

УЧРЕЖДЕНИЕ ОБРАЗОВАНИЯ  
«МОГИЛЕВСКИЙ ИНСТИТУТ  
МИНИСТЕРСТВА ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ БЕЛАРУСЬ»

Кафедра социально-гуманитарных дисциплин

ИНТЕРНЕТ-КОММУНИКАЦИЯ В ДЕЯТЕЛЬНОСТИ  
ОРГАНОВ ВНУТРЕННИХ ДЕЛ

методические рекомендации по изучению дисциплины для специальностей  
1-93 01 01 Правовое обеспечение общественной безопасности;  
1-93 01 03 Правовое обеспечение оперативно-розыскной деятельности

Форма получения образования: заочная

Курсы: 3-4

Семестры: 6-7

Разработчик:  
начальник кафедры  
майор милиции Венидиктов С.В.

Допущены к использованию в образовательном процессе  
кафедрой социально-гуманитарных дисциплин 28.09.2021, протокол № 1.1

2021 г.



## СОДЕРЖАНИЕ

Введение.....	4
Тематический план дисциплины.....	8
Рекомендации по изучению тем учебной дисциплины.....	9
Тема 1, 3-5. Теоретические основы изучения интернет-коммуникации. Личность в интернет-коммуникативном пространстве. Сообщества в коммуникативном интернет-пространстве. Массовая коммуникация в интернет-пространстве.....	9
Рекомендации по организации самостоятельной работы в межсессионный период.....	14
Тема 2, 6-7. Органы внутренних дел в современном интернет-коммуникативном пространстве. Интернет-преступность. Информационная безопасность.....	21
Литература по курсу.....	30
Перечень вопросов для подготовки к зачету.....	36
Глоссарий.....	38

## ВВЕДЕНИЕ

### Цели и задачи учебной дисциплины

Учебная дисциплина «Интернет-коммуникация в деятельности органов внутренних дел» направлена на изучение существующих в современной психологии и социологии концепций информационного общества, особенностей коммуникации и взаимодействия в сети Интернет, специфики сетевых сообществ как социальных групп, пространства интернет-коммуникации как места реализации различных социальных и правовых практик, а также влияния компьютерно-опосредованной коммуникации на личность пользователя.

Целью учебной дисциплины «Интернет-коммуникация в деятельности органов внутренних дел» является формирование социально-личностных компетенций курсанта, направленных на эффективное использование коммуникативных ресурсов сети Интернет в профессиональной деятельности.

Реализация этой цели предполагает решение следующих задач:

формирование знаний о структуре информационной среды Интернет и эффектах (в т. ч. патогенных), возникающих в ней;

усвоение современной методологии исследования коммуникации в Интернете;

приобретение навыков успешной сетевой коммуникации, поиска информации в Сети;

изучение вопросов психологии и технологий преступлений в сфере высоких технологий,

освоение методов изучения личности преступника по результатам анализа его сетевой активности;

рассмотрение проблем криминализации Интернета и киберпреступности, потенциальных возможностей использования Интернета и современных технологий сетевой коммуникации представителями криминального мира (в т. ч. организованными преступными сообществами);

раскрытие возможностей использования интернет-технологий в борьбе с негативными общественными явлениями, превентивных возможностей Сети;

формирование понятия об информационной безопасности на уровне индивида, социальной группы, государства.

Место учебной дисциплины в системе подготовки специалиста.

Связи с другими учебными дисциплинами

Изучение дисциплины «Интернет-коммуникация в деятельности органов внутренних дел» позволяет формировать целый ряд профессиональных компетенций, предусмотренных образовательными стандартами, касающихся вопросов профилактики правонарушений и преступлений, а также их раскрытия в условиях информатизации современного общества.

Стремительное развитие информационно-коммуникационных технологий в XXI в. привело к быстрому росту производительных сил общества, а также к пониманию информации как самостоятельного объекта человеческой деятельности. Развитие информационных и коммуникационных технологий не

только кардинально изменило структуру, способы функционирования средств массовой коммуникации и каналы распространения информации, но и привело к значительным трансформациям в профессиональных компетенциях.

Неотъемлемым элементом современной информационной среды стала всемирная компьютерная сеть Интернет, формирующая новые условия как взаимодействия граждан, так и осуществления профессиональной деятельности. Новые возможности, предоставляемые развитием информационных технологий, не только изменяют психологию коммуникации, но и формируют новую среду криминализации общества, изменяя способы совершения преступлений. В то же время органы внутренних дел в виде интернет-технологий получают доступный и эффективный инструмент мониторинга, профилактики и борьбы с преступностью.

В ходе изучения дисциплины «Интернет-коммуникация в деятельности органов внутренних дел» курсанты приобретают навыки успешной сетевой коммуникации, поиска информации, проведения мониторинга и анализа сетевых сообществ.

«Интернет-коммуникация в деятельности органов внутренних дел» является дисциплиной гуманитарного цикла, что обуславливает необходимость межпредметных связей с дисциплинами «Психология девиантного поведения», «Риторика», «Профессиональная этика».

### Требования к освоению учебной дисциплины

Изучение учебной дисциплины должно способствовать формированию следующих компетенций:

академических:

АК-7. Иметь навыки, связанные с использованием технических устройств, управлением информацией и работой с компьютером.

социально-личностных:

СЛК-10. Обеспечивать защиту сведений, составляющих государственную и служебную тайну, сведений конфиденциального характера и иных охраняемых законом тайн.

профессиональных:

ПК-5. Выявлять и предупреждать угрозы безопасности личности, общества и государства; принимать возможные меры по пресечению преступления, административного правонарушения.

ПК-12. Своевременно оказывать медицинскую и другую необходимую помощь лицам, пострадавшим от преступлений, административных правонарушений и несчастных случаев, лицам, находящимся в беспомощном или опасном для жизни или здоровья состоянии; обеспечивать личную безопасность и безопасность граждан в процессе решения служебных задач.

ПК-14 (специальность 1-93 01 01). Реализовывать законодательство Республики Беларусь о работе с обращениями.

В результате освоения учебной дисциплины «Интернет-коммуникация в деятельности органов внутренних дел» курсант должен:

знать:

особенности интернет-среды как медиасферы и виртуальной реальности;  
основные тенденции развития современного интернет-пространства;

психологическую типологизацию интернет-пользователей;  
особенности киберпространства и его воздействие на психику индивида, социальную организацию, познавательные процессы;  
основные направления использования сети Интернет в криминальных целях;  
патогенные эффекты интернет-среды;  
особенности конструирования виртуального «Я» и стратегии самопрезентации в Сети;  
социальные последствия расширения использования интернет-технологий;  
аксиологические характеристики киберпространства;  
направления обеспечения информационной безопасности;  
уметь:  
осуществлять самостоятельный мониторинг интернет-ресурсов;  
применять эффективные принципы общения в Интернете в процессе поиска оперативной информации;  
осуществлять психологическое и социальное категорирование на основе анализа продуктов сетевой активности;  
анализировать взаимосвязь между состоянием интернет-среды в локальном социуме и динамикой групповых социальных процессов;  
проводить первичную диагностику состояния интернет-зависимости в различных группах информационного риска;  
устанавливать психологические мотивы интернет-пользователей;  
определять характеристики наиболее распространенных типов интернет-субкультур;  
владеть:  
навыками эффективной сетевой коммуникации;  
методами и приемами самостоятельного поиска информации в Интернете;  
навыками рефлексивного потребления информационных продуктов, находящихся в открытом доступе в Интернете;  
приемами анализа информации в социальных сетях;  
инструментами обеспечения анонимности и защиты данных в Интернете;  
правилами сетевого этикета и успешного общения в Интернете.

В обучении предполагается сбалансированное использование традиционных и инновационных технологий обучения. Главными особенностями традиционных методик изучения предмета являются изложение учебного материала в виде лекций с последующей его проработкой на семинарских и практических занятиях. При этом работа на лекциях связана с освоением теоретического материала, в то время как на семинарских и практических занятиях предпочтение отдается его анализу, осмыслению и практическому применению. При использовании этих методик важная роль в изучении курса отводится самостоятельной работе как с литературными источниками, так и с открытыми сетевыми ресурсами сети Интернет.

Использование нетрадиционных технологий связано с активным использованием компьютерных технологий, сетевых образовательных ресурсов, электронным сопровождением научно-методического обеспечения учебного процесса. Среди применяемых технологий и методов следует выделить коммуникативные технологии (дискуссия, коллективный анализ сетевого

контента, учебные дебаты и другие); технологию учебно-исследовательской деятельности; метод анализа конкретных ситуаций (метод кейсов); метод анализа продуктов деятельности; игровые технологии, в рамках которых курсанты участвуют в деловых, ролевых, имитационных играх и др.

#### Объем учебной дисциплины, формы получения образования и формы текущей аттестации

Учебная дисциплина «Интернет-коммуникация в деятельности органов внутренних дел» изучается в очной и заочной формах получения высшего образования.

В соответствии с учебными планами учреждения образования по специальностям 1-93 01 01 Правовое обеспечение общественной безопасности, 1-93 01 03 Правовое обеспечение оперативно-розыскной деятельности на изучение учебной дисциплины отводится всего 80 часов.

На изучение учебной дисциплины в заочной форме отводится 12 аудиторных часов, из них лекций – 4, практических занятий – 4, семинарских занятий – 4. Учебная дисциплина изучается в 6 и 7 семестрах, форма текущей аттестации – зачет (7).

## ТЕМАТИЧЕСКИЙ ПЛАН ДИСЦИПЛИНЫ

Название раздела, темы	Всего часов	Аудиторные часы				Управляемая самостоятельная работа
		Всего	Лекции	Семинарские занятия	Практические занятия	
1	2	3	4	5	6	7
6 семестр						
Тема 1, 3-5. Теоретические основы изучения интернет-коммуникации. Личность в интернет-коммуникативном пространстве. Сообщества в коммуникативном интернет-пространстве. Массовая коммуникация в интернет-пространстве.	4	4	2	2		
7 семестр						
Тема 2, 6-7. Органы внутренних дел в современном интернет-коммуникативном пространстве. Интернет-преступность. Информационная безопасность.	8	8	2	2	4	
Зачет						
Всего часов по дисциплине	12	12	4	4	4	

## РЕКОМЕНДАЦИИ ПО ИЗУЧЕНИЮ ТЕМ УЧЕБНОЙ ПРОГРАММЫ

ТЕМА 1, 3-5. Теоретические основы изучения интернет-коммуникации.

Личность в интернет-коммуникативном пространстве.

Сообщества в коммуникативном интернет-пространстве.

Массовая коммуникация в интернет-пространстве.

