

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Шевелева Светлана Викторовна

Должность: декан ЮФ

Дата подписания: 06.02.2023 16:07:13

Уникальный программный ключ:

d30abf10bb7ea878d1188b1c003d300307761db43e1a290e1f3aa14b

Аннотация к рабочей программе дисциплины

«Противодействие посягательствам в уголовно-исполнительной

системе, совершаемых при помощи информационно-

телекоммуникационных сетей»

ОПОП ВО 40.05.02 Правоохранительная деятельность

направленность (профиль) «Обеспечение безопасности в уголовно-

исполнительной системе»

Цель преподавания дисциплины: подготовить выпускника, способного осуществлять деятельность, требующую углубленной фундаментальной и профессиональной подготовки, в том числе научно-исследовательскую работу, обладающего глубокими теоретическими знаниями и практическими навыками, касающимися особенностей квалификации преступлений, совершаемых с использованием новых информационных технологий и их криминологической характеристики, способного применять эти знания и навыки в рамках дальнейшей его практической деятельности.

Задачи изучения дисциплины: обучение студента навыкам обоснования и принятия решений, а также совершения действий, связанных с реализацией уголовно-правовых норм в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей; овладение необходимыми для успешной профилактики, предупреждения, выявления, пресечения преступлений, совершаемым при помощи информационно-телекоммуникационных сетей, знаниями норм и правовых институтов; обучение студента самостоятельной работе над нормативными актами, научной и учебной литературой, необходимой для сбора, анализа и оценки информации, имеющей значение для реализации правовых норм в сфере правоохранительной деятельности; формирование навыков проведения

прикладных научных исследований в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей; овладение умением критически анализировать действующее законодательство; обобщать следственную и судебную практику применения законодательства в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей; овладение методикой пополнения и закрепления правовых знаний и умений в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей на практике; сформировать понимание методологических основ и специфики методов, используемых в уголовно-правовой и криминологической теории, а также информационном праве в связи с проблематикой преступлений, совершаемых при помощи информационно-телекоммуникационных сетей.

Компетенции, формируемые в результате освоения дисциплины:

— способен осуществлять мероприятия по выявлению, документированию, пресечению преступлений и правонарушений на территории, где установлены режимные требования, применяет и использует технические средства надзора и контроля за отбыванием осужденными наказания без изоляции от общества (ПК-3);

— способен разрабатывать и реализовывать меры профилактического, воспитательного и иного воздействия в отношении лиц, склонных к совершению правонарушений на территории учреждений уголовно-исполнительной системы (ПК-7);

— способен самостоятельно выявлять причины и условия, способствующие совершению посягательств на права и свободы участников пенитенциарных правоотношений, осуществлять предупреждение соответствующих правонарушений, основываясь на

общепризнанных принципах и нормах международного права и положениях международных правовых актов (ПК-8).

Разделы дисциплины: Понятие и общая характеристика преступлений, связанных с использованием ИТС. Общая характеристика компьютерных преступлений. Неправомерный доступ к компьютерной информации. Создание, использование и распространение вредоносных компьютерных программ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру. Хищения с использованием новых информационных технологий. Преступления против личности, совершаемые с применением информационных технологий. Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий. Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий. Преступления против общественной безопасности, совершаемые с применением информационных технологий. Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС. Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС.

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета

юридического.

(наименование ф-та полностью)

С.В. Шевелева

(подпись, инициалы, фамилия)

«06» июля 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Противодействие посягательствам в уголовно-исполнительной системе,
совершаемых при помощи информационно-телекоммуникационных сетей

(наименование дисциплины)

ОПОП ВО 40.05.02 Правоохранительная деятельность

шифр и наименование направления подготовки (специальности)

специализация «Обеспечение безопасности в уголовно-исполнительной системе»

наименование направленности (профиля, специализации)

форма обучения очная

(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО — специалитет по специальности 40.05.02 Правоохранительная деятельность на основании учебного плана ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе», одобренного Ученым советом университета (протокол № 9 от «25» июня 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе» на заседании кафедры уголовного права протокол № 15 «03» июля 2021 г.

Зав. кафедрой УП



Байбарин А.А.

Разработчик программы

к.ю.н. доцент



Гребеньков А.А.

Согласовано:

/Директор научной библиотеки



Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе» на заседании кафедры уголовного права протокол № ___ «___» _____ 20__ г.

Зав. кафедрой УП

Байбарин А.А.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе» на заседании кафедры уголовного права протокол № ___ «___» _____ 20__ г.

Зав. кафедрой УП

Байбарин А.А.

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Подготовка выпускника, способного осуществлять деятельность, требующую углубленной фундаментальной и профессиональной подготовки, в том числе научно-исследовательскую работу, обладающего глубокими теоретическими знаниями и практическими навыками, касающимися особенностей квалификации преступлений, совершаемых с использованием новых информационных технологий и их криминологической характеристики, способного применять эти знания и навыки в рамках дальнейшей его практической деятельности.

1.2 Задачи дисциплины

— обучение студента навыкам обоснования и принятия решений, а также совершения действий, связанных с реализацией уголовно-правовых норм в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение необходимыми для успешной профилактики, предупреждения, выявления, пресечения преступлений, совершаемым при помощи информационно-телекоммуникационных сетей, знаниями норм и правовых институтов;

— обучение студента самостоятельной работе над нормативными актами, научной и учебной литературой, необходимой для сбора, анализа и оценки информации, имеющей значение для реализации правовых норм в сфере правоохранительной деятельности;

— формирование навыков проведения прикладных научных исследований в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение умением критически анализировать действующее законодательство; обобщать следственную и судебную практику применения законодательства в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение методикой пополнения и закрепления правовых знаний и умений в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей на практике;

— сформировать понимание методологических основ и специфики методов, используемых в уголовно-правовой и криминологической теории, а также информационном праве в связи с проблематикой преступлений, совершаемых при помощи информационно-телекоммуникационных сетей.

1.3 Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

| Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной) | | Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной | Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций |
|--|--|---|--|
| код компетенции | наименование компетенции | | |
| ПК-3 | Способен осуществлять мероприятия по выявлению, документированию, пресечению преступлений и правонарушений на территории, где установлены режимные требования, применяет и использует технические средства надзора и контроля за отбыванием осужденными наказания без изоляции от общества | ПК-3.2 Осуществляет мероприятия по пресечению преступлений и правонарушений на режимной территории исправительных учреждений | Знать: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ |
| ПК-7 | Способен разрабатывать и реализовывать меры профилактического, воспитательного и иного воздействия в отношении лиц, склонных к совершению правонарушений на территории учреждений уголовно-исполнительной системы | ПК-7.3 Применяет меры профилактического, воспитательного и иного воздействия, направленные на профилактику правонарушений и преступлений в отношении лиц, отбывающих уголовные наказания | Знать: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС |

| Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной) | | Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной | Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций |
|--|--|--|---|
| код компетенции | наименование компетенции | | |
| ПК-8 | Способен самостоятельно выявлять причины и условия, способствующие совершению посягательств на права и свободы участников пенитенциарных правоотношений, осуществлять предупреждение соответствующих правонарушений, основываясь на общепризнанных принципах и нормах международного права и положениях международных правовых актов | ПК-8.2 Пресекает угрозы, возникающие в пенитенциарных правоотношениях | Знать: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Владеть: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях |

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы специалитета 40.05.02 Правоохранительная деятельность, специализации «Обеспечение безопасности в уголовно-исполнительной системе». Дисциплина изучается на 5 курсе в 9 и 10 семестре.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 7 зачетных единиц (з.е.), 252 академических часа.

Таблица 3 — Объем дисциплины по видам учебных занятий

| Виды учебной работы | Всего, часов |
|---|------------------|
| Общая трудоемкость дисциплины | 252 |
| Контактная работа обучающихся с преподавателем (по видам учебных занятий) всего | 91,25 |
| в том числе: | |
| лекции | 36 |
| лабораторные занятия | не предусмотрены |
| практические занятия | 54 |

| Виды учебной работы | Всего, часов |
|---|------------------|
| Самостоятельная работа обучающихся (всего) | 133,75 |
| Контроль (подготовка к экзамену) | 27 |
| Контактная работа по промежуточной аттестации (всего АттКР) | 1,25 |
| в том числе | |
| зачет | 0,1 |
| зачет с оценкой | не предусмотрен |
| курсовая работа (проект) | не предусмотрена |
| экзамен (включая консультацию перед экзаменом) | 1,15 |

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

| № п/п | Раздел (тема) дисциплины | Содержание |
|-------|--|---|
| 1 | 2 | 3 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | Сфера высоких технологий и ИТС и её значение для современного мира. Виды преступлений в сфере высоких технологий и использования ИТС. Типовые особенности личности преступника. Общественная опасность преступлений в сфере высоких технологий и использования ИТС. Ознакомление студентов с процедурой проведения текущего контроля по дисциплине. |
| 2. | Общая характеристика компьютерных преступлений | Понятия «информация» и «компьютерная информация». Общие принципы информационной безопасности и защиты компьютерной информации в Российской Федерации. Объект преступлений в сфере компьютерной информации |
| 3. | Неправомерный доступ к компьютерной информации | Уголовно-правовая характеристика неправомерного доступа к компьютерной информации. Способы совершения неправомерного доступа к компьютерной информации. Криминологическая характеристика неправомерного доступа к компьютерной информации. |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ. Способы совершения создания, использования и распространения вредоносных компьютерных программ. Криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ. |

| № п/п | Раздел (тема) дисциплины | Содержание |
|-------|--|--|
| 1 | 2 | 3 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Криминологическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Перспективы совершенствования нормы об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС. Уголовно-правовая и криминологическая характеристика посягательств на критическую информационную инфраструктуру. |
| 6. | Хищения с использованием новых информационных технологий | Уголовно-правовая характеристика хищений с использованием новых информационных технологий. Способы совершения хищений с использованием новых информационных технологий. Криминологическая характеристика хищений с использованием новых информационных технологий |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против личности с использованием новых информационных технологий. Кибербуллинг. Развратные действия через Интернет. Нарушение авторских и смежных прав. Способы совершения преступлений против личности с использованием новых информационных технологий. Криминологическая характеристика преступлений против личности с использованием новых информационных технологий |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий. Сбыт наркотиков через Интернет и даркнет. Проституция в Интернете. Порнография в интернете. Способы совершения преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий. Криминологическая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий |

| № п/п | Раздел (тема) дисциплины | Содержание |
|-------|---|---|
| 1 | 2 | 3 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий. Экстремизм в интернете. Кибердиверсия. Государственная измена, шпионаж и разглашение государственной тайны. Способы совершения преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий. Криминологическая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против общественной безопасности с использованием новых информационных технологий. Сбыт оружия через Интернет и даркнет. Кибертерроризм. Пропаганда и оправдание терроризма. Организация массовых беспорядков. Способы совершения преступлений против общественной безопасности с использованием новых информационных технологий. Криминологическая характеристика преступлений против общественной безопасности с использованием новых информационных технологий |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | Особенности деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС. Сбор информации о посягательствах, совершаемых с использованием ИТС. Тактика пресечения преступных деяний по отдельным видам преступлений в сфере высоких технологий. |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | Особенности деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС. Сбор информации о планируемых посягательствах, совершаемых с использованием ИТС. Тактика профилактики преступных деяний по отдельным видам преступлений в сфере высоких технологий. |

