МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по выполнению лабораторных работ
по дисциплине «Технологии защиты информации в таможенных органах»
для студентов специальности
38.05.02 «Таможенное дело»
Направленность (профиль):
«Таможенный контроль»

Пятигорск
2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Дисциплина «Технологии защиты информации в таможенных органах» предназначена для студентов специальности 38.05.02 «Таможенное дело. Целью дисциплины является формирование у студентов навыков работы с поступающей информацией в таможенные органы и защиты ее от внешнего воздействия и утечки.

Задачами изучения дисциплины являются:

-изучение направлений политики ФТС России в области обеспечения информационной безопасности таможенных органов;

-формирование у студентов систематических знаний о каналах утечки информации в таможенных органах;

- изучение технологий защиты информации в таможенных органах;

МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОРГАНИЗАЦИИ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Практическое занятие является одной из форм проведения групповых занятий со студентами, имеющей своими целями более глубокое усвоение обучаемыми лекционного материала, развитие у них умения целенаправленной работы с научной, учебной литературой для самостоятельного добывания новых знаний, приобретение навыков публичных выступлений, ведения дискуссий и т.д. Практические занятия предполагают использование различных форм работы: обсуждение теоретических вопросов, решение задач, обсуждение докладов, анализ информации. Практические занятия проводятся с целью углубления и закрепления теоретических знаний, привития навыков анализа обстоятельств дела в конкретно заданной ситуации, что весьма важно для будущей практической деятельности. Они, являясь самостоятельной формой обучения студентов, углубляют знания, полученные на лекциях, способствуют самостоятельной работе с нормативным материалом, опубликованной практикой и литературой. Занятия проводятся в форме опроса студентов по теоретическим вопросам, обозначенным в планах, а также обсуждения вариантов решения практических заданий (ситуаций), которые были предложены в качестве подготовки к занятию. Готовясь к занятиям, студенты должны изучить:

-материалы лекции по предполагаемой теме, а также план практического (семинарского) занятия;

-соответствующие теме занятия положения нормативно-правовых актов;

-основные положения теории;

-материалы руководящих постановлений таможенных органов;

- рекомендованную в планах практических занятий базовую, а также дополнительную литературу и методические разработки для студентов, подготовленные кафедрой.

При подготовке к практическому занятию студент обязан, изучив действующее законодательство и рекомендованную литературу, письменно изложить в специальной тетради решение задач, заданных преподавателем. Их изложение не должно сводиться лишь к краткому ответу на вопрос. Необходимым признается такое обоснование вывода, которое в принципе является доказательным. Для решения таких задач соответственно требуется овладение техникой поиска предписаний, техникой субсумпции, то есть подведения менее общей посылки под общую, толкования закона и его конкретизации. Практические занятия строятся по следующей схеме:

- вначале преподаватель объявляет тему и задачи Практического занятия;

- производит опрос студентов по теоретическим вопросам, обозначенным в плане занятия, а также проверяет наличие у студентов письменных решений задач. Данные решения обсуждаются в форме дискуссии непосредственно на занятии;

- по окончании занятия подводятся итоги дискуссии и общие итоги.

Применительно к отдельным темам занятия, с учетом специфики обсуждаемой темы, указанная схема может корректироваться. Однако основе занятия, в любом случае, лежит решение практических ситуаций. Их количество определяется преподавателем с учетом всех особенностей изучаемой темы и масштабности ее проблемных вопросов. Отвечающий на семинаре студент обязан кратко изложить содержание практической ситуации.

ПЛАНЫ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема: 1 Классификаторы таможенной информации.

Цель: формирование у студентов знаний о видах таможенной информации.

В результате освоения темы обучающийся должен:

Знать: основные понятия классификации таможенной информации, цели разработки классификаторов таможенной информации.

Уметь: выявлять свойства системы классификации таможенной информации**.**

Актуальность темы: Решение проблемы классификации и кодирования таможенной информации является обязательной самостоятельной частью процесса осуществления таможенных операций, реализованной в любом прикладном программном обеспечении информационных таможенных технологий.

Теоретическая часть: Таможенная информация существует в двух формах: в форме таможенных показателей и документов. В подразделениях Федеральной таможенной службы России активно используется больше 250 различных автоматизированных систем. В зависимости от назначения и решаемых задач каждая система использует тот или иной набор классификаторов (справочников) и кодификаторов, которые входят в состав нормативно-справочной информации.

Классификатор — документ, с помощью которого осуществляется формализованное описание таможенной информации, содержащей наименования объектов, наименования классификационных группировок и их кодовые обозначения.

Структурной единицей таможенной информации является показатель. Он представляет собой контролируемый параметр таможенного объекта и состоит из совокупности реквизитов. Реквизит имеет законченное смысловое содержание и потребительскую значимость. Реквизит — это логически неделимый элемент показателя, отражающий определенные свойства объекта или процесса. Реквизит нельзя разбить на более мелкие единицы без разрушения его смысла. Каждый показатель состоит из одного реквизита-основания и одного или нескольких реквизитов-признаков. Реквизит-признак характеризует смысловое содержание показателя и определяет его наименование. Реквизит-основание характеризует, как правило, количественное значение показателя.

