой базе ОДКБ / М.А. Вус // Теоретические и прикладные аспекты информационной безопасности: материалы Междунар. науч.-практ. конф., Минск, 19 июня 2014 г. / Акад. МВД Респ. Беларусь; редкол.: В.Б. Шабанов [и др.]. – Минск, 2015. – С. 221–223.

40. Гаврилин, Ю.В. Особенности слепообразования при совершении мошенничества в сфере компьютерной информации / Ю.В. Гаврилин, В.В. Шипилов // Российский следователь. – 2013. – № 23 – С. 2–6.
41. Гаврилин, Ю.В. Практика организации взаимодействия при расследовании преступлений, совершенных с использованием информационно-коммуникативных технологий / Ю.В. Гаврилин // Труды Академии управления МВД России. – 2018. – № 4. – С. 145–150.
42. Гамко С.Л. Следственная деятельность в условиях изменения «ландшафта» киберпреступности: безопасность конфиденциальных данных и профилактика / С.Л. Гамко // Предварительное расследование. – 2019. – № 1. – С. 76–79.
43. Гамко, С.Л. Разоблачение преступной схемы хищения криптовалюты / С.Л. Гамко // Предварительное расследование. – 2019. – № 2. – С. 87–90.
44. Гамко, С.Л. О положительном опыте расследования преступлений, связанных с наложением ареста на криптовалюту, полученную преступным путем / С.Л. Гамко [и др.] // Предварительное расследование. – 2020. – № 2. – С. 78–81.
45. Гриб, В.Г. О международном сотрудничестве в противодействии преступлениям, совершаемым с использованием банковских карт / В.Г. Гриб, С.В. Васюков // Российский следователь. – 2013. – № 6. – С. 35–40.
46. Грибунов, О.П. Расследование преступлений в сфере компьютерной информации и высоких технологий: учеб. пособие / О.П. Грибунов, М.В. Старчиков. – М.: ДГСК МВД России, 2017. – 159 с.
47. Губич, М.В. Современное состояние и проблемы правового регулирования государственно-частного партнерства в сфере противодействия киберпреступности / М. В. Губич // Вестник Академии МВД Республики Беларусь. – 2020. – № 1. – С. 53–56.
48. Далинин, А.В. Преступления в сфере компьютерной информации: учеб. пособие / А.В. Далинин, Е.А. Зорина, О.А. Рослякова. – Санкт-Петербург: С.-Петерб. ун-т упр. и экономики, 2014. – 178 с.
49. Деятельность органов внутренних дел по борьбе с преступлениями, совершенными с использованием информационных, коммуникационных и высоких технологий: учебное пособие / [А.В. Аносов и др.]. – М.: Академия управления МВД России, 2019. – Ч. 1. – 208 с.
50. Дремлюга, Р.И. Международно-правовое регулирование сотрудничества в сфере борьбы с Интернет-преступностью / Р.И. Дремлюга // Библиотека криминалиста. – 2013. – №5(10). – С.339–346.
51. Дубко, М.А. Новый облик главы о киберпреступлениях: симбиоз результатов научных исследований и практики применения / М.А. Дубко // Право.by. – 2020. – № 6. – С. 30–35.
52. Зуев, С.В. Новые правила изъятия электронных носителей и копирования информации / С.В. Зуев, В.С. Черкасов // Законность. – 2019, № 5. – С. 40–43.
53. Евдокимов, К.Н. Актуальные вопросы противодействия компьютерной преступности в Российской Федерации (криминологическое исследование) / К.Н. Евдокимов // Российский следователь. – 2018. – № 10 – С. 56–61.
54. Евдокимов, К.Н. Криминологические и уголовно-правовые аспекты противодействия компьютерной преступности в России (социологическое исследование) / Евдокимов К.Н. // Российский следователь. – 2020. – № 11. – С. 41–44.
55. Зверьянская, Л.П. Информационные преступления как угроза информационной безопасности российского общества / Л.П. Зверьянская // Право и государство: теория и практика. – 2017. – № 1. – С. 127–130.
56. Иванов, Н.А. Экспертиза электронных документов и машинограмм / Н.А. Иванов. – М: Юрлитинформ, 2009. – 144 с.

57. Информационная революция и вызовы новой эпохи - стимулы формирования современных подходов к информационной безопасности: материалы Междунар. науч.-практ. конф. (Минск, 29–30 ноября 2018 г.): в 2 т. редкол.: С.Н. Князев (гл. ред.) [и др.]; Комитет государственной безопасности Республики Беларусь, Государственное учреждение образования «Ин-т национальной безопасности Республики Беларусь». – Минск: ИНБ, 2019.

58. Ищенко, Е.П. К вопросу об экспертном и криминалистическом обеспечении расследования киберпреступности / Е.П. Ищенко // Вестник Московского университета МВД России, – 2013. – № 3. – С. 15–17.

