МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Основы кибербезопасности»

профессионального цикла унифицированных программ профессиональной (первоначальной) подготовки по должности служащего «Полицейский»

Москва 2021

04.09.2021 21/11/14077

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

ДЕПАРТАМЕНТ ГОСУДАРСТВЕННОЙ СЛУЖБЫ И КАДРОВ

УТВЕРЖДАЮ
Начальник Департамента
государственной службы и кадров
МВД России
генерал-лейтенант внутренней службы

В.Л. Кубышко
«___» августа 2021 г.

ПРИМЕРНАЯ РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«Основы кибербезопасности»

профессионального цикла унифицированных программ профессиональной (первоначальной) подготовки по должности служащего «Полицейский»

Москва 2021

Примерная рабочая программа учебной дисциплины «Основы кибербезопасности» профессионального цикла унифицированных программ профессиональной (первоначальной) подготовки по должности служащего «Полицейский». – ДГСК МВД России, 2021. – 13 с.

Примерная рабочая программа учебной дисциплины подготовлена авторским коллективом Воронежского института МВД России.

Согласовано:
ГУЭБиПК МВД России, ГУУР МВД России, ГУНК МВД России, ГУПЭ МВД России, ГУТ МВД России, Следственный департамент МВД России, ДИТСиЗИ МВД России, УОД МВД России, БСТМ МВД России.

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

1. Место дисциплины в структуре основной профессиональной образовательной программы.

1.1. Цель изучения учебной дисциплины.

Подготовка обучающегося к правоприменительной, экспертно-консультационной, оперативно-служебной и организационно-управленческой деятельности в сфере регулирования отношений, складывающихся в процессе обеспечения кибербезопасности в правоохранительных органах.

1.2. Задачи учебной дисциплины:

способствовать успешному овладению обучающимся базовыми знаниями в области обеспечения кибербезопасности;

способствовать приобретению обучающимся навыков работы с нормативными документами в области обеспечения кибербезопасности;

сформировать у обучающегося систему профессиональных знаний, умений, навыков, необходимых для понимания принципов обеспечения кибербезопасности, основных методов и средств защиты информационных ресурсов;

содействовать формированию у обучающегося высокого уровня правосознания и правовой культуры, обеспечивающих неукоснительное соблюдение норм действующего законодательства в области кибербезопасности.

2. Планируемые результаты освоения учебной дисциплины.

В результате освоения учебной дисциплины «Основы кибербезопасности» обучающийся должен:

знать:

сущность и понятие кибербезопасности и характеристику ее составляющих;

место и роль кибербезопасности в системе национальной безопасности Российской Федерации, основы государственной информационной политики, стратегию развития информационного общества в России;

основные средства и способы обеспечения кибербезопасности, принципы построения систем обеспечения киберзащиты;

понятие о технических каналах утечки информации, возможности технических средств перехвата информации, способы и средства защиты информации от утечки по техническим каналам;

уметь:

применять нормативные правовые акты и нормативные методические документы в области обеспечения кибербезопасности;

осуществлять рациональный выбор средств и методов киберзащиты информационных систем;

владеть:
профессиональной терминологией в области кибербезопасности;
базовыми методами и средствами киберзащиты;
навыками рационального выбора средств и методов киберзащиты.

II. СОДЕРЖАТЕЛЬНЫЙ РАЗДЕЛ

2.1. Примерный учебный план

№ п/п	Наименование темы	Всего часов	В том числе:					
			Занятия лекционного типа	Занятия семинарского типа	Самостоятельная работа	промежуточная аттестация		
						Зачет	Консультация	Экзамен
20[1].	**Итого по дисциплине**	**22**	**10**	**8**	**2**	**2**	**-**	**-**
20.1[1].	Общие вопросы обеспечения кибербезопасности	4	2	-	2	-	-	-
20.2[1].	Нормативно-правовое обеспечение кибербезопасности	4	2	2	-	-	-	-
20.3[1].	Принципы обеспечения кибербезопасности одиночных устройств и составляющих информационных систем	4	2	2	-	-	-	-
20.4[1].	Понятие об источниках и каналах утечки информации, основы технической защиты информации	4	2	2	-	-	-	-
20.5[1].	Особенности следообразования и фиксации следов при расследовании преступлений, совершаемых с применением современных информационных технологий	4	2	2	-	-	-	-
Зачет		2	-	-	-	2	-	-

2.2. Примерное содержание учебных тем

20.1[1]. Общие вопросы обеспечения кибербезопасности.