Вопросы и задания:

Лабораторное занятие № 1

Вопросы для обсуждения: Основные понятия классификации таможенной информации. Цели разработки классификаторов таможенной информации.

Лабораторное занятие № 2

Задания: Проанализировать свойства системы классификации таможенной информации.

Список литературы, рекомендуемый к использованию по данной теме:

1. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов : монография / Ю. И. Сомов, Э. П. Купринов, С. В. Курихин, Л. Д. Зайцева. — Москва : Российская таможенная академия, 2014. — 186 с. — ISBN 978-5-9590-0823-9. — Текст : электронный // Электронно-

библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69852.html. — Режим доступа: для авторизир. Пользователей
2. Федоров, В. В. Информационные технологии и защита информации в правоохранительной деятельности таможенных органов Российской Федерации : монография / В. В. Федоров. — Москва : Российская таможенная академия, 2014. — 180 с. — ISBN 978-5-9590-0797-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69725.html. — Режим доступа: для авторизир. Пользователей
3. Афонин, П. Н. Информационная безопасность в таможенном деле : учебник / П. Н. Афонин, Д. Н. Афонин, А. И. Краснова. — Санкт-Петербург : Троицкий мост, 2016. — 512 с. — ISBN 978-5-4377-0039-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/40859.html— Режим доступа: для авторизир. пользователей

Тема: 2 Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов.

Цель: формирование у студентов знаний о системе правового обеспечения защиты информации в таможенных органах России.

В результате освоения темы обучающийся должен:

Знать: систему правового обеспечения защиты информации в таможенных органах России.

Уметь: проводить анализ направлений политики ФТС России в области обеспечения информационной безопасности таможенных органов. проанализировать этапы создания и развития электронных таможен.

Актуальность темы: Деятельность Федеральной таможенной службы направлена на обеспечение экономической безопасности Российской Федерации. В процессе выполнения своего функционала, а именно действий, направленных на выполнение таможенного администрирования, представители таможенных органов получают доступ к таким сведениям, как конфиденциальные данные участников ВЭД, персональные данные физических лиц и сведениям, относящимся к государственной тайне.

Теоретическая часть: С развитием информационно-коммуникационных технологий безусловно происходит усовершенствование и усложнение угроз, а это в свою очередь заставляет совершенствовать системы, выполняющие функции по защите информации. Из-за этого перед таможенной службой ставится одна из основополагающих задач – гарантия конфиденциальности, доступности и целостности информации. При проектировании системы безопасности необходимо учитывать все существующие и предполагаемые угрозы и уязвимости. Для выполнения данной задачи необходимо осуществлять непрерывный контроль, причем он должен учитывать весь жизненный цикл информации: от появления – до потери актуальности или полного уничтожения. Правильно подобранная концепция управления информационной безопасностью позволяет снизить риски до приемлемых параметров. В обширном смысле под безопасностью понимается защита законных интересов объектов от различных видов угроз. На сегодняшний день информация – один из самых важных и ценных активов любой организации. Защиту информации по определенным параметрам можно условно можно разделить на две составляющие.

Первая – собственно защита самой информации, то есть содержательной части, смысловой нагрузки. Вторая – защита информации от внешних воздействий, сюда включено и её полное уничтожение. Другими словами, защищать нужно не только саму информацию, но также информационные системы, помещения, в которых данные ресурсы расположены, сотрудников, имеющих доступ к информации с ограниченным доступом.

Для этого используют следующие виды контроля: административный, логический и физический контроль. Административный контроль подразумевает набор локальных актов, правил и стандартов. Логический контроль или иначе технические средства контроля включает в себя защиту и контроль доступа к ресурсам, программное обеспечение, парольную защиту. Все эти мероприятия направлены на нормальное функционирование организации, внутреннюю безопасность.

Таким образом, действия, направленные на повышение уровня информационной безопасности, отвечают за нахождение, оценивание и минимизацию рисков влияния на информационные технологии и системы. Нормативно вопросы выполнения положений информационной безопасности в Российской Федерации закрепляются Международными договорами РФ, Конституцией РФ, Федеральными законами РФ, Указами Президента РФ, Постановлениями Правительства РФ и иными правовыми актами. Существует еще ряд законов, действие которых непосредственно не направленно на регулирование отношений в области информационной безопасности, но включающие в себя отдельные статьи, посвященные информации, ее защите. Одним из основных документов, посвященных вопросам безопасности информации является «Доктрина информационной безопасности Российской Федерации».