Таблица 4.1.2 — Содержание дисциплины и его методическое обеспечение

| № п/п | Раздел (тема) дисциплины | Виды деятельности | | | Учебно-методические материалы | Формы текущего контроля успеваемости (по неделям семестра) | Компетенции |
|-------|--|-------------------|--------|-------|-------------------------------|--|------------------------|
| | | лек., час | № лаб. | № пр. | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 4 | | 1 | У-1-8 МУ-1-2 | Т, Р, УО 1-4 | ПК-3; ПК-7; ПК-8 |
| 2. | Общая характеристика компьютерных преступлений | 2 | | 2 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 5-6 | ПК-3; ПК-7; ПК-8 |

| | | | | | | | |
|-----|--|---|--|----|-----------------|------------------------|------------------------|
| 3. | Неправомерный доступ к компьютерной информации | 2 | | 3 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 7-8 | ПК-3; ПК-7; ПК-8 |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | 2 | | 4 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 9-10 | ПК-3; ПК-7; ПК-8 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 2 | | 5 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 11-12 | ПК-3; ПК-7; ПК-8 |
| 6. | Хищения с использованием новых информационных технологий | 6 | | 6 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 13-18 | ПК-3; ПК-7; ПК-8 |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | 2 | | 7 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 1 | ПК-3; ПК-7; ПК-8 |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | 4 | | 8 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 2-3 | ПК-3; ПК-7; ПК-8 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | 2 | | 9 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 4 | ПК-3; ПК-7; ПК-8 |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | 4 | | 10 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 5-6 | ПК-3; ПК-7; ПК-8 |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | 2 | | 11 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 7 | ПК-3; ПК-7; ПК-8 |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | 4 | | 12 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 8-9 | ПК-3; ПК-7; ПК-8 |

УО – устный опрос, К-3 – кейс-задачи, Р — защита (проверка) рефератов, Т — тестирование

4.2 Лабораторные и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

| № | Наименование практического занятия | Объём, час. |
|--------|--|-------------|
| 1 | 2 | 3 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 8 |
| 2. | Общая характеристика компьютерных преступлений | 4 |
| 3. | Неправомерный доступ к компьютерной информации | 4 |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | 4 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 4 |
| 6. | Хищения с использованием новых информационных технологий | 12 |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | 2 |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | 4 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | 2 |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | 4 |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | 2 |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | 4 |
| Итого: | | 54 |

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 — Самостоятельная работа студентов

| № раздела (темы) | Наименование раздела (темы) дисциплины | Срок выполнения | Время, затрачиваемое на выполнение СРС, час. |
|------------------|--|------------------------|--|
| 1 | 2 | 3 | 4 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 1-4-я нед. 9 сем. | 16 |
| 2. | Общая характеристика компьютерных преступлений | 5-6-я нед. 9 сем. | 8 |
| 3. | Неправомерный доступ к компьютерной информации | 7-8-я нед. 9 сем. | 8 |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | 9-10-я нед. 9 сем. | 8 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 11-12-я нед. 9 сем. | 8 |
| 6. | Хищения с использованием новых информационных технологий | 13-18-я нед. 9 сем. | 23,9 |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | 1-я нед. 10 сем. | 7 |

| № раз-дела (темы) | Наименование раздела (темы) дисциплины | Срок выполнения | Время, затрачиваемое на выполнение СРС, час. |
|-------------------|---|-----------------------|--|
| 1 | 2 | 3 | 4 |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | 2-3-я нед. 10 сем. | 14 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | 4-я нед. 10 сем. | 7 |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | 5-6-я нед. 10 сем. | 14 |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | 7 нед. 10 сем. | 7 |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | 8-10 нед. 10 сем. | 12,85 |
| Итого: | | | 133,75 |

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплины пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:
- методических рекомендаций, пособий по организации самостоятельной работы студентов;
- заданий для самостоятельной работы;
- тем рефератов и докладов;
- тем курсовых работ;

– вопросов к зачету;

– методических указаний к выполнению практических работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с ведущими экспертами и специалистами органов МВД, следственного комитета и прокуратуры.

Интерактивные образовательные технологии, используемые при проведении аудиторных занятий — не предусмотрены

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован исторический и современный социокультурный и научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует духовно-нравственному, гражданскому, патриотическому, правовому, экономическому, профессионально-трудовому, экологическому воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

- целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых и юристов, их ответственности за результаты и последствия деятельности для природы, человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и юридической практики, а также примеры высокой духовной культуры, патриотизма, гражданственности, гуманизма, творческого мышления;
- применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, представителями работодателей (командная работа, проектное обучение, разбор конкретных ситуаций, решение кейсов и др.);
- личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

| Код и наименование компетенции | Этапы формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция | | |
|--------------------------------|--|----------|-------------|
| | начальный | основной | завершающий |
| ПК-3 | Административно-правовые режимы в сфере обеспечения безопасности в уголовно-исполнительной системе | | |

| | |
|------|--|
| | <p>Делопроизводство и режим секретности в подразделениях обеспечения безопасности в уголовно-исполнительной системе</p> <p>Оперативно-розыскная деятельность в уголовно-исполнительной системе</p> <p>Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей</p> <p>Пенитенциарная криминология</p> <p>Обеспечение безопасности в уголовно-исполнительной системе</p> <p>Организация охраны и конвоирования в уголовно-исполнительной системе</p> <p>Производственная правоприменительная практика</p> <p>Подготовка к процедуре защиты и защита выпускной квалификационной работы</p> |
| ПК-7 | <p>Административно-правовые режимы в сфере обеспечения безопасности в уголовно-исполнительной системе</p> <p>Пенитенциарная криминология</p> <p>Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей</p> <p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты и защита выпускной квалификационной работы</p> |
| ПК-8 | <p>Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей</p> <p>Пенитенциарная криминология</p> <p>Обеспечение безопасности в уголовно-исполнительной системе</p> <p>Организация охраны и конвоирования в уголовно-исполнительной системе</p> <p>Международное пенитенциарное право</p> <p>Предупреждение пенитенциарной преступности</p> <p>Производственная правоприменительная практика</p> <p>Подготовка к процедуре защиты и защита выпускной квалификационной работы</p> |

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

| Код компетенции / этап (указывается название этапа из п.7.1) | Показатели оценивания компетенций | Уровни сформированности компетенции | | |
|--|---|--|--|---|
| | | пороговый (удовлетворительный) | продвинутый (хорошо) | высокий (отлично) |
| ПК-3 / начальный, основной, завершающий | ПК-3.2 Осуществляет мероприятия по пресечению преступлений и правонарушений на режимной территории исправительных учреждений | Знать: общие: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: в типовых ситуациях: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: реализуемыми в типовых ситуациях: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ | Знать: общие и специальные: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: в типовых и стандартных ситуациях: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: реализуемыми в типовых и стандартных ситуациях: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ | Знать: общие, специальные и специфические: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: в типовых, стандартных и нестандартных ситуациях: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: реализуемыми в типовых, стандартных и нестандартных ситуациях: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ |
| ПК-7 / начальный, основной, завершающий | ПК-7.3 Применяет меры профилактического, воспитательного и иного | Знать: общие: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности | Знать: общие и специальные: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические | Знать: общие, специальные и специфические: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности |

| | | | | |
|--|--|--|--|--|
| | <p>воздействия, направленные на профилактику правонарушений и преступлений в отношении лиц, отбывающих уголовные наказания</p> | <p>преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: в типовых ситуациях: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: реализуемыми в типовых ситуациях: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС</p> | <p>особенности преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: в типовых и стандартных ситуациях: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: реализуемыми в типовых и стандартных ситуациях: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС</p> | <p>преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: в типовых, стандартных и нестандартных ситуациях: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: реализуемыми в типовых, стандартных и нестандартных ситуациях: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС</p> |
| <p>ПК-8 / начальный, основной, завершающий</p> | <p>ПК-8.2 Пресекает угрозы, возникающие в пенитенциарных правоотношениях</p> | <p>Знать: общие: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: в типовых ситуациях: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях</p> | <p>Знать: общие и специальные: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: в типовых и стандартных ситуациях: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях</p> | <p>Знать: общие, специальные и специфические: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: в типовых, стандартных и нестандартных ситуациях: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Владеть: реализуемыми в типовых, стандартных и нестандартных</p> |

| | | | | |
|--|--|---|---|---|
| | | Владеть: реализуемыми в типовых ситуациях: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях | Владеть: реализуемыми в типовых и стандартных ситуациях: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях | ситуациях: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях |
|--|--|---|---|---|

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

| № п/п | Раздел (тема) дисциплины | Код контролируемой компетенции (или её части) | Технология формирования | Оценочные средства | | Описание шкал оценивания |
|-------|--|---|-----------------------------------|--|----------------------------------|--------------------------|
| | | | | наименование | №№ заданий | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады | 1-5 1-5 1-3 | Согласно табл. 7.2. |
| 2 | Общая характеристика компьютерных преступлений | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 6-10 6-10 4-6 1-5 | Согласно табл. 7.2. |
| 3 | Неправомерный доступ к компьютерной информации | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 11-20 11-15 7-9 6-10 | Согласно табл. 7.2. |
| 4 | Создание, использование и распространение вредоносных компьютерных программ | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 21-30 16-20 10-12 11-15 | Согласно табл. 7.2. |
| 5 | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 31-40 21-25 13-15 16-20 | Согласно табл. 7.2. |
| 6 | Хищения с использованием новых информационных технологий | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 41-50 26-30 16-18 21-25 | Согласно табл. 7.2. |
| 7 | Преступления против личности, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 51-60 31-35 19-21 26-30 | Согласно табл. 7.2. |

| № п/п | Раздел (тема) дисциплины | Код контролируемой компетенции (или её части) | Технология формирования | Оценочные средства | | Описание шкал оценивания |
|-------|---|---|-----------------------------------|--|-----------------------------------|--------------------------|
| | | | | наименование | №№ заданий | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 61-70 36-40 22-24 31-35 | Согласно табл. 7.2. |
| 9 | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 71-80 41-45 25-27 36-40 | Согласно табл. 7.2. |
| 10 | Преступления против общественной безопасности, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 81-90 46-50 28-30 41-45 | Согласно табл. 7.2. |
| 11 | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 91-95 51-55 31-33 46-50 | Согласно табл. 7.2. |
| 12 | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 96-100 56-60 34-36 51-55 | Согласно табл. 7.2. |

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Понятие и общая характеристика преступлений, связанных с использованием ИТС»

1. Чем обусловлена актуальность изучения преступности в сфере высоких технологий в современный период?
2. Какие виды преступности относятся к высокотехнологичным?
3. Каково состояние киберпреступности и перспективы борьбы с ней?
4. В чём отличие распространённых представлений о личности киберпреступников от реальной действительности?
5. Чем обусловлено вовлечение в киберпреступность всё большего числа граждан?

