МВД России
Санкт-Петербургский университет

А. И. Локнов

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Учебно-методическое пособие

Санкт-Петербург
2024

План-график 2024, поз. 70

УДК 004.056
ББК 32.97
Л73

Локнов А. И.

Л73 Основы кибербезопасности : учебно-методическое пособие / А. И. Локнов. — Санкт-Петербург : СПбУ МВД России, 2024. — 64 с.

ISBN 978-5-91837-824-3
EDN: ZDRBAZ

Учебно-методическое пособие соответствует программе учебной дисциплины «Основы кибербезопасности» и предназначено для использования при обучении на всех специальностях и направлениях подготовки высшего образования как по очной форме обучения, так и по заочной.

В учебно-методическом пособии представлены методические рекомендации по подготовке к семинарским и практическим занятиям, примерный перечень контрольных вопросов текущей аттестации, примерный перечень вопросов для подготовки к промежуточной аттестации (зачету), рекомендации слушателям факультета заочного обучения. Использование данного учебно-методического пособия в образовательном процессе создает условия для более качественного освоения учебной дисциплины «Основы кибербезопасности».

Адресовано курсантам, слушателям, адъюнктам, научно-педагогическим работникам образовательных организаций высшего образования системы МВД России, интересующихся вопросами кибербезопасности.

УДК 004.056
ББК 32.97

Рецензенты:
Еськов А. В., доктор технических наук, профессор
(Краснодарский университет МВД России);
Симаков А. А., кандидат технических наук, доцент
(Омская академия МВД России)

ISBN 978-5-91837-824-3

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Целью изучения дисциплины «Основы кибербезопасности» является подготовка обучающегося к правоприменительной, экспертно-консультационной, оперативно-служебной и организационно-управленческой деятельности в сфере регулирования отношений, складывающихся в процессе обеспечения кибербезопасности в органах внутренних дел. В рамках обучения предполагается способствовать приобретению у обучающихся базовых знаний и навыков работы с нормативными документами в области кибербезопасности; сформировать у курсантов и слушателей систему профессиональных умений и навыков, необходимых для понимания принципов обеспечения кибербезопасности, основных методов и средств защиты информационных ресурсов; содействовать формированию у обучающихся высокого уровня правосознания и правовой культуры, обеспечивающих неукоснительное соблюдение норм действующего законодательства в области кибербезопасности.

Дисциплина «Основы кибербезопасности» входит в обязательную часть учебного плана «Блок 1. Дисциплины (модули)» и изучается на всех специальностях и направлениях подготовки реализуемыми Санкт-Петербургским университетом МВД России (далее — университет).

В учебно-методическом пособии представлены методические рекомендации по подготовке к семинарским и практическим занятиям для оказания помощи курсантам и слушателям в самостоятельной подготовке при усвоении знаний по дисциплине «Основы кибербезопасности».

Семинары в силу многоплановости мировоззренческого восприятия материальных и духовных явлений, множественности подходов к проблеме их познания и оценки, предполагают формирование у курсантов и слушателей умений аргументировано излагать свою точку зрения по изучаемой проблеме и доказывать значимость того или иного подхода к рассматриваемому предмету. При обсуждении проблем предусматривается раскрытие роли и значения получаемых знаний в сфере кибербезопасности.

Для наиболее логичного ответа на занятии обучающимся необходимо соблюдать ряд определенных правил.

Примерная структура ответа:

— обосновать значимость обсуждаемой проблемы по соответствующей теме учебной дисциплины;

— представить различные точки зрения по данной проблематике;

— изложить концепцию, которая по своему содержанию близка выступающему, и соответствующие аргументы, обосновывающие верность его позиции;

— сформулировать собственные выводы по предложенному выступлению.

На каждом семинарском занятии предусматривается заслушивание доклада и сообщений.

Доклад — это публичное сообщение, представляющее собой развернутое изложение на определенную тему. Доклад предполагает определенный творческий подход докладчика к отбору и использованию представляемого материала и обеспечивает изложение точки зрения докладчика по проблеме или кругу проблем.

Реферативное сообщение — по своей сути это реферат, только представленный в форме доклада. В реферативном сообщении предполагается как можно более точное раскрытие позиции автора монографии, научной статьи, учебного издания, а также собственное выражение отношения к раскрываемой позиции составителя реферата.

Время, отводимое на доклад, как правило, не должно превышать 8 минут учебного времени. Время, отводимое на сообщение, составляет 5–7 минут учебного времени.

Структурно доклад или реферативное сообщение включает: краткое выступление, один или два вопроса, заключение (выводы) и список использованных источников при работе над докладом или сообщением.

Подготовка доклада или реферативного сообщения не освобождает слушателя от подготовки по всем вопросам семинара.

Обсуждение современных проблем по исследуемой области кибербезопасности на семинарах и практических занятиях является

подготовкой курсантов и слушателей к зачету. В ходе данных занятий оформляется и совершенствуется методика ответа на зачёте.

В настоящее время чаще всего используется форма семинара, предполагающая наличие вопросов и ответов к ним. Такая концепция направленна на повторение и углубление знаний материала лекции и рекомендованной литературы.

Семинары по курсу «Основы кибербезопасности» проводятся как с использованием традиционных дискуссионно-диалоговых форм, так и с применением интерактивных методов обучения: «мозговой штурм», «сократический диалог», «круглый стол», «ролевая игра», «учебная конференция», «работа в малых группах».

Применение диалоговых методов на семинаре включающих обсуждение докладов и дискуссию, позволяет проверить, насколько полно и правильно обучающийся усвоил предлагаемый учебный материал, выявить пробелы в знаниях, дать дополнительные пояснения или новые задания для более глубокого и всестороннего изучения проблемы. Диалоговые формы дают возможность курсантам и слушателям высказать накопленную ими информацию по данной теме. Они позволяют не только закрепить знания обучающихся, но и учат их методике устного выступления, навыкам ведения дискуссии, умению аргументировать свое мнение, развивают навыки восприятия и анализа другого мнения.

Практические занятия — это метод репродуктивного обучения, обеспечивающий связь теории и практики, содействующий выработке у курсантов и слушателей умений и навыков применения знаний, полученных на лекции и в ходе самостоятельной работы. В ходе практических занятий по дисциплине «Основы кибербезопасности» ставятся следующие задачи:

— помочь обучающимся систематизировать, закрепить и углубить знания теоретического характера, овладеть методами сравнительного анализа фактов и явлений в области кибербезопасности;

— научить их работать с научной литературой и источниками в области кибербезопасности;

— формировать умение учиться самостоятельно, то есть овладевать методами, способами и приемами самообучения, саморазвития и самоконтроля;

— развивать у курсантов и слушателей навыки приёмов работы с различным современным техническим оборудованием.

Представленный материал включает в себя учебные вопросы в соответствии с рабочей программой дисциплины, основные понятия и определения, вопросы для самоконтроля и задания для проверки усвоения знаний, примерный перечень контрольных вопросов текущей аттестации, примерный перечень вопросов для подготовки к промежуточной аттестации (зачёту), рекомендации слушателям факультета заочного обучения по изучению дисциплины «Основы кибербезопасности» список нормативно-правовых актов, основную и дополнительную литературы.

ТЕМА 1. ОБЩИЕ ВОПРОСЫ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ

***Учебные вопросы*:**

1. Введение в дисциплину.
2. Кибербезопасность: современные киберугрозы.
3. Методы совершения киберпреступлений.
4. Уязвимости интернета вещей.
5. Центры мониторинга и управления безопасностью как составляющие системы борьбы с киберпреступлениями.
6. Группы ролей специалистов в центрах управления событиями кибербезопасности.
7. Понятие Критической информационной инфраструктуры (КИИ).

Методические рекомендации по подготовке к семинарскому занятию:

1. Изучить содержание лекции 1/1. При необходимости обратиться к нормативным правовым актам, основной и дополнительной литературе.

2. Вспомнить смысл и содержание следующих основных терминов и понятий с их краткой фиксацией в конспекте (при необходимости): «кибернетика», «киберпространство», «кибербезопасность», «сетевая безопасность», «безопасность приложений», «Интернет-безопасность», «информационная безопасность», «критическая информационная инфраструктура (КИИ)», «защита информации», «киберзащита информации».

3. Готовясь к семинару, следует иметь в виду, что:

— доклад должен включать введение, основную часть и заключение:

а) во введение следует отразить (кратко) важность вопроса;

б) в основной части нужно изложить суть докладываемого;

в) в заключении необходимо подвести итоги (сделать вводы);

г) время доклада не должно превышать 8 минут.

— наличие презентаций и слайдов приветствуется.

4. Отвечая на учебные вопросы, указанные выше, следует иметь в виду, что:

— ответы на учебные вопросы не должны превышать 2–5 минут;

— при ответах в сжатой форме излагать основное содержание, приводить требуемые определения, в заключительной части ответов целесообразно рассматривать практическую значимость или область применения обсуждаемых вопросов;

— выступления по вопросам должны быть без использования конспектов;

— уточнения и обсуждения вопроса не должны превышать, как правило, 1–2 минуты;

— допускается обсуждение проблемных вопросов, не вошедших в план семинара, но связанных с темой.