В этом документе описаны способы, объекты, а также процедуры, необходимые для обеспечения информационной безопасности. Однако, следует отметить, что изучаемый вопрос безопасности информации данным набором правовых актов не ограничивается. Защита информации требует системного и комплексного подхода, так как представляет собой сложный комплекс мероприятий, подразумевающих большой круг различных процедур и явлений, связанных с противодействием угрозам безопасности. Информационные комплексы, используемые таможенной службой, представляют собой сложные системы, объединяющие центральные и региональные базы данных и телекоммуникационные сети, гарантирующие качественное выполнение всех видов деятельности таможенной службы. Данные системы постоянно модернизируются и развиваются вместе с развитием таможенных органов. Развитие систем наглядно прослеживается в процессе интеграции взаимодействия с информационными системами участников ВЭД, около таможенных структур, государственных органов. Защита информации в таможенных органах разделяется два направления. С одной стороны, мероприятия по информационной безопасности таможенных органов выполняется для достижения национальной безопасности. С другой, определенные процедуры направлены для обеспечения своего естественного функционирования. Острота проблемы отражена в приказе, которым утверждена «Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года».

Данная Концепция определяет штатную структуру и основные задачи. Необходимо также указать, что, опираясь на Стратегию национальной безопасности и Доктрину информационной безопасности в Концепции уделено внимание лишь защите информации в целях защиты национальных интересов, при этом упущенным остается уровень внутренней безопасности. В положении «Стратегии развития таможенной службы Российской Федерации до 2020 года» в разделе 8 «Совершенствование информационно-технического обеспечения» установлено, что повышение уровня безопасности информационных ресурсов, увеличение форм и способов по обеспечению защиты информации, в том числе при организации защищенного обмена информацией с федеральными органами исполнительной власти – это одна из главных задач, получение ответа на которую будет способствовать совершенствованию информационно-технического обеспечения деятельности таможенных органов.

Лабораторное занятие № 3

Вопросы для обсуждения: Система правового обеспечения защиты информации в таможенных органах России.

Лабораторное занятие № 4

Вопросы для обсуждения: Политика ФТС России в области обеспечения информационной безопасности таможенных органов. проанализировать этапы создания и развития электронных таможен.

Список литературы, рекомендуемый к использованию по данной теме:

1. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов : монография / Ю. И. Сомов, Э. П. Купринов, С. В. Курихин, Л. Д. Зайцева. — Москва : Российская таможенная академия, 2014. — 186 с. — ISBN 978-5-9590-0823-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69852.html. — Режим доступа: для авторизир. Пользователей
2. Федоров, В. В. Информационные технологии и защита информации в правоохранительной деятельности таможенных органов Российской Федерации : монография / В. В. Федоров. — Москва : Российская таможенная академия, 2014. — 180 с. — ISBN 978-5-9590-0797-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69725.html. — Режим доступа: для авторизир. Пользователей
3. Афонин, П. Н. Информационная безопасность в таможенном деле : учебник / П. Н. Афонин, Д. Н. Афонин, А. И. Краснова. — Санкт-Петербург : Троицкий мост, 2016. — 512 с. — ISBN 978-5-4377-0039-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/40859.html— Режим доступа: для авторизир. пользователей

Тема: 3 Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы обеспечения информационной безопасности ЕАИС. Средства управления защитой информации в таможенных органах.

Цель: освоение обучаемыми знаний о порядке обеспечения информационной безопасности в таможенных органах.

В результате освоения темы обучающийся должен:

Знать: понятие и структура информационной безопасности, характер и формы угроз, каналы утечки информации в таможенных органах, формы обеспечения информационной безопасности ЕАИС.

Уметь: анализировать средства управления защитой информации в таможенных органах. особенности организации деятельности электронной таможни.

Актуальность темы: С развитием информационно-коммуникационных технологий безусловно происходит усовершенствование и усложнение угроз, а это в свою очередь заставляет совершенствовать системы, выполняющие функции по защите информации. Из-за этого перед таможенной службой ставится одна из основополагающих задач – гарантия конфиденциальности, доступности и целостности информации.

Теоретическая часть: Информационные комплексы, используемые таможенной службой, представляют собой сложные системы, объединяющие центральные и региональные базы данных и телекоммуникационные сети, гарантирующие качественное выполнение всех видов деятельности таможенной службы. Данные системы постоянно модернизируются и развиваются вместе с развитием таможенных органов. Развитие систем наглядно прослеживается в процессе интеграции взаимодействия с информационными системами участников ВЭД, около таможенных структур, государственных органов. Защита информации в таможенных органах разделяется два направления. С одной стороны, мероприятия по информационной безопасности таможенных органов выполняется для достижения национальной безопасности. С другой, определенные процедуры направлены для обеспечения своего естественного функционирования. Острота проблемы отражена в приказе, которым утверждена

«Концепция обеспечения информационной безопасности таможенных органов РФ на период до 2020 года».