Кейс-задача по разделу (теме) 9. «Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий»

Сотрудники отдела «К» УВД г. Энска А. и З. для повышения показателей раскрываемости компьютерных преступлений решили провести «оперативный эксперимент». Найдя в газете бесплатных объявлений объявление об оказании услуг «компьютерной помощи», они позвонили давшему его Р. и попросили его оказать помощь в установке на компьютер программного продукта Autodesk Alias Surface 2016 (стоимость лицензии на который составляла

1 млн. 145 тыс. рублей). Поначалу Р. отказался, однако после повторных звонков и обещания дополнительного вознаграждения всё же согласился. Требуемую программу он скачал из Интернета, там же он нашёл средства, позволяющие обойти технические ограничения, связанные с защитой авторских прав. Для установки программы был подготовлен компьютер, содержащий «чистую» ОС Windows. После того, как Р. закончил установку и «взломал» программу, оперативники задержали его. Р. было предъявлено обвинение в покушении на совершение нарушения авторских и смежных прав в особо крупном размере, неправомерный доступ к компьютерной информации, совершённый из корыстной заинтересованности и причинивший крупный ущерб, а также в использовании вредоносных компьютерных программ, предназначенных для нейтрализации средств защиты компьютерной информации, совершённое из корыстной заинтересованности и причинивший крупный ущерб. Правильна ли такая квалификация? Правомерны ли действия оперативников?

Темы рефератов и докладов по разделу (теме) 6. «Хищения с использованием новых информационных технологий»

1. Хищения с использованием банковских платёжных карт
2. История использования компьютеров для совершения хищений
3. Компьютерное вымогательство

Вопросы в тестовой форме по разделу (теме) 2. «Общая характеристика компьютерных преступлений»

Понятие доступа к информации включает в себя получение возможности:

- изменения информации
- получения информации
- использования информации
- удаления информации

Субъективная сторона неправомерного доступа к компьютерной информации может выражаться:

- в умысле по отношению к последствиям
- в неосторожности по отношению к последствиям
- в неосторожности по отношению к деянию
- в умысле по отношению к деянию

Неправомерный доступ к компьютерной информации не образует:

- временное ограничение доступа к информации легальных пользователей
- простое ознакомление с информацией
- уничтожение носителя компьютерной информации
- внесение изменений в информацию, не нарушающих её целостности

Крупным ущербом в статьях о преступлениях в сфере компьютерной информации признаётся ущерб, сумма которого превышает:

- 1 миллион рублей
- 250 тысяч рублей
- 1,5 миллиона рублей
- 100 тысяч рублей

Квалифицирующим признаком неправомерного доступа к компьютерной информации является совершение его:

- по экстремистским мотивам
- из хулиганских побуждений
- из низменных побуждений
- из корыстной заинтересованности

Вредоносность компьютерной программы определяется сочетанием:

- способностью к распространению в компьютерных сетях («червь»)
- характера совершаемых ей действий (уничтожение, модификация, блокирование информации и т.д.)
- способностью к саморазмножению («компьютерный вирус»)

- совершения действий без разрешения пользователя

Написание программы, предназначенной для повреждения компьютерного оборудования или иного нарушения работы компьютерной системы образует состав:

- неправомерного доступа к компьютерной информации
- создания, использования и распространения вредоносных компьютерных программ
- не охватывается составом ни одного из преступлений, предусмотренных гл. 28 УК

РФ

○ нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Создание, использование и распространение вредоносных компьютерных программ окончено с момента:

- совершения любого из указанных действий
- фактического наступления последствий (например, уничтожения информации)
- начала работы программиста над созданием программы
- нет правильного ответа

Создание, использование и распространение вредоносных компьютерных программ (ч. 1 ст. 273 УК РФ) может быть совершено с виной в форме:

- преступной небрежности
- прямого умысла
- косвенного умысла
- преступного легкомыслия

Под правилами эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в уголовно-правовой литературе понимается:

- всё перечисленное
- нормативные правовые акты, принимаемые органами государственной власти, например, санитарные нормы
- техническая документация на компьютерную технику
- локальные нормативные документы (правила внутреннего распорядка, должностные инструкции)

Осуществляемое через компьютерную сеть воздействие на подключённую к ней информационную систему, направленное на то, чтобы «перегрузить» её запросами (атака типа Denial of Service), не предполагающее возможности ознакомления с информацией, хранящейся в данной системе, образует состав:

- создания, использования и распространения вредоносных компьютерных программ
- не охватывается составом ни одного из преступлений, предусмотренных гл. 28 УК

РФ

○ нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

- неправомерного доступа к компьютерной информации

Использование для доступа в сеть Интернет случайно подсмотренных учётных данных (логина и пароля), принадлежащих другому пользователю, образует состав:

- неправомерного доступа к компьютерной информации
- создания, использования и распространения вредоносных компьютерных программ
- нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
- не охватывается составом ни одного из преступлений, предусмотренных гл. 28 УК

РФ

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей может быть совершено только путём активных действий виновного.

- да

○ нет

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачетов и экзаменов. Зачеты и экзамены проводятся в виде бланкового и/или компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 3 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Компьютерная информация может быть представлена в форме:

- 1) электрических сигналов
- 2) магнитной записи
- 3) распечатки машинного кода
- 4) QR-кода

Задание в открытой форме:

Сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи — это _____.

Задание на установление правильной последовательности,

Установите последовательность этапов совершения преступления в сфере компьютерной информации:

- 1) формирование умысла
- 2) приготовление
- 3) покушение
- 4) оконченное преступление

Задание на установление соответствия:

Установите соответствие объектов преступления:

| | |
|------------------------------------|--------------------------------|
| А) Информационная безопасность | 1) Неправомерный доступ к КИ |
| Б) Общественная нравственность | 2) Распространение порнографии |
| В) Конституционные права и свободы | 3) Нарушение авторских прав |
| Г) Собственность | 4) Компьютерное мошенничество |

Компетентностно-ориентированная задача:

АО «Окно» разработало и продавало компьютерную игру. При установке игры на компьютер некоторые стандартные драйверы устройств заменялись на драйверы, разработанные АО «Окно», в результате была нарушена нормальная работа нескольких тысяч компьютеров. При установке программа тестировала компьютерное оборудование и программное обеспечение пользователя, сведения о которых при регистрации с помощью модема сообщались в АО «Окно». В документации к игре не сообщалось об этом. Квалифицируйте содеянное.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* успеваемости по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

| Форма контроля | Минимальный балл | | Максимальный балл | |
|---|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 1. Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 2 | Недостаточно полное и точное изложение материала. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 2. Общая характеристика компьютерных преступлений | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |

| Форма контроля | Минимальный балл | | Максимальный балл | |
|---|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 3. Неправомерный доступ к компьютерной информации | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 4. Создание, использование и распространение вредоносных компьютерных программ | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 6. Хищения с использованием новых информационных технологий | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| СРС | 12 | | 24 | |
| Итого | 24 | | 48 | |
| Посещаемость | 0 | | 16 | |
| Зачёт | 0 | | 36 | |
| Итого | 24 | | 100 | |

| Форма контроля | Минимальный балл | | Максимальный балл | |
|--|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 7. Преступления против личности, совершаемые с применением информационных технологий | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 8. Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 9. Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 10. Преступления против общественной безопасности, совершаемые с применением информационных технологий | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие №11. Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |

| Форма контроля | Минимальный балл | | Максимальный балл | |
|--|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 12. Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| СРС | 12 | | 24 | |
| Итого | 24 | | 48 | |
| Посещаемость | 0 | | 16 | |
| Экзамен | 0 | | 36 | |
| Итого | 24 | | 100 | |

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ – 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование – 36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 "Информационная безопасность", 400301 "Юриспруденция", 380301 "Экономика"] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. Текст: электронный.
2. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 "Информационная безопасность", 400301 "Юриспруденция", 380301 "Экономика"] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. Текст: непосредственный.
3. Криминология. Особенная часть [Текст] : учебник для академического бакалавриата : в 2 т. / Академия Генеральной прокуратуры РФ ; под общ. ред. ректора Академии Генеральной прокуратуры РФ, д-ра юрид. наук, проф. О. С. Капинус. - Москва : Юрайт, 2017. - ISBN 978-5-534-03382-3. - Текст : непосредственный. Т. 1. - 312 с.
4. Байбарин, Андрей Андреевич. Уголовное право России. Общая часть : учебное пособие : [для студентов и слушателей, обучающихся по программам специалистов, бакалавров и магистров, профессорско-преподавательского состава высших учебных заведений, научных работников] / А. А. Байбарин, А. А. Гребеньков, С. В. Шевелева ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 428 с. - Текст : электронный.

5. Байбарин, Андрей Андреевич. Уголовное право России. Общая часть : учебное пособие : [для студентов и слушателей, обучающихся по программам специалистов, бакалавров и магистров, профессорско-преподавательского состава высших учебных заведений, научных работников] / А. А. Байбарин, А. А. Гребеньков, С. В. Шевелева ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 428 с. - Текст : непосредственный.

8.2 Дополнительная учебная литература

6. Байбарин, Андрей Андреевич. Практикум по курсу "Уголовное право" : учебное пособие / А. А. Байбарин, А. А. Гребеньков, М. Н. Урда ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - Курск : ЮЗГУ, 2013. - 209 с. - Текст : электронный.
7. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
8. Криминология. Особенная часть [Текст] : учебник для академического бакалавриата : в 2 т. / Академия Генеральной прокуратуры РФ ; под общ. ред. ректора Академии Генеральной прокуратуры РФ, д-ра юрид. наук, проф. О. С. Капинус. - Москва : Юрайт, 2017. - Текст : непосредственный. Т. 2. - 311 с.

8.3 Перечень методических указаний

1. Криминология : методические рекомендации по подготовке к практическим занятиям для студентов всех форм обучения направления подготовки 40.03.01 Юриспруденция / Юго-Зап. гос. ун-т ; сост.: М. И. Синяева, А. А. Байбарин, А. А. Гребеньков. - Курск : ЮЗГУ, 2017. - 35 с. - Текст: электронный.
2. Преступления в сфере высоких технологий : методические рекомендации по подготовке к практическим занятиям для студентов всех форм обучения направления подготовки 40.04.01 Юриспруденция / Юго-Зап. гос. ун-т ; сост.: М. И. Синяева, А. А. Байбарин, А. А. Гребеньков. - Курск : ЮЗГУ, 2017. - 33 с. - Текст: электронный.