Время на изучение темы – 4 часа

Лекция – 2 часа

Семинарское занятие – 2 часа

### *Содержание учебного материала*

Интернет-коммуникация как элемент информационного общества. Понятие, концепции и характеристики информационного общества. Современные информационные технологии, информатизация общества. Государственная программа развития цифровой экономики и информационного общества в Республике Беларусь.

Доступ в Интернет: права и возможности. Понятие «цифровых прав» и «цифрового барьера». Динамика роста пользователей Интернета и статистика использования коммуникационных ресурсов Интернета в современном мире. Особенности использования информационно-коммуникационных технологий населением Республики Беларусь.

Понятие интернет-коммуникации. Основные коммуникационные ресурсы Интернета. Виды коммуникационных интернет-услуг: ресурсы Всемирной паутины, веб-форумы, блоги, социальные сети, электронная почта, мессенджеры, чаты, массовые многопользовательские онлайн игры.

Особенности среды интернет-коммуникации: понятия «виртуальная реальность» и «киберпространство». Характеристики интернет-коммуникации: глобальность, опосредованность, анонимность, добровольность и доступность контактов, нетипичность поведения, совмещение виртуального и реального. Формы и уровни интернет-коммуникации.

Самопрезентация личности в интернет-коммуникации. Стратегии виртуальной самопрезентации. Конструирование виртуального «Я». Причины модификации идентичности в сети. Особенности использования стратегий виртуальной самопрезентации.

Вопрос публичности и приватности в Интернете. Проблемы и угрозы для личности в коммуникационном интернет-пространстве.

Интернет как публичное пространство. Отражение и организация социальных взаимоотношений в Интернете. Характер распространения и обмена информацией.

Характеристики онлайн-сообществ. Особенности групповой коммуникации с использованием различных видов социальных сетей.

Особенности интернет-солидарности. Протестная коммуникация в социальной сети. Формирование макросолидарности в онлайн-среде. Опасности социальных сетей.

Массовая информация и массовая коммуникация. Основные формы, элементы, особенности массовой информации. Виды массово-информационной деятельности. Медиа как субъекты массовой коммуникации.

Система средств массовой коммуникации (СМК), ее структурные элементы и среда. Типологические характеристики СМК. Функции СМК. Аудитория СМК. Массовая коммуникация в глобальной сети Интернет.

Принципы регулирования деятельности СМК (правовые и этические). Законодательство в области СМИ в Республике Беларусь. Право на информацию.

Проблемы формирования общественного мнения. Общественная апатия.

Мониторинг материалов в средствах массовой коммуникации в Интернете. Контент-анализ.

Особенности массовой коммуникации в интернет-пространстве Республики Беларусь.

### ***Вопросы, рассматриваемые на лекционном занятии***

1. Интернет-коммуникация в контексте информационного общества.
2. Самопрезентация личности в интернет-коммуникации.
3. Особенности коммуникации в рамках интернет-сообществ.
4. СМИ и другие информационные ресурсы Интернета.

Изучив тему, курсант должен

Знать:

– понятия «информационное общество», «информатизация» «информационные технологии», «интернет-технологии», «интернет-коммуникация», «цифровые права», «цифровой барьер»;

– характеристики информационного общества;

– направления развития цифровой экономики и информационного общества в Республике Беларусь;

– основные показатели использования Интернета в мире и Республике Беларусь;

– виды коммуникационных ресурсов Интернета;

– понятия виртуальности и виртуальной реальности, свойства виртуальной реальности;

– понятие и основные аспекты киберпространства;

– характеристики и формы коммуникации в интернет-пространстве;

– стратегии виртуальной самопрезентации;

– понятие и признаки интернет-аддикции;

– понятие, возможности и типы социальных сетей в Интернете, наиболее популярные социальные сети в мире и Республике Беларусь;

– понятие интернет-солидарности, условия и этапы ее формирования;

– типы субъектов интернет-солидарности, способы создания и функционирования солидарных отношений в Интернете;

– виртуальные и реальные последствия интернет-солидарности;

– основные формы, элементы, особенности массовой информации;

– виды массово-информационной деятельности;

- типологические характеристики, функции и аудиторию СМК;
- принципы регулирования деятельности СМК.

Уметь:

- сравнивать особенности использования информационно-коммуникационных технологий населением в разных регионах мира;
- анализировать основные тенденции развития интернет-технологий, выявлять их способ и степень влияния на жизнь людей и общества;
- классифицировать интернет-ресурсы в зависимости от вида и уровня коммуникации;
- анализировать особенности использования стратегий виртуальной самопрезентации;
- аргументировать позитивное и негативное влияние интернет-коммуникации на личность;
- анализировать социальные проблемы, вызванные эволюцией социальных сетей в Интернете;
- анализировать проблемы формирования общественного мнения.

Владеть:

- навыками обращения к различным коммуникативным видам интернет-ресурсов для их эффективного использования в личных целях, а также для выполнения задач в рамках служебной деятельности;
- навыками конструирования социально-психологического портрета личности на основании анализа образа, характеристик и функций его виртуальной модели;
- навыками анализа сетевых групп и сообществ на предмет выявления деструктивных черт их деятельности;
- навыками контент-анализа материалов, размещаемых в средствах массовой коммуникации в Интернете.

### ***Вопросы для подготовки к семинарскому занятию***

1. Интернет-коммуникация в контексте информационного общества.
2. Самопрезентация личности в интернет-коммуникации.
3. Особенности коммуникации в рамках интернет-сообществ.
4. Интернет-солидарность.
5. СМИ и другие информационные ресурсы Интернета.

### ***Задания на самостоятельную подготовку (устно)***

1. Изучите статистические данные показателей использования Интернета в мире и Республике Беларусь.
2. Сравните основные тенденции использования информационно-коммуникационных ресурсов населением в разных странах мира.

## ***Материалы для самоконтроля по теме***

### *Вопросы для самоконтроля*

1. Как соотносятся понятия информационное общество и постиндустриальное общество?
2. Какие основные характеристики информационного общества принято выделять?
3. С чем связано появление термина «информатизация» и как отличаются процессы информатизации в разных регионах мира?
4. Чем отличаются традиционные и современные информационные технологии?
5. Что приводит к «цифровому неравенству» между различными регионами и странами мира?
6. Какое место занимают интернет-технологии среди других информационных технологий и в чем особенность их влияния на жизнь общества?
7. В каком виде организованы основные коммуникационные ресурсы Интернета?
8. Какие возможности представляет пользователям веб-форумы?
9. Каковы основные черты блогов в пространстве Интернета и каковы мотивы использования данного ресурса?
10. В чем привлекательность массовых многопользовательских игр, и каким образом в них реализуется аспект общения?
11. Что общего и различного в личном разговоре и общении в чате в Интернете?
12. С чем связана популярность социальных сетей среди пользователей Интернета во всем мире?
13. Что такое виртуальность и виртуальная реальность, создаваемая информационными технологиями?
14. Каковы характеристики виртуальной реальности?
15. Какие существуют виды и технологии виртуальной реальности? Каково практическое применение данных технологий?
16. Что такое виртуальная личность? Перечислите различные определения понятия «виртуал».
17. В каких случаях используются разные типы виртуальной личности?
18. Каковы особенности и направления самопрезентации личности в виртуальном пространстве сети Интернет?
19. Каковы основные направления самопрезентации личности в виртуальном пространстве сети Интернет?
20. Как взаимодействуют виртуальность и реальность в современном мире?
21. Каковы позитивные и негативные последствия интенсивного взаимодействия с интернет-пространством?
22. Что такое интернет-аддикция и как она проявляется?
23. Какой процесс способствует тому, что полученная информация начинает влиять на человека/группу, меняя их установки и поведение?
24. Какие особенности приобретают информационные потоки в социальной

сети, учитывая множественность независимых центров аккумуляции и распространения информации в интернете?

25. Какую форму социального взаимодействия называют интернет-солидарностью?

26. Каковы основные условия формирования интернет-солидарности?

27. Каковы специфические способы создания и функционирования солидарных отношений в интернете?

28. Что такое протестная форма коммуникации в социальных сетях? Какие социальные последствия она может иметь?

29. Как вы понимаете закон «доминирования слабых связей» в контексте интернет-коммуникации?

30. Каковы основные этапы образования солидарности в онлайн-пространстве?

31. Кто может являться участником протестной интернет-солидарности?

32. Какими могут быть результаты различных видов интернет-солидарности?

33. Что такое массовая информация и массовая коммуникация?

34. Каковы основные формы, элементы и особенности массовой информации?

35. Какие существуют виды массово-информационной деятельности?

36. Что включает в себя система средств массовой коммуникации (СМК)?

37. Каковы структурные элементы и среда СМК?

38. Что относят к типологическим характеристикам СМК?

39. Каковы функции, а также аудитория СМК?

40. В чем состоят отличительные особенности массовой коммуникации в глобальной сети Интернет?

41. Какие принципы регулируют деятельности СМК (правовые и этические)?

42. В чем состоит проблемы формирования общественного мнения в Интернете?

## **РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ САМОСТОЯТЕЛЬНОЙ РАБОТЫ В МЕЖСЕССИОННЫЙ ПЕРИОД**

### *Теоретические вопросы для самостоятельного изучения*

Проблемы и угрозы для личности в коммуникационном интернет-пространстве.

Приватное и публичное в Интернете. Проблема приватности в интернет-коммуникациях.

Понятие и проявления интернет-аддикции.

Коммуникация в сетевом пространстве.

Проблемы формирования общественного мнения.

Контент-анализ материалов в средствах массовой коммуникации в Интернете.

### *Методические рекомендации по самостоятельному изучению теоретических вопросов по теме 1,3-5*

Обратите внимание на различия в подходах в соотношении понятий постиндустриального общества и информационного общества. Сравните эффект воздействия на общество информационных технологий прошлого и современных информационных технологий. Сделайте различие между видами интернет-технологиями, непосредственно связанными с общением между людьми и теми, в которых коммуникация минимальна. Обозначьте основные акценты в проблеме доступа и прав в Интернете. Сравните показатели использования Интернета в Беларуси с данными по другим регионам мира и обозначьте общие и различные тенденции. Обратите внимание на особенности организации коммуникационных ресурсов Интернета и сделайте вывод о влиянии, которое может оказывать такой способ взаимодействия на стиль общения пользователей.

Обратите внимание на тот факт, что характерные черты общения в Интернете являются следствием особенностей устройства и организации сетевого пространства, вовлекающего пользователей в специфическую коммуникационную среду. Рассмотрение специфических особенностей функционирования виртуальной реальности и киберпространства, даст возможность сформироваться более глубокому пониманию того, почему общение в Интернете выглядит тем или иным образом. Сделайте акцент на отличительных особенностях интернет-общения, обозначить, чем именно коммуникация в сети отличается от взаимодействия в реальной жизни. Рассмотрите мотивы конструирования разных типов виртуальной идентичности, попытайтесь определить конструктивные и деструктивные черты использования виртуальной личности. Обозначьте наиболее существенные проблем и угрозы для личности, возникающее в коммуникативном интернет-пространстве.

