Федеральное государственное бюджетное образовательное учреждение
высшего образования
«КАЛИНИНГРАДСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

А. Г. Жестовский

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 Информационная безопасность автоматизированных систем

Калининград
Издательство ФГБОУ ВО «КГТУ»
2023

Рецензент:
заведующий кафедрой информационной безопасности
Института цифровых технологий ФГБОУ ВО
«Калининградский государственный технический университет»,
кандидат физико-математических наук, доцент
Н. Я. Великите

Жестовский, А. Г.

Управление информационной безопасностью: учеб.-метод. пособие по изучению дисциплины для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем / А. Г. Жестовский. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 20 с.

В учебно-методическом пособии приведен тематический план по дисциплине и даны методические указания по ее самостоятельному изучению, подготовке к практическим занятиям, подготовке и сдаче экзамена, выполнению самостоятельной работы. Пособие подготовлено в соответствии с требованиями утвержденной рабочей программы модуля «Методы и средства обеспечения информационной безопасности автоматизированных систем» специальности 10.05.03 Информационная безопасность автоматизированных систем.

Табл. 3, список лит. – 20 наименований.

Учебно-методическое пособие рассмотрено и одобрено в качестве локального электронного методического материала на заседании кафедры ИБ ФГБОУ ВО «Калининградский государственный технический университет» 30 июня 2023 г., протокол № 11

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в качестве локального электронного методического материала в учебном процессе методической комиссией ИЦТ 5 июля 2023 г., протокол № 8

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

Данное учебно-методическое пособие предназначено для студентов специальности 10.05.03 Информационная безопасность автоматизированных систем, специализация Безопасность открытых информационных систем, изучающих дисциплину «Управление информационной безопасностью».

Цель освоения дисциплины: обучить студентов процессам управления информационной безопасностью.

Для успешного освоения дисциплины, в соответствии с учебным планом, ей предшествуют дисциплины: «Безопасность вычислительных сетей», «Безопасность систем баз данных», «Безопасность операционных систем».

Далее в пособии представлен тематический план, содержащий перечень изучаемых тем, обязательных практических работ, мероприятий текущей аттестации и отводимое на них аудиторное время (занятия в соответствии с расписанием) и самостоятельную работу. При формировании личного образовательного плана на семестр следует оценивать рекомендуемое время на изучение дисциплины; возможно, вам потребуется больше времени на выполнение отдельных заданий или проработку отдельных тем.

В разделе «Содержание дисциплины» приведены подробные сведения об изучаемых вопросах, по которым вы можете ориентироваться в случае пропуска каких-то занятий, а также методические рекомендации преподавателя для самостоятельной подготовки. Каждая тема имеет ссылки на литературу (или иные информационные ресурсы), а также контрольные вопросы для самопроверки.

Раздел «Текущая аттестация» содержит описание обязательных мероприятий контроля самостоятельной работы и усвоения разделов или отдельных тем дисциплины. Далее изложены требования к завершающей аттестации – зачету и/или экзамену.

В разделе «Балльно-рейтинговая система» приведен порядок применения балльно-рейтинговой системы контроля успеваемости.

Помимо данного пособия, студентам следует использовать материалы, размещенные в соответствующем данной дисциплине разделе ЭИОС, в которые более оперативно вносятся изменения для адаптации дисциплины под конкретную группу.

Программное обеспечение

1. Microsoft Desktop Education. Операционные системы: Microsoft Windows Desktop operating systems, офисные приложения (Microsoft Office), по соглашению V9002148 Open Value Subscription (срок действия: три года).

2. Программное обеспечение, распространяемое по лицензии GNU General Public License (лицензия на свободное программное обеспечение, созданная в рамках проекта GNU, по которой автор передаёт программное обеспечение в общественную собственность):

– Snort (свободная сетевая система предотвращения вторжений (IPS) и обнаружения вторжений (IDS) с открытым исходным кодом);
– Ethereal (Программы перехвата и анализа сетевых пакетов);
– NMAP (Программа сканирование сетевых ресурсов);
– MySQL (Система управления базами данных).

Типовое ПО на всех ПК:

1. Microsoft Desktop Education (операционные системы Microsoft Windows Desktop operating system, офисные приложения Microsoft Office, по соглашению V9002148 Open Value Subscription). Дата заключения контракта 05.07.2018. Номер контракта 0335100016118000073-0484577-02.

2. Антивирусное программное обеспечение Kaspersky Total Space Security Russian Edition, лицензия 17EO-171225-104659-470-270, срок использования с 2017-12-26 до 2020-03-13

Специализированное ПО:

1.VMWare Workstation, Страж-NT, Панцирь-К (по государственному контракту №10/13А от 19 апреля 2013 года), (на два компьютера – Vmware License Purchase Information № 22033811ОВ);

Open Value Subscription.