8.4 Другие учебно-методические материалы

Отраслевые научные журналы в библиотеке университета

1. Административное право и процесс
2. Гражданское право
3. Конституционное и муниципальное право
4. Пробелы в российском законодательстве. Юридический журнал
5. Российская газета – ежедневная, без Российской газеты «Неделя»
6. Российская юстиция
7. Российский следователь
8. Российский судья
9. Уголовное право

9 Перечень ресурсов информационно-телекоммуникационной сети

Интернет

1. <http://www.cyberpol.ru/> – компьютерная преступность и борьба с ней.
2. <http://www.crime-research.ru/> – Центр исследования компьютерной преступности.
3. Электронная библиотека elibrary.ru.
4. Электронная библиотека cyberleninka.ru.
5. Сайт кафедры уголовного права: <http://www.swsu.ru/structura/up/uf/kup/index.php>.

10 Методические указания для обучающихся по освоению дисциплины

Программа дисциплины ориентирует студентов на всестороннее и системное изучение основных институтов уголовного права, его принципов и категорий, с помощью которых осмысливаются и решаются проблемы формирования и вывода специфических понятий, суждений, умозаключений, реализуется аргументационный процесс.

Важнейшим условием успешного изучения курса является систематическая самостоятельная работа с рекомендованной литературой. Студент должен овладеть понятийным аппаратом дисциплины, знать и понимать основные её категории.

На лекциях студенты должны работать с особым вниманием, стремясь вести подробный конспект, в котором должны быть отражены все важнейшие положения лекции. Если какой-то фрагмент лекции студент не успевает отразить в конспекте, целесообразно оставить место для дальнейшей доработки конспекта во время самостоятельной работы. Если какой-то положение лекции студентом не понято, следует обязательно задать преподавателю вопрос, желательно - в письменной форме, чтобы не прерывать ход лекции. В этом случае преподаватель сам найдёт удобное время, чтобы ответить на заданный вопрос.

При доработке конспекта лекций следует стремиться, чтобы в нем нашло отражение основное содержание изучаемой темы. Желательно, чтобы определения, примеры судебной практики и другие важные положения были ярко выделены. Не следует жалеть места для широких полей, где делаются соответствующие пометки.

Большое место в успешном овладении дисциплиной отводится семинарским занятиям. Семинар — это средство коллективного творческого раздумья, школа творческого мышления, столь необходимых будущему специалисту в его практической деятельности. Семинарское занятие требует от студента глубокого самостоятельного изучения рекомендованных источников и литературы по теме занятия.

Рекомендуется следующий алгоритм подготовки к семинару.

1. Внимательное изучение плана семинарского занятия, списка рекомендованных источников и литературы, методических рекомендаций преподавателя.

2. Изучение программы курса - с целью уяснения требований к объему и содержанию знаний по изучаемой теме.

3. Изучение и доработка конспекта лекций, прочитанных преподавателем по темам, выносимым на семинарское занятие.

4. Изучение вопросов темы по учебнику и основным рекомендованным пособиям.

5. Изучение дополнительной литературы.

При этом перед собой нужно иметь соответствующие статьи нормативных актов, которые неоднократно перечитывать. Рекомендуется вести конспект прочитанного, записывать научные определения, краткие формулировки, сопоставлять различные точки зрения. Следует продумать свой ответ по вопросам, составить краткий план ответа по каждому вопросу.

От студента не требуется изучения всей рекомендуемой литературы. Количество и объем изучаемых работ зависит от конкретной задачи: подготовки доклада, реферата, фиксированного выступления и т.д.

При ответе не следует повторять сказанное предыдущими выступающими, повторять самому, злоупотреблять временем другим способом. Пользоваться при ответе учебниками, лекциями, нормативными актами можно лишь с разрешения преподавателя.

Обязательно наличие изучаемых нормативных актов в последней редакции на практических занятиях, методических пособий кафедры по дисциплине. Рекомендуется выполнять творческие задания и решать задачи письменно в отдельной тетради. Рекомендуется самостоятельно решать задачи и тесты по дисциплине.

Перед консультацией, проводимой преподавателем, студент должен хорошо продумать и четко сформулировать вопросы по тем темам, которые оказались недостаточно усвоенными им в процессе самостоятельной работы.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. СПС «Консультант+: Высшая школа».
2. СПС «ГАРАНТ-Студент».
3. Программа для ЭВМ «Программа для формирования бланков тестовых заданий», авторы: Калашникова А. А., Гребеньков А. А.
4. Программа для ЭВМ «Программа для осуществления тестового контроля знаний студентов», авторы: Калашникова А. А., Гребеньков А. А.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционная аудитория; оснащенная учебной мебелью для обучающихся; стол, стул для преподавателя; доска; компьютерные классы университета (20-23 ПК) ОС Windows XP; программное обеспечение Microsoft Office; мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/14``/1024Mb/160Gb/ сумка/проектор inFocus IN24+ (инвентарный номер 1043239); экран на штативе (инвентарный номер 434345) ; телевизор – Samsung PS51E537 (инвентарный номер 434349); ноутбук ASUS k501UQ 15,6``(FHD i3-6100U/4Gb/500Gb/GF940MX/noDVD/W10 (инвентарный номер 2341598); вычислительная сеть университета с локальными версиями СПС Консультант Плюс, Гарант; сеть Интернет.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую

техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу**дисциплины**

| Номер изменения | Номера страниц | | | | Всего страниц | Дата | Основание для изменения и подпись лица, проводившего изменения |
|--------------------|----------------|------------|----------------|-------|------------------|------|---|
| | Изменённых | Заменённых | Аннулированных | Новых | | | |
| | | | | | | | |

МИНОБРНАУКИ РОССИИ

Юго-Западный государственный университет

УТВЕРЖДАЮ:

Декан факультета

юридического.

(наименование ф-та полностью)

С.В. Шевелева

(подпись, инициалы, фамилия)

« 06 » июль 2021 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Противодействие посягательствам в уголовно-исполнительной системе,
совершаемых при помощи информационно-телекоммуникационных сетей

(наименование дисциплины)

ОПОП ВО 40.05.02 Правоохранительная деятельность

шифр и наименование направления подготовки (специальности)

специализация «Обеспечение безопасности в уголовно-исполнительной системе»

наименование направленности (профиля, специализации)

форма обучения заочная

(очная, очно-заочная, заочная)

Курск – 2021

Рабочая программа дисциплины составлена в соответствии с ФГОС ВО — специалитет по специальности 40.05.02 Правоохранительная деятельность на основании учебного плана ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе», одобренного Ученым советом университета (протокол № 9 от «25» июня 2021 г.).

Рабочая программа дисциплины обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе» на заседании кафедры уголовного права протокол № 15 «03» июля 2021 г.

Зав. кафедрой УП



Байбарин А.А.

Разработчик программы

к.ю.н. доцент



Гребеньков А.А.

Согласовано:

/Директор научной библиотеки



Макаровская В.Г.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе» на заседании кафедры уголовного права протокол № ___ «___» _____ 20__ г.

Зав. кафедрой УП

Байбарин А.А.

Рабочая программа дисциплины пересмотрена, обсуждена и рекомендована к реализации в образовательном процессе для обучения студентов по ОПОП ВО 40.05.02 Правоохранительная деятельность, специализация «Обеспечение безопасности в уголовно-исполнительной системе» на заседании кафедры уголовного права протокол № ___ «___» _____ 20__ г.

Зав. кафедрой УП

Байбарин А.А.

1 Цель и задачи дисциплины. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения основной профессиональной образовательной программы

1.1 Цель дисциплины

Подготовка выпускника, способного осуществлять деятельность, требующую углубленной фундаментальной и профессиональной подготовки, в том числе научно-исследовательскую работу, обладающего глубокими теоретическими знаниями и практическими навыками, касающимися особенностей квалификации преступлений, совершаемых с использованием новых информационных технологий и их криминологической характеристики, способного применять эти знания и навыки в рамках дальнейшей его практической деятельности.

1.2 Задачи дисциплины

— обучение студента навыкам обоснования и принятия решений, а также совершения действий, связанных с реализацией уголовно-правовых норм в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение необходимыми для успешной профилактики, предупреждения, выявления, пресечения преступлений, совершаемым при помощи информационно-телекоммуникационных сетей, знаниями норм и правовых институтов;

— обучение студента самостоятельной работе над нормативными актами, научной и учебной литературой, необходимой для сбора, анализа и оценки информации, имеющей значение для реализации правовых норм в сфере правоохранительной деятельности;

— формирование навыков проведения прикладных научных исследований в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение умением критически анализировать действующее законодательство; обобщать следственную и судебную практику применения законодательства в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей;

— овладение методикой пополнения и закрепления правовых знаний и умений в сфере противодействия посягательствам, совершаемым при помощи информационно-телекоммуникационных сетей на практике;

— сформировать понимание методологических основ и специфики методов, используемых в уголовно-правовой и криминологической теории, а также информационном праве в связи с проблематикой преступлений, совершаемых при помощи информационно-телекоммуникационных сетей.

1.3 Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Таблица 1.3 – Результаты обучения по дисциплине

| Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной) | | Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной | Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций |
|--|--|---|--|
| код компетенции | наименование компетенции | | |
| ПК-3 | Способен осуществлять мероприятия по выявлению, документированию, пресечению преступлений и правонарушений на территории, где установлены режимные требования, применяет и использует технические средства надзора и контроля за отбыванием осужденными наказания без изоляции от общества | ПК-3.2 Осуществляет мероприятия по пресечению преступлений и правонарушений на режимной территории исправительных учреждений | Знать: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ |
| ПК-7 | Способен разрабатывать и реализовывать меры профилактического, воспитательного и иного воздействия в отношении лиц, склонных к совершению правонарушений на территории учреждений уголовно-исполнительной системы | ПК-7.3 Применяет меры профилактического, воспитательного и иного воздействия, направленные на профилактику правонарушений и преступлений в отношении лиц, отбывающих уголовные наказания | Знать: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС |

| Планируемые результаты освоения основной профессиональной образовательной программы (компетенции, закрепленные за дисциплиной) | | Код и наименование индикатора достижения компетенции, закрепленного за дисциплиной | Планируемые результаты обучения по дисциплине, соотнесенные с индикаторами достижения компетенций |
|--|--|--|---|
| код компетенции | наименование компетенции | | |
| ПК-8 | Способен самостоятельно выявлять причины и условия, способствующие совершению посягательств на права и свободы участников пенитенциарных правоотношений, осуществлять предупреждение соответствующих правонарушений, основываясь на общепризнанных принципах и нормах международного права и положениях международных правовых актов | ПК-8.2 Пресекает угрозы, возникающие в пенитенциарных правоотношениях | Знать: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Владеть: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях |

2 Указание места дисциплины в структуре основной профессиональной образовательной программы

Дисциплина «Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей» входит в часть, формируемую участниками образовательных отношений, блока 1 «Дисциплины (модули)» основной профессиональной образовательной программы – программы специалитета 40.05.02 Правоохранительная деятельность, специализации «Обеспечение безопасности в уголовно-исполнительной системе». Дисциплина изучается на 5 курсе в 1, 2 и 3 сессии.