Данная Концепция определяет штатную структуру и основные задачи. Необходимо также указать, что, опираясь на Стратегию национальной безопасности и Доктрину информационной безопасности в Концепции уделено внимание лишь защите информации в целях защиты национальных интересов, при этом упущенным остается уровень внутренней безопасности. В положении «Стратегии развития таможенной службы Российской Федерации до 2020 года» в разделе 8 «Совершенствование информационно-технического обеспечения» установлено, что повышение уровня безопасности информационных ресурсов, увеличение форм и способов по обеспечению защиты информации, в том числе при организации защищенного обмена информацией с федеральными органами исполнительной власти – это одна из главных задач, получение ответа на которую будет способствовать совершенствованию информационно-технического обеспечения деятельности таможенных органов.

Взаимодействие в сфере обмена информацией между ФТС России и иными органами власти разделяется на три основных направления. Первое направление – обмен информацией, проводимый в рамках протоколов об информационном взаимодействии. Этот вариант предполагает обмен юридически значимыми документами в электронном виде. В данном обмене участвуют также сведения, содержащие информацию с ограниченным доступом, но не отнесенные к государственной тайне. Второе – обмен информацией в рамках реализации норм закона о предоставлении государственных и муниципальных услуг служит для исполнения и контроля электронных регламентов. Третий вид обмена направлен на выполнение функций контроля, совершаемых таможенными органами.

Вопросы и задания:

Лабораторное занятие № 5

Вопросы для обсуждения: Понятие и структура информационной безопасности. Характер и формы угроз.

Лабораторное занятие № 6

Вопросы для обсуждения: Каналы утечки информации в таможенных органах. Формы обеспечения информационной безопасности ЕАИС.

Задания: Проанализировать средства управления защитой информации в таможенных органах. особенности организации деятельности электронной таможни.

Список литературы, рекомендуемый к использованию по данной теме:

1. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов : монография / Ю. И. Сомов, Э. П. Купринов, С. В. Курихин, Л. Д. Зайцева. — Москва : Российская таможенная академия, 2014. — 186 с. — ISBN 978-5-9590-0823-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69852.html. — Режим доступа: для авторизир. Пользователей
2. Федоров, В. В. Информационные технологии и защита информации в правоохранительной деятельности таможенных органов Российской Федерации : монография / В. В. Федоров. — Москва : Российская таможенная академия, 2014. — 180 с. — ISBN 978-5-9590-0797-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69725.html. — Режим доступа: для авторизир. Пользователей
3. Афонин, П. Н. Информационная безопасность в таможенном деле : учебник / П. Н. Афонин, Д. Н. Афонин, А. И. Краснова. — Санкт-Петербург : Троицкий мост, 2016. — 512 с. — ISBN 978-5-4377-0039-6. — Текст : электронный // Электронно-библиотечная

система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/40859.html— Режим доступа: для авторизир. пользователей

Тема: 4 Модель нарушителя информационной безопасности ЕАИС. Обеспечение антивирусной защиты информации. Реализация правового режима коммерческой тайны в таможенной деятельности.

Цель: получений знаний о нарушениях порядка защиты информации в таможенных органах.

В результате освоения темы обучающийся должен:

Знать: модель нарушителя информационной безопасности ЕАИС, особенности реализации правового режима коммерческой тайны в таможенной деятельности.

Уметь: обеспечивать антивирусную защиту информации.

Актуальность темы: Уже сегодня таможенной службой установлены договоренности с различными органами исполнительной власти и иными ведомствами. Обмен информацией с одними уже налажен и активно используется, с другими продолжаются работы по определению технических условий, описывающих процесс информационного взаимодействия для дальнейшей практической реализации обмена в соответствии с заключенными соглашениями. Одним из динамичных информационных обменов ФТС России осуществляет с Федеральной налоговой службой России

Теоретическая часть: Электронный информационный обмен между ведомствами осуществляется несколькими способами. Среди них, с применением защищенных выделенных каналов связи, электронной почты, а также съемных носителей информации. Центральное информационно-техническое таможенное управление в основном весь информационный обмен, происходящий на федеральном уровне, пропускает через себя. ФТС России выполняет все возложенные на нее обязательства по передаче информации федеральным органам исполнительной власти, которые предусмотрены соглашениями об информационном обмене. Тем не менее, существует ряд проблемных точек, на которых необходимо заострить внимание. 1. Отсутствие необходимого уровня развития отдельных систем органов исполнительной власти влечет за собой отсутствие единых требований к форматам, предоставляемой информации, способов ее передачи, регламентов взаимодействия. 2. Отдельные органы власти не готовы к предоставлению информации, с требуемой степенью актуальности, необходимую для исполнения ФТС своих функций. 3. Административные преграды, повышенные сроки утверждения с органами исполнительной власти технических условий, необходимых для проведения информационного обмена в рамках реализации соглашений об информационном взаимодействии. Таким образом, существует необходимость совершенствования механизмов межведомственного взаимодействия в целях повышения качества и эффективности при реализации функций, закрепленных за таможенными органами Российской Федерации. Для государственных структур задача защиты информации всегда являлась актуальной. С совершенствованием механизмов организации кибератак она вышла на принципиально новый уровень. Отсюда следует задача по защите информации и информационных систем от вирусных атак. В целях качественного построения системы антивирусной защиты действует приказ ФТС России от 28.05.2007 № 660 «О системе антивирусной защиты информации в таможенных органах Российской Федерации». Данным приказом введено в действие положение об антивирусной защите в таможенных органах. Здесь подробно описана структура системы по борьбе с вирусной активностью, порядок оснащения программными и аппаратными средствами защиты таможенных органов, а также схема эксплуатации данной системы и распределение обязанностей между сотрудниками. Данная система позволяет предотвращать факты заражения компьютерными вирусами, а также нежелательными программами вычислительных ресурсов автоматизированных систем таможенных органов. Система антивирусной защиты включает несколько участников. Главное управление информационных