Обратите внимание на то, что сетевые структуры Интернета являются фундаментом информационного общества, основой становления новых типов социальных групп и социальных взаимодействий. В реальной практике социальных взаимодействий коммуникация осуществляется во многом благодаря традициям и привычкам, которые слабеют, если не кодируют себя в новой системе. В результате роль традиционных социальных сообществ в массовых коммуникациях начала постепенно снижаться, сохранили влияние лишь те

традиции, которые приняли логику сети. Особенности публичного пространства Интернета наиболее очевидны при рассмотрении феномена социальных сетей. Появление и развитие социальных сетей способствует развитию новой культуры и всего общества. Такой способ коммуникации выполняет большое количество функций, позволяет человеку самореализоваться, получать новую полезную информацию, самосовершенствоваться и оценивать результаты. Также социальные сети постепенно превращаются в социальное пространство, которое служит своеобразным полигоном для создания и тестирования различных коммуникативных стратегий и приемов взаимодействий, свидетельствует о ее огромном социальном потенциале.

Четко обозначьте основные формы, элементы, особенности массовой информации, определите виды массово-информационной деятельности. Рассмотрите систему средств массовой коммуникации, ее структурные элементы и среду. Дайте типологические характеристики СМК, обозначьте их функции, аудиторию. Определите, в чем особенность массовой коммуникации в глобальной сети Интернет. Остановитесь на особенностях формирования общественного мнения в коммуникационном пространстве Интернета. Найдите отличительные черты, усиливающие воздействие информации, размещаемой в виртуальном пространстве, на пользователей сети. Сформулируйте основные приемы контент-анализа, используемые в рамках изучения материалов, размещаемых в средствах массовой информации в Интернете.

### ***Материалы для анализа и самоконтроля***

Для анализа используются материалы, размещенные в открытом доступе в сети Интернет: веб-порталы, социальные сети, блоги, форумы и т. п.

Теоретический материал для самостоятельного изучения размещен в ЭУМКД «Интернет-коммуникация в деятельности ОВД» в системе [sdo.institutemvd.by](http://sdo.institutemvd.by).

Самоконтроль осуществляется посредством выполнения тестовых заданий в обучающем режиме.

### ***Перечень источников для изучения***

#### ***Основная литература***

Венидиктов, С. В. Интернет-коммуникация в деятельности органов внутренних дел : учебное пособие / С. В. Венидиктов, Н. В. Вашрова. – Минск : РИВШ, 2020. – 236 с.

Психология и коммуникация в правовой системе [Электронный ресурс] : сборник статей / [редкол.: С. В. Венидиктов (отв. ред.) [и др.] ; Мин-во внутр. дел Респ. Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь». – Могилев : Могилевский институт МВД Республики Беларусь, 2016. – 1 электрон. опт. диск (CD-R).

Пыжова, Н. Н. Психология электронной коммуникации : пособие / Н. Н. Пыжова, Н. В. Волох ; Академия управления при Президенте Республики Беларусь. – Минск : Академия управления при Президенте, 2017. – 134 с.

Формирование позитивного общественного мнения о работе органов внутренних дел Республики Беларусь : методические рекомендации / Министерство внутренних дел Республики Беларусь ; под общ. ред. И. А.

Поздеева. – Минск : Штаб МВД Республики Беларусь : [Академия МВД Республики Беларусь], 2016. – 55 с.

*Дополнительная литература*

Бакулев, Г. П. Массовая коммуникация: Западные теории и концепции: Учеб. пособие для студентов вузов. – 2-е изд., перераб. и доп. / Г. П. Бакулев. – М: Аспект Пресс, 2010. – 192 с.

Белинская, Е. П. Психология интернет-коммуникации / Е. П. Белинская. – М.: НОУ ВПО Московский психолого-социальный университет, МОДЭК, 2013. – 192 с.

Белл, Д. Социальные рамки информационного общества / Д. Белл // Новая технократическая волна на Западе. – М. : Прогресс, 1986. – С. 330–342.

Информационное общество в Республики Беларусь. Статистический сборник. – Минск: Национальный статистический комитет Республики Беларусь, 2017. – 105 с.

Кастельс М. Информационная эпоха: Экономика, общество и культура // Пер. с англ. под науч. ред. О. И. Шкаратана; Гос. ун-т. Высш. шк. экономики. – М., 2000. – 606 с.

Республика Беларусь. Статистический ежегодник 2018. – Минск: Национальный статистический комитет Республики Беларусь, 2018. – 489 с.

***Практические задания для самостоятельного выполнения  
в межсессионный период***

Преподаватель определяет задания, которые необходимо выполнить в межсессионный период. Используется следующий перечень заданий:

*Задание 1.*

Ознакомиться с различными видами веб-форумов, представленными в интернет-пространстве и охарактеризовать:

1) веб-форумы, наиболее популярные в русскоязычной среде Интернета (название, возможности, предоставляемые данными ресурсами, их аудитория, стиль обсуждения);

2) тематические веб-форумы (название, возможности, предоставляемые данными ресурсами, их аудитория, стиль обсуждения);

3) найти примеры веб-форумов с различным типом организации комментариев (линейным, древовидным).

*Задание 2.*

Ознакомиться с различными блогами, представленными в интернет-пространстве и охарактеризовать:

1) блоги, наиболее популярные в русскоязычной среде Интернета (название, возможности, предоставляемые данными ресурсами, их аудитория, топ авторов и тем);

2) тематические блоги (название, возможности, предоставляемые данными ресурсами, их аудитория, топ авторов и тем).

*Задание 3.*

Ознакомиться с различными видами социальных сетей, представленными в

интернет-пространстве и охарактеризовать:

1) социальные сети, наиболее популярные в мире (название, возможности, предоставляемые данными ресурсами, их аудитория);

2) социальные сети, наиболее популярные в русскоязычной среде Интернета, а также в Республике Беларусь (название, возможности, предоставляемые данными ресурсами, их аудитория).

Курсанты предоставляют заполненный электронный документ практических заданий в формате MicrosoftWord (*обязательная форма*).

Работы высылаются на адрес электронной почты, согласованный с преподавателем. Срок выполнения задания – не позднее, чем за 1 неделю до начала лабораторно-экзаменационной сессии 7 семестра.

*Образец формы, заполняемой курсантами в ходе выполнения заданий по теме.*

### ЗАДАНИЕ №1

ВЕБ-ФОРУМЫ	
Название	
Возможности	
Тематика	
Аудитория	
Особенности комментирования	

### ЗАДАНИЕ №2

БЛОГИ	
Название	
Возможности	
Топ авторов	
Тематика топовых постов	
Аудитория	
Особенности комментирования	

### ЗАДАНИЕ №3

СОЦИАЛЬНЫЕ СЕТИ	
Популярные во всем мире	
Название	
Возможности	
Сферы применения	
Аудитория	
Популярные в русскоязычной среде и в Беларуси	
Название	
Возможности	
Сферы применения	
Аудитория	

#### Задание 4.

Проанализировать примеры присвоения чужой личности в интернет-пространстве. Для выполнения задания необходимо:

1. Изучить пользователей на различных интернет-площадках и найти среди них тех, кто действует под чужими именами, используя персональные данные других людей.

Для поиска в качестве интернет-площадок можно использовать веб-порталы, социальные сети, блоги, форумы и т.п. Обратите внимание: персональные данные пользователя должны быть не вымышленными (произвольными, фантастическими, историческими и т.п.), а действительными, отсылающими к живому конкретному человеку. В качестве примера можно использовать фейковые аккаунты и действия в Интернете известных людей, за которыми скрываются анонимные пользователи.

2. Выбрать один пример пользователя, о котором можно утверждать, что он/она не является тем человеком, за которого себя выдает (на основании его/её персонального аккаунта либо модерации группы в социальных сетях или блогах, личной веб-страницы или веб-сайта, веб-публикаций (заметок, аудио, видео, визуальных материалов) на различных веб-ресурсах, диалоги на форумах и т.п.

3. Проанализировать особенности самопрезентации выбранного пользователя, изучив следующие черты:

а) *степень фальсификации*. В какой мере пользователь старается убедить аудиторию в том, что он является тем лицом, за которое себя выдает. Перечислите все элементы, которые он для этого использует.

б) *особенности образа, созданного путем фальсификации*. Определите социальные и психологические черты, которые приписываются личности конкретного человека вследствие действий анонима. Обозначьте признаки, на основании которых можно сделать подобное заключение.

в) *черты фальсификатора*. Определите социальные и психологические черты самого анонима, действующего под чужим именем. Объясните, на основании чего можно сделать вывод о характеристиках анонима.

4. Предположить, какие цели преследует фальсификатор и какие могут быть последствия подобной фальсификации для реального человека, личность, которого используют (материальные, репутационные, психологические и т.д.)

5. Зафиксировать все ответы в электронном формате.

Работы высылаются на адрес электронной почты, согласованный с преподавателем. Срок выполнения задания – не позднее, чем за 1 неделю до начала лабораторно-экзаменационной сессии 7 семестра.

*Образец формы, заполняемой курсантами в ходе выполнения задания.*

Имя пользователя	
Сетевой ресурс	
Степень фальсификации	
Особенности сконструированного образа	
Черты фальсификатора	

Социальные характеристики (указать элементы самопрезентации, на основании которой сделаны выводы о характеристиках)	
Психологические характеристики (указать элементы самопрезентации, на основании которой сделаны выводы о характеристиках)	

### *Задание 5.*

#### *Подготовка докладов (сообщений) по темам*

1. Современные интернет-технологии и концепция «интерактивного общества».
2. Информационное общество в Республике Беларусь: основные направления и факторы развития.
3. Основные коммуникационные ресурсы Интернета.
4. Формы социального взаимодействия в виртуальной среде.
5. Публичное пространство Интернета: понятие, соотношение публичности, общедоступности и приватности.
6. Деструктивная деятельность в социальных сетях.
7. Правовое регулирование массовой информации в Интернете.
8. Отличительные признаки средств массовой коммуникации в Интернете.

Тема доклада (сообщения) выбирается курсантом самостоятельно. Текст сообщения высылается на адрес электронной почты, согласованный с преподавателем. Срок выполнения задания – не позднее, чем за 1 неделю до начала лабораторно-экзаменационной сессии 7 семестра. Доклад (сообщение) озвучивается в ходе аудиторных занятий 7 семестра.

### *Задание 6.*

Необходимо найти в социальной сети «ВКонтакте» группы/сообщества, содержащие провокационные материалы, склоняющие людей к тяжелым формам депрессии и сомнению в смысле своего существования, способствующие появлению и укреплению суицидальных наклонностей (явными или завуалированными способами).