Введение в дисциплину. Кибербезопасность: современные киберугрозы. Методы совершения киберпреступлений. Уязвимости интернета вещей. Центры мониторинга и управления безопасностью как составляющие системы противодействия киберпреступлениям. Группы ролей специалистов в центрах управления событиями кибербезопасности. Понятие Критической информационной инфраструктуры[1].

20.2[1]. Нормативно-правовое обеспечение кибербезопасности.

Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации как компонент государственной политики развития национального сектора применения информационных технологий. Законодательство Российской Федерации в области защиты информации. Основы государственной политики Российской Федерации в области международной информационной безопасности. Международные стандарты в области обеспечения кибербезопасности.

20.3[1]. Принципы обеспечения кибербезопасности одиночных устройств и составляющих информационных систем.

Обеспечение кибербезопасности оконечных устройств (сетевые камеры видеонаблюдения, сетевые контроллеры, компьютеры, серверы, ноутбуки, смартфоны). Способы совершения кибератак на средства хранения, обработки и передачи данных. Основные способы защиты от вредоносного программного обеспечения.

20.4[1]. Понятие об источниках и каналах утечки информации, основы технической защиты информации.

Понятие о технических каналах утечки информации: состав и характеристики. Оптические, радиоэлектронные, акустические, материально-вещественные каналы утечки информации. Основные и вспомогательные технические средства и системы. Технические каналы утечки информации при ее передаче по каналам связи. Технические каналы утечки акустической информации: воздушные, вибрационные, параметрические, электроакустические, оптико-электронные. Технические каналы утечки информации, обрабатываемой основными техническими средствами и системами. Побочные электромагнитные излучения[2].

---

[1] Далее – «КИИ».
[2] Далее – «ПЭМИ».

20.5[1]. Особенности следообразования и фиксации следов при расследовании преступлений, совершаемых с применением современных информационно-коммуникационных технологий.

Интернет как способ и как средство совершения и подготовки «традиционных» преступлений. Криминалистически значимая классификация интернет-преступлений. Группы преступных деяний с учетом механизма следообразования и особенностей реализации объективной стороны. Обнаружение действий по сокрытию фактов совершения преступлений. Понятие о средствах журналирования, обеспечивающих получение следовой информации с систем обработки и передачи информации.

2.3. Примерный перечень рекомендуемой литературы, необходимой для освоения учебной дисциплины

2.3.1. Нормативные правовые акты:

1. Конституция Российской Федерации (принята всенародным голосованием 2 декабря 1993 г.) [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

2. Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

4. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

5. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

6. Федеральный закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

7. Федеральный закон от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

8. Федеральный закон от 26 июля 2017 г. № 193-ФЗ «О внесении изменений в отдельные законодательные акты Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

9. Федеральный закон от 26 июля 2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

10. Указ Президента Российской Федерации от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

11. Указ Президента Российской Федерации от 2 июля 2021 г. № 400 «О Стратегии национальной безопасности Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

12. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

2.3.2. Основная литература:

1. Бабкин А.Н. Основы проектирования и технической эксплуатации защищенных телекоммуникационных систем ОВД : практикум / А.Н. Бабкин, А.Н. Глушков. - Воронеж : Воронежский институт МВД России, 2011. – 63 с.

2. Зайцев А. П. Технические средства и методы защиты информации : учебное пособие : рек. Мин. образ. и науки РФ / А. П. Зайцев, Р. В. Мещеряков, А.А. Шелупанов ; под ред. А.П. Зайцева и А.А. Шелупанова. – 7-е изд. Москва : Горячая линия - Телеком, 2014.

3. Нестеровский О.И. Основы информационной безопасности в ОВД [Электронный ресурс] : учебное пособие / О.И. Нестеровский. Воронеж : Воронежский институт МВД России, 2015. – URL : https://library.vimvd.ru/MegaPro/Download/Resource.

4. Основы информационной безопасности : учебник : рек. УМО в обл. национальной безопасности / В.Ю. Рогозин и др. – Москва: ЮНИТА-ДАНА, 2017.

5. Основы управления информационной безопасностью : учебное пособие для вузов. 2-е изд., испр. / А.П. Курило [и др.] – Москва : Горячая линия Телеком, 2014.

6. Рекомендации Центра защиты информации и специальной связи Федеральной службы безопасности Российской Федерации (8 Центр) от 24 декабря 2016 г. № 149/2/7-200 «Методические рекомендации по созданию ведомственных и корпоративных центров государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации» [Электронный ресурс] // Доступ из справочной правовой системы «КонсультантПлюс».