59. Ищенко, Е.П. Криминалистические аспекты расследования киберпреступлений / Е.П. Ищенко // Уголовное производство: процессуальная теория и криминалистическая практика: материалы V Международной научно-практической конференции, 27–29 апреля 2017 года, г. Симферополь-Алушта / отв. ред. М.А. Михайлов, Т.В. Омельченко ; Крымский федеральный университет имени В.И. Вернадского. – Симферополь: ИТ «АРИАЛ», 2017. – С. 62–64.

60. Криминалистика XXI века: стратегия и тактика развития: коллективная монография. – Москва: Проспект, 2016. – 208 с.

61. Криминалистика: учебник / под ред. Т.А. Седовой, С.П. Кушниренко, В.Д. Пристанкова. – М.: ЮСТИЦИЯ, 2019. – 712 с.

62. Козлов, В.Е. Отдельные аспекты получения криминалистически значимой информации при осуществлении противодействия компьютерной преступности / В.Е. Козлов // Вестник Академии МВД Республики Беларусь. – 2016. – № 1 – С. 63–67.

63. Колиев, В.В. Проблемы производства экспертизы электронных документов / В.В. Колиев // Право и государство: теория и практика. – 2020. – № 4. – С. 168–170.

64. Колычева, А.Н. К вопросу об использовании ресурсов сети Интернет в преступной деятельности / А.Н. Колычева // Российский следователь. – 2016. – № 24 – С. 42–44.

65. Климов, Д.В. Расследование хищений, связанных с использованием сети «Интернет»: учеб. пособие / Д.В. Климов. – Н. Новгород: Нижегородская академия МВД России, 2017. – 24 с.

66. Косович, М.В., Лимож, Н.И. Компьютерная преступность: уголовно-правовые и криминологические вопросы // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр». Минск, 2022.

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

68. Левшук, О.И. Киберпреступность как масштабная угроза мировому сообществу / О.И. Левшук // Юстыцыя Беларусі = Юстиция Беларуси. – 2020. – № 1. – С. 20–24.

69. Лопатина, Т.М. Проблемы формирования уголовно-правового способа борьбы с компьютерным мошенничеством / Т.М. Лопатина // Библиотека криминалиста. – 2013. – № 5(10). – С. 32–41.

70. Лопатина, Т.М. Отдельные вопросы характеристики уголовно-правовых признаков субъекта преступлений в сфере компьютерной информации [Электронный ресурс] / Т.М. Лопатина // Консультант Плюс: Россия. Технология Проф / ООО «ЮрСпектр». Минск, 2018.

71. Лунева, А.В. Алгоритм действий следователей на стадии возбуждения уголовного дела о хищении, совершенном бесконтактным способом путем использования дистанционного банковского обслуживания / Лунева А.В., Клименко А.К. // Российский следователь. – 2020. – № 11. – С. 3–6.

72. Маликов, В.В. Комплексный методический подход оперативной оценки уровня киберпреступлений / В.В. Маликов, Е.А. Криштопова // Вестник Полоцкого государственного университета. Сер. С, Фундаментальные науки. – 2013. – № 12. – С. 54–58.

73. Мальцагов, И.Д. Современные технологии в расследовании преступлений: компьютерная криминалистика / И.Д. Мальцагов // Экономика. Бизнес. Право. – 2018. – № 4–6(26). – С. 44–48.

74. Макаров, О.С. Концептуальные направления правового регулирования в сфере информационной безопасности Республики Беларусь / О.С. Макаров, А.Л. Баньковский // Право.by. – 2018. – № 5. – С. 53–58.

75. Медведев, И.В. Компьютерная криминалистика «Форензика» и киберпреступность в России / И.В. Медведев // Пролог: журнал о праве. – 2013. – № 3. – С. 66–69.

76. Минин, А.Я. О специфике противодействия киберпреступности / А.Я. Минин // Российский следователь. – 2013. – № 8. – С. 37–39.

77. Мороз, Н.О. Основные этапы развития сотрудничества в борьбе с преступностью в сфере высоких технологий [Электронный ресурс] / Н.О. Мороз. – Режим доступа: <http://www.pac.by/dfiles/001353466563moro4.pdf>.

78. Мороз, Н.О. Оговорки и поправки к международным договорам: на примере международных соглашений по борьбе с киберпреступностью / Мороз Н.О. // Право.by. – 2013. – № 1. – С. 94–99.

79. Мороз, Н.О. Роль ООН в координации международного сотрудничества в борьбе с преступностью в сфере высоких технологий / Н.О. Мороз // Право.by. – 2014. – № 3. – С. 90–95.