3 Объем дисциплины в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 7 зачетных единиц (з.е.), 252 академических часа.

Таблица 3 — Объем дисциплины по видам учебных занятий

| Виды учебной работы | Всего, часов |
|---|------------------|
| Общая трудоемкость дисциплины | 252 |
| Контактная работа обучающихся с преподавателем (по видам учебных занятий) всего | 18,22 |
| в том числе: | |
| лекции | 6 |
| лабораторные занятия | не предусмотрены |
| практические занятия | 12 |

| Виды учебной работы | Всего, часов |
|---|------------------|
| Самостоятельная работа обучающихся (всего) | 220,78 |
| Контроль (подготовка к экзамену) | 13 |
| Контактная работа по промежуточной аттестации (всего АттКР) | 0,22 |
| в том числе | |
| зачет | 0,1 |
| зачет с оценкой | не предусмотрен |
| курсовая работа (проект) | не предусмотрена |
| экзамен (включая консультацию перед экзаменом) | 0,12 |

4 Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Содержание дисциплины

Таблица 4.1.1 – Содержание дисциплины, структурированное по темам (разделам)

| № п/п | Раздел (тема) дисциплины | Содержание |
|-------|--|---|
| 1 | 2 | 3 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | Сфера высоких технологий и ИТС и её значение для современного мира. Виды преступлений в сфере высоких технологий и использования ИТС. Типовые особенности личности преступника. Общественная опасность преступлений в сфере высоких технологий и использования ИТС. Ознакомление студентов с процедурой проведения текущего контроля по дисциплине. |
| 2. | Общая характеристика компьютерных преступлений | Понятия «информация» и «компьютерная информация». Общие принципы информационной безопасности и защиты компьютерной информации в Российской Федерации. Объект преступлений в сфере компьютерной информации |
| 3. | Неправомерный доступ к компьютерной информации | Уголовно-правовая характеристика неправомерного доступа к компьютерной информации. Способы совершения неправомерного доступа к компьютерной информации. Криминологическая характеристика неправомерного доступа к компьютерной информации. |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | Уголовно-правовая характеристика создания, использования и распространения вредоносных компьютерных программ. Способы совершения создания, использования и распространения вредоносных компьютерных программ. Криминологическая характеристика создания, использования и распространения вредоносных компьютерных программ. |

| № п/п | Раздел (тема) дисциплины | Содержание |
|----------|--|--|
| 1 | 2 | 3 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | Уголовно-правовая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Криминологическая характеристика нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Перспективы совершенствования нормы об ответственности за нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС. Уголовно-правовая и криминологическая характеристика посягательств на критическую информационную инфраструктуру. |
| 6. | Хищения с использованием новых информационных технологий | Уголовно-правовая характеристика хищений с использованием новых информационных технологий. Способы совершения хищений с использованием новых информационных технологий. Криминологическая характеристика хищений с использованием новых информационных технологий |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против личности с использованием новых информационных технологий. Кибербуллинг. Развратные действия через Интернет. Нарушение авторских и смежных прав. Способы совершения преступлений против личности с использованием новых информационных технологий. Криминологическая характеристика преступлений против личности с использованием новых информационных технологий |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий. Сбыт наркотиков через Интернет и даркнет. Проституция в Интернете. Порнография в интернете. Способы совершения преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий. Криминологическая характеристика преступлений против здоровья населения и общественной нравственности с использованием новых информационных технологий |

| № п/п | Раздел (тема) дисциплины | Содержание |
|-------|---|---|
| 1 | 2 | 3 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий. Экстремизм в интернете. Кибердиверсия. Государственная измена, шпионаж и разглашение государственной тайны. Способы совершения преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий. Криминологическая характеристика преступлений против конституционного строя и безопасности государства с использованием новых информационных технологий |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | Уголовно-правовая характеристика преступлений против общественной безопасности с использованием новых информационных технологий. Сбыт оружия через Интернет и даркнет. Кибертерроризм. Пропаганда и оправдание терроризма. Организация массовых беспорядков. Способы совершения преступлений против общественной безопасности с использованием новых информационных технологий. Криминологическая характеристика преступлений против общественной безопасности с использованием новых информационных технологий |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | Особенности деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС. Сбор информации о посягательствах, совершаемых с использованием ИТС. Тактика пресечения преступных деяний по отдельным видам преступлений в сфере высоких технологий. |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | Особенности деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС. Сбор информации о планируемых посягательствах, совершаемых с использованием ИТС. Тактика профилактики преступных деяний по отдельным видам преступлений в сфере высоких технологий. |

Таблица 4.1.2 — Содержание дисциплины и его методическое обеспечение

| № п/п | Раздел (тема) дисциплины | Виды деятельности | | | Учебно-методические материалы | Формы текущего контроля успеваемости (по неделям семестра) | Компетенции |
|-------|--|-------------------|--------|-------|-------------------------------|--|------------------------|
| | | лек., час | № лаб. | № пр. | | | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 1 | | 1 | У-1-8 МУ-1-2 | Т, Р, УО 5 | ПК-3; ПК-7; ПК-8 |
| 2. | Общая характеристика компьютерных преступлений | 1 | | 2 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 6 | ПК-3; ПК-7; ПК-8 |

| | | | | | | | |
|-----|--|---|--|----|-----------------|------------------------|------------------------|
| 3. | Неправомерный доступ к компьютерной информации | 1 | | 3 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 23-24 | ПК-3; ПК-7; ПК-8 |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | 1 | | 4 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 25 | ПК-3; ПК-7; ПК-8 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 1 | | 5 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 37 | ПК-3; ПК-7; ПК-8 |
| 6. | Хищения с использованием новых информационных технологий | 1 | | 6 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 37 | ПК-3; ПК-7; ПК-8 |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | | | 7 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 37 | ПК-3; ПК-7; ПК-8 |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | | | 8 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 38 | ПК-3; ПК-7; ПК-8 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | | | 9 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 38 | ПК-3; ПК-7; ПК-8 |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | | | 10 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 38 | ПК-3; ПК-7; ПК-8 |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | | | 11 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 39 | ПК-3; ПК-7; ПК-8 |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | | | 12 | У-1-8 МУ-1-2 | Т, Р, УО, К-3 39 | ПК-3; ПК-7; ПК-8 |

УО – устный опрос, К-3 – кейс-задачи, Р — защита (проверка) рефератов, Т — тестирование

4.2 Лабораторные и (или) практические занятия

4.2.1 Практические занятия

Таблица 4.2.1 – Практические занятия

| № | Наименование практического занятия | Объём, час. |
|--------|--|-------------|
| 1 | 2 | 3 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 1 |
| 2. | Общая характеристика компьютерных преступлений | 1 |
| 3. | Неправомерный доступ к компьютерной информации | 1 |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | 1 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 1 |
| 6. | Хищения с использованием новых информационных технологий | 1 |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | 1 |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | 1 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | 1 |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | 1 |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | 1 |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | 1 |
| Итого: | | 12 |

4.3 Самостоятельная работа студентов (СРС)

Таблица 4.3 — Самостоятельная работа студентов

| № раздела (темы) | Наименование раздела (темы) дисциплины | Срок выполнения | Время, затрачиваемое на выполнение СРС, час. |
|------------------|--|-----------------|--|
| 1 | 2 | 3 | 4 |
| 1. | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 5-7 нед. | 22,78 |
| 2. | Общая характеристика компьютерных преступлений | 8-10 нед. | 18 |
| 3. | Неправомерный доступ к компьютерной информации | 11-13 нед. | 18 |
| 4. | Создание, использование и распространение вредоносных компьютерных программ | 14-16 нед. | 18 |
| 5. | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 17-19 нед. | 18 |
| 6. | Хищения с использованием новых информационных технологий | 20-22 нед. | 18 |
| 7. | Преступления против личности, совершаемые с применением информационных технологий | 23-25 нед. | 18 |

| № раз-дела (темы) | Наименование раздела (темы) дисциплины | Срок выполнения | Время, затрачиваемое на выполнение СРС, час. |
|-------------------|---|-----------------|--|
| 1 | 2 | 3 | 4 |
| 8. | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | 26-28 нед. | 18 |
| 9. | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | 29-31 нед. | 18 |
| 10. | Преступления против общественной безопасности, совершаемые с применением информационных технологий | 32-34 нед. | 18 |
| 11. | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | 35-37 нед. | 18 |
| 12. | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | 38-39 нед. | 18 |
| Итого: | | | 220,78 |

5 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине

Студенты могут при самостоятельном изучении отдельных тем и вопросов дисциплины пользоваться учебно-наглядными пособиями, учебным оборудованием и методическими разработками кафедры в рабочее время, установленное Правилами внутреннего распорядка работников.

Учебно-методическое обеспечение для самостоятельной работы обучающихся по данной дисциплине организуется:

библиотекой университета:

- библиотечный фонд укомплектован учебной, методической, научной, периодической, справочной и художественной литературой в соответствии с УП и данной РПД;
- имеется доступ к основным информационным образовательным ресурсам, информационной базе данных, в том числе библиографической, возможность выхода в Интернет.

кафедрой:

- путем обеспечения доступности всего необходимого учебно-методического и справочного материала;
- путем предоставления сведений о наличии учебно-методической литературы, современных программных средств.
- путем разработки:
- методических рекомендаций, пособий по организации самостоятельной работы студентов;
- заданий для самостоятельной работы;
- тем рефератов и докладов;
- тем курсовых работ;

– вопросов к зачету;

– методических указаний к выполнению практических работ и т.д.

типографией университета:

- помощь авторам в подготовке и издании научной, учебной и методической литературы;
- удовлетворение потребности в тиражировании научной, учебной и методической литературы.

6 Образовательные технологии

Реализация компетентностного подхода предусматривает широкое использование в образовательном процессе активных и интерактивных форм проведения занятий в сочетании с внеаудиторной работой с целью формирования универсальных, общепрофессиональных и профессиональных компетенций обучающихся. В рамках дисциплины предусмотрены встречи с ведущими экспертами и специалистами органов МВД, следственного комитета и прокуратуры.

Интерактивные образовательные технологии, используемые при проведении аудиторных занятий — не предусмотрены

Технологии использования воспитательного потенциала дисциплины

Содержание дисциплины обладает значительным воспитательным потенциалом, поскольку в нем аккумулирован исторический и современный социокультурный и научный опыт человечества. Реализация воспитательного потенциала дисциплины осуществляется в рамках единого образовательного и воспитательного процесса и способствует непрерывному развитию личности каждого обучающегося. Дисциплина вносит значимый вклад в формирование общей и профессиональной культуры обучающихся. Содержание дисциплины способствует духовно-нравственному, гражданскому, патриотическому, правовому, экономическому, профессионально-трудовому, экологическому воспитанию обучающихся.

