**МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ**

**МОСКОВСКИЙ УНИВЕРСИТЕТ имени В.Я. КИКОТЯ**

**МОСКОВСКИЙ ОБЛАСТНОЙ ФИЛИАЛ**

**Кафедра административного права и оперативно-разыскной деятельности ОВД**

УТВЕРЖДАЮ

Заместитель начальника филиала по учебной и научной работе - начальник учебного отдела

полковник полиции

 Г.Н. Жогов

 «\_\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_\_ 2015 г.

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ**

тематика домашних контрольных работ

и методические рекомендации по их написанию

для слушателей заочной формы обучения

по специальности 40.05.02 – Правоохранительная деятельность (юрист)

Начальник кафедры административного права и оперативно-разыскной деятельности ОВД

подполковник полиции

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.В. Абрамочкин

*Обсуждена и одобрена на заседании кафедры протокол № \_\_
от «\_\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2015 г.*

РУЗА

2015

**Основы информационной безопасности в органах внутренних дел:** Тематика (задания) домашних контрольных работ и методические рекомендации по их написанию для заочной формы обучения по специальности 40.05.02 – Правоохранительная деятельность (юрист). – Руза: Московский областной филиал МосУ МВД России имени В.Я. Кикотя. 2015. – 10 с.

Подготовлены: старшим преподавателем кафедры административного права и оперативно-разыскной деятельности ОВД подполковником полиции Темнышовым А.А.

Обсуждена и одобрена:

на заседании кафедры административного права и оперативно-разыскной деятельности ОВД протокол № «\_\_» от «\_\_» \_\_\_\_\_\_\_\_\_\_\_ 2015 г.

на заседании Методического совета Московского областного филиала МосУ МВД России имени В.Я. Кикотя

протокол №\_\_\_\_ от «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_20\_г.

Аннотация: Тематика домашних контрольных работ и методические рекомендации по их написанию по дисциплине «Основы информационной безопасности в органах внутренних дел» подготовлены в соответствии с Федеральными государственными образовательными стандартами высшего профессионального образования по специальности 40.05.02 – Правоохранительная деятельность (юрист). Включает в себя методические рекомендации по выполнению контрольных работ, образец титульного листа, перечень вариантов контрольных работ и список рекомендованной литературы.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ВЫПОЛНЕНИЮ
КОНТРОЛЬНЫХ РАБОТ**

Преподавание в Московском областном филиале Московского университета МВД России имени В.Я. Кикотя дисциплины «Основы информационной безопасности в ОВД» ставит своей целью предоставление слушателям комплекса необходимых теоретических знаний и практических навыков.

В соответствии с учебным планом слушатели заочной формы обучения должны выполнить контрольную работу по курсу «Основы информационной безопасности в ОВД»*.*

Выполнение контрольной работы заключается в выполнении индивидуального задания по одному из вариантов, предлагаемых кафедрой.

**Выбор варианта контрольной работы осуществляется последней цифре номера зачетной книжки.**

Решение контрольной работы должно быть полным и четким. Выводы слушателя по выполнению задания необходимо аргументировать ссылками на статьи законов, действующих ко времени написания контрольной работы.

Слушатели должны ориентироваться в вопросах правового обеспечения информационных технологий, в нормах информационного права.

Выполнение контрольной работы необходимо для уяснения теоретических положений курса и выработки умений и навыков в применении правовых норм информатики.

**Контрольная работа выполняется с обязательным учетом всех требований, предъявляемых к работам подобного рода:**

1. Контрольная работа должна содержать:

* введение,
* рассматриваемые вопросы,
* заключение
* список использованной литературы и источников.
* 2. Работа должна быть написана разборчивым почерком или напечатана, страницы пронумерованы; левое поле – 30 мм, остальные – 20 мм; межстрочный интервал – полуторный, шрифт – Times New Roman, размер шрифта – 13-14 пт.
* 3. Ксерокопии работ запрещены.
* 4. Рассмотрение вопросов должно быть четким и полным. Свои выводы необходимо аргументировать ссылками на конкретные нормативные акты с указанием, какая работа или часть ее используется для ответа на вопрос.
* 5. При оформлении контрольной работы следует подготовить титульный лист с указанием названия кафедры, номера варианта, своей фамилии и инициалов, номера учебной группы и номера зачетной книжки.
* 6. Работа должна быть написана аккуратно: без ошибок, помарок, исправлений, сокращений.
* 7. Рассмотрение вопроса должно начинаться с новой страницы, с указанием номера вопроса. При использовании монографических материалов следует делать сноски с указанием источника, откуда взята соответствующая цитата, место и год издания источника.
* 8. По завершению контрольная работа подписывается автором, ставится дата ее окончания, регистрируется на кафедре и сдается на проверку.
* 9. Титульный лист оформляется в соответствии с образцом (см. рис. 1)