***Рекомендуемые темы для докладов*:**

1. Современные киберугрозы.
2. Методы совершения киберпреступлений.
3. Интернет вещей и его информационные уязвимости.
4. Центры мониторинга и управления безопасностью как составляющие системы борьбы с киберпреступлениями.
5. Группы ролей специалистов в центрах управления событиями кибербезопасности.
6. Подход к защите критических информационных инфраструктур в России.
7. Функционирование информационных систем МВД России в условиях деструктивных кибервоздействий.

Методические рекомендации по подготовке к практическому занятию:

Проанализируйте структуру и функциональные особенности системы обеспечения кибербезопасности в соответствии с заданием. Для этого нужно:

1) изучить содержание лекции 1/1 и учебно-справочные материалы по дисциплине «Основы кибербезопасности»:

2) найти ответы на следующие вопросы:

— Что включают в себя информационные системы?

— Как применяются информационные технологии в целях идентификации физических лиц?

— Что такое национальная система доменных имен и как она используется в целях идентификации физических лиц?

— Определите порядок доступа к копиям заблокированных сайтов.

— В чем заключается информационно-психологическое обеспечение кибербезопасности?

— Как используется приёмы манипуляций при информационно-психологических операциях?

— Какие технологии используются для достижения эффективного результата в создании у населения определенных политических убеждений и ориентаций?

— Перечислите методы противодействия информационно-психологическим операциям при обеспечении кибербезопасности.

Вопросы для самоконтроля:

1. Что такое информационная угроза?
2. Дайте определение утечки информации.
3. Что такое информационная уязвимость?
4. Какие признаки используют при классификации киберугроз?
5. Перечислите основные направления реализации информационных угроз.
6. Какие методы реализации угроз информационной безопасности известны Вам?
7. Для чего предназначены центры мониторинга и управления при борьбе с киберпреступлениями?
8. Что такое КИИ?
9. Какие объекты КИИ Вам известны?
10. Что относят к субъектам КИИ?

Перечень нормативных правовых актов и литературы

Нормативные правовые акты:

1. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

4. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

5. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

6. 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“».

7. 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 «Гарант».

8. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

Основная литература:

1. Основы информационной безопасности в органах внутренних дел : учебник. Санкт-Петербург: Изд-во СПб ун-та МВД России, 2019. 312 с.

2. Средства и системы обработки информации: учебное пособие. Санкт-Петербург: СПБУ МВД России, 2023. 124 с.

3. Основы защищенного электронного документооборота в органах внутренних дел : учебное пособие / науч. ред. : Ю. И. Синещук, А. И. Локнов. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2022. 76 с.

Дополнительная литература:

1. Основы информационной безопасности в органах внутренних дел : учебное пособие / О. Г. Смирнова, И. Н. Васильева. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. 148 с.

2. Основы информационной безопасности в органах внутренних дел : учебное пособие / М. Г. Гизатуллин, И. Ф. Файсханов. Екатеринбург: Уральский юридический институт МВД России, 2020. 51 с.

3. Основы информационной безопасности : учебное пособие / В. Н. Галатенко. 4-е изд. Москва : Бином, 2008. 206 с.

ТЕМА 2. НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ КИБЕРБЕЗОПАСНОСТИ

***Учебные вопросы*:**

1. Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации как компонент государственной политики развития национального сектора применения информационных технологий.

2. Законодательство Российской Федерации в области защиты информации.

3. Основы государственной политики Российской Федерации в области международной информационной безопасности.

4. Международные стандарты в области обеспечения кибербезопасности.

5. Противодействие преступлениям и правонарушениям в сфере компьютерной информации.

Методические рекомендации по подготовке к семинарскому занятию:

1. Изучить содержание лекции 2/1. При необходимости обратиться к нормативным правовым актам, основной и дополнительной литературе.

2. Вспомнить смысл и содержание следующих основных терминов и понятий с их краткой фиксацией в конспекте (при необходимости): «информационная безопасность», «кибернетика», «киберпространство», «кибербезопасность», «безопасность приложений», «Интернет-безопасность», «критическая информационная инфраструктура», «защита информации», «киберзащита информации».

3. Готовясь к семинару, следует иметь в виду, что:

— доклад должен включать введение, основную часть и заключение:

а) во введение следует отразить (кратко) важность вопроса;

б) в основной части нужно изложить суть докладываемого;

в) в заключении необходимо подвести итоги (сделать вводы);

г) время доклада не должно превышать 8 минут;

— наличие презентаций и слайдов приветствуется.

4. Отвечая на учебные вопросы, указанные выше, следует иметь в виду, что:

— ответы на учебные вопросы не должны превышать 2–5 минут;

— при ответах в сжатой форме излагать основное содержание, приводить требуемые определения, в заключительной части ответов целесообразно рассматривать практическую значимость или область применения обсуждаемых вопросов;

— выступления по вопросам должно быть без использования конспектов;

— уточнения и обсуждения вопроса не должны превышать, как правило, 1–2 минут;

— допускается обсуждение проблемных вопросов, не вошедших в план семинара, но связанных с темой.

Рекомендуемые темы для докладов:

1. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА).
2. Внутренние и внешние источники угроз кибербезопасности.
3. Субъекты информационных отношений в деятельности подразделений МВД России и обеспечение их кибербезопасности.
4. Нормативное правовое регулирование в органах внутренних дел по обеспечению кибербезопасности.
5. Функции и органы МВД России по обеспечению кибербезопасности государства, общества, личности.
6. Международные стандарты в области обеспечения кибербезопасности.
7. Роль и место ФСТЭК России в вопросах обеспечения кибербезопасности.

Методические рекомендации по подготовке к практическому занятию:

Проанализируйте структуру и функциональные особенности системы обеспечения кибербезопасности в соответствии с заданием. Для этого нужно:

1) изучить содержание лекции 2/1 и учебно-справочные материалы по дисциплине «Основы кибербезопасности»;

2) найти ответы на следующие вопросы:

— Дайте определение понятия Система обеспечения информационной безопасности (СОИБ).

— Что входит в состав СОИБ?

— Куда входит СОИБ в качестве подсистемы?

— Что составляет организационную основу СОИБ?

— В чем выражается руководящая роль Президента РФ в части СОИБ?

— В чем проявляется роль Палат Федерального Ссобрания РФ в части СОИБ?

— В чем выражается роль Правительства РФ в части СОИБ?

— В чем вклад Совета Безопасности РФ в части СОИБ?

— Какова роль федеральных органов исполнительной власти в части СОИБ?

— Какова роль органов исполнительной власти субъектов РФ в части СОИБ?

— Что возлагается на межведомственные и государственные комиссии в части СОИБ?

— Какие федеральные органы осуществляют функции по обеспечению информационной безопасности?

— Каким нормативом регламентировано создание системы ГосСОПКА?

— Какая федеральная служба отвечает за ведение банка данных угроз информации?

— Какая федеральная служба отвечает за обеспечение безопасности значимых объектов КИИ?

Вопросы для самоконтроля:

1. Как формулируются цель и задачи системы информационной безопасности?
2. Какие задачи в части кибербезопасности сформулировал Президент РФ на специальном заседании Совета Безопасности РФ 20 мая 2022 г.?
3. Какие нормативно-правовые документы относят к актам федерального законодательства?
4. Что относят к методическим документам государственных органов России?
5. В чем суть стратегии кибербезопасности РФ?
6. Перечислите основные принципы стратегии развития информационного общества в РФ?
7. Какой орган государственной власти осуществляет разработку и корректировку критериев и показателей обеспечения национальной безопасности Российской Федерации?
8. Как определено понятие кибербезопасность в ГОСТ Р 56205-2014?
9. В чем сходства и различия личной, корпоративной и государственной экосистем?

Перечень нормативных правовых актов и литературы

Нормативные правовые акты:

1. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).
2. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации».
3. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».
4. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

5. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

6. 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“».

7. 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 «Гарант».

8. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

Основная литература:

1. Основы информационной безопасности в органах внутренних дел : учебник. Санкт-Петербург: Изд-во СПб ун-та МВД России, 2019. 312 с.

2. Средства и системы обработки информации: учебное пособие. Санкт-Петербург: СПБУ МВД России, 2023. 124 с.

3. Основы защищенного электронного документооборота в органах внутренних дел : учебное пособие / науч. ред. : Ю. И. Синещук, А. И. Локнов. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2022. 76 с.

Дополнительная литература:

1. Основы информационной безопасности в органах внутренних дел : учебное пособие / О. Г. Смирнова, И. Н. Васильева. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. 148 с.

2. Основы информационной безопасности в органах внутренних дел : учебное пособие / М. Г. Гизатуллин, И. Ф. Файсханов. Екатеринбург: Уральский юридический институт МВД России, 2020. 51 с.

3. Основы информационной безопасности : учебное пособие / В. Н. Галатенко. 4-е изд. Москва : Бином, 2008. 206 с.