Реализация воспитательного потенциала дисциплины подразумевает:

- целенаправленный отбор преподавателем и включение в лекционный материал, материал для практических и (или) лабораторных занятий содержания, демонстрирующего обучающимся образцы настоящего научного подвижничества создателей и представителей данной отрасли науки, высокого профессионализма ученых и юристов, их ответственности за результаты и последствия деятельности для природы, человека и общества; примеры подлинной нравственности людей, причастных к развитию науки и юридической практики, а также примеры высокой духовной культуры, патриотизма, гражданственности, гуманизма, творческого мышления;
- применение технологий, форм и методов преподавания дисциплины, имеющих высокий воспитательный эффект за счет создания условий для взаимодействия обучающихся с преподавателем, другими обучающимися, представителями работодателей (командная работа, проектное обучение, разбор конкретных ситуаций, решение кейсов и др.);
- личный пример преподавателя, демонстрацию им в образовательной деятельности и общении с обучающимися за рамками образовательного процесса высокой общей и профессиональной культуры.

Реализация воспитательного потенциала дисциплины на учебных занятиях направлена на поддержание в университете единой развивающей образовательной и воспитательной среды. Реализация воспитательного потенциала дисциплины в ходе самостоятельной работы обучающихся способствует развитию в них целеустремленности, инициативности, креативности, ответственности за результаты своей работы – качеств, необходимых для успешной социализации и профессионального становления.

7 Фонд оценочных средств для проведения промежуточной аттестации обучающихся по дисциплине

7.1 Перечень компетенций с указанием этапов их формирования в процессе освоения основной профессиональной образовательной программы

| Код и наименование компетенции | Этапы формирования компетенций и дисциплины (модули) и практики, при изучении/прохождении которых формируется данная компетенция | | |
|--------------------------------|--|----------|-------------|
| | начальный | основной | завершающий |
| ПК-3 | Административно-правовые режимы в сфере обеспечения безопасности в уголовно-исполнительной системе | | |

| | |
|------|--|
| | <p>Делопроизводство и режим секретности в подразделениях обеспечения безопасности в уголовно-исполнительной системе</p> <p>Оперативно-розыскная деятельность в уголовно-исполнительной системе</p> <p>Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей</p> <p>Пенитенциарная криминология</p> <p>Обеспечение безопасности в уголовно-исполнительной системе</p> <p>Организация охраны и конвоирования в уголовно-исполнительной системе</p> <p>Производственная правоприменительная практика</p> <p>Подготовка к процедуре защиты и защита выпускной квалификационной работы</p> |
| ПК-7 | <p>Административно-правовые режимы в сфере обеспечения безопасности в уголовно-исполнительной системе</p> <p>Пенитенциарная криминология</p> <p>Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей</p> <p>Производственная преддипломная практика</p> <p>Подготовка к процедуре защиты и защита выпускной квалификационной работы</p> |
| ПК-8 | <p>Противодействие посягательствам в уголовно-исполнительной системе, совершаемых при помощи информационно-телекоммуникационных сетей</p> <p>Пенитенциарная криминология</p> <p>Обеспечение безопасности в уголовно-исполнительной системе</p> <p>Организация охраны и конвоирования в уголовно-исполнительной системе</p> <p>Международное пенитенциарное право</p> <p>Предупреждение пенитенциарной преступности</p> <p>Производственная правоприменительная практика</p> <p>Подготовка к процедуре защиты и защита выпускной квалификационной работы</p> |

7.2. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

| Код компетенции / этап (указывается название этапа из п.7.1) | Показатели оценивания компетенций | Уровни сформированности компетенции | | |
|--|---|--|--|---|
| | | пороговый (удовлетворительный) | продвинутый (хорошо) | высокий (отлично) |
| ПК-3 / начальный, основной, завершающий | ПК-3.2 Осуществляет мероприятия по пресечению преступлений и правонарушений на режимной территории исправительных учреждений | Знать: общие: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: в типовых ситуациях: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: реализуемыми в типовых ситуациях: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ | Знать: общие и специальные: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: в типовых и стандартных ситуациях: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: реализуемыми в типовых и стандартных ситуациях: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ | Знать: общие, специальные и специфические: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности преступлений, совершаемых при помощи ИТС, необходимые для пресечения преступлений на режимной территории ИУ Уметь: в типовых, стандартных и нестандартных ситуациях: пресекать преступления, совершаемые при помощи ИТС, на режимной территории ИУ Владеть: реализуемыми в типовых, стандартных и нестандартных ситуациях: навыками осуществления мероприятий по пресечению преступлений, совершаемых при помощи ИТС, на режимной территории ИУ |
| ПК-7 / начальный, основной, завершающий | ПК-7.3 Применяет меры профилактического, воспитательного и иного | Знать: общие: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности | Знать: общие и специальные: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические | Знать: общие, специальные и специфические: нормы уголовного права, касающиеся преступлений, совершаемых при помощи ИТС, криминологические особенности |

| | | | | |
|--|--|--|--|--|
| | <p>воздействия, направленные на профилактику правонарушений и преступлений в отношении лиц, отбывающих уголовные наказания</p> | <p>преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: в типовых ситуациях: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: реализуемыми в типовых ситуациях: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС</p> | <p>особенности преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: в типовых и стандартных ситуациях: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: реализуемыми в типовых и стандартных ситуациях: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС</p> | <p>преступлений, совершаемых при помощи ИТС, необходимые для профилактики преступлений в отношении лиц, отбывающих уголовные наказания Уметь: в типовых, стандартных и нестандартных ситуациях: предупреждать преступления, совершаемые при помощи ИТС, в отношении лиц, отбывающих уголовные наказания Владеть: реализуемыми в типовых, стандартных и нестандартных ситуациях: навыками применения мер профилактического, воспитательного и иного воздействия для предупреждения преступлений, совершаемых при помощи ИТС</p> |
| <p>ПК-8 / начальный, основной, завершающий</p> | <p>ПК-8.2 Пресекает угрозы, возникающие в пенитенциарных правоотношениях</p> | <p>Знать: общие: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: в типовых ситуациях: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях</p> | <p>Знать: общие и специальные: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: в типовых и стандартных ситуациях: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях</p> | <p>Знать: общие, специальные и специфические: основные угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Уметь: в типовых, стандартных и нестандартных ситуациях: выявлять угрозы, связанные с преступлениями, совершаемыми при помощи ИТС, возникающие в пенитенциарных правоотношениях Владеть: реализуемыми в типовых, стандартных и нестандартных</p> |

| | | | | |
|--|--|---|---|---|
| | | Владеть: реализуемыми в типовых ситуациях: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях | Владеть: реализуемыми в типовых и стандартных ситуациях: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях | ситуациях: навыками пресечения угроз, связанных с преступлениями, совершаемыми при помощи ИТС, возникающих в пенитенциарных правоотношениях |
|--|--|---|---|---|

7.3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения основной профессиональной образовательной программы

Таблица 7.3 – Паспорт комплекта оценочных средств для текущего контроля успеваемости

| № п/п | Раздел (тема) дисциплины | Код контролируемой компетенции (или её части) | Технология формирования | Оценочные средства | | Описание шкал оценивания |
|-------|--|---|-----------------------------------|--|----------------------------------|--------------------------|
| | | | | наименование | №№ заданий | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Понятие и общая характеристика преступлений, связанных с использованием ИТС. | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады | 1-5 1-5 1-3 | Согласно табл. 7.2. |
| 2 | Общая характеристика компьютерных преступлений | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 6-10 6-10 4-6 1-5 | Согласно табл. 7.2. |
| 3 | Неправомерный доступ к компьютерной информации | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 11-20 11-15 7-9 6-10 | Согласно табл. 7.2. |
| 4 | Создание, использование и распространение вредоносных компьютерных программ | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 21-30 16-20 10-12 11-15 | Согласно табл. 7.2. |
| 5 | Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 31-40 21-25 13-15 16-20 | Согласно табл. 7.2. |
| 6 | Хищения с использованием новых информационных технологий | ПК-3; ПК-7; ПК-8 | Лекции, практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 41-50 26-30 16-18 21-25 | Согласно табл. 7.2. |
| 7 | Преступления против личности, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 51-60 31-35 19-21 26-30 | Согласно табл. 7.2. |

| № п/п | Раздел (тема) дисциплины | Код контролируемой компетенции (или её части) | Технология формирования | Оценочные средства | | Описание шкал оценивания |
|-------|---|---|---------------------------|--|-----------------------------------|--------------------------|
| | | | | наименование | №№ заданий | |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 8 | Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 61-70 36-40 22-24 31-35 | Согласно табл. 7.2. |
| 9 | Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 71-80 41-45 25-27 36-40 | Согласно табл. 7.2. |
| 10 | Преступления против общественной безопасности, совершаемые с применением информационных технологий | ПК-3; ПК-7; ПК-8 | Практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 81-90 46-50 28-30 41-45 | Согласно табл. 7.2. |
| 11 | Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | ПК-3; ПК-7; ПК-8 | Практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 91-95 51-55 31-33 46-50 | Согласно табл. 7.2. |
| 12 | Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | ПК-3; ПК-7; ПК-8 | Практические занятия, СРС | БТЗ, устный опрос, рефераты и доклады, кейс-задачи | 96-100 56-60 34-36 51-55 | Согласно табл. 7.2. |

Примеры типовых контрольных заданий для проведения текущего контроля успеваемости

Вопросы для устного опроса по разделу (теме) 1. «Понятие и общая характеристика преступлений, связанных с использованием ИТС»

1. Чем обусловлена актуальность изучения преступности в сфере высоких технологий в современный период?
2. Какие виды преступности относятся к высокотехнологичным?
3. Каково состояние киберпреступности и перспективы борьбы с ней?
4. В чём отличие распространённых представлений о личности киберпреступников от реальной действительности?
5. Чем обусловлено вовлечение в киберпреступность всё большего числа граждан?

Кейс-задача по разделу (теме) 9. «Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий»

Сотрудники отдела «К» УВД г. Энска А. и З. для повышения показателей раскрываемости компьютерных преступлений решили провести «оперативный эксперимент». Найдя в газете бесплатных объявлений объявление об оказании услуг «компьютерной помощи», они позвонили давшему его Р. и попросили его оказать помощь в установке на компьютер программного продукта Autodesk Alias Surface 2016 (стоимость лицензии на который составляла

1 млн. 145 тыс. рублей). Поначалу Р. отказался, однако после повторных звонков и обещания дополнительного вознаграждения всё же согласился. Требуемую программу он скачал из Интернета, там же он нашёл средства, позволяющие обойти технические ограничения, связанные с защитой авторских прав. Для установки программы был подготовлен компьютер, содержащий «чистую» ОС Windows. После того, как Р. закончил установку и «взломал» программу, оперативники задержали его. Р. было предъявлено обвинение в покушении на совершение нарушения авторских и смежных прав в особо крупном размере, неправомерный доступ к компьютерной информации, совершённый из корыстной заинтересованности и причинивший крупный ущерб, а также в использовании вредоносных компьютерных программ, предназначенных для нейтрализации средств защиты компьютерной информации, совершённое из корыстной заинтересованности и причинивший крупный ущерб. Правильна ли такая квалификация? Правомерны ли действия оперативников?