2. ТЕМАТИЧЕСКИЙ ПЛАН

№ п. п.	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
	Лекции		
1	Тема 1. Введение. Основы управленческой деятельности в ИБ	6+3(РЭ)	-
2	Тема 2. Система управления информационной безопасностью автоматизированных систем	8+3(РЭ)	17
3	Тема 3. Организация обеспечения информационной безопасности автоматизированных систем	8+3(РЭ)	17
4	Тема 4. Политика безопасности автоматизированных систем	8+3(РЭ)	18
5	Тема 5. Аудит информационной безопасности автоматизированных систем	2+3(РЭ)	-
6	Тема 6. Средства поддержки процессов управления информационной безопасностью АС	2+2(РЭ)	24
		34+17(РЭ)	**76**
	Практические занятия		
1	Практическое занятие № 1. «Менеджмент в сфере информационной безопасности»	8+2(КА)	-
2	Практическое занятие № 2. «Менеджмент в сфере информационной безопасности на государственном уровне в РФ»	8+2(КА)	-
3	Практическое занятие № 3. «Международные организации в сфере менеджмента информационной безопасности»	8+2(КА)	-
4	Практическое занятие № 4. «Система прав доступа»	8+3(КА)	-
5	Практическое занятие № 5. «Организация аттестации АС по требованиям безопасности информации в части защиты от НСД»	2+3,25(КА)	-
		34+12,25(КА)	**-**
	Рубежный (текущий) и итоговый контроль		
	Итоговый контроль (экзамен)	-	42,75
			42,75
	Всего	**68+17(РЭ)+12,25(КА)**	**118,75**

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

Тема 1. Введение. Основы управленческой деятельности в ИБ

Перечень изучаемых вопросов:

Введение. Основные понятия, термины и определения. Предмет и задачи дисциплины. Введение. Цели и задачи обучения. Основы управленческой деятельности в ИБ.

Методические указания к изучению:

Предварительно требуется определить понятие «средство защиты». Рассмотреть классификации средств защиты по областям, по типам и т. п. Требуется рассмотреть руководящие документы по классификациям средств, механизмов и систем защиты. Рассмотреть проблемы полного и неполного перекрытия угроз средствами защиты информации.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками / А.М. Астахов. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Приведите классификацию уязвимостей компьютерных систем.
2. Приведите состав компонентов комплексной системы обеспечения информационной безопасности (КСИБ).
3. Охарактеризуйте проблему состава компонентов комплексной системы обеспечения информационной безопасности (КСИБ).

Тема 2. Система управления информационной безопасностью автоматизированных систем

Перечень изучаемых вопросов:

Система управления информационной безопасностью автоматизированных систем. Основные угрозы автоматизированным системам. Формирование защиты информации.

Методические указания к изучению:

Основными требованиями к целевой функции защиты информации при эксплуатации систем защиты являются:

- система защиты должна выявлять факт несанкционированного запуска программы;
- система защиты должна реагировать на факт несанкционированного запуска программы;
- система защиты должна противостоять возможным атакам злоумышленников, направленным на нейтрализацию системы защиты.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие. для вузов / А.П. Курило, Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью: учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Охарактеризуйте методологию формирования задач защиты.
2. Охарактеризуйте основные угрозы автоматизированным системам.

Тема 3. Организация обеспечения информационной безопасности автоматизированных систем

Перечень изучаемых вопросов:

Организация обеспечения информационной безопасности автоматизированных систем. Предпроектное обследование. Функциональные подсистемы управления.

Методические указания к изучению:

Требуется обратить внимание на этапы проектирования КСИБ и требования к ним. Требуется обратить внимание на сопровождение.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАСи / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Охарактеризуйте этапы проектирования КСИБ и требования к ним.
2. Охарактеризуйте предпроектное обследование, техническое задание, техническое проектирование, рабочее проектирование, испытания и внедрение в эксплуатацию, сопровождение.

Тема 4. Политика безопасности автоматизированных систем

Перечень изучаемых вопросов:

Политика безопасности автоматизированных систем. Несанкционированный доступ к информации, возможные последствия. Классы каналов НСД АС и средств вычислительной техники.

Методические указания к изучению:

Требуется обратить внимание на классы каналов НСД АС и классы каналов НСД АС и средств вычислительной техники.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

Контрольные вопросы:

1. Привести классы каналов НСД АС и средств вычислительной техники.
2. Охарактеризовать типовую структуру комплексной системы защиты информации от несанкционированного доступа (НСД).
3. Привести классификацию и особенности методов и средств атаки.

Тема 5. Аудит информационной безопасности автоматизированных систем

Перечень изучаемых вопросов:

Аудит информационной безопасности автоматизированных систем. Окружающая среда как потенциальный источник угроз защиты АС. Параметры окружающей среды систем.

Методические указания к изучению:

Рассмотреть особенности информационной базы данных КСИБ. Рассмотреть параметры окружающей среды, шкалы, среды, воздействующие на технологический процесс и автоматизированную систему. Рассмотреть использование объединенной базы данных параметров окружающей среды для формирования особых функций защиты с элементами прогнозирования.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Охарактеризуйте особенности информационной базы данных КСИБ.
2. Охарактеризуйте параметры окружающей среды, шкалы, среды, воздействующие на технологический процесс и автоматизированную систему.
3. Охарактеризуйте использование объединенной базы данных параметров окружающей среды для формирования особых функций защиты с элементами прогнозирования.