Для выполнения задания необходимо:

1) найти группы, посвященные теме смерти. Данные группы не должны быть сообществами, которые направлены на аудиторию пользователей, потерявших близких людей и стремящихся рассказать о своих переживаниях другим людям, получить эмоциональную поддержку и попробовать пережить свое горе. Коммуникация в группах такого типа может носить жизнеутверждающий характер. Кроме этого, не учитываются сообщества, которые представляют определенные виды субкультуры (чаще молодежной субкультуры) интересующиеся тематикой и символикой смерти, но трактующие

ее как сферу мистических загадочных и протестных смыслов жизни. Целью поиска являются именно те группы, в которых ценность жизни ставится под сомнение и нагнетаются негативные эмоции.

2) выбрать несколько таких групп и проанализировать следующие аспекты:

– кого можно считать целевой аудиторией данного сообщества (на основании заявленной темы, типа и содержания размещаемых материалов);

– кто является модератором группы, кто те участники группы, которые размещают материалы (что это за категории пользователей: социально-демографические характеристики, интересы, предпочтения);

– кто является подписчиками данной группы, кто чаще всего оставляет комментарии;

– какие материалы размещаются в группе, какие средства медиа используются;

– какие темы пользуются наибольшей популярностью, какие акценты (смыслы) расставляют пользователи;

– какие эмоции преобладают в группе, посредством чего создается тот или иной эмоциональный настрой.

3) оценить, какова степень риска попасть под влияние идей и настроений данной группы и укрепиться в суицидальных наклонностях у подростков, молодежи, взрослых людей.

Отчет по выполнению задания оформляется в свободной форме и высылается на адрес электронной почты, согласованный с преподавателем. Срок выполнения задания – не позднее, чем за 1 неделю до начала лабораторно-экзаменационной сессии 7 семестра.

### ***Контрольные мероприятия межсессионного периода***

В течение межсессионного периода курсанты выполняют тестовые задания (темы 1, 3, 4, 5), размещенные в ЭУМКД «Интернет-коммуникация в деятельности ОВД» в системе [sdo.institutemvd.by](http://sdo.institutemvd.by). Срок выполнения тестовых заданий – не позднее, чем за день до начала лабораторно-экзаменационной сессии 7 семестра.

ТЕМА 2, 6-7. ОРГАНЫ ВНУТРЕННИХ ДЕЛ В СОВРЕМЕННОМ  
ИНТЕРНЕТ-КОММУНИКАТИВНОМ ПРОСТРАНСТВЕ.  
ИНТЕРНЕТ-ПРЕСТУПНОСТЬ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Время на изучение темы – 8 часов

Лекция – 2 часа

Семинарское занятие – 2 часа

Практические занятия – 4 часа

*Содержание учебного материала*

Задачи информационно-коммуникативной деятельности ОВД в Интернете. Стихийный и целенаправленный факторы присутствия ОВД в Интернете. Причины влияния стихийного фактора (распространение слухов, влияние СМИ, специфика интернет-пространства, влияние индекса социального-доверия). Позиционирование органов внутренних дел в коммуникативном пространстве Интернета. Организация работы ОВД с масс-медиа, формирование информационных потоков, изучение общественного мнения. Примеры эффективной деятельности в Интернете подразделений ОВД

Взаимодействие органов внутренних дел с интернет-ресурсами. Понятия интернет-ресурса и сетевого издания. Закон Республики Беларусь «О средствах массовой информации». Информация, распространение и (или) предоставление которой ограничено. Информация, распространение которой в средствах массовой информации, на интернет-ресурсах запрещено.

Имиджевые модели сотрудников ОВД в коммуникативном пространстве. Понятие имиджа. Имидж ОВД как устойчивый, действенный, эмоционально окрашенный образ правоохранительной системы. Имиджирование и его субъекты. Фактор, атрибут, компонент имиджа. Компоненты имиджа ОВД. Внешний и внутренний имидж ОВД. Функции внутреннего имиджа. Причины противоречий между внешним и внутренним имиджем ОВД. Репутация органов внутренних дел.

Особенности интернет-преступности. Интернет-преступность и киберпреступность: соотношение понятий. Характеристики интернет-преступности.

Типология интернет-преступлений. Классификации интернет-преступлений. Мотивы совершения интернет-преступлений. Личностные особенности интернет-преступников и их типология. Преступники-хакеры, преступники-кракеры (взломщики), преступники-вирмейкеры, преступники-реализаторы. Спамеры, кардеры, фишеры, вишеры, винлокеры и др. типы преступников.

Криминализация Интернета и интернет-преступность в Республике Беларусь. Интернет-преступность и уголовное законодательство Республики Беларусь. История и статистика интернет-преступности в Республике Беларусь, примеры наиболее резонансных преступлений. Опасность неконтролируемого использования Интернета детьми и подростками. Противодействие криминализации Интернета в Республике Беларусь, взаимодействие государственных органов, правоохранительных структур, организаций гражданского общества.

Понятие информационной безопасности. Угрозы информационной безопасности. Способы противодействия информационным угрозам. Уровни противодействия угрозам информационной безопасности. Концепция информационной безопасности Республики Беларусь. Меры обеспечения кибербезопасности Республики Беларусь.

Сохранение анонимности и защита данных в Интернете. Правила создания и хранения паролей от интернет-аккаунтов. Правила безопасности при использовании банковских карточек. Открытые для пользователей инструменты, позволяющие сохранить анонимность и защитить данные при работе в Интернете.

Правила поведения в социальных сетях. Требования к сотрудникам ОВД при использовании социальных сетей. Правила этикета при общении в социальных сетях, по электронной почте, в мессенджерах. Условия сохранности информации в социальных сетях.

Деятельность ОВД в направлении обеспечения информационной безопасности.

### ***Вопросы, рассматриваемые на лекционном занятии***

1. Органы внутренних дел в интернет-коммуникативном пространстве.
2. Особенности интернет-преступности. Личность и типы интернет-преступников
3. Криминализация Интернета и интернет-преступность в Республике Беларусь.
4. Информационная безопасность. Деятельность ОВД в направлении обеспечения информационной безопасности.

Изучив тему, курсант должен

Знать:

- принципы информационно-коммуникативной деятельности ОВД;
- факторы, влияющие присутствие органов внутренних дел в коммуникативном пространстве на Интернета;
- задачи подразделений по связям с общественностью в структуре ОВД;
- понятия «имидж ОВД», «репутация ОВД»;
- особенности и характеристики интернет-преступности;
- основные мотивы совершения интернет-преступлений;
- типологию интернет-преступников;
- негативные явления, связанные с неконтролируемым использованием Интернета детьми и подростками;
- статьи Уголовного кодекса Республики Беларусь, в которых предусмотрена ответственность за преступления в сфере информационной безопасности;
- понятие информационной безопасности;
- основные угрозы информационной безопасности;
- основное содержание Концепции информационной безопасности Республики Беларусь;
- правила личной информационной безопасности;
- направления противодействия угрозам информационной безопасности;

– основные направления обеспечения информационной безопасности деятельности ОВД в Интернете;

Уметь:

– выявлять причины распространения слухов в коммуникативном пространстве;

– анализировать законодательство, регулирующее взаимодействие органов внутренних дел и внутренних войск МВД Республики Беларусь со СМИ;

– анализировать содержание интернет-ресурсов как источников информации об органах внутренних дел;

– устанавливать причины противоречий между внешним и внутренним имиджем ОВД;

– анализировать социальные предпосылки распространения интернет-преступности;

– устанавливать степень общественной опасности различных интернет-преступлений;

– выявлять социальные риски, связанные с совершением интернет-преступлений;

– приводить примеры резонансных преступлений в интернет-пространстве;

– выявлять последствия деструктивного информационного воздействия на личность и распространения искаженной информации;

– выявлять риски, связанные с информационной безопасностью, в деятельности сотрудников ОВД;

– обеспечивать сохранение анонимности и защиту личных данных в Интернете;

Владеть:

– методами критической рефлексии материалов о деятельности ОВД, размещаемых в сети Интернет;

– навыками анализа содержания аккаунтов в социальных сетях, посвященных деятельности ОВД;

– методами мониторинга сетевых ресурсов на наличие негативного контента;

– методами выявления социального портрета лица, причастного к совершению конкретного интернет-преступления;

– открытыми для пользователей инструментами, позволяющими сохранить анонимность и защитить данные при работе в Интернете;

– правилами этикета при общении в социальных сетях, по электронной почте, в мессенджерах.

### ***Вопросы для подготовки к семинарскому занятию***

1. Органы внутренних дел в интернет-коммуникативном пространстве.
2. Особенности интернет-преступности.
3. Личность и типы интернет-преступников
4. Криминализация Интернета и интернет-преступность в Республике Беларусь.
5. Информационная безопасность.
6. Деятельность ОВД в направлении обеспечения информационной безопасности.

### ***Задания на самостоятельную подготовку***

1. Проанализируйте причины противоречий между внутренним и внешним имиджем органов внутренних дел.
2. Опишите атрибуты имиджа сотрудника ОВД.

### ***Методические рекомендации по самостоятельному изучению вопросов темы***

Проведите различия между стихийным фактором присутствие ОВД в Интернете и целенаправленным позиционированием – результатом деятельности службы по связям с общественностью. Рассмотрите причины влияния стихийного фактора (слухи, влияние СМИ, специфика интернет-пространства). Раскройте структуру, задачи, правовые основы деятельности подразделений по связям с общественностью в ОВД. Дайте характеристику присутствию ОВД во всех секторах информационного пространства республики (печатные, электронные СМИ, Интернет).

Проанализируйте актуальные проекты подразделений по связям с общественностью ОВД в Интернете (проект «Перехват», проект «#МояМилиция», «Вместе против преступности» и др). Сравните их содержание и тональность сообщений с видеоблогами, в которых размещаются материалы о работе милиции критической направленности (например, видеоблог Василия Телогрейкина). Уделите внимание анализу актуального законодательства, регулирующего деятельность информационных интернет-ресурсов. Изучите нормы, которые ограничивают либо запрещают распространение информации.

Уясните значение понятий «имидж», «репутация», «реноме». Как вы понимаете значение понятия «имидж милиции»? В чем различие внешних и внутренних факторов его формирования? Приведите примеры противоречий между внешним и внутренним имиджем ОВД.

Дайте определение интернет-преступности. Проведите различие с понятием «киберпреступность». Какое из этих понятий шире? Назовите основные характеристики интернет-преступности.

Проанализируйте кодификатор, который используется для описания преступлений в информационной сфере Генеральным секретариатом Интерпола. Укажите входящие в его преступления, представляющие наибольшую общественную опасность. Какие из преступлений теряют актуальность с развитием информационных технологий? Какие организации чаще всего становятся жертвами компьютерного шпионажа?