80. Мороз, Н.О. Международно-правовое сотрудничество в борьбе с преступностью в сфере высоких технологий: автореф. дис. на соиск. учен. степ. канд. юрид. наук: по спец. 12.00.10 – международное право; европейское право / БГУ. – Минск., 2014. – 23 с. – Библиогр.: С. 18–20.

81. Мукашев, С.И. Международно-правовое сотрудничество государств-участников СНГ в борьбе с преступностью в сфере компьютерной информации / С.И. Мукашев // Право.by. – 2014. – № 5. – С. 81–86.

82. Новые способы совершения преступлений в сфере информационных технологий на территории государств – участников СНГ: аналитический обзор / И.Б. Колчевский, В.М. Журавлев, А.Г. Кузнецов и О.В. Демковец, Д.А. Брехов. – М.: ФГКУ «ВНИИ МВД России», 2018. – 76 с.

83. Овсейко, С. Информация как объект права: понятие, передача, защита / С. Овсейко // Юстыця Беларусі. – 2014. – № 3. – С. 55–60.

84. Организация расследования преступлений в сфере высоких технологий: учебное пособие для обучающихся учреждений высшего образования Министерства внутренних дел Республики Беларусь / П.В. Гридюшко [и др.]; под общ. ред. И.Г. Мухина; учреждение образования «Академия Министерства внутренних дел Республики Беларусь». – Минск: Академия МВД Республики Беларусь, 2017 – 139 с.

85. Основы борьбы с киберпреступностью и кибертерроризмом: хрестоматия / сост. В.С. Овчинский. – М.: Норма, 2017. – 527 с.

86. Павловец, Г.А. Фиксация доказательственной информации с помощью цифровых средств: автореф. дис. ... канд. юрид. наук: 12.00.09 / Академия МВД Республики Беларусь. – Минск, 2012. – 24 с.

87. Побегайло, А.Э. Борьба с киберпреступностью: учеб. пособие / А.Э. Побегайло; Ун-т прокуратуры Рос. Федерации. – М., 2018. – 184 с.

88. Полещук, Д.Г. Понятие и объект преступления против информационной безопасности / Д.Г. Полещук // Право.by. – 2016. – № 6. С. 87–92.



89. Полещук Д.Г. Уголовно-правовая охрана информационной безопасности (на примере отдельных аспектов охраны кибербезопасности и защиты информации ограниченного распространения): автореф. дис. на соиск. учен. степ. канд. юрид. наук: по специальности 12.00.08 – уголовное право и криминология; уголовно-исполнительное право / Белорусский государственный университет. – Минск, 2020. – 32 с.
90. Попов, А.Н. Преступления в сфере компьютерной информации: учебное пособие / А.Н. Попов. – Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. – 68 с.
91. Радыно, Т.В. Правовые меры защиты информации [Электронный ресурс] / Т.В. Радыно // Консультант Плюс: Беларусь. Технология 3000 / ООО «ЮрСпектр», Нац. центр правовой информ. Респ. Беларусь. Минск, 2022.
92. Расследование мошенничества в сфере компьютерной информации: учеб. пособие / авт.-сост. П.А. Капустюк [и др.]. – Иркутск: Восточно-Сибирский ин-т МВД России, 2018. – 47 с.
93. Россинская, Е.Р., Рядовский, И.А. Современные способы компьютерных преступлений и закономерности их реализации / Е.Р. Россинская, И.А. Рядовский // Московский государственный юридический университет имени О.Е. Кутафина (МГЮА) “Lex russica (Русский закон)” – 2019. № 3(148). – С. 87–99.
94. Россинская, Е.Р. Теория информационно-компьютерного обеспечения криминалистической деятельности: концепция, система, основные закономерности / Е.Р. Россинская // Вестник Восточно-сибирского института МВД России. – 2019. – № 2(89). – С. 193–202.
95. Русскевич, Е.А. Уголовная ответственность за преступления в сфере компьютерной информации по законодательству Китайской Народной Республики: сравнительно-правовой анализ / Е.А. Русскевич // Журнал зарубежного законодательства и сравнительного правоведения. – 2018. – № 5 – С. 108–113.
96. Русскевич, Е.А. Уголовное наказание и цифровые технологии: точка бифуркации / Е.А. Русскевич // Государство и право. – 2020. – № 7. – С. 77–84.
97. Саванович, Н. Уголовная ответственность за незаконные действия с персональными данными / Н. Саванович [Электронный ресурс]. – Режим доступа: <https://pravo.by/novosti/analitika/2021/june/65306/>. – Дата доступа: 26.12.2021.
98. Саркисян, А.Ж. Криминологическая характеристика преступлений, совершаемых в сфере информационно-коммуникационных технологий / А.Ж. Саркисян // Российский следователь. – 2019. – № 3 – С. 54–59.
99. Семькина, О.И. Противодействие киберпреступности за рубежом / О.И. Семькина // Журнал зарубежного законодательства и сравнительного правоведения. – 2016. – № 6 (61) – С. 104–113.
100. Смушкин А.Б. К вопросу о наименовании теории «Электронная цифровая криминалистика» / А.Б. Смушкин // Проблемы уголовного процесса, криминалистики и судебной экспертизы. – 2019. – № 1(13). – С. 15–21.
101. Степаненко Д.А. Цифровая реальность и криминалистика / Д.А. Степаненко, В.В. Коломинов // Глаголь правосудия. – 2018. – № 3(17). – С. 38–43.
102. Стаценко, В.Г. Киберкриминология как область криминологического знания: объект исследования и перспективы развития / В.Г. Стаценко // Право. Экономика. Психология. – 2020. – № 3(19). – С. 29–34.
103. Степаненко, Д.А. “Адаптивная модификация” криминалистики в информационном обществе как закономерная реакция на распространение киберпреступности / Д.А. Степаненко // Российский следователь. – 2015. – № 15. – С. 17–20.