7. Язов Ю.К. Защита информации в информационных системах от несанкционированного доступа / Ю.К. Язов, С.В. Соловьев. – Воронеж : Кварта, 2015.

2.3.3. Дополнительная литература:

1. Бузов Г.А. Практическое пособие по выявлению специальных технических средств несанкционированного получения информации / Г.А. Бузов. – Москва : Горячая линия – Телеком, 2010.

2. Меньшаков Ю.К. Виды и средства иностранных технических разведок : учебное пособие. Под ред. М. П. Сычева. Москва : Изд-во МГТУ им. Н.Э. Баумана, 2009.

3. Бузов Г.А. Защита от утечки по информации техническим каналам: учебное Пособие / Г.А. Бузов, С.В. Калинин, А.В. Кондратьев. – Москва : Горячая линия – Телеком, 2005.

4. Гордейчик С. В. Безопасность беспроводных сетей / С.В. Гордейчик,

В.В. Дубровин. – М. : Горячая линия – Телеком, 2008.

5. Скляров Д. Искусство защиты и взлома информации / Д. Скляров. Санкт-Петербург : БХВ-Петербург, 2004.

6. Филиппова Н.В. Правовое обеспечение информационной безопасности Российской Федерации (учебное пособие) / Н.В. Филиппова. – Воронеж : Воронежский институт МВД России, 2012.

2.4. Примерный перечень ресурсов информационно-телекоммуникационной сети Интернет, рекомендуемых для освоения учебной дисциплины

1. Официальный сайт Федеральной службы по техническому и экспортному контролю. – URL: http://fstec.ru/

2. Справочная правовая система «КонсультантПлюс». – URL: http://www.consultant.ru/

3. Информационно-правовое обеспечение «Гарант». – URL: http://www.garant.ru/

4. ЭБС «Книгафонд». – URL: http://www.knigafund.ru/

2.5. Примерный перечень материально-технической базы, необходимой для осуществления образовательного процесса

1. Мультимедийное оборудование (проектор, экран, ноутбук, колонки).

2. Компьютерный класс.

III. РАЗДЕЛ ОЦЕНОЧНЫХ МАТЕРИАЛОВ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ)

Примерный перечень вопросов для подготовки к зачету

1. Виды и содержание угроз для оконечных устройств в сети.
2. Состав средств защиты от вредоносного программного обеспечения на уровне оконечного узла.
3. Определение и содержание понятия «технический канал утечки информации».
4. Определение и содержание понятия «угроза безопасности информации».
5. Классификация угроз информационной безопасности.
6. Определение понятия «система защиты информации». Примеры систем защиты информации.
7. Общая классификация каналов утечки информации.
8. Классификация каналов утечки информации по виду среды распространения.
9. Состав и содержание целей защиты информации.
10. Содержание методики определения статуса защищенности информации.
11. Определение показателя защищенности информации.
12. Принципы функционирования системы обнаружения вторжений уровня хоста.
13. Какие источники информации об уязвимостях существуют?
14. Перечислите и охарактеризуйте классы инструментов сканирования и взлома сетей, приведите примеры конкретных программ для операционной системы Windows.
15. Перечислите и охарактеризуйте классы инструментов сканирования и взлома сетей, приведите примеры конкретных программ для операционной системы Linux.
16. Перечислите основные способы реализации атак методом социальной инженерии и сценарии противодействия этим атакам.
17. Перечислите причины использования операционной системы Linux в центрах управления событиями кибербезопасности.
18. Опишите содержание проблемы туннелирования сетевого трафика с использованием прикладных протоколов на примере DNS, https.
19. Опишите способы обнаружения и блокирования трафика одноранговых сетей и трафика анонимизирующих сетей P2P и TOR.
20. Опишите принципы работы системы журналирования событий в операционной системе Linux.
21. Опишите принципы работы системы журналирования событий в операционной системе Windows.
22. Приведите содержание проекта документа «Концепция стратегии кибербезопасности Российской Федерации».

23. Каким основным вопросам уделено внимание в Федеральном законе от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры российской федерации».

24. Перечислите основные пункты плана мероприятий по направлению Информационная безопасность программы Цифровая экономика Российской Федерации и раскройте их содержание.

25. Какими документами определяется ответственность за преступления в киберпространстве в России?