Раскройте основные мотивы совершения интернет-преступлений, приведите социальную характеристику лиц, причастных к ним. Раскройте направления деятельности преступников-хакеров, кракеров, вирмекеров, реализаторов.

Уясните, чем обусловлены высокая латентность, анонимность и интеллектуальность интернет-преступности. Приведите факторы, которые способствуют широкому ее распространению.

Анализ состояния киберпреступности проведите с указанием конкретных примеров преступлений, имевших место в Республике Беларусь в последние годы. Какие виды преступлений получили наибольшее распространение? Возможна ли их профилактика? В частности, укажите возможные меры

профилактики преступлений и правонарушений в отношении несовершеннолетних. Наконец, шестой вопрос предусматривает анализ изменений в законодательстве, направленных против криминализации Интернета.

### ***Задания для подготовки к практическому занятию***

#### **Занятие 2,6-7.1**

##### ***Задание 1***

Необходимо найти в открытых интернет-источниках (социальные сети, форумы, мессенджеры и т. д.) тематические группы (в том числе иноязычные), связанные с деятельностью:

- хакеров,
- кракеров,
- вирмейкеров,
- спамеров.

Проанализировать их по следующим показателям:

- а) состав участников (половой, возрастной, социальный, профессиональный и т. д.);
- б) характер открыто обсуждаемой информации (какие вопросы выносятся на обсуждение? связаны ли они напрямую с нарушением законодательства?);
- в) наличие открыто публикуемых инструментов противоправной деятельности (вирусное программное обеспечение, инструкции по незаконной деятельности в Интернете и т. п.);
- г) возможные правовые и социальные последствия открыто публикуемой и обсуждаемой информации.
- д) меры противодействия распространению подобного рода информации.

##### ***Задание 2***

Необходимо найти в информационных интернет-источниках (сайты СМИ, информационных агентств, сетевые издания) примеры резонансных преступлений в сфере высоких технологий. Проанализировать их по следующим показателям:

- а) лица, совершившие преступление;
- б) лица (либо организации), пострадавшие от преступления;
- в) социальные предпосылки совершения подобных преступлений;
- г) отношение в обществе к подобным преступлениям (обратите внимание на обсуждение информации в Интернете);
- д) возможные меры профилактики преступлений.

#### **Занятие 2,6-7.2**

##### ***Задание 1***

Необходимо найти в открытых интернет-источниках (сайты СМИ, информационных агентств, сетевые издания) национальную статистику относительно интернет-преступности за последний год (полугодие, квартал).

Какие преступления преобладают в ее структуре? Имеется ли динамика (снижение либо рост количества определенных преступлений)? В чем ее причины? Имеются ли негативные предпосылки для роста количества преступлений в какой-либо сфере? Ответы на вопросы обоснуйте.

### *Задание 2*

Необходимо найти в социальной сети объект для изучения, которым должен стать один из профилей пользователей данной сети. Объект должен обладать характеристиками виктимности.

При выборе необходимого профиля следует руководствоваться следующими параметрами:

- а) возраст: 20-25 лет;
- б) пол: любой;
- в) место проживания: Республика Беларусь;
- г) особенности профиля: достаточный объем информации о пользователе, активное ведение профиля (постоянная актуализация, частое посещение);
- д) особенности пользователя: состоит в группах, связанных с девиантными формами поведения, проявляет иные формы активности, свидетельствующие о потенциальной виктимности.

Обосновать проявление характеристик виктимности у объекта.

### *Задание 3*

Создать вымышленный аккаунт в социальной сети, руководствуясь следующими принципами:

- а) аккаунт не должен быть связан с персональными данными обучающихся, не должен указывать на профессиональную принадлежность.
- б) аккаунт должен быть достаточно наполнен (фото, музыкальные и видеозаписи, интересы, предпочтения, предполагаемый список друзей, сообществ и т. д.);
- в) аккаунт должен выглядеть достоверно (отсылки на другие ресурсы, например, e-mail, связность информации внутри профиля, например, совпадение месяца рождения и фото с празднованием его в этот период, наличие поздравлений от друзей в этом же месяце и т. п.).
- г) аккаунт должен иметь пересечения в интересах с профилем изучаемого лица (см. задание 2) либо содержать возможность такому пересечению появиться.

Объяснить, каким образом в профессиональной деятельности сотрудников ОВД, связанной с профилактикой преступлений и правонарушений, а также раскрытием преступлений, могут использоваться вымышленные аккаунты в социальных сетях.

## ***Материалы для самоконтроля по теме***

### *Вопросы для самоконтроля*

1. Какими факторами опосредовано присутствие органов внутренних дел в коммуникативном пространстве Интернета?
2. Каковы причины распространения слухов в коммуникативном

пространстве? В чем заключается их негативное влияние на деятельность ОВД?

3. Назовите задачи подразделений по связям с общественностью в структуре ОВД.

4. Перечислите собственные общереспубликанские издания МВД. Как считаете, способны ли данные СМИ выйти за рамки формата корпоративных изданий?

5. Как на законодательном уровне регулируется взаимодействие органов внутренних дел и внутренних войск МВД Республики Беларусь со СМИ?

6. Как считаете, насколько велико значение для граждан интернет-ресурсов как источника информации об органах внутренних дел?

7. В чем состоят причины роста популярности в белорусском интернет-пространстве видеоблогов, в которых размещаются материалы о работе милиции критической направленности?

8. Какие популярные социальные сети используются в деятельности пресс-служб ОВД?

9. Что такое имидж?

10. Дайте определение понятию «имидж милиции».

11. Назовите основные субъекты имиджирования.

12. В чем заключается различие между имиджем и репутацией (реноме)?

13. Перечислите основные атрибуты внешнего имиджа ОВД.

14. В чем заключаются причины противоречий между внешним и внутренним имиджем ОВД?

15. Что такое Интернет-преступность?

16. В чем состоит отличие интернет-преступности от киберпреступности?

17. Назовите основные характеристики интернет-преступности.

18. С какой особенностью интернет-преступности связана ее интеллектуальность?

19. Чем обусловлен стремительный рост интернет-преступности?

20. Укажите преступления из кодификатора Генерального секретариата Интерпола, представляющие наибольшую общественную опасность.

21. Что такое «логическая бомба» и «троянский конь»?

22. Каковы причины распространения пиратства в Интернете?

23. Раскройте основные мотивы совершения интернет-преступлений.

24. Обрисуйте усредненный социальный портрет лица, причастного к совершению интернет-преступлений.

25. Кто такие преступники-хакеры? Каковы типы и характеристики данной группы преступников?

26. Кто такие преступники-взломщики? Каковы типы и характеристики данной группы преступников?

27. Кто такие преступники-вирмейкеры? Каковы типы и характеристики данной группы преступников?

28. Кто такие преступники-реализаторы? Каковы типы и характеристики данной группы преступников?

29. Что такое кардинг? Приведите примеры.

30. В какой период в Беларуси начала распространяться киберпреступность?

31. Приведите примеры резонансных преступлений в интернет-

пространстве, раскрытых в Беларуси.

32. Назовите негативные явления, связанные с неконтролируемым использованием Интернета детьми и подростками.

33. Какие законодательные меры предпринимаются в Беларуси для противодействия киберпреступности?

34. В каких статьях Уголовного кодекса Республики Беларусь предусмотрена ответственность за преступления в сфере информационной безопасности?

35. Приведите определение информационной безопасности.

36. Что такое «преступление как услуга»?

37. Поясните содержание концепции «Интернета вещей».

38. С какими рисками связана «кража личности» в Интернете?

39. Почему деструктивное информационное воздействие на личность и распространение искаженной информации входят в число основных угроз в информационной сфере?

40. Перечислите основные способы противодействия информационным угрозам.

41. Назовите уровни противодействия угрозам информационной безопасности.

42. С какой целью была принята Концепция информационной безопасности Республики Беларусь?

43. Какое определение информационной безопасности приводится в Концепции информационной безопасности Республики Беларусь?

44. Назовите направления противодействия угрозам информационной безопасности, указанные в Концепции информационной безопасности Республики Беларусь.

45. Какие меры обеспечения кибербезопасности предусмотрены Концепцией информационной безопасности Республики Беларусь?

46. Перечислите основные правила создания и хранения паролей от интернет-аккаунтов.

47. Перечислите основные правила безопасности при использовании банковских карточек.

48. Кратко охарактеризуйте принципы функционирования открытых инструментов, которые позволяют сохранить анонимность и защитить данные при работе в Интернете.

49. Почему при работе в социальных сетях пользователь оставляет после себя «психологические следы»? Можно ли избежать их появления?

50. Назовите основные правила этикета при общении в социальных сетях, по электронной почте и в мессенджерах.

51. Каковы условия сохранности информации в социальных сетях? В чем состоит опасность публикации фотографий личного характера?

52. С какой целью была принята Стратегия совершенствования информационно-коммуникативной деятельности органов внутренних дел и внутренних войск Министерства внутренних дел Республики Беларусь?

53. Назовите основные направления обеспечения информационной безопасности деятельности ОВД в Интернете.

54. Почему расширение присутствия в Интернете является важным

фактором информационной безопасности ОВД?

***Перечень тем для подготовки докладов (сообщений)***

1. Белорусская милиция: отражение в видеоблогах.
2. Законодательство, регулирующее деятельность средств массовой информации в Интернете.
3. Зарубежный опыт формирования имиджа правоохранительных структур.
4. Эволюция интернет-преступности.
5. Вишинг – новый вид вымогательства в Сети.
6. «Интернет-гигиена» как способ безопасного использования Интернета.
7. Личность интернет-преступника: психологическая и социологическая характеристика.
8. Профилактика интернет-преступности.
9. Интернет вещей: концепция и прогнозы развития.
10. Безопасные браузеры: преимущества и риски.
11. Правовые основы распространения личной информации в социальных сетях.
12. Зарубежный опыт обеспечения информационной безопасности правоохранительных органов.

## ЛИТЕРАТУРА ПО КУРСУ

### Нормативные правовые акты

1. Конституция Республики Беларусь. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2016. – 62 с.