ТЕМА 3. ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

***Учебные вопросы*:**

1. Обеспечение кибербезопасности оконечных устройств (сетевые камеры видеонаблюдения, сетевые контроллеры, компьютеры, серверы, ноутбуки, смартфоны).

2. Способы совершения кибератак на средства хранения, обработки и передачи данных.

3. Способы защиты от вредоносного программного обеспечения.

4. Система обнаружения вторжений на объекты критической информационной инфраструктуры.

5. Управление рисками.

6. Принципы обеспечения сетевой безопасности.

7. Особенности подсистем обеспечения безопасности и журналирования в операционных системах Windows, Linux.

Методические рекомендации по подготовке к семинарскому занятию:

1. Изучить содержание лекции 3/1. При необходимости обратиться к нормативным правовым актам, основной и дополнительной литературе.

2. Вспомнить смысл и содержание следующих основных терминов и понятий с их краткой фиксацией в конспекте: «кибератака», «сетевые ресурсы», «виды кибератак», «разведывательные атаки», «атаки доступа», «атаки методами социальной инженерии», «атаки, направленные на истощение информационного ресурса», «требование по защите информации».

3. Готовясь к семинару, следует иметь в виду, что:

— доклад должен включать введение, основную часть и заключение:

а) во введение нужно отразить (кратко) важность вопроса;

б) в основной части следует изложить суть докладываемого;

в) в заключении необходимо подвести итоги (сделать вводы);

г) время доклада не должно превышать 8 минут;

— наличие презентаций и слайдов приветствуется.

4. Отвечая на учебные вопросы, указанные выше, следует иметь в виду, что:

— ответы на учебные вопросы не должны превышать 2–5 минут;

— при ответах в сжатой форме излагать основное содержание, приводить требуемые определения, в заключительной части ответов целесообразно рассматривать практическую значимость или область применения обсуждаемых вопросов;

— выступления по вопросам должны быть без использования конспектов;

— уточнения и обсуждения вопроса не должны превышать 1–2 минут;

— допускается обсуждение проблемных вопросов, не вошедших в план семинара, но связанных с темой.

Рекомендуемые темы для докладов:

1. Классификация киберугроз компьютерной безопасности.
2. Особенности реализации сетевых кибератак.
3. Кибератаки на основе методов социальной инженерии.
4. Кибератаки на мобильные устройства.
5. Международный подход к выявлению и анализу уязвимостей, базы данных уязвимостей.
6. Операционная система специального назначения Astra Linux.
7. Основные способы защиты от вредоносного программного обеспечения.

Методические рекомендации по подготовке к практическому занятию:

Проанализируйте возможности методов и средств обеспечения компьютерной безопасности в соответствии с заданием. Для этого нужно:

1) изучить содержание лекции 3/1 и учебно-справочные материалы по дисциплине «Основы кибербезопасности», охарактеризовать:

— методы социальной инженерии;

— организационные методы защиты компьютерных систем при обработке конфиденциальной информации;

— технические методы и средства защиты компьютерных систем при обработке конфиденциальной информации;

2) найти ответы на следующие вопросы:

— В чем суть методов защиты компьютерной безопасности?

— В чем основная цель программно-аппаратной защиты компьютерной безопасности?

— Перечислите основные задачи программно-аппаратной защиты компьютерной безопасности. Приведите примеры.

— Приведите классификацию программно-аппаратных средств защиты компьютерной безопасности (в зависимости от защищаемого объекта, функционального назначения, и места установки).

— Охарактеризуйте возможности аппаратных средств защиты информации, встроенных в BIOS компьютера.

— Охарактеризуйте возможности аппаратных средств защиты информации, встроенных в операционную систему компьютера.

— Охарактеризуйте возможности автономных средств защиты информации, включаемых в состав СЗИ.

— Охарактеризуйте возможности добавочных средств защиты информации, включаемых в состав СЗИ.

— Охарактеризуйте возможности средств сетевой защиты информации в компьютерных системах и сетях.

Вопросы для самоконтроля:

1. Как в 149-ФЗ от 27 июля 2006 г. сформулирован принцип комплексного подхода к информационной безопасности?
2. В чем цель принципа национального нормирования?
3. Какие факторы учитываются при реализации принципа сертификации?
4. Расшифруйте запись: ИТ.МЭ.А4.ПЗ.
5. Какие технологические операции используют при реализации принципа проактивности?

6. Почему важен принцип нулевого доверия и какие цели он преследует?

7. В чем существо принципа управления рисками?

8. В чем проявляется ограничение рисков применительно к вопросам киберзащиты?

9. Приведите пример передачи риска третьей стороне.

10. Что стоит за формулировкой «принятие риска»?

11. Перечислите основные виды кибератак на сетевые ресурсы.

12. Охарактеризуйте разведывательные атаки и атаки доступа.

13. Охарактеризуйте атаки, проводимые методами социальной инженерии.

Перечень нормативных правовых актов и литературы

Нормативные правовые акты:

1. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

4. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5. 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»».

6. 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”».

7. Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации 5 декабря 2016 г. № 646.

8. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

Основная литература:

1. Средства и системы обработки информации : учебное пособие. Санкт-Петербург : СПБУ МВД России, 2023. 124 с.

2. Системы и сети передачи информации : учебно-методическое пособие / А. И. Локнов, И. Н. Васильева. Санкт-Петербург : СПБУ МВД России, 2023. 72 с.

3. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие / В. Олифер, Н. Олифер. Юбилейное изд. Санкт-Петербург ; Москва ; Екатеринбург : Питер, 2021.1005 с.

Дополнительная литература:

1. Организация и обеспечение безопасности информационно-технологических сетей и систем: учебник для вузов / Д. А. Мельников. Москва : Университетская книга; Москва : IDO PRESS, 2013. 598 с.

2. Защита информации в персональном компьютере : учебное пособие / Н. З. Емельянова. Москва : Форум, 2009. 368 с.

ТЕМА 4. ИСТОЧНИКИ И КАНАЛЫ УТЕЧКИ ИНФОРМАЦИИ. ОСНОВЫ ТЕХНИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

***Учебные вопросы*:**

1. Понятие о технических каналах утечки информации: состав и характеристики.

2. Оптические, радиоэлектронные, акустические, материально-вещественные каналы утечки информации.

3. Основные и вспомогательные технические средства, и системы.

4. Технические каналы утечки информации при ее передаче по каналам связи.

5. Технические каналы утечки акустической информации: воздушные, вибрационные, параметрические, электроакустические, оптико-электронные.

6. Технические каналы утечки информации, обрабатываемой основными техническими средствами и системами.

7. Побочные электромагнитные излучения (ПЭМИ).

8. Перехват излучений на частотах работы ВЧ-генераторов.

9. Технические каналы утечки видеоинформации.

Методические рекомендации по подготовке к семинарскому занятию:

1. Изучить содержание лекции 4/1. При необходимости обратиться к нормативным правовым актам, основной и дополнительной литературе.

2. Вспомнить смысл и содержание следующих основных терминов и понятий с их краткой фиксацией в конспекте (при необходимости): «утечка информации», «объект информатизации», «несанкционированный доступ», «защищенный документооборот», «правовое регулирование», «регулятор», «защита персональных данных», «защита в государственных информационных системах».

3. Готовясь к семинару, следует иметь в виду, что:

— доклад должен включать введение, основную часть и заключение:

а) во введение нужно отразить (кратко) важность вопроса;

б) в основной части следует изложить суть докладываемого;

в) в заключении необходимо подвести итоги (сделать вводы);

г) время доклада не должно превышать 8 минут;

— наличие презентаций и слайдов приветствуется.

4. Отвечая на учебные вопросы, указанные выше, следует иметь в виду, что:

— ответы на учебные вопросы не должны превышать 2–5 минут;

— при ответах в сжатой форме излагать основное содержание, приводить требуемые определения, в заключительной части ответов целесообразно рассматривать практическую значимость или область применения обсуждаемых вопросов;

— выступления по вопросам должны быть без использования конспектов;

— уточнения и обсуждения вопроса не должны превышать 1–2 минут;

— допускается обсуждение проблемных вопросов, не вошедших в план семинара, но связанных с темой.

Рекомендуемые темы для докладов:

1. Аттестация информационных систем на соответствие требованиям о защите информации.
2. Генераторы шума.
3. Средства обнаружения каналов утечки информации.
4. Нелинейные локаторы.
5. Досмотровая техника.