технологий ФТС России – отвечает за общее управление. Сюда входят функции по проработке документальной стороны защиты информации, проектированию процедур по защите, оснащению структурных подразделений, мониторинг функционирования систем защиты, постановка и сопровождение эксплуатации системы, а также организация проверок по выявленным случаям заражения систем обработки информации. Руководитель службы, отвечающей за формы и средства информационной безопасности и технической защиты, осуществляет управление мероприятиями, направленными на информационную защиту в таможенном органе. Руководители структурных подразделений несут персональную ответственность за выполнение требований информационной безопасности подчиненными должностными лицами. Выполнение функций по координации антивирусной защиты в структурных подразделениях таможенных органов проводит назначенное приказом должностное лицо – администратор системы защиты. После назначения на роль администратора дополнительные обязанности, закрепленные за должностным лицом, должны быть отражены в должностной инструкции. Администратор системы несет персональную ответственность за установку и настройку, эксплуатацию средств защиты информации, а также за обновление лицензионных ключей и баз данных средств антивирусной защиты.

Вопросы и задания:

Лабораторное занятие № 7

Вопросы для обсуждения: Модель нарушителя информационной безопасности ЕАИС.

Лабораторное занятие № 8

Вопросы для обсуждения: Обеспечение антивирусной защиты информации. Реализация правового режима коммерческой тайны в таможенной деятельности.

Список литературы, рекомендуемый к использованию по данной теме:

1. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов : монография / Ю. И. Сомов, Э. П. Купринов, С. В. Курихин, Л. Д. Зайцева. — Москва : Российская таможенная академия, 2014. — 186 с. — ISBN 978-5-9590-0823-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69852.html. — Режим доступа: для авторизир. Пользователей
2. Федоров, В. В. Информационные технологии и защита информации в правоохранительной деятельности таможенных органов Российской Федерации : монография / В. В. Федоров. — Москва : Российская таможенная академия, 2014. — 180 с. — ISBN 978-5-9590-0797-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69725.html. — Режим доступа: для авторизир. Пользователей
3. Афонин, П. Н. Информационная безопасность в таможенном деле : учебник / П. Н. Афонин, Д. Н. Афонин, А. И. Краснова. — Санкт-Петербург : Троицкий мост, 2016. — 512 с. — ISBN 978-5-4377-0039-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/40859.html— Режим доступа: для авторизир. пользователей

Тема: 5 Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности.

Цель: привитие навыков у студентов умений классификаций и расследования дел о преступлениях в сфере информационной безопасности.

В результате освоения темы обучающийся должен:

Знать: особенности классификаций дел о преступлениях в сфере информационной безопасности, особенности расследования дел о преступлениях в сфере информационной безопасности.

Уметь: классифицировать дела о преступлениях в сфере информационной безопасности.

Актуальность темы: В последние десятилетия информация стала неотъемлемой частью таких важных сфер деятельности государства, как связь, транспорт, энергетика, добыча и хранение стратегически важных ресурсов, банковская система, системы жизнеобеспечения населения, оборона, структуры обеспечения устойчивой работы государственного аппарата, что закономерно привело к проникновению преступности в сферу компьютерной информации. Возможность совершать противоправные действия, находясь на значительном удалении от места совершения преступления, оставаясь при этом не только не замеченным, но и не обнаруженным впоследствии привлекает все больше преступников.

Теоретическая часть: Под преступлениями в сфере компьютерной информации мы понимаем виновно совершенное общественно опасное деяние, совершенное в сфере информационных технологий путем воздействия на сведения (сообщения, данные), представленные в электронно-цифровой форме, независимо от средств их хранения, обработки и передачи. Традиционно, к числу преступлений рассматриваемой категории относят, прежде всего, составы 28 главы Уголовного кодекса. Однако они часто являются лишь способом совершения других преступлений. Так, по статистике МВД1 о состоянии преступности за 2018 год, 8,4% всех зарегистрированных преступлений за отчетный период совершены с использованием компьютерных и телекоммуникационных технологий.