2. Гражданский кодекс Республики Беларусь : принят 7 декабря 1998 г. № 218-3 : в ред. Закона Респ. Беларусь от 5 января 2021 г. № 95-3 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

3. Уголовный кодекс Республики Беларусь : принят 9 июля 1999 г. № 275-3 : в ред. Закона Респ. Беларусь от 26 мая 2021 г. № 112-3 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

4. О мерах по совершенствованию использования национального сегмента сети Интернет: Указ Президента Респ. Беларусь от 1 февраля 2010 г. № 60 : в ред. от 18 сентября 2019 г. № 350 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

5. О средствах массовой информации : Закон Респ. Беларусь от 17 июля 2008 г. № 427-3 : в ред. от 24 мая 2021 г. № 110-3 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

6. Об информации, информатизации и защите информации: Закон Респ. Беларусь от 10 ноября 2008 г. № 455-3 : в ред. от 11 мая 2016 г. № 362-3 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

7. Об органах внутренних дел Республики Беларусь : Закон Респ. Беларусь от 17 июля 2007 г. № 263-3 : в ред. от 17 мая 2021 г. № 106-3 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

8. Об утверждении Концепции национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь от 9 ноября 2010 г. № 575 : в ред. от 24 января 2014 г. № 49 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

9. О дополнительных мерах по работе с обращениями граждан и юридических лиц : Указ Президента Респ. Беларусь от 15 октября 2007 г. № 498 : в ред. от 26 декабря 2019 г. № 485 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

10. О Концепции информационной безопасности Республики Беларусь : Постановление Совета Безопасности Респ. Беларусь от 18 марта 2019 г. № 1 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

11. Об утверждении Правил профессиональной этики сотрудников органов внутренних дел Респ. Беларусь : Приказ Министерства внутренних дел Республики Беларусь от 04.03.2013 № 67 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2021.

## Основная литература

12. Венидиктов, С. В. Интернет-коммуникация в деятельности органов внутренних дел : учебное пособие / С. В. Венидиктов, Н. В. Вашрова. – Минск : РИВШ, 2020. – 236 с.

13. Венидиктов, С. В. Интернет-коммуникация в деятельности органов внутренних дел : методические рекомендации / С. В. Венидиктов, Н. В. Вашрова; М-во внутр. дел Респ. Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь». – Могилев : Могилев. институт МВД, 2019. – 52 с.

14. Венидиктов, С. В. Психология девиантного поведения : учебное пособие / С. В. Венидиктов, С. И. Даниленко, Е. А. Ярошевич ; Министерство внутренних дел Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь». – Могилев : Могилев. институт МВД, 2017. – 320 с.

15. Психология и коммуникация в правовой системе [Электронный ресурс] : сборник статей / [редкол.: С. В. Венидиктов (отв. ред.) [и др.] ; Мин-во внутр. дел Респ. Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь». – Могилев : Могилевский институт МВД Республики Беларусь, 2016. – 1 электрон. опт. диск (CD-R).

16. Пыжова, Н. Н. Психология электронной коммуникации : пособие / Н. Н. Пыжова, Н. В. Волох ; Академия управления при Президенте Республики Беларусь. – Минск : Академия управления при Президенте, 2017. – 134 с.

17. Формирование позитивного общественного мнения о работе органов внутренних дел Республики Беларусь : методические рекомендации / Министерство внутренних дел Республики Беларусь ; под общ. ред. И. А. Поздеева. – Минск : Штаб МВД Республики Беларусь : [Академия МВД Республики Беларусь], 2016. – 55 с.

## Дополнительная литература

18. Ануфриева, В. С. Сеть Интернет как средство незаконного оборота наркотических средств, психотропных веществ, их прекурсоров и аналогов / В. С. Ануфриева // Борьба с преступностью: теория и практика: тезисы докладов III Международной научно-практической конференции (Могилев, 20 марта 2015 года) в 2-х ч. Ч. 1 ; [ред. кол.: Ю. П. Шкаплеров (отв. ред.) и др.] ; Министерство внутренних дел Республики Беларусь, учреждение образования «Могилевский институт Министерства внутренних дел Республики Беларусь». – Могилев, 2015. – С. 16–18.

19. Бакулев, Г. П. Массовая коммуникация: Западные теории и концепции: Учеб. пособие для студентов вузов. – 2-е изд., перераб. и доп. / Г. П. Бакулев. – М: Аспект Пресс, 2010. – 192 с.

20. Баландюк, Р. О. Методика расследования отдельных видов преступлений, совершаемых в сфере интернет-технологий / Р. О. Баландюк, О. В. Баландюк, О. С. Баландин, Д. В. Олейник // Вестник Белгородского юридического института МВД России. – 2015. – № 1. – С. 69–75.

21. Батоев, В. Б. Проблемы противодействия экстремистской деятельности, осуществляемой с использованием сети Интернет / В. Б. Батоев // Вестник Воронежского института МВД России. – 2016. – № 2. – С. 37–43.

22. Белинская, Е. П. Психология интернет-коммуникации / Е. П. Белинская. – М.: НОУ ВПО Московский психолого-социальный университет, МОДЭК, 2013. – 192 с.

23. Белл, Д. Социальные рамки информационного общества / Д. Белл // Новая технократическая волна на Западе. – М. : Прогресс, 1986. – С. 330–342.

24. Белошейкин, Д. А. Защита деловой репутации в сети Интернет / Белошейкин Д. А. // Промышленно-торговое право. – 2015. – № 5. – С. 39–41.

25. Большечев, Н. И. О зарубежном опыте правового регулирования противодействия экстремизму в сети Интернет / Н. И. Большечев // Вестник Воронежского института МВД России. – 2015. – № 3. – С. 209–214.

26. Борьба с использованием Интернета в террористических целях [Электронный ресурс] : Решение Совета Министров ОБСЕ, № 3/04 (MC.DEC/3/04/Corr.1), 7 декабря 2004 г. – Режим доступа: <https://www.osce.org/ru/resources/csce-osce-key-documents/>.

27. Бутусова, Л. И. Киберпреступность: глобальная проблема и пути решения / Л. И. Бутусова // Актуальные проблемы борьбы с преступлениями и иными правонарушениями : материалы четырнадцатой международной научно-практической конференции. Ч. 2. – Барнаул : Барнаульский юрид. институт МВД России, 2016. – С. 125–126.

28. Введенская, О. Ю. Обстановка совершения интернет-преступлений / О. Ю. Введенская // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений : сборник материалов всероссийской научно-практической конференции (Воронеж, 16-17 апреля 2015 г.). – Воронеж : Воронежский институт МВД России, 2015. – С. 41–45.

29. Венидиктов, С. В. Диагностика информационной культуры в условиях образовательного пространства системы Министерства внутренних дел / С. В. Венидиктов // Актуальные проблемы огневой, тактико-специальной и профессионально-прикладной физической подготовки. Сборник статей ; Учреждение образования «Могилевский институт МВД Республики Беларусь». – Могилев, 2014. – С. 336–340.

30. Войскунский, А. Е. Альтернативная идентичность в социальных сетях / А. Е. Войскунский, А. С. Евдокименко, Н. Ю. Федунина // Вестник Московского университета. 2013. – Сер. 14. – № 1. – С. 66–83.

31. Войскунский, А. Е. Психология и Интернет / А. Е. Войскунский. – Акрополь, 2010. – 440 с.

32. Войскунский, А. Е. Социальная перцепция в социальных сетях // Вестник Московского университета. – Серия 14. Психология. – 2014. – № 2. – С. 90–104.

33. Войскунский, А. Е. Поведение в киберпространстве: психологические принципы / А. Е. Войскунский // Человек. – 2016. – № 1. – С. 36–49.

34. Гридюшко, П. В. Методика расследования уголовных дел о распространении порнографических материалов с использованием компьютерной техники в сети Интернет, локальных сетях : Рекомендовано Министерством внутренних дел Республики Беларусь в качестве пособия для обучающихся в

учреждениях высшего образования Министерства внутренних дел Республики Беларусь по специальности 1-24 01 02 «Правоведение» / П. В. Гридюшко, И. Г. Мухин ; Учреждение образования «Академия Министерства внутренних дел Республики Беларусь». – Минск : Академия МВД Республики Беларусь, 2014. – 40 с.

35. Гурский, В. М. Основы безопасной работы в сети Интернет / В. М. Гурский, А. А. Высоцкий, А. В. Гуца // Организация образовательного процесса. Информационно-методический сборник № 12. – Минск : Академия МВД Республики Беларусь, 2014. – С. 69–73.

36. Добринская, Д. Е. Сообщества в эпоху интернета / Д. Е. Добринская // Вестник Московского университета. – Серия 18: Социология и политология. 2018. – Т. 24. – № 4. – С. 59–79.

37. Добринская, Д. Е. Киберпространство: территория современной жизни / Д. Е. Добринская // Вестник Московского университета. – Сер. 18: Социология и политология. – 2018. – Т. 24. – № 1. – С. 52–70.

38. Добринская, Д. Е. Социологическое осмысление интернета: теоретические подходы к исследованию сети (окончание) / Д. Е. Добринская // Вестник Московского университета. – Сер. 18. Социология и политология. – 2016. – № 4. – С. 85–103.

39. Добринская, Д. Е. Социологическое осмысление интернета: теоретические подходы к исследованию сети (начало) / Д. Е. Добринская // Вестник Московского университета. – Сер. 18. Социология и политология. – 2016. – № 3. – С. 21–39.

40. Дремлюга, Р. И. Интернет-преступность : монография / Р. И. Дремлюга. – Владивосток : Изд во Дальневост. ун та, 2008. – 240 с.

41. Захарченко, В. Ю. Компьютерные преступления: их выявление и предотвращение : учебное пособие / В. Ю. Захарченко, В. И. Лазуренко, А. В. Олифинов / под общ. редакцией В. И. Лазуренко. – К. : Центр учебной литературы, 2007. – 170 с.

42. Земцова, С. И. Методика расследования незаконного сбыта синтетических наркотических средств, совершенного с использованием интернет-магазинов [Текст] : учебное пособие / С. И. Земцова, О. А. Суров, П. А. Галушин ; Сибирский юридический институт МВД России. - Красноярск: СибЮИ МВД России, 2019. – 181 с.

43. Интернет-СМИ: Теория и практика: Учеб. пособие для студентов вузов / Под ред. М. М. Лукиной. – М.: Аспект Пресс, 2010. – 348 с.

44. Информационное общество в Республики Беларусь. Статистический сборник. – Минск: Национальный статистический комитет Республики Беларусь, 2017. – 105 с.

45. Канашевич, Н. М. Информационно-коммуникационный фактор изменения парадигмы войны / Н. М. Канашевич // Психология и коммуникация в правовой системе : сборник статей. – Могилев : Могилевский институт МВД Республики Беларусь, 2016. – С. 51–58.

46. Кастельс М. Информационная эпоха: Экономика, общество и культура // Пер. с англ. под науч. ред. О. И. Шкаратана; Гос. ун-т. Высш. шк. экономики. – М., 2000. – 606 с.

47. Конвенция о защите физических лиц при автоматизированной обработке персональных данных [Электронный ресурс]. – Режим доступа: [http://www.consultant.ru/document/cons\\_doc\\_LAW\\_121499/](http://www.consultant.ru/document/cons_doc_LAW_121499/).