Методические рекомендации по подготовке к практическому занятию:

1. Проанализируйте возможности средств технической защиты речевой информации. Для этого:

1) изучите содержание лекции 4/1 и учебно-справочные материалы по дисциплине «Основы кибербезопасности», охарактеризуйте:

— состав средств защиты в помещениях для конфиденциальных переговоров;

— средства защиты телефонных и слаботочных линий;

— средства пространственного и линейного зашумления;

— средства защиты мобильных телефонов и смартфонов- акустические сейфы;

— подавители и блокираторы;

— системы контроля радиоизлучений;

— нелинейные локаторы;

— обнаружители диктофонов;

— аппаратура обследования проводных телекоммуникаций;

2) ознакомьтесь с составом и возможностями пассивных средств защиты (ПСЗ) информации от утечки за счет ПЭМИН. Для этого:

— находясь в Государственном реестре сертифицированных средств защиты информации, в окне «Текст для поиска», наберите ПСЗ;

— упорядочите полученные данные по убыванию, используя поле «Срок действия сертификата»;

— ответьте на вопросы: сколько всего таких ПСЗ; сколько СЗИ можно будет использовать в следующем году (у каких СЗИ еще будет действовать сертификат);

3) проанализируйте примеры практических заданий, планируемых для рассмотрения в ходе практического занятия:

Практическое задание № 1

В актовом зале, имеющем статус защищенного помещения, предполагается проведение совещания с обсуждением конфиденциальных сведений. В последний момент выяснилось, что многоящичный шкаф с индивидуальными запирающимися ячейками для временного хранения мобильных телефонов, демонтировали с целью ремонта. Кто-то предложил мобильные телефоны во время совещания разместить на одном из свободных столов актового зала, выключив их предварительно. Является ли приемлемым такое решение? Обоснуйте Вашу точку зрения.

Практическое задание № 2

На территории объекта ОВД задержан человек, прошедший по поддельному электронному пропуску. Предполагается, что копия использованного электронного пропуска была изготовлена с помощью имитатора терминала, считывающего данные электронных пропусков. Какие меры Вы можете предложить для исключения подобного инцидента?

Практическое задание № 3

Источник сообщил, что в помещении ОВД, где ведется работа с конфиденциальной информацией, ожидается несанкционированный съем данных с электромагнитного технического канала утечки информации (ТКУИ).

Необходимо: подготовить и доложить экспертам и преподавателю следующие материалы:

1. Описание сути процесса утечки информации с такого ТКУИ.
2. Суть организационных мероприятий, защищающих от несанкционированного съема данных с такого ТКУИ.
3. Предложения по целесообразным техническим мероприятиям, обеспечивающим защиту информации с ТКУИ.
4. Правовую основу защиты информации в данном случае.

Вопросы для самоконтроля:

1. Перечислите основные формы информации, представляющие интерес с точки зрения защиты?
2. Чем речевая форма информации отличается от остальных? В чем особенности защиты такой информации?
3. Что такое основные технические средства и системы (ОТСС)?
4. Что такое вспомогательные технические средства и системы (ВТСС)?
5. Дайте определение объекта ТСПИ?
6. Что такое технический канал утечки информации?
7. Приведите определение понятия контрольной зоны (КЗ).
8. В чем сходства и различия КЗ1 и КЗ2?

9. Какие ТКУИ актуальны при защите речевой информации?

10. Какие ТКУИ актуальны при обработке видеоинформации?

11. Назовите меры защиты информации от утечки речевой информации по ТКУИ?

Перечень нормативных правовых актов и литературы

Нормативные правовые акты:

1. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

4. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5. 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»».

6. 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”».

7. Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации 5 декабря 2016 г. № 646.

8. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

Основная литература:

1. Средства и системы обработки информации : учебное пособие. Санкт-Петербург : СПБУ МВД России, 2023. 124 с.

2. Системы и сети передачи информации : учебно-методическое пособие / А. И. Локнов, И. Н. Васильева. Санкт-Петербург : СПБУ МВД России, 2023. 72 с.

3. Компьютерные сети. Принципы, технологии, протоколы : учебное пособие / В. Олифер, Н. Олифер. Юбилейное изд. Санкт-Петербург ; Москва ; Екатеринбург : Питер, 2021.1005 с.

Дополнительная литература:

1. Основы информационной безопасности в органах внутренних дел: учебное пособие / О. Г. Смирнова, И. Н. Васильева. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. 148 с.

2. Основы информационной безопасности в органах внутренних дел: учебное пособие / М. Г. Гизатуллин, И. Ф. Файсханов. Екатеринбург : Уральский юридический институт МВД России, 2020. 51 с.

3. Основы информационной безопасности: учебное пособие / В. Н. Галатенко. 4-е изд. Москва : Бином, 2008. 206 с.

ТЕМА 5. ОСНОВЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

***Учебные вопросы*:**

1. Роль криптографии в глобальной задаче защиты коммуникаций.
2. Криптология, криптография, криптоанализ.
3. Исторические примеры шифрования: шифр Сциталя, шифр Цезаря, шифр Виженера, Enigma Machine.
4. Подстановочные, перестановочные, многоалфавитные шифры.
5. Термины и характеристики для описания криптоключей.
6. Понятия об инструментах открытого программного обеспечения OpenSSL.
7. Криптографические хэш-функции.
8. Алгоритмы симметричного и ассиметричного шифрования.
9. Решение задач обеспечения целостности, конфиденциальности и аутентификации асимметричными алгоритмами шифрования.
10. Цифровые подписи и сценарии их использования.
11. Инфраструктура общих ключей.
12. Управление общими ключами.
13. Системы доверия на основе инфраструктуры открытых ключей.
14. Регистрация и отзыв сертификатов.

Методические рекомендации по подготовке к семинарскому занятию:

1. Изучить содержание лекции 5/1. При необходимости обратиться к нормативным правовым актам, основной и дополнительной литературе.

2. Вспомнить смысл и содержание следующих основных терминов и понятий с их краткой фиксацией в конспекте (при необходимости): «криптогра́фия», «криптосистема», «шифр», «криптограмма», «ключ», «шифрование», «расшифровывание», «асимметричный шифр», «симметричный шифр», «шифр с открытым ключом», «закрытый ключ», «дешифровка», «криптографическая стойкость».

3. Готовясь к семинару, следует иметь в виду, что:

— доклад должен включать введение, основную часть и заключение:

а) во введение нужно отразить (кратко) важность вопроса;

б) в основной части следует изложить суть докладываемого;

в) в заключении необходимо подвести итоги (сделать вводы);

г) время доклада не должно превышать 8 минут;

— наличие презентаций и слайдов приветствуется.

4. Отвечая на учебные вопросы, указанные выше, следует иметь в виду, что:

— ответы на учебные вопросы не должны превышать 2–5 минут;

— при ответах в сжатой форме излагать основное содержание, приводить требуемые определения, в заключительной части ответов целесообразно рассматривать практическую значимость или область применения обсуждаемых вопросов;

— выступления по вопросам должны быть без использования конспектов;

— уточнения и обсуждения вопроса не должны превышать 1–2 минут;

— допускается обсуждение проблемных вопросов, не вошедших в план семинара, но связанных с темой.

Рекомендуемые темы для докладов:

1. Энигма – оружие «Блицкрига».
2. Эволюция криптографической деятельности до XX века.
3. Периоды становления криптографии в XX веке.
4. Стеганография и развитие ее возможностей.
5. Электронная подпись.
6. Понятие об инструментах открытого программного обеспечения OpenSSL.

Методические рекомендации по подготовке к практическому занятию:

1. Проанализируйте способы криптографической защиты информации и криптосистем в соответствии с заданием. Для этого изучите содержание лекции 5/1 и учебно-справочные материалы по дисциплине «Основы кибербезопасности».

2. Найдите ответы на следующие вопросы:

— В чем разница между криптосистемой и шифром?

— Какие симметричные криптосистемы относят к числу традиционных?

— Что обозначает термин «симметричные криптосистемы»?

— Чем характеризуется шифр простой перестановки? Приведите примеры.

— В чем суть шифра маршрутной перестановки?

— Поясните понятие Магического квадрата.

— Чем характеризуется шифр простой замены? Приведите примеры.

— В чем суть шифра сложной замены?

— Что используется при практическом использовании такого шифра?

— Что предложил Альберти для упрощения процесса шифрования путем много алфавитной замены?

— Какие симметричные криптосистемы относят к современным?

— Сформулируйте достоинства и недостатки симметричных криптосистем.

— Дайте определение асимметричной криптосистемы.

— Сформулируйте область применения асимметричных криптосистем.

— Перечислите достоинства и недостатки асимметричных криптосистем.

3. Проанализируйте примеры практических заданий, планируемых для рассмотрения в ходе практического занятия:

Практическое задание № 1

Дешифровать криптограмму, полученную шифром Виженера.