104. Топорикова, О.О. Перспективы криминализации в Республике Беларусь сексуальных домогательств в отношении детей с использованием сети Интернет / О.О. Топорикова // *Право.by* – 2015. – № 4. – С. 108–114.
105. Харина, Э.Н. Киберпреступления: уголовно-правовой и криминалистический аспект / Э.Н. Харина // *Вестник университета имени О.Е. Кутафина (МГЮА)*. – 2017. – № 5. – С. 164–171. DOI: 10.17803/2311-5998.2017.33.5.164–171.
106. Хлус, А. Защита информации – основное направление обеспечения национальной безопасности Республики Беларусь / А. Хлус // *Юстыцыя Беларусі*. – 2014. – № 5. – С. 54–59.
107. Чекунов, И.Г. Понятие и отличительные особенности киберпреступности / И.Г. Чекунов // *Российский следователь*. – 2014. – № 18. – С. 53–56.
108. Шаталов, А.С. Разработка методических основ расследования преступлений, совершаемых с помощью компьютерных и сетевых технологий: проблемы, перспективы и тенденции / А.С. Шаталов // *Вестник Сибирского юридического института МВД России*. – 2018. – № 3(32). – С. 7–15.
109. Швед, Н.А. Несанкционированный доступ к компьютерной информации: анализ состава преступления [Электронный ресурс] / Н.А. Швед // *КонсультантПлюс: Беларусь. Технология 3000 / ООО «Юрспектр», Нац. центр правовой информ. Респ. Беларусь*. – Минск, 2022.
110. Шидловский, А.В. Некоторые аспекты противодействия кибертерроризму и кибердиверсиям / А.В. Шидловский // *Право.by*. – 2018. – № 1. – С. 86–91.
111. Электронные носители информации в криминалистике: монография / под ред. О.С. Кучина. – М.: Юрлитинформ, 2017. – 304 с.
112. Сведения о регистрации и предварительном расследовании преступлений по Республике Беларусь за 2006–2021 годы / МВД Республики Беларусь – Информационно-аналитическое управление. – Минск, 2007–2022.

Учебное издание

**УГОЛОВНО-ПРАВОВЫЕ,  
КРИМИНОЛОГИЧЕСКИЕ И КРИМИНАЛИСТИЧЕСКИЕ  
ПРОБЛЕМЫ РАССЛЕДОВАНИЯ И ПРЕДУПРЕЖДЕНИЯ  
КИБЕРПРЕСТУПЛЕНИЙ  
ДЛЯ СПЕЦИАЛЬНОСТИ II СТУПЕНИ ВЫСШЕГО ОБРАЗОВАНИЯ  
(МАГИСТРАТУРА) 1-24 80 01 ЮРИСПРУДЕНЦИЯ**

Учебно-методический комплекс по учебной дисциплине

Составители:

**ДМИТРИЕВА** Татьяна Федоровна

**СТАЦЕНКО** Владимир Григорьевич

Технический редактор

*Г.В. Разбоева*

Компьютерный дизайн

*Л.И. Ячменёва*

Подписано в печать 21.03.2022. Формат 60x84 <sup>1</sup>/<sub>16</sub>. Бумага офсетная.

Усл. печ. л. 5,21. Уч.-изд. л. 5,91. Тираж 34 экз. Заказ 24.

Издатель и полиграфическое исполнение – учреждение образования  
«Витебский государственный университет имени П.М. Машерова».

Свидетельство о государственной регистрации в качестве издателя,  
изготовителя, распространителя печатных изданий

№ 1/255 от 31.03.2014.

Отпечатано на ризографе учреждения образования  
«Витебский государственный университет имени П.М. Машерова».

210038, г. Витебск, Московский проспект, 33.