48. Коновалова, И. Интернет-сети как средство социальной мобилизации молодежи / И. Коновалова // Беларуская думка = Белорусская мысль. – 2016. – № 2. – С. 92–96.

49. Консолидированная концептуальная база ОБСЕ для борьбы с терроризмом [Электронный ресурс]: решение № 1063, 7 декабря 2012 г. – Режим доступа: <https://www.osce.org/ru/resources/csce-osce-key-documents/>.

50. Кузнецова, Е. В. Информационное пространство сети Интернет в системе детерминант преступности несовершеннолетних / Е. В. Кузнецова // Вестник Московского университета МВД Российской Федерации. – 2015. – № 9. – С. 71–74.

51. Кузнецова, Е. В. Некоторые аспекты влияния онлайн и сетевых игр на формирование девиантного поведения несовершеннолетних / Е. В. Кузнецова // Вестник Московского университета МВД Российской Федерации. – 2014. – № 10. – С. 85–88.

52. Кузнецова, Ю.М. Психология жителей Интернета / Ю. М. Кузнецова, Н. М. Чудова. – М.: Издательство ЛКИ, 2008. – 224 с.

53. Кутюгин Д. И. Интернет как коммуникативное пространство информационного общества диссертация ... кандидата социологических наук: 22.00.04 / Кутюгин Дмитрий Игоревич; [Место защиты: Моск. гос. ун-т им. М.В. Ломоносова]. – Москва, 2009. – 171 с.: ил. РГБ ОД, 61 09-22/116

54. Лузько, А. В. Личностные особенности студентов, склонных к интернет-зависимому поведению / Лузько А. В. // Научные труды Республиканского института высшей школы. Исторические и психолого-педагогические науки. Выпуск 13. Часть 2. – 2013. – № 13. – С. 151–158.

55. Майерс, Д. Социальная психология : учебное пособие / Д. Майерс ; пер. с англ. З. Замчук. – СПб. : Питер, 2007. – 793 с.

56. Маклюэн, М. Понимание медиа: внешние расширения человека / М. МакЛюэн. – М.: Кучково Поле, 2011. – 464 с.

57. Мишина, Е. Д. Интернет-коммуникации как способ развития информационно-коммуникативных компетентностей студента / Е. Д. Мишина, Л. Э. Кевляк-Домбровкая // Дистанционное обучение – образовательная среда XXI века : материалы VII Международной научно-методической конференции (Минск, 1-2 декабря 2011 г.). – Минск : БГУИР, 2011. – С. 66–68.

58. Молоков, В. В. Использование информационно-телекоммуникационных технологий в противодействии незаконному обороту наркотиков : учебно-практическое пособие / В. В. Молоков, П. В. Галушин, Н. В. Тугаринов ; Сибирский юридический институт МВД России. – Красноярск : СибЮИ МВД России, 2019. – 83 с.

59. Назаров, М. М. Массовая коммуникация и общество: Введение в теорию и исследования / М. А. Назаров. – 4-е изд., перераб. и доп. – М.: Книжный дом «ЛИБРОКОМ», 2010. – 360 с.

60. Осипенко, А. Л. Оперативно-розыскной мониторинг информационных ресурсов глобальных компьютерных сетей / А. Л. Осипенко // Оперативник (сыщик). – 2009. – № 3. – С. 27–31.

61. Противодействие использованию Интернета в террористических целях [Электронный ресурс] : Решение Совета Министров ОБСЕ, № 7/06 (MC.DEC/7/06/Corr.1), 5 декабря 2006 г. – Режим доступа: <https://www.osce.org/ru/resources/csce-osce-key-documents/>.

62. Редько, А. А. Влияние сети Интернет на формирование правовой политики / А. А. Редько // Вестник Краснодарского университета МВД России. – 2015. – № 1. – С. 16–20.

63. Республика Беларусь. Статистический ежегодник 2018. – Минск: Национальный статистический комитет Республики Беларусь, 2018. – 489 с.

64. Республика Беларусь. Статистический ежегодник 2019. – Минск: Национальный статистический комитет Республики Беларусь, 2019. – 472 с.

65. Рьдченко, К. Д. Дети в сети Интернет: развлечение или вовлечение? / К. Д. Рьдченко // Преступность в сфере информационно-телекоммуникационных технологий: проблемы предупреждения, раскрытия и расследования преступлений : сборник материалов всероссийской научно-практической конференции (Воронеж, 16-17 апреля 2015 г.). – Воронеж : Воронежский институт МВД России, 2015. – С. 31–38.

66. Самошин, А. В. Особенности предупреждения распространения экстремистских материалов в молодежной среде по глобальной сети Интернет / А. В. Самошин, В. В. Горовой // Труды Академии управления МВД России. – 2016. – № 3. – С. 61–65.

67. Терещенко, О. В. Социальные риски в интернет-среде / О. В. Терещенко // Социология. – 2016. – № 1. – С. 62–67.

## **ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К ЗАЧЕТУ ПО ТЕМАМ №1-7 ДИСЦИПЛИНЫ «ИНТЕРНЕТ-КОММУНИКАЦИЯ В ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ»**

1. Понятие, концепции и характеристики информационного общества.
2. Современные информационные технологии, понятие и направления информатизации общества.
3. Направления Государственной программы развития цифровой экономики и информационного общества в Республике Беларусь.
4. Понятие «цифровых прав» и «цифрового барьера».
5. Динамика роста пользователей Интернета и статистика использования коммуникационных ресурсов Интернета в современном мире.
6. Особенности использования информационно-коммуникационных технологий населением Республики Беларусь.
7. Понятие интернет-коммуникации. Основные коммуникационные ресурсы Интернета.
8. Виды коммуникационных интернет-услуг: ресурсы Всемирной паутины, веб-форумы, блоги, социальные сети, электронная почта, мессенджеры, чаты, массовые многопользовательские онлайн игры.
9. Задачи информационно-коммуникативной деятельности ОВД в Интернете.
10. Стихийный и целенаправленный факторы присутствия ОВД в Интернете.
11. Позиционирование органов внутренних дел в коммуникативном пространстве Интернета.
12. Организация работы ОВД с масс-медиа, формирование информационных потоков, изучение общественного мнения.
13. Взаимодействие органов внутренних дел с интернет-ресурсами. Понятия интернет-ресурса и сетевого издания.
14. Закон Республики Беларусь «О средствах массовой информации». Информация, распространение и (или) предоставление которой ограничено.
15. Имиджевые модели сотрудников ОВД в коммуникативном пространстве.
16. Внешний и внутренний имидж ОВД, функции внутреннего имиджа, причины противоречий между внешним и внутренним имиджем ОВД.
17. Особенности среды интернет-коммуникации: понятия «виртуальная реальность» и «киберпространство».
18. Характеристики интернет-коммуникации: глобальность, опосредованность, анонимность, добровольность и доступность контактов, нетипичность поведения, совмещение виртуального и реального.
19. Формы и уровни интернет-коммуникации.
20. Стратегии виртуальной самопрезентации, причины модификации идентичности в сети.
21. Особенности использования стратегий виртуальной самопрезентации.
22. Проблемы и угрозы для личности в коммуникационном интернет-пространстве.
23. Отражение и организация социальных взаимоотношений в Интернете.

24. Характер распространения и обмена информацией в Интернет.
25. Характеристики онлайн-сообществ, особенности групповой коммуникации с использованием различных видов социальных сетей.
26. Особенности интернет-солидарности, этапы формирования макросолидарности в онлайн-среде.
27. Понятия массовой информации и массовой коммуникации.
28. Основные формы, элементы, особенности массовой информации.
29. Виды массово-информационной деятельности.
30. Система СМК, ее структурные элементы и среда.
31. Типологические характеристики СМК.
32. Функции, аудитория СМК.
33. Отличительные особенности массовой коммуникации в глобальной сети Интернет.
34. Принципы регулирования деятельности СМК (правовые и этические).
35. Законодательство в области СМИ в Республике Беларусь. Право на информацию.
36. Проблемы формирования общественного мнения в Интернете.
37. Особенности массовой коммуникации в интернет-пространстве Республики Беларусь.
38. Интернет-преступность и киберпреступность: соотношение понятий. Характеристики интернет-преступности.
39. Типология и классификации интернет-преступлений.
40. Мотивы совершения интернет-преступлений. Личностные особенности интернет-преступников и их типология.
41. Криминализация Интернета и интернет-преступность в Республике Беларусь.
42. Интернет-преступность и уголовное законодательство Республики Беларусь.
43. Понятие информационной безопасности, угрозы информационной безопасности.
44. Способы и уровни противодействия информационным угрозам.
45. Концепция информационной безопасности Республики Беларусь.
46. Сохранение анонимности и защита данных в Интернете.
47. Правила поведения в социальных сетях. Требования к сотрудникам ОВД при использовании социальных сетей.
48. Правила этикета при общении в социальных сетях, по электронной почте, в мессенджерах.
49. Условия сохранности информации в социальных сетях.
50. Деятельность ОВД в направлении обеспечения информационной безопасности.

## ГЛОССАРИЙ

**АНАЛИЗ СОЦИАЛЬНЫХ СЕТЕЙ** – исследование отношений в социальных сетях Интернета, представленных в виде серии узлов (профили) и связей (дружба) между ними.

**АНОНИМ** – частный случай виртуала. Обозначает автора сообщений, который никак себя не идентифицирует в системах, где возможно оставление сообщений без регистрации.

**АНОНИМАЙЗЕР** – средство для скрытия информации о компьютере или пользователе в сети от удалённого сервера.

**АНОНИМНЫЕ СЕТИ** – компьютерные сети, созданные для достижения анонимности в Интернете и работающие поверх глобальной сети.

**БЛОГ** (интернет-журнал событий, интернет-дневник, онлайн-дневник) – веб-сайт, основное содержимое которого – регулярно добавляемые записи, содержащие текст, изображения или мультимедиа.

**БОЛЬШИЕ ДАННЫЕ** (англ. BIG DATE) – социально-экономический феномен, связанный с появлением технологических возможностей анализировать огромные массивы данных.

**ВЕБ-АНАЛИТИКА** – система измерения, сбора, анализа, представления и интерпретации информации о посетителях веб-сайтов.

**ВЕБ-ФОРУМ** – Размещение сообщений пользователей внутри тем, созданных посетителями форума для обсуждения

**ВИНЛОКЕРЫ** – семейство вредоносных программ, блокирующих или затрудняющих работу с операционной системой и требующих перечисление денег злоумышленникам за восстановление работоспособности компьютера, частный случай Ransomware (программ-вымогателей).

**ВИРМЕЙКЕРЫ** (англ. virus – вирус и maker – создавать) – создатели компьютерных вирусов.

**ВИРТУАЛЬНАЯ ЛИЧНОСТЬ (ВИРТУАЛ)** – фиктивная личность, которая появляется в тех случаях, когда пользователь Интернета выдает себя за другое лицо.