«влцдутжбюцхъяррмшбрхцэооэцгбрьцмйфктъъюьмшэсяцпунуящэйтаьэдкцибрьцгбрпачкъуцпъбьсэгкцъгуущарцёэвърюуоюэкааэбрняфукабъарпяъафкъиьжяффнйояфывбнэнфуюгбрьсшьжэтбэёчюъюръегофкбьчябашвёэуъъюаднчжчужцёэвлрнчулбюпцуруньъшсэюъзкцхъяррнрювяспэмасчкпэужьжыатуфуярюравртубурьпэщлафоуфбюацмнубсюкйтаьэдйюнооэгюожбгкбръндэпотчмёодзцвбцшщвщепчдчдръюьскасэгъппэгюкдойрсрэвоопчщшоказръббнэугнялёкьсрбёуыэбдэулбюасшоуэтъшкрсдугэфлбубуъчнчтртпэгюкиугюэмэгюккъпэгяапуфуэзьрадзьжчюрмфцхраююанчёчюъыхьъцомэфъцпоирькнщпэтэузуябащущбаыэйчдфрпэцъърьцъцпоилуфэдцойэдятррачкубуфнйтаьэдкцкрннцюабугюууубурьпйюэъжтгюркующоъуфъэгясуоичщщчдцсфырэдщэъуяфшёчцюйрщвяхвмкршрпгюопэуцчйтаьэдкцибрьцыяжтюрбуэтэбдуящэубъибрювъежагибрбагбрымпуноцшяжцечкфодщоъчжшйуъцхчщвуэбдлдъэгясуахзцэбдэулькнъщбжяцэьрёдъьвюврнуяфуоухфекьгцччгэъжтанопчынажпачкъуъмэнкйрэфщэъьбудэндадъярьеюэлэтчоубъцэфэвлнёэгфдсэвэёкбсчоукгаутэыпуббцчкпэгючсаъбэнэфъркацхёваетуфяепьрювържадфёжбьфутощоявьъгупчршуитеачйчирамчюфчоуяюонкяжыкгсцбрясшчйотъъжрсщчл».

Практическое задание № 2

Дешифровать криптограмму «СВПООЗЛУЙЬСТЬ_ЕДПСКОКАОЙЗ», полученную методами столбцовой и двойной перестановок. Известно, что текст записывался в шифрующую таблицу построчно, знаки пробела в тексте сохранены.

Вопросы для самоконтроля:

1. Перечислите способы защиты информации.
2. Что обозначает термин «криптография».
3. Эволюция криптографической деятельности.
4. Понятие криптологии.
5. Понятие криптоанализа.

6. Что называется криптограммой.
7. Что представляет собой криптостойкость системы.
8. Симметричные криптосистемы.
9. Асимметричные криптосистемы.

Перечень нормативных правовых актов и литературы

Нормативные правовые акты:

1. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

4. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5. 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»».

6. 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”».

7. Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации 5 декабря 2016 г. № 646.

8. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

Основная литература:

1. Основы информационной безопасности в органах внутренних дел: учебник. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2019. 312 с.

2. Основы защищенного электронного документооборота в органах внутренних дел : учебное пособие / науч. ред. : Ю. И. Синещук, А. И. Локнов. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2022. 76 с.

Дополнительная литература:

1. Криптографическая защита информации : учебное пособие. / И. Н. Васильева, В. И. Куватов, В. С. Потехин. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2016. 151 с.

2. Криптографическая защита информации : практикум / И. Н. Васильева, В. И. Куватов. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. 260 с.

3. Основы информационной безопасности в органах внутренних дел : учебное пособие / О. Г. Смирнова, И. Н. Васильева. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. 148 с.

4. Основы информационной безопасности в органах внутренних дел : учебное пособие / М. Г. Гизатуллин, И. Ф. Файсханов. Екатеринбург : Уральский юридический институт МВД России, 2020. 51 с.

ТЕМА 6. РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ КИБЕРБЕЗОПАСНОСТИ И ИХ ОБРАБОТКА

***Учебные вопросы*:**

1. Банк данных угроз безопасности информации ГНИИИ ПТЗИ ФСТЭК России.

2. Уровневая структура описания инцидентов в международной базе данных VERIS.

3. Реагирование на инциденты в сфере сетевой безопасности.

4. Реагирование на уязвимости, связанные с компьютерной безопасностью.

5. Системы обнаружения вторжений, принципы построения и использования.

6. Мониторинг кибербезопасности.

7. Анализ данных сетевых вторжений.

8. Системы управления событиями и данными безопасности (SIEM).

Методические рекомендации по подготовке к семинарскому занятию:

1. Изучить содержание лекции 6/1. При необходимости обратиться к нормативным правовым актам, основной и дополнительной литературе.

2. Вспомнить смысл и содержание следующих основных терминов и понятий с их краткой фиксацией в конспекте (при необходимости): «киберпреступление», «кибератака», «инцидент кибербезопасности», «APT-атака», «SIEM система» «киберугроза», «компрометация информационной системы».

3. Готовясь к семинару, следует иметь в виду, что:

— доклад должен включать введение, основную часть и заключение:

а) во введение нужно отразить (кратко) важность вопроса;

б) в основной части следует изложить суть докладываемого;

в) в заключении необходимо подвести итоги (сделать вводы);

г) время доклада не должно превышать 8 минут;

— наличие презентаций и слайдов приветствуется.

4. Отвечая на учебные вопросы, указанные выше, следует иметь в виду, что:

— ответы на учебные вопросы не должны превышать 2–5 минут;

— при ответах в сжатой форме излагать основное содержание, приводить требуемые определения, в заключительной части ответов целесообразно рассматривать практическую значимость или область применения обсуждаемых вопросов;

— выступления по вопросам должны быть без использования конспектов;

— уточнения и обсуждения вопроса не должны превышать 1–2 минут;

— допускается обсуждение проблемных вопросов, не вошедших в план семинара, но связанных с темой.

Рекомендуемые темы для докладов:

1. Банк данных угроз безопасности информации ГНИИИ ПТЗИ ФСТЭК России.

2. Уровневая структура описания инцидентов в международной базе данных VERIS.

3. Системы обнаружения вторжений, принципы построения и использования.

4. Мониторинг кибербезопасности.

5. Особенности обнаружения, фиксации, изъятия и исследования электронных следов преступления.

По данной теме практическое занятие не предусмотрено.

Вопросы для самоконтроля:

1. Приведите этапы алгоритма совершения типового киберпреступления.

2. Приведите основные этапы алгоритма реагирования на инциденты информационной безопасности.

3. Перечислите и охарактеризуйте особенности выявления и фиксации следов киберпреступления.

4. Что составляет правовые основы участия специалиста при проведении следственных действий при осмотре средств вычислительно техники?

5. Каким образом могут быть получены сведения о работе операционной системы компьютера и его подсистем?

6. Каким образом можно получить сведения о сетевых соединениях, настроенных на компьютере?

7. Охарактеризуйте программы и утилиты, наиболее часто применяемые при извлечении следовой информации из персонального компьютера.

Перечень нормативных правовых актов и литературы

Нормативные правовые акты:

1. Конституция Российской Федерации: (принята всенародным голосованием 12 декабря 1993 г. с изменениями, одобренными в ходе общероссийского голосования 01.07.2020).

2. Федеральный закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности».

3. Федеральный закон от 7 июля 2003 г. № 126-ФЗ «О связи».

4. Федеральный закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

5. 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»».

6. 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”».

7. Доктрина информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации 5 декабря 2016 г. № 646.

8. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35).

Основная литература:

1. Основы информационной безопасности в органах внутренних дел: учебник. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2019. 312 с.

2. Средства и системы обработки информации : учебное пособие. Санкт-Петербург : СПБУ МВД России, 2023. 124 с.

3. Основы защищенного электронного документооборота в органах внутренних дел : учебное пособие / науч. ред. : Ю. И. Синещук, А. И. Локнов. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2022. 76 с.

Дополнительная литература:

1. Основы информационной безопасности в органах внутренних дел : учебное пособие / О. Г. Смирнова, И. Н. Васильева. Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. 148 с.

2. Основы информационной безопасности в органах внутренних дел : учебное пособие / М. Г. Гизатуллин, И. Ф. Файсханов. Екатеринбург : Уральский юридический институт МВД России, 2020. 51 с.

3. Основы информационной безопасности : учебное пособие / В. Н. Галатенко. 4-е изд. Москва : Бином, 2008. 206 с.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ КОНТРОЛЬНЫХ ВОПРОСОВ ТЕКУЩЕЙ АТТЕСТАЦИИ

Тема 1. Общие вопросы обеспечения кибербезопасности

1. Доступ к информации:

1. Состояние информации, при котором ее можно беспрепятственно использовать.

2. Право на чтение, изменение, хранение, копирование, уничтожение, изменение информации.

3. Возможность получения информации и ее использования.

2. Конфиденциальность информации:

1. Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.

2. Служебные сведения, доступ к которым ограничен.

3. Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

3. Ограничение доступа к информации:

1. Это разграничение доступа субъектов к объектам, основанное на назначении метки конфиденциальности для информации, содержащейся в объектах, и выдаче официальных разрешений (допуска) субъектам на обращение к информации.

2. Устанавливается владельцем информации и федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц и безопасности государства.

3. Устанавливается федеральными законами в целях защиты основ конституционного строя, нравственности, здоровья, прав и законных интересов других лиц, обеспечения обороны страны и безопасности государства.

4. Что понимается под термином «Безопасность информации»?

1. Такое ее состояние, при котором исключается возможность ознакомления с этой информацией, ее изменения или уничтожения лицами, не имеющими на это права, а также утечки за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники.