**В случае невыполнения вышеуказанных требований контрольная работа оценивается как неудовлетворительная и отправляется на доработку.**

|  |  |
| --- | --- |
|  | Министерство внутренних дел РоссииМосковский областной филиалМосковского университета МВД России имени В.Я. КикотяЗаочное отделение143100 г. Руза п. Старотеряево Кафедра административного права и оперативно-разыскной деятельности ОВД |
| Адрес места жительства:Индекс\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Обл.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Город \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Ул.\_\_\_\_\_\_\_\_\_ Дом №\_\_\_\_\_Корп. №\_\_\_\_\_ Кв. №\_\_\_\_\_\_ тел. служ.\_\_\_\_\_\_\_\_\_\_\_тел. дом.\_\_\_\_\_\_\_\_\_\_ | Ф.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_И.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_О.\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Курс\_\_\_\_\_\_(набор)\_\_200\_\_\_\_\_\_года\_\_\_№ группы\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_№ зачетной книжки\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Контрольная работа по дисциплине «Основы информационной безопасности в ОВД»Тема (№ варианта) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |
| Дата получения работы секретариатом \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Дата сдачи работы в секретариат \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | Дата получения работы кафедрой \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Дата окончания проверки работы \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ |

Руза 2016

Рис. 1. Образец оформления титульного листа

**Тематика контрольных работ**Номер варианта выбирается по последней цифре номера зачетной книжки.

Вариант 1

1. Уязвимость компьютерных систем. Понятие несанкционированного доступа (НСД). Классы и виды НСД.
2. Сравнительный анализ методов воздействия и противодействия в сети Internet.
3. Вирусы как особый класс разрушающих программных воздействий. Защита от разрушающих программных воздействий.

Вариант 2

1. Несанкционированное копирование программ как тип несанкционированного доступа. Юридические аспекты несанкционированного копирования программ. Способы защиты от копирования.
2. «Типовые» каналы утечки информации объектов информатизации ОВД. Условия и факторы, способствующие утечке информации ограниченного доступа.
3. Понятие атрибутов доступа к файлам. Защита сетевого файлового ресурса на примерах организации доступа в различных операционных системах.

Вариант 3

1. Направления по защите от враждебных воздействий на безопасность сетей.
2. Распространённые способы блокирования каналов утечки информации и виды специальных технических средств защиты.
3. Актуальность обеспечения информационной безопасности органов внутренних дел. Обеспечение информационной безопасности как составляющая информационного противоборства организованной преступности.

Вариант 4

1. Понятие и виды каналов утечки информации ограниченного доступа. «Типовые» каналы утечки информации объектов информатизации ОВД.
2. Способы фиксации фактов доступа. Журналы доступа. Выявление следов несанкционированного доступа к файлам.
3. Особенности построения защиты информации в телекоммуникационных сетях. Современные технические и программные средства сетевой защиты компьютерной информации.

Вариант 5

1. Уязвимость компьютерных систем. Модель злоумышленника.
2. Необходимые и достаточные условия предотвращения разрушающего воздействия вируса.
3. Сведения об оперативно-розыскной деятельности, подлежащие засекречиванию в системе органов внутренних дел.

Вариант 6

1. Основные составляющие национальных интересов в информационной сфере; виды и источники угроз информационной безопасности страны (на примере России).
2. Правовые основы защиты оперативно-розыскной информации как реализованной функции по добыванию, обработке и использованию данных и сведений.
3. Методы и средства защиты данных от несанкционированного доступа.

Вариант 7

1. Основные угрозы безопасности информации. Общая характеристика технических средств несанкционированного получения информации и технологий их применения.
2. Важнейшие составляющие интересов в информационной сфере и основные угрозы информационной безопасности органов внутренних дел.
3. Понятие информации, информационной сферы, безопасности информации и информационной безопасности субъекта.

Вариант 8

1. Правовая защита сотрудников оперативных подразделений органов внутренних дел от негативных информационно-психологических воздействий.
2. Понятие «идентификации пользователя». Задача идентификации пользователя. Использование идентификации в защите информационных процессов.
3. Угрозы безопасности современных информационно-вычислительных и телекоммуникационных сетей. Классификация угроз безопасности.