Общее количество зарегистрированных преступлений в сфере высоких технологий с каждым годом возрастает, при этом раскрываемость преступлений остается на крайне низком уровне. По данным МВД на 2017 год зарегистрировано 90587 таких преступлений, из них раскрыто 20424. За 2018 год зарегистрировано уже 156307 преступлений, из них раскрыто только 38773. Основными причинами, на наш взгляд, является недостаточность специальных знаний следователей, отсутствие видимых материальных следов преступлений, а так же обезличенный характер информации, не позволяющий указать на преступника. В сложившейся ситуации, особое внимание правоохранительных органов должно быть сосредоточено на уточнении и повышении эффективности применения частной методики расследования преступлений в сфере компьютерной информации. Одной из наиболее значимых структурных частей в системе частной криминалистической методики обоснованно считают криминалистическую характеристику преступления. Рассмотрим некоторые элементы, входящие в вышеназванную характеристику. Криминалистическая характеристика личности преступника дается в научной литературе достаточно подробно, однако, она не в полной мере соответствуют действительности, поскольку статистика исходит только из тех случаев, которые удалось раскрыть [1; 2]. Достаточно высокая степень сложности современной компьютерной техники и программных средств ее защиты, предполагает высокий образовательный уровень преступников и нетривиальное мышление. К примеру, если рассматривать преступления против безопасности критической инфраструктуры Российской Федерации, то в силу высокой степени защиты объектов, круг профессионалов соответствующего класса даже на сегодняшний день не велик. Следует особо обратить внимание, что субъектом данного состава в соответствии с положениями уголовного закона может выступать иностранный гражданин, совершивший преступление вне пределов Российской Федерации. Обобщая информацию из различных источников, можно предположить, что типичный преступник - молодой человек, имеющий среднее - специальное или высшее образование, преимущественно техническое. Поскольку под данное описание на сегодняшний день попадет каждый второй представитель молодого поколения, считаем разумным обращать

большее внимание на психологические аспекты характеристики личности. Будущий преступник, скорее всего, начал увлекаться программированием еще в школьные годы. В этом возрасте молодые люди, имея ряд комплексов и проблемы с общением или столкнувшись с непониманием со стороны окружающих, активно ищут пути самовыражения в виртуальном пространстве. Постепенно происходит психологическая трансформация, выраженная в подмене реальности, компьютерная сеть становится средой обитания. Таким образом, мотивами совершения противоправных действий в информационном пространстве могут быть и такие, как месть, желание самоутвердиться, сделать вызов обществу и т.п.

Вопросы и задания:

Вопросы и задания:

Лабораторное занятие № 9

Вопросы для обсуждения: Особенности классификаций дел о преступлениях в сфере информационной безопасности. Особенности расследования дел о преступлениях в сфере информационной безопасности.

Список литературы, рекомендуемый к использованию по данной теме:

1. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов : монография / Ю. И. Сомов, Э. П. Купринов, С. В. Курихин, Л. Д. Зайцева. — Москва : Российская таможенная академия, 2014. — 186 с. — ISBN 978-5-9590-0823-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69852.html. — Режим доступа: для авторизир. Пользователей
2. Федоров, В. В. Информационные технологии и защита информации в правоохранительной деятельности таможенных органов Российской Федерации : монография / В. В. Федоров. — Москва : Российская таможенная академия, 2014. — 180 с. — ISBN 978-5-9590-0797-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69725.html. — Режим доступа: для авторизир. Пользователей
3. Афонин, П. Н. Информационная безопасность в таможенном деле : учебник / П. Н. Афонин, Д. Н. Афонин, А. И. Краснова. — Санкт-Петербург : Троицкий мост, 2016. — 512 с. — ISBN 978-5-4377-0039-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/40859.html— Режим доступа: для авторизир. пользователей

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

Методические указания

по организации и проведению самостоятельной работы
по дисциплине «Технологии защиты информации в таможенных органах»
для студентов специальности
38.05.02 «Таможенное дело»
Направленность (профиль):
«Таможенный контроль»

Пятигорск
2024

СОДЕРЖАНИЕ

Введение

Дисциплина «Технологии защиты информации в таможенных органах» предназначена для студентов специальности 38.05.02 «Таможенное дело. Целью дисциплины является формирование у студентов навыков работы с поступающей информацией в таможенные органы и защиты ее от внешнего воздействия и утечки.

Задачи:

- изучение направлений политики ФТС России в области обеспечения информационной безопасности таможенных органов;
- формирование у студентов систематических знаний о каналах утечки информации в таможенных органах;
- изучение технологий защиты информации в таможенных органах;

2. Общая характеристика самостоятельной работы

Обучение в вузе состоит из двух равнозначных по объему и взаимовлиянию частей – процесса обучения и процесса самообучения. Процесс самообучения или самостоятельная работа студентов (далее СРС) вуза, являясь важным видом учебной и научной деятельности студента, может осуществляться при определенных условиях, организация которых способствует повышению качественного уровня самостоятельной деятельности обучающихся по приобретению профессиональных компетенций.

Цель организации и осуществления СРС совпадает с целью обучения студента– подготовкой специалиста.