2. Защищенность информации от нежелательного (для соответствующих субъектов информационных отношений) ее разглашения (нарушения конфиденциальности), искажения (нарушения целостности), утраты или снижения степени доступности информации, а также незаконного ее тиражирования.

3. Свойство системы, в которой циркулирует информация, характеризующееся способностью обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

5. Что понимается под термином «Политика безопасности»?

1. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности.

2. Это формальное изложение правил, которым должны подчиняться лица, получающие доступ к корпоративной технологии и обработки информации.

3. Это защита информации с помощью организационных мер.

Тема 2. Нормативно-правовое обеспечение кибербезопасности

1. Носителями сведений, составляющих государственную тайну, являются:

1. Материальные объекты, в том числе физические поля, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

2. Текстовые и графические материалы, выполненные любым способом, кино-, фото-, фонематериалы и другие материальные объекты, содержащие информацию, отнесенную к государственной тайне.

3. Материальные объекты, в которых сведения, составляющие государственную тайну, находят свое отображение в виде символов, образов, сигналов, технических решений и процессов.

2. Система защиты государственной тайны в РФ это:

1. Комплекс мероприятий, проводимых государством, по созданию условий, ограничивающих распространение и исключающих несанкционированный, незаконный доступ к засекреченной информации и ее носителям.

2. Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну, и их носителей, а также мероприятий, проводимых в этих целях.

3. Система, определяющая порядок доступа в служебных целях конкретных сотрудников к определенной защищаемой информации и в конкретные помещения, где ведутся конфиденциальные или секретные работы.

3. Обеспечение информационной безопасности государства это:

1. Государственные органы, а также подразделения и должностные лица государственных органов, органов местного самоуправления и организаций, уполномоченные на решение в соответствии с законодательством Российской Федерации задач по обеспечению информационной безопасности.

2. Совокупность сил обеспечения информационной безопасности, осуществляющих скоординированную и спланированную деятельность, и используемых ими средств обеспечения информационной безопасности.

3. Осуществление взаимоувязанных правовых, организационных, оперативно-розыскных, разведывательных, контрразведывательных, научно-технических, информационно-аналитических, кадровых, экономических и иных мер по прогнозированию, обнаруже-

нию, сдерживанию, предотвращению, отражению информационных угроз и ликвидации последствий их проявления.

4. В особом порядке допускаются к государственной тайне (на период исполнения ими своих полномочий):

1. Депутаты Государственной Думы, члены Совета Федерации, судьи, адвокаты, военнослужащие специальных подразделений, ученые.

2. Депутаты Государственной Думы, члены Совета Федерации, судьи, адвокаты.

3. Депутаты Государственной Думы, судьи, адвокаты.

5. Вопросами лицензирования и сертификации технических средств защиты информации занимается:

1. Министерство Обороны Российской Федерации.

2. Роспотребнадзор.

3. ФСТЭК России.

Тема 3. Принципы обеспечения компьютерной безопасности

1. При получении спама на электронную почту с приложенным файлом, какие следует выполнить действия?

1. Прочитать приложение, если оно не содержит ничего ценного — удалить.

2. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама.

3. Удалить письмо с приложением, не раскрывая (не читая) его.

2. Какие наиболее распространённые средства воздействия на локальные сети?

1. Слабый трафик, информационный обман, вирусы в сети «Интернет».

2. Вирусы в сетях передачи данных, логические мины (закладки), информационный перехват.

3. Компьютерные сбои, изменение администрирования, топологии.

3. Какое вредоносное программное обеспечение активизируется после включения операционной системы?

1. Снифферы.

2. Загрузочное.

3. Троянские вирусы, черви.

4. Для чего служит фильтрация контента?

1. Защищает от скрытой загрузки вредоносного программного обеспечения.

2. Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени.

3. Отключает назойливую рекламу и спам.

5. Что такое Brute Force?

1. Взлом методом заражения системы через вредоносный файл.

2. Получение конфиденциальной информации с компьютера методом электронной рассылки.

3. Взлом методом перебора паролей.

Тема 4. Источники и каналы утечки информации. Основы технической защиты информации

1. К техническим каналам утечки информации следует отнести:

1. Оптические; радиоэлектронные; акустические; материально-вещественные.

2. Любые физические поля способные передавать сигналы и волны.

3. Линии электропередачи, оптические световоды, атмосфера.

2. Утечка информации по техническому каналу это -:

1. Бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена;

2. Неконтролируемое распространение информации от носителя защищаемой информации через физическую среду до технического средства, осуществляющего перехват информации;

3. Распространение информации от носителя информации через физическую среду до технического средства, осуществляющего перехват информации.

3. К техническим каналам утечки информации не относится:

1. Материально-вещественный канал.

2. Визуально-оптический канал.

3. Электромагнитный канал.

4. Электронно-вычислительный канал.

4. Информационно-техническая экспертиза назначается для:

1. Определения технического состояния компьютерного оборудования и пригодности его для решения задач, предусмотренных проектной и эксплуатационной документацией на данную автоматизированную систему.

2. Исследования технического состояния компьютерного оборудования и его пригодность для решения в полном объеме задач, предусмотренных проектной и эксплуатационной документацией на данную компьютерную систему или сеть.

3. Специального исследования непосредственно технической части: отдельных узлов, блоков, периферийных устройств, оборудования, составляющих компьютерные системы или сети, пластиковых карт, дисков, дискет, других носителей информации, обрабатываемых компьютерами, а также программных средств.

5. Объектом информационно-технологической экспертизы является:

1. Проектная документация на разработку и эксплуатацию компьютерных систем и сетей, отражающая процессы сбора, обработки, накопления, хранения, поиска и распространения информации.

2. Установленный порядок обработки информации, осуществляемый по заданным алгоритмам, или информационная технология, основанная на применении современной информационно-вычислительной техники, средств связи и телекоммуникаций, составляющих основу информатизации общества.

3. Схемы движения информации от источников к потребителю с указанием пунктов ее сбора, контроля, накопления, обработки и использования.

Тема 5. Основы криптографической защиты информации

1. Что означает термин криптография?

1. Это метод специального преобразования информации в целях сокрытия от посторонних лиц.

2. Это преобразование информации в виде условных сигналов в целях автоматизации ее хранения, обработки, передачи и ввода-вывода.

3. Это криптографическое преобразование информации при ее передаче по каналам связи от одного элемента информационной сети к другому.

4. Это преобразования информации, скрывающие сам факт ее передачи по открытым каналам связи.

2. Шифрование это:

1. Совокупность тем или иным способом структурированных данных и комплексом аппаратно-программных средств.

2. Преобразовательный процесс: исходный текст, который носит также название открытого текста, заменяется шифрованным текстом.

3. Альтернативная среда для вычисления конечного пользователя.

3. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования:

1. 1.

2. 2.

3. 3.

4. Криптостойкость это:

1. Алгоритм аналитических преобразований.

2. Характеристика шифра, определяющая его стойкость к дешифрованию без знания ключа.

3. Упорядоченный набор из элементов алфавита.

4. Нет правильного ответа.

5. Что понимается под понятием «ключ криптографической системы»?

1. Ключ — информация, необходимая для беспрепятственного шифрования и дешифрования текстов.

2. Ключ — совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных.

3. Ключ — техническое устройство для обеспечения недоступности к информации в автоматизированных информационных системах.

4. Ключ — техническое устройство для скрытия смысла (семантики) передаваемого по коммуникационным каналам сообщения.

Тема 6. Реагирование на инциденты кибербезопасности и их обработка

1. Что такое APT-атака (Advanced persistent threat)?

1. Перехват всех сетевых пакетов прикладной программой, которые передаются через определённый домен.

2. Сложная, продолжительная, хорошо спланированная атака, использующая сложное вредоносное ПО, методы социальной инженерии и данные об информационной структуре атакуемого.

3. Целенаправленная кибератака по заражению вредоносным ПО веб-сайтов, часто посещаемых их потенциальными жертвами.

2. Для чего используются SIEM (Security information and event management) системы?

1. Для анализа событий информационной безопасности, исходящих от сетевых устройств и приложений в реальном времени.

2. Для поиска в открытых источниках необходимой информации, в том числе индикаторов компрометации, отчётов по конкретным угрозам и другой информации, которая может способствовать расследованию инцидента ИБ.

3. Для атаки, нацеленной на одного человека, компанию или группу людей.

3. Какие тенденции прослеживаются в распространении киберугроз (что встречается всё чаще)?

1. Реализация внутренних угроз (внутренний нарушитель, утечка данных).

2. Использование методов социальной инженерии.

3. Использование уязвимостей в бизнес-процессах.

4. Какие данные требуются для анализа инцидента безопасности?

1. Только системные файлы.

2. Полный образ диска включая неиспользованные области.

3. Только файлы пользователя.

5. Что такое C&C?

1. Вредоносная программа, похищающая деньги с банковских счетов.

2. Центр управления вредоносной бот-сетью.

3. Название мошеннической группировки, специализирующейся на хищении средств с банковских счетов.