Темы рефератов и докладов по разделу (теме) 6. «Хищения с использованием новых информационных технологий»

1. Хищения с использованием банковских платёжных карт
2. История использования компьютеров для совершения хищений
3. Компьютерное вымогательство

Вопросы в тестовой форме по разделу (теме) 2. «Общая характеристика компьютерных преступлений»

Понятие доступа к информации включает в себя получение возможности:

- изменения информации
- получения информации
- использования информации
- удаления информации

Субъективная сторона неправомерного доступа к компьютерной информации может выражаться:

- в умысле по отношению к последствиям
- в неосторожности по отношению к последствиям
- в неосторожности по отношению к деянию
- в умысле по отношению к деянию

Неправомерный доступ к компьютерной информации не образует:

- временное ограничение доступа к информации легальных пользователей
- простое ознакомление с информацией
- уничтожение носителя компьютерной информации
- внесение изменений в информацию, не нарушающих её целостности

Крупным ущербом в статьях о преступлениях в сфере компьютерной информации признаётся ущерб, сумма которого превышает:

- 1 миллион рублей
- 250 тысяч рублей
- 1,5 миллиона рублей
- 100 тысяч рублей

Квалифицирующим признаком неправомерного доступа к компьютерной информации является совершение его:

- по экстремистским мотивам
- из хулиганских побуждений
- из низменных побуждений
- из корыстной заинтересованности

Вредоносность компьютерной программы определяется сочетанием:

- способностью к распространению в компьютерных сетях («червь»)
- характера совершаемых ей действий (уничтожение, модификация, блокирование информации и т.д.)
- способностью к саморазмножению («компьютерный вирус»)

- совершения действий без разрешения пользователя

Написание программы, предназначенной для повреждения компьютерного оборудования или иного нарушения работы компьютерной системы образует состав:

- неправомерного доступа к компьютерной информации
- создания, использования и распространения вредоносных компьютерных программ
- не охватывается составом ни одного из преступлений, предусмотренных гл. 28 УК

РФ

○ нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

Создание, использование и распространение вредоносных компьютерных программ окончено с момента:

- совершения любого из указанных действий
- фактического наступления последствий (например, уничтожения информации)
- начала работы программиста над созданием программы
- нет правильного ответа

Создание, использование и распространение вредоносных компьютерных программ (ч. 1 ст. 273 УК РФ) может быть совершено с виной в форме:

- преступной небрежности
- прямого умысла
- косвенного умысла
- преступного легкомыслия

Под правилами эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей в уголовно-правовой литературе понимается:

- всё перечисленное
- нормативные правовые акты, принимаемые органами государственной власти, например, санитарные нормы
- техническая документация на компьютерную технику
- локальные нормативные документы (правила внутреннего распорядка, должностные инструкции)

Осуществляемое через компьютерную сеть воздействие на подключённую к ней информационную систему, направленное на то, чтобы «перегрузить» её запросами (атака типа Denial of Service), не предполагающее возможности ознакомления с информацией, хранящейся в данной системе, образует состав:

- создания, использования и распространения вредоносных компьютерных программ
- не охватывается составом ни одного из преступлений, предусмотренных гл. 28 УК

РФ

○ нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

- неправомерного доступа к компьютерной информации

Использование для доступа в сеть Интернет случайно подсмотренных учётных данных (логина и пароля), принадлежащих другому пользователю, образует состав:

- неправомерного доступа к компьютерной информации
- создания, использования и распространения вредоносных компьютерных программ

○ нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей

- не охватывается составом ни одного из преступлений, предусмотренных гл. 28 УК

РФ

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей может быть совершено только путём активных действий виновного.

- да

○ нет

Полностью оценочные материалы и оценочные средства для проведения текущего контроля успеваемости представлены в УММ по дисциплине.

Типовые задания для проведения промежуточной аттестации обучающихся

Промежуточная аттестация по дисциплине проводится в форме зачетов и экзаменов. Зачеты и экзамены проводятся в виде бланкового и/или компьютерного тестирования.

Для тестирования используются контрольно-измерительные материалы (КИМ) – вопросы и задания в тестовой форме, составляющие банк тестовых заданий (БТЗ) по дисциплине, утвержденный в установленном в университете порядке.

Проверяемыми на промежуточной аттестации элементами содержания являются темы дисциплины, указанные в разделе 3 настоящей программы. Все темы дисциплины отражены в КИМ в равных долях (%). БТЗ включает в себя не менее 100 заданий и постоянно пополняется. БТЗ хранится на бумажном носителе в составе УММ и электронном виде в ЭИОС университета.

Для проверки *знаний* используются вопросы и задания в различных формах:

- закрытой (с выбором одного или нескольких правильных ответов),
- открытой (необходимо вписать правильный ответ),
- на установление правильной последовательности,
- на установление соответствия.

Умения, навыки и компетенции проверяются с помощью компетентностно-ориентированных задач (ситуационных, производственных или кейсового характера) и различного вида конструкторов.

Все задачи являются многоходовыми. Некоторые задачи, проверяющие уровень сформированности компетенций, являются многовариантными. Часть умений, навыков и компетенций прямо не отражена в формулировках задач, но они могут быть проявлены обучающимися при их решении.

В каждый вариант КИМ включаются задания по каждому проверяемому элементу содержания во всех перечисленных выше формах и разного уровня сложности. Такой формат КИМ позволяет объективно определить качество освоения обучающимися основных элементов содержания дисциплины и уровень сформированности компетенций.

Примеры типовых заданий для проведения промежуточной аттестации обучающихся

Задание в закрытой форме:

Компьютерная информация может быть представлена в форме:

- 1) электрических сигналов
- 2) магнитной записи
- 3) распечатки машинного кода
- 4) QR-кода

Задание в открытой форме:

Сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи — это _____.

Задание на установление правильной последовательности,

Установите последовательность этапов совершения преступления в сфере компьютерной информации:

- 1) формирование умысла
- 2) приготовление
- 3) покушение
- 4) оконченное преступление

Задание на установление соответствия:

Установите соответствие объектов преступления:

| | |
|------------------------------------|--------------------------------|
| А) Информационная безопасность | 1) Неправомерный доступ к КИ |
| Б) Общественная нравственность | 2) Распространение порнографии |
| В) Конституционные права и свободы | 3) Нарушение авторских прав |
| Г) Собственность | 4) Компьютерное мошенничество |

Компетентностно-ориентированная задача:

АО «Окно» разработало и продавало компьютерную игру. При установке игры на компьютер некоторые стандартные драйверы устройств заменялись на драйверы, разработанные АО «Окно», в результате была нарушена нормальная работа нескольких тысяч компьютеров. При установке программа тестировала компьютерное оборудование и программное обеспечение пользователя, сведения о которых при регистрации с помощью модема сообщались в АО «Окно». В документации к игре не сообщалось об этом. Квалифицируйте содеянное.

7.4 Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, регулируются следующими нормативными актами университета:

– положение П 02.016 «О балльно-рейтинговой системе оценивания результатов обучения по дисциплинам (модулям) и практикам при освоении обучающимися образовательных программ»;

– методические указания, используемые в образовательном процессе, указанные в списке литературы.

Для *текущего контроля* успеваемости по дисциплине в рамках действующей в университете балльно-рейтинговой системы применяется следующий порядок начисления баллов:

Таблица 7.4 – Порядок начисления баллов в рамках БРС

| Форма контроля | Минимальный балл | | Максимальный балл | |
|---|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 1. Понятие и общая характеристика преступлений, связанных с использованием ИТС. | 4 | Недостаточно полное и точное изложение материала. Правильное решение не менее 50-70% тестовых заданий | 8 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 2. Общая характеристика компьютерных преступлений | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |

| Форма контроля | Минимальный балл | | Максимальный балл | |
|---|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 3. Неправомерный доступ к компьютерной информации | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 4. Создание, использование и распространение вредоносных компьютерных программ | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| СРС | 8 | | 16 | |
| Итого | 18 | | 36 | |
| Посещаемость | 0 | | 14 | |
| Зачёт | 0 | | 60 | |
| Итого | 18 | | 100 | |
| Практическое занятие № 5. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и ИТС и посягательства на критическую информационную инфраструктуру | 1 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 2 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 6. Хищения с использованием новых информационных технологий | 1 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 2 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |

| Форма контроля | Минимальный балл | | Максимальный балл | |
|--|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 7. Преступления против личности, совершаемые с применением информационных технологий | 1 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 2 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 8. Преступления против здоровья населения и общественной нравственности, совершаемые с применением информационных технологий | 1 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 2 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 9. Преступления против конституционного строя и безопасности государства, совершаемые с применением информационных технологий | 1 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 2 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие № 10. Преступления против общественной безопасности, совершаемые с применением информационных технологий | 1 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 2 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| Практическое занятие №11. Частные вопросы организации деятельности сотрудников УИС по пресечению угроз и преступлений, связанных с использованием ИТС | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |

| Форма контроля | Минимальный балл | | Максимальный балл | |
|--|------------------|--|-------------------|---|
| | балл | примечание | балл | примечание |
| 1 | 2 | 3 | 4 | 5 |
| Практическое занятие № 12. Частные вопросы организации деятельности сотрудников УИС по профилактике преступлений, связанных с использованием ИТС | 2 | Недостаточно полное и точное изложение материала. Типовое решение задач. Правильное решение не менее 50-70% тестовых заданий | 4 | Свободное владение материалом, умение аргументировать, обобщать, делать выводы. Оригинальное решение задач. Правильное решение более 70% тестовых заданий |
| СРС | 8 | | 16 | |
| Итого | 18 | | 36 | |
| Посещаемость | 0 | | 14 | |
| Экзамен | 0 | | 60 | |
| Итого | 18 | | 100 | |

Для промежуточной аттестации обучающихся, проводимой в виде тестирования, используется следующая методика оценивания знаний, умений, навыков и (или) опыта деятельности. В каждом варианте КИМ – 16 заданий (15 вопросов и одна задача).

Каждый верный ответ оценивается следующим образом:

- задание в закрытой форме – 2 балла,
- задание в открытой форме – 2 балла,
- задание на установление правильной последовательности – 2 балла,
- задание на установление соответствия – 2 балла,
- решение компетентностно-ориентированной задачи – 6 баллов.

Максимальное количество баллов за тестирование – 36 баллов.