**ВИРТУАЛЬНАЯ РЕАЛЬНОСТЬ** – созданный техническими средствами мир, передаваемый человеку через его ощущения: зрение, слух, обоняние, осязание и другие.

**ВИРТУАЛЬНОСТЬ** (от лат. *virtualis* – возможный) – объект или состояние, которые реально не существуют, но могут возникнуть при определенных условиях.

**ВИРТУАЛЬНЫЙ РЕДАКТОР** – процесс в Интернете, при котором аудитория, выбирая важную для себя информацию, распространяет ее в сети дальше; информация, не заинтересовавшая пользователей социальных сетей, фильтрацию / виртуальное редактирование не проходит.

**ВИРУС** – специальная программа, способная «заражать» действующие программы, распространяться в компьютерной среде, выполняя нежелательные действия.

**ВИШИНГ** – действия злоумышленников по выманиванию у владельца банковской карты ее данных либо по вынуждению к совершению определенных операций со счетом.

**ВСЕМИРНАЯ ПАУТИНА** (англ. *World Wide Web*) – распределённая система, предоставляющая доступ к связанным между собой документам, расположенным на различных компьютерах, подключённых к сети Интернет. Для обозначения Всемирной паутины также используют слово веб (англ. *web* «паутина») и аббревиатуру WWW.

**ГИПЕРТЕКСТУАЛЬНОСТЬ** – возможность пользователя самостоятельно определять, моделировать и организовывать текстовое пространство по своему желанию.

**ГРУМИНГ** – действия злоумышленников по соращению несовершеннолетних в Интернете.

**ДОПОЛНЕННАЯ ВИРТУАЛЬНОСТЬ** – виртуальная реальность, в которой присутствуют объекты из реального мира.

**ДОПОЛНЕННАЯ РЕАЛЬНОСТЬ** – дополнение реальности, различными виртуальными объектами, визуальными элементами.

**ИМИДЖ** (от англ. *image* – «образ», «изображение», «отражение») – совокупность представлений, сложившихся в общественном мнении о том, как должен вести себя человек в соответствии со своим статусом.

**ИМИДЖ ОБЪЕКТА** – это мнение рационального или эмоционального характера об объекте (человеке, предмете, системе), возникшее в психике группы людей на основе образа, сформированного в их психике в результате восприятия ими тех или иных характеристик данного объекта.

**ИМИДЖ ОВД** – сформировавшийся, действенный, эмоционально окрашенный образ ОВД и отдельных их составляющих, наделенных определенными характеристиками, основанными на реальных или приписываемых свойствах организации, обладающих социальной значимостью.

**ИНТЕРНЕТ ВЕЩЕЙ** – концепция, согласно которой в Интернете взаимодействуют не люди напрямую, а подключенные к Сети устройства, способные обмениваться информацией и генерировать активность самостоятельно.

**ИНТЕРНЕТ-КОММУНИКАЦИЯ** –общение, при котором передача информации происходит по каналам Интернета.

**ИНТЕРНЕТ-ПРЕСТУПНОСТЬ** – противоправные общественно опасные деяния, совершенные с использованием сети Интернет.

**ИНТЕРНЕТ-РЕСУРС** – интернет-сайт, страница интернет-сайта, форум, блог, приложение для мобильного устройства, иной информационный ресурс

(его составная часть), размещенный в глобальной компьютерной сети Интернет, посредством которых распространяется массовая информация.

**ИНТЕРНЕТ-СОЛИДАРНОСТЬ** – форма социального взаимодействия в онлайн-пространстве, появляющейся в результате объединения пользователей на основе доверия и общности интересов в ситуации интенсивного регулярного обмена информацией в ходе интернет-коммуникации.

**ИНФОРМАТИЗАЦИЯ** – процесс построения и развитие инфраструктуры, основанной на информационных технологиях, в рамках какой-либо территории.

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ** – состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере (глава 3 Концепции информационной безопасности Республики Беларусь).

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ИНТЕРНЕТ-ПОЛЬЗОВАТЕЛЯ** – это действия, направленные на предотвращение несанкционированного доступа, использования, распространения, изменения, искажения, записи, уничтожения информации, размещенной в Интернете.

**ИНФОРМАЦИОННОЕ ОБЩЕСТВО** – общество, в котором информация является главным экономическим ресурсом и фактором социокультурных изменений.

**ИНФОРМАЦИОННОЕ ПРОСТРАНСТВО** – область деятельности, связанная с созданием, преобразованием, передачей, использованием, хранением информации, оказывающая воздействие в том числе на индивидуальное и общественное сознание и собственно информацию.

**КАРДЕР** – преступник, занимающийся кардингом.

**КАРДИНГ** (от англ. *carding*) – мошенничество с платежными картами – вид мошенничества, при котором производится операция с использованием платежной карты или её реквизитов, не инициированная или не подтвержденная её держателем.

**КИБЕРАТАКА** – целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения) их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации.

**КИБЕРПРЕСТУПНОСТЬ** – действия преступного характера, реализуемые в информационном пространстве с использованием компьютерной техники и технологий, ресурсов глобальной компьютерной сети Интернет, иных сетей и ресурсов обмена данными.

**КИБЕРПРОСТРАНСТВО** – воспринимаемое пользователем виртуальное пространство, создаваемое электронными устройствами.

**КОМПОНЕНТ ИМИДЖА** – некоторая характеристика носителя имиджа, которая воплощается в восприятии реципиентов.

**КОМПЬЮТЕРНЫЙ АБОРДАЖ** – несанкционированное проникновение в компьютер либо компьютерную сеть третьих лиц, направленное на незаконное получение, использование, передачу, распространение информации.

**КОМПЬЮТЕРНЫЙ ШПИОНАЖ** – незаконное завладение информацией, представляющей коммерческую тайну, с целью получения экономической выгоды.

**КРАЖА ЛИЧНОСТИ** – использование для совершения преступных деяний добытых незаконным путем персональных данных (информация с банковских карточек, учтеные записи интернет-банкинга и др.).

**КРАКЕРЫ** (взломщики) – преступники, которые осуществляют взлом компьютерной системы с целью получения несанкционированного доступа к чужой информации.

**КРЕАТИВНОСТЬ** – характеристика сетевой коммуникации, позволяющая пользователю постоянно изобретать новые способы самопрезентации.

**«ЛОГИЧЕСКАЯ БОМБА»** – тайно встроенные в программное обеспечение команды, которые должны срабатывать при достижении определенных условий.

**ПЛОТНОСТЬ СОЦИАЛЬНОЙ СЕТИ** – отношение прямых связей в сети к общему возможному количеству связей.

**ПРЕСТУПЛЕНИЯ В ИНФОРМАЦИОННОЙ СФЕРЕ** – предусмотренные Уголовным кодексом Республики Беларусь преступления против информационной безопасности (киберпреступления) и иные преступления, предметом или средством совершения которых являются информация, информационные системы и сети.

**«ПРЕСТУПЛЕНИЕ КАК УСЛУГА»** – предоставление киберпреступными сообществами услуг по подготовке и совершению преступлений в Интернете.

**ПРЕСТУПНИКИ-РЕАЛИЗАТОРЫ** – лица, деятельность которых направлена на получение выгоды от применения вредоносных программ.

**ПУБЛИЧНОЕ ПРОСТРАНСТВО ИНТЕРНЕТА** – сфера межличностных коммуникаций, в которой создаются и транслируются общественно значимые идеи.

**РЕПУТАЦИЯ** (англ. reputation), **РЕНОМЕ́** (фр. renommée) – закрепившееся определённое мнение о человеке или группе людей.

**РЕПУТАЦИЯ ОВД** – это развёрнутый комплекс оценочных представлений граждан об ОВД, сформированный на основе объективных параметров ОВД (факторов репутации), имеющих значение для населения.

**СЕКСТИНГ** – обмен в Интернете эротическими сообщениями и фото.

**СЕКСТИНГ** – обмен эротическими сообщениями и фото.

**СЕКСТОРШН** – шантаж в Интернете с использованием материалов интимного характера.

**СЕКС-ЧАТТИНГ** – электронная переписка эротического характера.

**СЕРВИСЫ МНОГОФАКТОРНОЙ АВТОРИЗАЦИИ (МФА)** – метод контроля доступа к компьютеру либо мобильному устройству, при котором для получения доступа необходимо предъявить более одного «доказательства».

**СЕТЕВОЕ ИЗДАНИЕ** – интернет-ресурс, прошедший установленную законом государственную регистрацию.

**СИЛА СВЯЗИ СОЦИАЛЬНОЙ СЕТИ** определяется линейной комбинацией времени, эмоциональной интенсивности, близости и взаимности (то есть обоюдности). Сильные связи определяются гомогенностью, родством и транзитивностью, в то время как слабые – мостами.

**СОЛИДАРНОСТЬ** – единство (группы или класса), которое порождает единство интересов, задач, стандартов и взаимопонимание, или же основывается на них.

**СОЦИАЛЬНАЯ СЕТЬ** – интерактивный многопользовательский сайт, содержание которого наполняется его посетителями, с возможностью указания какой-либо информации об отдельном человеке, по которой страницу пользователя смогут найти другие участники этой сети.

**СПАМ** (англ. spam) – массовая рассылка писем / сообщений, содержащих рекламу, лицам, которые не выразили желание ее получать.

**СПАМЕР** – распространитель спама.

**ТРАНЗИТИВНОСТЬ (ЗАКРЫТОСТЬ СОЦИАЛЬНОЙ СЕТИ)** – присвоение индивидам степени закрытости сети (то есть тот факт, что их друзья также являются друзьями между собой).

**ТРОЛЛИНГ** – вид виртуальной коммуникации с нарушением этики, выражающейся в виде проявления различных форм агрессивного, издевательского и оскорбительного поведения.

**ТРОЯНСКИЙ КОНЬ** – программа либо команда, тайно внедренная в программное обеспечение (преимущественно с использованием Интернета) для осуществления действий, не запланированных пользователем, но сохраняющих функциональность компьютерной техники.

**ФИШЕРЫ** (от англ. fishing – рыбная ловля) – распространители массовой рассылки посредством электронной почты и иных ресурсов, которая позволяет получить доступ к персональным данным (логин, пароль и т. п.) пользователей.

**ХАКЕРЫ** – профессионалы, осуществляющие «взлом» систем компьютерной защиты и безопасности.

**ЦИФРОВОЙ БАРЬЕР** – ограничение возможностей социальной группы из-за отсутствия у нее доступа к современным средствам коммуникации.

Начальник кафедры  
социально-гуманитарных дисциплин  
майор милиции



С.В.Венидиктов