Вариант 9

1. Информационная сфера и информационная безопасность органов внутренних дел.
2. Основные направления инженерно-технической защиты информации: физическая защита, скрытие информации, поиск и нейтрализация источников утечки.
3. Методы и средства воздействия на безопасность сетей.

Вариант 10

1. Основные угрозы информационной безопасности, возникающие в процессе деятельности оперативных подразделений органов внутренних дел.
2. Понятие и цели проведения специальных проверок объектов информатизации; основные этапы проведения проверки.
3. Аппаратные и программно-аппаратные средства криптозащиты данных.

**Список рекомендованной литературы**

**Основная литература:**

1. Организация защиты информации в органах внутренних дел: учебное пособие. Ч. II / С.И. Козьминых. – М.: Московский университе МВД России, 2013. – 148 с.
2. Системы защиты информации в ведущих зарубежных странах: учебное пособие: в 2 ч. / К.К. Борзунов; А.С. Овчинский; Н.И. Журавленко; В.Е. Кадулин / под общей ред. А.С. Овчинского. – М.: Московский университет МВД России, 2013. Ч. 1. – 161 с.
3. В. В. Трофимов. Информационные технологии: учебник. Юрайт, 2011.
4. А.В. Бабаш, Е.К. Баранова, Д.А. Ларин. Информационная безопасность. История защиты информации в России. - М.: ИД КДУ, 2013.
5. П.Н. Девянин. Модели безопасности компьютерных систем. Управление доступом и информационными потоками: учебное пособие. - М.: Горячая линия–Телеком, 2013.
6. Т.Л. Партыка, И.И. Попов. Информационная безопасность. – М.: Форум, 2012.
7. В.П. Мельников, С.А. Клейменов, А.М. Петраков. Информационная безопасность: учебное пособие. – М.: Академия, 2013.
8. А.А. Бирюков. Информационная безопасность: защита и нападение. – М.: ДМК Пресс, 2012.
9. Жуков Ю. В. Основы веб-хакинга: нападение и защит. – СПб.: Питер, 2012.
10. Аверченков В.И. Аудит информационной безопасности: учебное пособие для вузов. – М.: ФЛИНТА, 2011.
11. Сердюк В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие. // Издательский дом Государственного университета – Высшей школы экономики, 2011
12. Кочерга С.А., Ефимова Л.Л. Информационная безопасность детей. Российский и зарубежный опыт: монография. – М.: Юнити-Дана, 2013.
13. Смирнов А.А. Обеспечение информационной безопасности в условиях виртуализации общества. Опыт Европейского Союза: монография. – М.: ЮНИТИ-ДАНА; Закон и право, 2012.

**Дополнительная литература:**

1. Белов Е.Б, Лось В.П. Основы информационной безопасности. М.: Горячая линя - Телеком, 2006.
2. Белоглазов Е.Г. и др. Основы информационной безопасности органов внутренних дел: Учебное пособие. – М.: МосУ МВД России, 2005.
3. Н.И.Журавленко, В.Е.Кадулин, К.К.Борзунов. Основы информационной безопасности: Учебное пособие. – М.: МосУ МВД России. 2007.
4. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. – М.: Академи­че­ский Проект; Гаудеамус, 2007.
5. Э. Бот, К. Зихерт. Безопасность Windows. – СПб.: Питер, 2006.
6. Прохода А.Н. Обеспечение интернет-безопасности. Практикум: Учебное пособие для вузов. – М.: Горячая линия–Телеком, 2007.
7. Торокин А.А. Инженерно-техническая защита информации: Учебное пособие. – М.: «Гелиос АРВ», 2005.
8. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности - Учебное пособие для ВУЗов - - 2006
9. Гатчин Ю.А., Климова Е.В. Основы информационной безопасности: Учебное пособие. - СПб: СПбГУ ИТМО, 2009
10. Овчинский А.С. Информационные воздействия и организованная преступность. Курс лекций. – М.: ИНФРА-М, 2007.
11. Информационная безопасность органов внутренних дел в борьбе с орга­низованной преступностью / Учебное пособие. Под ред. А.С. Овчин­ско­го. – М.: МИ МВД России, 2001.
12. Никифоров С.В. Введение в сетевые технологии. – М.: Финансы и статистика, 2005.
13. Мандиа К. Защита от вторжений. Расследование компьютерных преступлений. – СПб.: Лори, 2005.
14. Яковец Е.Н. Проблемы аналитической работы в оперативно-розыск­ной деятельности органов внутренних дел: Монография. – М.: Издательский дом Шумиловой И.И., 2005.