8 Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

8.1 Основная учебная литература

1. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 "Информационная безопасность", 400301 "Юриспруденция", 380301 "Экономика"] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. Текст: электронный.
2. Спеваков, Александр Геннадьевич. Информационная безопасность : учебное пособие : [для студентов, обучающихся по специальностям 100301 "Информационная безопасность", 400301 "Юриспруденция", 380301 "Экономика"] / А. Г. Спеваков, М. О. Таныгин, В. С. Панищев ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 196 с. Текст: непосредственный.
3. Криминология. Особенная часть [Текст] : учебник для академического бакалавриата : в 2 т. / Академия Генеральной прокуратуры РФ ; под общ. ред. ректора Академии Генеральной прокуратуры РФ, д-ра юрид. наук, проф. О. С. Капинус. - Москва : Юрайт, 2017. - ISBN 978-5-534-03382-3. - Текст : непосредственный. Т. 1. - 312 с.
4. Байбарин, Андрей Андреевич. Уголовное право России. Общая часть : учебное пособие : [для студентов и слушателей, обучающихся по программам специалистов, бакалавров и магистров, профессорско-преподавательского состава высших учебных заведений, научных работников] / А. А. Байбарин, А. А. Гребеньков, С. В. Шевелева ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 428 с. - Текст : электронный.

5. Байбарин, Андрей Андреевич. Уголовное право России. Общая часть : учебное пособие : [для студентов и слушателей, обучающихся по программам специалистов, бакалавров и магистров, профессорско-преподавательского состава высших учебных заведений, научных работников] / А. А. Байбарин, А. А. Гребеньков, С. В. Шевелева ; Юго-Зап. гос. ун-т. - Курск : ЮЗГУ, 2017. - 428 с. - Текст : непосредственный.

8.2 Дополнительная учебная литература

6. Байбарин, Андрей Андреевич. Практикум по курсу "Уголовное право" : учебное пособие / А. А. Байбарин, А. А. Гребеньков, М. Н. Урда ; Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования "Юго-Западный государственный университет". - Курск : ЮЗГУ, 2013. - 209 с. - Текст : электронный.
7. Уголовный кодекс Российской Федерации: федер. закон Рос. Федерации от 13.06.1996 № 63-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_10699/
8. Криминология. Особенная часть [Текст] : учебник для академического бакалавриата : в 2 т. / Академия Генеральной прокуратуры РФ ; под общ. ред. ректора Академии Генеральной прокуратуры РФ, д-ра юрид. наук, проф. О. С. Капинус. - Москва : Юрайт, 2017. - Текст : непосредственный. Т. 2. - 311 с.

8.3 Перечень методических указаний

1. Криминология : методические рекомендации по подготовке к практическим занятиям для студентов всех форм обучения направления подготовки 40.03.01 Юриспруденция / Юго-Зап. гос. ун-т ; сост.: М. И. Синяева, А. А. Байбарин, А. А. Гребеньков. - Курск : ЮЗГУ, 2017. - 35 с. - Текст: электронный.
2. Преступления в сфере высоких технологий : методические рекомендации по подготовке к практическим занятиям для студентов всех форм обучения направления подготовки 40.04.01 Юриспруденция / Юго-Зап. гос. ун-т ; сост.: М. И. Синяева, А. А. Байбарин, А. А. Гребеньков. - Курск : ЮЗГУ, 2017. - 33 с. - Текст: электронный.

8.4 Другие учебно-методические материалы

Отраслевые научные журналы в библиотеке университета

1. Административное право и процесс
2. Гражданское право
3. Конституционное и муниципальное право
4. Пробелы в российском законодательстве. Юридический журнал
5. Российская газета – ежедневная, без Российской газеты «Неделя»
6. Российская юстиция
7. Российский следователь
8. Российский судья
9. Уголовное право

9 Перечень ресурсов информационно-телекоммуникационной сети

Интернет

1. <http://www.cyberpol.ru/> – компьютерная преступность и борьба с ней.
2. <http://www.crime-research.ru/> – Центр исследования компьютерной преступности.
3. Электронная библиотека elibrary.ru.
4. Электронная библиотека cyberleninka.ru.
5. Сайт кафедры уголовного права: <http://www.swsu.ru/structura/up/uf/kup/index.php>.

10 Методические указания для обучающихся по освоению дисциплины

Программа дисциплины ориентирует студентов на всестороннее и системное изучение основных институтов уголовного права, его принципов и категорий, с помощью которых осмысливаются и решаются проблемы формирования и вывода специфических понятий, суждений, умозаключений, реализуется аргументационный процесс.

Важнейшим условием успешного изучения курса является систематическая самостоятельная работа с рекомендованной литературой. Студент должен овладеть понятийным аппаратом дисциплины, знать и понимать основные её категории.

На лекциях студенты должны работать с особым вниманием, стремясь вести подробный конспект, в котором должны быть отражены все важнейшие положения лекции. Если какой-то фрагмент лекции студент не успевает отразить в конспекте, целесообразно оставить место для дальнейшей доработки конспекта во время самостоятельной работы. Если какой-то положение лекции студентом не понято, следует обязательно задать преподавателю вопрос, желательно - в письменной форме, чтобы не прерывать ход лекции. В этом случае преподаватель сам найдёт удобное время, чтобы ответить на заданный вопрос.

При доработке конспекта лекций следует стремиться, чтобы в нем нашло отражение основное содержание изучаемой темы. Желательно, чтобы определения, примеры судебной практики и другие важные положения были ярко выделены. Не следует жалеть места для широких полей, где делаются соответствующие пометки.

Большое место в успешном овладении дисциплиной отводится семинарским занятиям. Семинар — это средство коллективного творческого раздумья, школа творческого мышления, столь необходимых будущему специалисту в его практической деятельности. Семинарское занятие требует от студента глубокого самостоятельного изучения рекомендованных источников и литературы по теме занятия.

Рекомендуется следующий алгоритм подготовки к семинару.

1. Внимательное изучение плана семинарского занятия, списка рекомендованных источников и литературы, методических рекомендаций преподавателя.
2. Изучение программы курса - с целью уяснения требований к объему и содержанию знаний по изучаемой теме.
3. Изучение и доработка конспекта лекций, прочитанных преподавателем по темам, выносимым на семинарское занятие.
4. Изучение вопросов темы по учебнику и основным рекомендованным пособиям.
5. Изучение дополнительной литературы.

При этом перед собой нужно иметь соответствующие статьи нормативных актов, которые неоднократно перечитывать. Рекомендуется вести конспект прочитанного, записывать научные определения, краткие формулировки, сопоставлять различные точки зрения. Следует продумать свой ответ по вопросам, составить краткий план ответа по каждому вопросу.

От студента не требуется изучения всей рекомендуемой литературы. Количество и объем изучаемых работ зависит от конкретной задачи: подготовки доклада, реферата, фиксированного выступления и т.д.

При ответе не следует повторять сказанное предыдущими выступающими, повторять самому, злоупотреблять временем другим способом. Пользоваться при ответе учебниками, лекциями, нормативными актами можно лишь с разрешения преподавателя.

Обязательно наличие изучаемых нормативных актов в последней редакции на практических занятиях, методических пособий кафедры по дисциплине. Рекомендуется выполнять творческие задания и решать задачи письменно в отдельной тетради. Рекомендуется самостоятельно решать задачи и тесты по дисциплине.

Перед консультацией, проводимой преподавателем, студент должен хорошо продумать и четко сформулировать вопросы по тем темам, которые оказались недостаточно усвоенными им в процессе самостоятельной работы.

11 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине, включая перечень программного обеспечения и информационных справочных систем (при необходимости)

1. СПС «Консультант+: Высшая школа».
2. СПС «ГАРАНТ-Студент».
3. Программа для ЭВМ «Программа для формирования бланков тестовых заданий», авторы: Калашникова А. А., Гребеньков А. А.
4. Программа для ЭВМ «Программа для осуществления тестового контроля знаний студентов», авторы: Калашникова А. А., Гребеньков А. А.

12 Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине

Лекционная аудитория; оснащенная учебной мебелью для обучающихся; стол, стул для преподавателя; доска; компьютерные классы университета (20-23 ПК) ОС Windows XP; программное обеспечение Microsoft Office; мультимедиа центр: ноутбук ASUS X50VL PMD-T2330/14``/1024Mb/160Gb/ сумка/проектор inFocus IN24+ (инвентарный номер 1043239); экран на штативе (инвентарный номер 434345) ; телевизор – Samsung PS51E537 (инвентарный номер 434349); ноутбук ASUS k501UQ 15,6``(FHD i3-6100U/4Gb/500Gb/GF940MX/noDVD/W10 (инвентарный номер 2341598); вычислительная сеть университета с локальными версиями СПС Консультант Плюс, Гарант; сеть Интернет.

13 Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

При обучении лиц с ограниченными возможностями здоровья учитываются их индивидуальные психофизические особенности. Обучение инвалидов осуществляется также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).

Для лиц с нарушением слуха возможно предоставление учебной информации в визуальной форме (краткий конспект лекций; тексты заданий, напечатанные увеличенным шрифтом), на аудиторных занятиях допускается присутствие ассистента, а также сурдопереводчиков и тифлосурдопереводчиков. Текущий контроль успеваемости осуществляется в письменной форме: обучающийся письменно отвечает на вопросы, письменно выполняет практические задания. Доклад (реферат) также может быть представлен в письменной форме, при этом требования к содержанию остаются теми же, а требования к качеству изложения материала (понятность, качество речи, взаимодействие с аудиторией и т. д.) заменяются на соответствующие требования, предъявляемые к письменным работам (качество оформления текста и списка литературы, грамотность, наличие иллюстрационных материалов и т.д.). Промежуточная аттестация для лиц с нарушениями слуха проводится в письменной форме, при этом используются общие критерии оценивания. При необходимости время подготовки к ответу может быть увеличено.

Для лиц с нарушением зрения допускается аудиальное предоставление информации, а также использование на аудиторных занятиях звукозаписывающих устройств (диктофонов и т.д.). Допускается присутствие на занятиях ассистента (помощника), оказывающего обучающимся необходимую техническую помощь. Текущий контроль успеваемости осуществляется в устной форме. При проведении промежуточной аттестации для лиц с нарушением зрения тестирование может быть заменено на устное собеседование по вопросам.

Для лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата, на аудиторных занятиях, а также при проведении процедур текущего контроля успеваемости и промежуточной аттестации могут быть предоставлены необходимые технические средства (персональный компьютер, ноутбук или другой гаджет); допускается присутствие ассистента (ассистентов), оказывающего обучающимся необходимую

техническую помощь (занять рабочее место, передвигаться по аудитории, прочитать задание, оформить ответ, общаться с преподавателем).

14. Лист дополнений и изменений, внесенных в рабочую программу

дисциплины

| Номер изменения | Номера страниц | | | | Всего страниц | Дата | Основание для изменения и подпись лица, проводившего изменения |
|--------------------|----------------|------------|----------------|-------|------------------|------|---|
| | Изменённых | Заменённых | Аннулированных | Новых | | | |
| | | | | | | | |