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ВОПРОСОВ ДЛЯ ПОДГОТОВКИ К ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ (ЗАЧЁТУ)

1. Кибербезопасность как новое информационно-техническое направление системной защиты государства, общества, человека.
2. Базовые понятия и определения кибербезопасности.
3. Принципы обеспечения кибербезопасности.
4. Кибербезопасность: современные киберугрозы.
5. Методы совершения киберпреступлений.
6. Уязвимости интернета вещей.
7. Центры мониторинга и управления безопасностью как составляющие системы борьбы с киберпреступлениями.
8. Группы ролей специалистов в центрах управления событиями кибербезопасности.
9. Понятие Критической информационной инфраструктуры (КИИ).
10. Функционирование информационных систем МВД России в условиях деструктивных кибервоздействий.
11. Задача нормативно-правового регулирования обеспечения кибербезопасности в Российской Федерации как компонент государственной политики развития национального сектора применения информационных технологий.
12. Законодательство Российской Федерации в области защиты информации.
13. Деятельность МВД России в области обеспечения кибербезопасности.
14. Внутренние и внешние источники угроз кибербезопасности.
15. Система подготовки кадров в области борьбы с киберпреступностью.
16. Функции и органы МВД России по обеспечению кибербезопасности государства, общества, личности.
17. Международные стандарты в области обеспечения кибербезопасности.
18. Роль и место ФСТЭК России в вопросах обеспечения кибербезопасности.

19. Административные правонарушения в области кибербезопасности.

20. Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы (ГосСОПКА).

21. Уголовно-правовая характеристика преступлений в сфере кибербезопасности.

22. Принципы обеспечения безопасности устройств на базе операционных систем семейства Windows.

23. Базовая архитектура и файловые системы Windows.

24. Типы файловых систем в Linux.

25. Принципы обеспечения безопасности устройств на базе операционных систем семейства Linux.

26. Классификация киберугроз компьютерной безопасности.

27. Особенности реализации сетевых кибератак.

28. Кибератаки на основе методов социальной инженерии.

29. Кибератаки на мобильные устройства.

30. Международный подход к выявлению и анализу уязвимостей, базы данных уязвимостей.

31. Операционная система специального назначения Astra Linux.

32. Основные способы защиты от вредоносного программного обеспечения.

33. Особенности подсистем обеспечения безопасности и журналирования в операционных системах Windows, Linux.

34. Управление рисками.

35. Обеспечение кибербезопасности оконечных устройств (сетевые камеры видеонаблюдения, сетевые контроллеры, компьютеры, серверы, ноутбуки, смартфоны).

36. Понятие о технических каналах утечки информации: состав и характеристики.

37. Оптические, радиоэлектронные, акустические, материально-вещественные каналы утечки информации.

38. Основные и вспомогательные технические средства, и системы.

39. Технические каналы утечки информации при ее передаче по каналам связи.

40. Технические каналы утечки акустической информации: воздушные, вибрационные, параметрические, электроакустические, оптико-электронные.

41. Технические каналы утечки информации, обрабатываемой основными техническими средствами и системами.

42. Побочные электромагнитные излучения (ПЭМИ).

43. Перехват излучений на частотах работы ВЧ-генераторов.

44. Технические каналы утечки видеоинформации.

45. Аттестации объектов информатизации на соответствие требованиям о защите информации.

46. Средства обнаружения каналов утечки информации.

47. Роль криптографии в глобальной задаче защиты коммуникаций.

48. Криптология, криптография, криптоанализ.

49. Алгоритмы симметричного и ассиметричного шифрования.

50. Исторические примеры шифрования: шифр Сциталя, Квадрат Полибия, шифр Цезаря, шифр Виженера, Enigma Machine.

51. Криптографические хэш-функции.

52. Эволюция криптографической деятельности до XX века.

53. Периоды становления криптографии в XX веке.

54. Стеганография и развитие ее возможностей.

55. Понятие об инструментах открытого программного обеспечения OpenSSL.

56. Электронная подпись

57. Инфраструктура и управление общими ключами.

58. Алгоритм совершения киберпреступления.

59. Основные этапы процесса реагирования на инциденты кибербезопасности.

60. Выявление и фиксация следов киберпреступления.

61. Распространенные виды инцидентов кибербезопасности.

62. Особенности реагирования на сетевые кибератаки.

РЕКОМЕНДАЦИИ СЛУШАТЕЛЯМ ФАКУЛЬТЕТА ЗАОЧНОГО ОБУЧЕНИЯ ПО ИЗУЧЕНИЮ ДИСЦИПЛИНЫ «ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ»

Учебная дисциплина «Основы кибербезопасности» изучается на всех специальностях и направлениях подготовки высшего образования, реализуемых университетом по заочной форме обучения. Такая форма обучения сочетает в себе как черты самостоятельной подготовки, так и свойства очного обучения и характеризуется определенной этапностью. На первом этапе обучающийся в ходе установочной сессии осваивает базовые знания, умения, компетенции путем изучения учебно-методической литературы и иных информационных ресурсов; на втором этапе ведущим преподавателем проводится проверка освоенного обучающимся учебного материала. При заочной форме обучения изучение учебной дисциплины «Основы кибербезопасности» предусматривает учебные занятия в виде лекций или практических занятий.

Лекция — основная форма систематического устного изложения учебного материала, проводимого наиболее профессионально подготовленными научно-педагогическими работниками кафедры информационной безопасности. В условиях заочной формы обучения практикуется чтение только установочных лекций, цель которых состоит не в исчерпывающей передаче научной информации по дисциплине «Основы кибербезопасности», а лишь в изложении ряда наиболее важных положений данной науки. Основные задачи установочных лекций: ознакомление слушателей со структурой изучаемой дисциплины и ее связи с сопредельными науками, краткое изложение комплекса основных научных категорий, терминов и понятий данной дисциплины, краткое изложение наиболее принципиальных базовых положений, раскрытие особенно сложных для понимания вопросов, освещение дискуссионных проблем, определение перспектив и актуальных направлений дальнейшего развития научного знания в данной области общественной жизни.

Установочные лекции нацеливают слушателя на самостоятельный поиск и изучение научной литературы, ориентируют на выявле-

ние и изучение наиболее актуальных и проблемных вопросов, на активизацию творческого начала в освоении учебной дисциплины «Основы кибербезопасности».

Немаловажным фактором полноценной работы слушателя на установочной лекции является культура ведения конспекта лекции. Принципиально неверным является отношение к лекции как к «диктанту», который должен быть лишь аккуратно и дословно записан. Надо научиться вычленять ключевые моменты в лекции, наиболее важные формулы и технические схемы записывая их более полно и выделяя каким-либо способом из общего текста. Следует четко фиксировать рубрикацию материала: разграничение вопросов и соответствующих под вопросов. Обязательно нужно делать специальные пометки, если какое-либо положение осталось непонятым, сомнительным, либо просто не успели его записать, чтобы не забыть, потом восполнить этот пробел, обратившись за консультацией к ведущему преподавателю или к нормативным правовым актам, учебной или научной литературе.

Полезно выработать свою систему сокращений и условных обозначений. Например, «технический канал утечки информации» — сокращенно *ТКУИ*, «побочные электромагнитные излучения и наводки» — *ПЭМИН*. Это значительно ускорит процесс записи текста, снизит напряжение и опасение «не успеть» записать все необходимое. Не следует писать конспект на случайных листках, которые потом могут затеряться либо трудно будет скомплектовать их в единый конспект. Тогда восприятие установочной лекции будет более полноценным и не сведется к механической записи текста. Рекомендуется в конспекте предусмотреть место для последующих дополнительных записей и формул, оставляя незаполненной либо оборотную сторону листа, либо разделить страницу по вертикали пополам и использовать для конспекта только одну половину страницы.

Качественный конспект установочных лекций поможет слушателям факультета заочного обучения в процессе самостоятельной работы и при сдаче итогового зачёта.

При заочной форме обучения рекомендуется большую часть учебного времени посвящать самостоятельной работе. Этот метод обучения способствует творческому овладению специальными знаниями, навыками и компетенциями. В процессе самостоятельной работы слушатель должен воспринимать, осмысливать и углублять получаемую информацию, решать практические задачи, овладевать профессионально необходимыми навыками.

Самостоятельная работа слушателя весьма многообразна и содержательна. Она включает следующие виды занятий:

— самостоятельный подбор, изучение, конспектирование, анализ учебной, учебно-методической и научной литературы, периодических научных изданий, нормативно-правовых документов, числовой информации, содержащейся в публикуемых источниках с техническим уклоном;

— индивидуальная творческая работа по осмыслению собранной информации, проведению сравнительного анализа и обобщению материалов, полученных по разным направлениям и формулировка выводов и рекомендаций;

— завершающий этап самостоятельной работы — подготовка к сдаче итогового зачета, предполагающая интеграцию и систематизацию всей совокупности полученных знаний по дисциплине «Основы кибербезопасности».