Задачи организации СРС:

развитие у студентов навыков самостоятельной учебной работы и формирование потребностей в самообразовании;

освоение содержания дисциплины в ходе аудиторных занятий;

освоение содержания дисциплин во внеаудиторное время в рамках тем, выносимых на самостоятельное изучение студента;

использование материала, собранного и полученного в ходе самостоятельных занятий, на семинарах при написании курсовых и дипломной работ, для эффективной подготовки к итоговым зачетам и экзаменам.

Самостоятельная работа студентов по дисциплине «Технологии защиты информации в таможенных органах» предусматривает следующие виды: самостоятельное изучение литературы; подготовка к практическому занятию.

Цели самостоятельной работы:

- овладение новыми знаниями, а также методами их получения;
- развитие умения приобретения научных знаний путем личного поиска и переработки информации;
- сбор и систематизация знаний по конкретной теме или проблеме

Задачи самостоятельной работы:

- формирование умений использовать справочную документацию и специальную литературу;
- развитие познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности.
- систематизация и закрепление полученных теоретических знаний и практических умений студентов;
- углубление и расширение теоретических знаний;
- формирование самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации
- развитие исследовательских умений.

3 План-график выполнения самостоятельной работы

Код оцениваемой компетенции, индикатора (ов)	Этап формирования компетенции (№ темы) *(в соответствии с рабочей программой дисциплины)*	Средства и технологии оценки	Вид контроля, аттестация *(текущий/промежуточный)*	Тип контроля *(устный, письменный или с использованием технических средств)*	Наименование оценочного средства
ИД-1$_{ОПК-2}$ ИД-2$_{ОПК-2}$ ИД-3$_{ОПК-2}$ ИД-4$_{ОПК-2}$ ИД-1$_{ПК-9}$	1-5	Собеседование	Текущий	Устный	Вопросы для собеседования
ИД-1$_{ОПК-2}$ ИД-2$_{ОПК-2}$ ИД-3$_{ОПК-2}$ ИД-4$_{ОПК-2}$ ИД-1$_{ПК-9}$	1,3	Собеседование	Текущий	Устный	Комплект типовых задач (заданий)

4. Методические рекомендации по изучению теоретического материала

Тема: 1 Классификаторы таможенной информации.

Цель: формирование у студентов знаний о видах таможенной информации.

Форма контроля СРС: индивидуальное собеседование, проверка текста конспекта.

Вопросы для собеседования: Основные понятия классификации таможенной информации. Цели разработки классификаторов таможенной информации.

Задания: Проанализировать свойства системы классификации таможенной информации.

Требования к представлению и оформлению результатов СРС: ответы на вопросы, выносимые на самостоятельное изучение (собеседование), изучаются студентом и конспектируются в тетради. Для подготовки к данному оценочному мероприятию необходимо до 15 часов самостоятельной работы. Студенту необходимо выбрать необходимые источники информации, позволяющие раскрыть предложенные вопросы и составить краткий конспект своего ответа.

При подготовке к ответу студенту предоставляется право пользования текстом конспекта составленного самостоятельно при подготовке к практическому занятию.

При проверке задания, оцениваются умение анализировать ситуацию, умение затребовать дополнительную информацию, необходимую для уточнения ответа; умение моделировать решения в соответствии с заданием, умение принять правильное решение на основе анализа ситуации. Навыки четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения; навык критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки.

Тема: 2 Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов.

Цель: формирование у студентов знаний о системе правового обеспечения защиты информации в таможенных органах России.

Форма контроля СРС: индивидуальное собеседование, проверка текста конспекта.

Вопросы для собеседования: Система правового обеспечения защиты информации в таможенных органах России. Политика ФТС России в области обеспечения информационной безопасности таможенных органов.

Требования к представлению и оформлению результатов СРС: ответы на вопросы, выносимые на самостоятельное изучение (собеседование), изучаются студентом и конспектируются в тетради. Для подготовки к данному оценочному мероприятию необходимо до 15 часов самостоятельной работы. Студенту необходимо выбрать необходимые источники информации, позволяющие раскрыть предложенные вопросы и составить краткий конспект своего ответа.

При подготовке к ответу студенту предоставляется право пользования текстом конспекта составленного самостоятельно при подготовке к практическому занятию.

При проверке задания, оцениваются умение анализировать ситуацию, умение затребовать дополнительную информацию, необходимую для уточнения ответа; умение моделировать решения в соответствии с заданием, умение принять правильное решение на основе анализа ситуации. Навыки четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения; навык критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки.

Тема: 3 Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы обеспечения информационной безопасности ЕАИС. Средства управления защитой информации в таможенных органах.

Цель: освоение обучаемыми знаний о порядке обеспечения информационной безопасности в таможенных органах.

Форма контроля СРС: индивидуальное собеседование, проверка текста конспекта.