Важный элемент специфики заочной формы обучения — отсутствие постоянных непосредственных контактов слушателей с ведущим преподавателем в межсессионный период. В этих условиях на первый план выходит роль самоорганизации и самодисциплины слушателя. Повышается также значимость тех ограниченных прямых контактов с преподавателем, которые имеют форму установочных аудиторных занятий. Осознавая это, слушатель должен стремиться с максимальной эффективностью использовать все возможности получения доводимой информации непосредственно от преподавателя.

Слушатели факультета заочного обучения должны помнить, что очная и заочная формы обучения осуществляются по единым программам при единых требованиях к объему и качеству знаний по

всем дисциплинам. При единстве конечного результата образовательного процесса, методы и способы овладения знаниями дифференцированы по очной и заочной форме обучения, поэтому очень важно обрести навыки самостоятельной учебной работы.

Успешное достижение целей самостоятельной работы каждого слушателя в значительной степени определяется его личными качествами, уровнем подготовки, а также настойчивостью и целеустремленностью. Эффективность во многом зависит от органического единства форм, методов и содержания аудиторной и внеаудиторной самостоятельной работы слушателя, от того, насколько качественно он владеет методикой и техникой самостоятельного поиска и добывания знаний, навыками творческого решения вопросов. При поиске литературы рекомендуется, в первую очередь, обратить внимание на ту, которую предлагает ведущий преподаватель. Приоритетом пользуются учебные и учебно-методические пособия, изданные кафедрой информационной безопасности университета. Кроме этого необходимо обратить внимание на источники из электронных библиотечных систем, среди них:

1. Электронно-библиотечная система «Университетская библиотека онлайн»: URL: https://biblioclub.ru/

2. Научная электронная библиотека: URL: http://elibrary.ru

3. Информационный ресурс ФГБУ «Президентская библиотека имени Б.Н. Ельцина»: URL: http://prilab.ru

4. Электронная библиотека: URL:http://cyberleninka.ru.

Нормативные правовые акты можно посмотреть в современных базах данных и информационно-справочных системах, таких как:

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

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

3. Специализированная территориально распределенная автоматизированная система СТРАС «Юрист»: URL: http://www.stras-yrist.ru/

Кроме того, обязательны к изучению ресурсы информационно-телекоммуникационной сети «Интернет», использование которых рекомендовано при изучении дисциплины «Основы кибербезопасности»:

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

2. Официальный сайт Министерства внутренних дел Российской Федерации: URL:http://www.mvd.ru

3. Сайт с материалами об обеспечении информационной безопасности: URL: http://www.securitylab.ru

Заканчивается изучение дисциплины на итоговой сессии за учебный курс сдачей зачета без оценки (не дифференцированного). На зачете при оценке теоретических знаний, навыков и умений (владений) слушателей учитываются также их текущая успеваемость по дисциплине, результаты работы на практических занятиях. В случае необходимости ведущий преподаватель может задавать обучающемуся дополнительные вопросы по разделам (темам) дисциплины, по которым его знания вызывают сомнения (с учетом результатов текущей успеваемости и посещаемости занятий).

ЗАКЛЮЧЕНИЕ

Предложенные в учебно-методическом пособии методические рекомендации по подготовке к семинарским и практическим занятиям, примерный перечень контрольных вопросов текущей аттестации, примерный перечень вопросов для подготовки к промежуточной аттестации (зачету), рекомендации слушателям факультета заочного обучения служат необходимым условием для качественного освоения учебной дисциплины «Основы кибербезопасности».

Ввиду того что в целом кибербезопасность заявлена в области естественных наук, имея соответствующую фундаментальность, она не может оставаться изолированной и должна как открывать новые возможности и методы решения практических задач, так и осуществлять определенную преемственность в историческом плане. В частности, давать понимание современных тенденций, разъяснять устоявшиеся базовые концепции, востребованность изысканий в том числе усложняющуюся картину киберпреступности.

Знание институциональных основ кибербезопасности раскрывает для обучающихся возможности проявления профессиональных навыков в учебной деятельности, а в дальнейшем в профессиональной.

Использование данного учебно-методического пособия в образовательном процессе позволит развивать у курсантов и слушателей самоконтроль, самооценку, на должном уровне подготовиться к сдаче зачета по учебной дисциплине «Основы кибербезопасности».

СПИСОК РЕКОМЕНДУЕМЫХ ИСТОЧНИКОВ

Нормативные правовые акты:

1. *Конституция* Российской Федерации (принята всенародным голосованием 12 дек. 1993 г. с изменениями, одобренными в ходе общероссийского голосования 1 июля 2020 г.) // Российская газета. — 1993. — 25 дек.

2. *Федеральный* закон от 7 февраля 2011 г. № 3-ФЗ «О полиции» // Российская газета. — 2011. — 8 февр.

3. *Федеральный* закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации // Собрание законодательства Российской Федерации. — 2006. — 31 июля. — № 31 (Ч. I). — Ст. 3448.

4. *Федеральный* закон от 28 декабря 2010 г. № 390-ФЗ «О безопасности» // Собрание законодательства Российской Федерации. —2011. —3 янв. — № 1. — Ст. 2.

5. *Федеральный* закон от 7 июля 2003 г. № 126-ФЗ «О связи» // Российская газета. — 2003. — 10 июля.

6. *Федеральный* закон от 26 июля 2017 г. №187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // Собрание законодательства Российской Федерации. — 2017. — 2006. — 31 июля. — № 31 (Ч. I). — Ст. 4736.

7. *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“» // Российская газета. — 2017. — 31 июля.

8. *Закон* Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне» // Российская газета. — 1993. — 21 сент.

9. *Доктрина* информационной безопасности Российской Федерации : утверждена Указом Президента Российской Федерации 5 декабря 2016 г. № 646. Доступ из справочно-правовой системы «Гарант».

10. *Приказ* ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Рос-

сийской Федерации» (в ред. приказов ФСТЭК России от 9 августа 2018 г. № 138, от 26 марта 2019 г. № 60, от 20 февраля 2020 г. № 35). — URL: https://fstec.ru/en/53- normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239.

Основная литература:

1. *Основы* информационной безопасности в органах внутренних дел : учебник. — Санкт-Петербург : Изд-во СПб ун-та МВД России, 2019. — 312 с.

2. *Средства* и системы обработки информации : учебное пособие / А. И. Локнов, Ю. И. Синещук, В. Н. Родин. — Санкт-Петербург : СПБУ МВД России, 2023. — 124 с.

3. *Системы* и сети передачи информации : учебно-методическое пособие / А. И. Локнов, И. Н. Васильева. — Санкт-Петербург : СПБУ МВД России, 2023. — 72 с.

4. *Основы* защищенного электронного документооборота в органах внутренних дел : учебное пособие / науч. ред. : Ю. И. Синещук, А. И. Локнов. — Санкт-Петербург : Изд-во СПб ун-та МВД России, 2022. — 76 с.

5. *Компьютерные* сети. Принципы, технологии, протоколы : учебное пособие / В. Олифер, Н. Олифер. — Санкт-Петербург ; Москва ; Екатеринбург : Питер, 2021. — 1005 с.

Дополнительная литература:

1. *Основ*ы информационной безопасности в органах внутренних дел : учебное пособие / О. Г. Смирнова, И. Н. Васильева. — Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. —148 с.

2. *Основы* информационной безопасности в органах внутренних дел: учебное пособие / М. Г. Гизатуллин, И. Ф. Файсханов. — Екатеринбург : Уральский юридический институт МВД России, 2020. — 51 с.

3. *Криптографическая* защита информации : учебное пособие / И. Н. Васильева, В. И. Куватов, В. С. Потехин. — Санкт-Петербург : Изд-во СПб ун-та МВД России, 2016. — 151 с.

4. *Криптографическая* защита информации : практикум / И. Н. Васильева, В. И. Куватов. — Санкт-Петербург : Изд-во СПб ун-та МВД России, 2017. — 260 с.

5. *Организация* и обеспечение безопасности информационно-технологических сетей и систем: учебник для вузов / Д. А. Мельников. — Москва : Университетская книга, 2013. — 598 с.

6. *Основы* информационной безопасности : учебное пособие / В. Н. Галатенко. — 4-е изд. — Москва : Бином, 2008. — 206 с.

7. *Защита* информации в персональном компьютере : учебное пособие/ Н. З. Емельянова. — Москва : Форум, 2009. — 368 с.

Для заметок

Для заметок

Для заметок

Учебное издание

Локнов Алексей Игоревич,
кандидат технических наук, доцент

ОСНОВЫ КИБЕРБЕЗОПАСНОСТИ

Учебно-методическое пособие

Редактор *Великих А. Н.*
Компьютерная вёрстка *Душкова А. Ю.*
Дизайн обложки *Шеряй А. Н.*

ISBN 978-5-91837-824-3

EDN: ZDRBAZ

Подписано в печать 03.05.2024. Формат 60x84 1/8
Печать цифровая. Объем 4,0 п. л. Заказ № 19/24
Тираж 200 экз. 1-й завод 1–100 экз.

Отпечатано в Санкт-Петербургском университете МВД России
198206, Санкт-Петербург, ул. Летчика Пилютова, д. 1