Вопросы для собеседования: Понятие и структура информационной безопасности. Характер и формы угроз. Каналы утечки информации в таможенных органах. Формы обеспечения информационной безопасности ЕАИС.

Задания: Проанализировать средства управления защитой информации в таможенных органах. особенности организации деятельности электронной таможни.

Требования к представлению и оформлению результатов СРС: ответы на вопросы, выносимые на самостоятельное изучение (собеседование), изучаются студентом и конспектируются в тетради. Для подготовки к данному оценочному мероприятию необходимо до 15 часов самостоятельной работы. Студенту необходимо выбрать необходимые источники информации, позволяющие раскрыть предложенные вопросы и составить краткий конспект своего ответа.

При подготовке к ответу студенту предоставляется право пользования текстом конспекта составленного самостоятельно при подготовке к практическому занятию.

При проверке задания, оцениваются умение анализировать ситуацию, умение затребовать дополнительную информацию, необходимую для уточнения ответа; умение моделировать решения в соответствии с заданием, умение принять правильное решение на основе анализа ситуации. Навыки четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения; навык критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки.

Тема: 4 Модель нарушителя информационной безопасности ЕАИС. Обеспечение антивирусной защиты информации. Реализация правового режима коммерческой тайны в таможенной деятельности.

Цель: получений знаний о нарушениях порядка защиты информации в таможенных органах.

Форма контроля СРС: индивидуальное собеседование, проверка текста конспекта.

Вопросы для собеседования: Модель нарушителя информационной безопасности ЕАИС. Обеспечение антивирусной защиты информации. Реализация правового режима коммерческой тайны в таможенной деятельности.

Требования к представлению и оформлению результатов СРС: ответы на вопросы, выносимые на самостоятельное изучение (собеседование), изучаются студентом и конспектируются в тетради. Для подготовки к данному оценочному мероприятию необходимо до 15 часов самостоятельной работы. Студенту необходимо выбрать необходимые источники информации, позволяющие раскрыть предложенные вопросы и составить краткий конспект своего ответа.

При подготовке к ответу студенту предоставляется право пользования текстом конспекта составленного самостоятельно при подготовке к практическому занятию.

При проверке задания, оцениваются умение анализировать ситуацию, умение затребовать дополнительную информацию, необходимую для уточнения ответа; умение моделировать решения в соответствии с заданием, умение принять правильное решение на основе анализа ситуации. Навыки четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения; навык критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки.

Тема: 5 Особенности классификаций и расследования дел о преступлениях в сфере информационной безопасности.

Цель: привитие навыков у студентов умений классификаций и расследования дел о преступлениях в сфере информационной безопасности.

Форма контроля СРС: индивидуальное собеседование, проверка текста конспекта.

Вопросы для собеседования: Особенности классификаций дел о преступлениях в сфере информационной безопасности. Особенности расследования дел о преступлениях в сфере информационной безопасности.

Требования к представлению и оформлению результатов СРС: *о*ответы на вопросы, выносимые на самостоятельное изучение (собеседование), изучаются студентом и конспектируются в тетради. Для подготовки к данному оценочному мероприятию необходимо до 15 часов самостоятельной работы. Студенту необходимо выбрать необходимые источники информации, позволяющие раскрыть предложенные вопросы и составить краткий конспект своего ответа.

При подготовке к ответу студенту предоставляется право пользования текстом конспекта составленного самостоятельно при подготовке к практическому занятию.

При проверке задания, оцениваются умение анализировать ситуацию, умение затребовать дополнительную информацию, необходимую для уточнения ответа; умение моделировать решения в соответствии с заданием, умение принять правильное решение на основе анализа ситуации. Навыки четкого и точного изложения собственной точки зрения в устной и письменной форме, убедительного отстаивания своей точки зрения; навык критического оценивания различных точек зрения, осуществление самоанализа, самоконтроля и самооценки.

5. Список рекомендуемой литературы

Основная литература:

1. Экономическая оценка и оптимизация затрат на разработку программных продуктов и средств защиты информации таможенных органов : монография / Ю. И. Сомов, Э. П. Купринов, С. В. Курихин, Л. Д. Зайцева. — Москва : Российская таможенная академия, 2014. — 186 с. — ISBN 978-5-9590-0823-9. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69852.html. — Режим доступа: для авторизир. Пользователей
2. Федоров, В. В. Информационные технологии и защита информации в правоохранительной деятельности таможенных органов Российской Федерации : монография / В. В. Федоров. — Москва : Российская таможенная академия, 2014. — 180 с. — ISBN 978-5-9590-0797-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/69725.html. — Режим доступа: для авторизир. Пользователей

Перечень дополнительной литературы:

1. Афонин, П. Н. Информационная безопасность в таможенном деле : учебник / П. Н. Афонин, Д. Н. Афонин, А. И. Краснова. — Санкт-Петербург : Троицкий мост, 2016. — 512 с. — ISBN 978-5-4377-0039-6. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/40859.html— Режим доступа: для авторизир. пользователей