Тема 6. Средства поддержки процессов управления информационной безопасностью АС

Перечень изучаемых вопросов:

Средства поддержки процессов управления информационной безопасностью АС. Последовательность работ управления информационной безопасностью АС.

Методические указания к изучению:

Рассмотрите специфику работ и особенности при проектировании системы защиты информации от НСД. Рассмотрите общие методы и методики проектирования.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В. Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Приведите специфику работ и особенности при проектировании системы защиты информации от НСД.
2. Приведите общие методы и методики проектирования.

Тема 7. Методы и методики оценки качества КСИБ

Перечень изучаемых вопросов:

Требования к эксплуатационной документации КСИБ. Метод экспертных структурных вопросников.

Методические указания к изучению:

Обратите внимание на методы и методики оценки качества КСИБ: методы. Обратите внимание на метод экспертных структурных вопросников, метод оценки уязвимости информации Хоффмана. Обратите внимание на метод оценки риска Фишера.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса: Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Охарактеризуйте методы и методики оценки качества КСИБ: методы нормативного функционального наблюдения.
2. Охарактеризуйте требования к эксплуатационной документации КСИБ.
3. Охарактеризуйте метод оценки риска Фишера.

Тема 8. Особенности аудита современных информационных систем по стандартам

Перечень изучаемых вопросов:

Стандарты аудита. Управление информационной безопасностью сетевой инфраструктуры.

Методические указания к изучению:

Рассмотрите:

1. Управление информационной безопасностью сетевой инфраструктуры.
2. Особенности аудита информационной безопасности удаленных автоматизированных рабочих.
3. Особенности аудита информационной безопасности.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Охарактеризуйте специфику аттестации по требованиям безопасности; особенности эксплуатации КСИБ на объекте защиты.
2. Охарактеризуйте общие организационно-функциональные задачи службы безопасности.

Тема 9. Практические аспекты проведения аудита

Перечень изучаемых вопросов:

Реализация журнала аудита с помощью функций ОС. Аудит событий безопасности посредством применения методик.

Методические указания к изучению:

Особенности применения методик аудита. Особенности использования применения методик в ОС Windows. Особенности реализации журнала аудита. Особенности аудита событий безопасности.

Литература:

1. Кузнецов, А.В. Основы защиты информации: учеб. пособие для студентов специальности – КОИБАС / В.А. Иванов, О.П. Пономарев, И.А. Ветров. – Калининград: Издательство БГАРФ, 2014. – 180 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: учеб. пособие / В.Ф. Шаньгин. – Москва: ИД «Форум», 2013. – 416 с.

3. Серия «Вопросы управления информационной безопасностью». Часть 1: Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 206 с.

4. Серия «Вопросы управления информационной безопасностью». Часть 2: Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 113 с.

5. Серия «Вопросы управления информационной безопасностью». Часть 3: Управление инцидентами информационной безопасности и непрерывность бизнеса. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 139 с.

6. Серия «Вопросы управления информационной безопасностью». Часть 4: Технические, организационные и кадровые аспекты управления информационной безопасностью: Учебное пособие для вузов / Н. Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – М.: Горячая линия–Телеком, 2014. – 186 с.

7. Серия «Вопросы управления информационной безопасностью». Часть 5: Проверка и оценка деятельности по управлению информационной безопасностью. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия–Телеком, 2014. – 145 с.

8. Астахов А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.

Контрольные вопросы:

1. Охарактеризуйте требования к эксплуатационной документации КСИБ.
2. Охарактеризуйте состав и содержание эксплуатационной документации.

4. ТРЕБОВАНИЯ К АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1. Текущая аттестация

В ходе изучения дисциплины студенты проходят текущую аттестацию в виде опросов во время практических занятий и путем прохождения теста.

Текущий контроль осуществляется путем опроса по материалу, пройденному на предшествующих лекциях. Оценивается (Таблица 1):

- полнота усвоения пройденного материала,
- качество изложения пройденного материала (устно и письменно).

Таблица 1. Шкала оценок уровня усвоения материала обучающимся в результате опроса

Неудовлетворительный	**Пороговый**	**Углубленный**	**Продвинутый**
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не может ответить на вопросы по пройденному материалу или графически изобразить на доске	Отвечает сбивчиво, путается в определениях и обозначениях, нуждается в помощи других обучающихся	Допускает незначительные ошибки при изложении пройденного материала, не полностью представляет связи между разделами изучаемой дисциплины	Четко отвечает на вопросы, может точно изобразить графическую часть пройденного материала, увязывает последовательность изученных разделов дисциплины

Критерии оценивания знаний по результатам тестирования приведены в Таблице 2.

Таблица 2. Шкала оценок уровня освоения дисциплины по тесту

Неудовлетворительный	**Пороговый**	**Углубленный**	**Продвинутый**
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
< 50 % правильных ответов	50-70 % правильных ответов	71-90 % правильных ответов	91-100 % правильных ответов

4.2. Условия получения положительной оценки

Завершающим этапом изучения дисциплины является промежуточная аттестация, проводимая в форме экзамена (Таблица 3).

Допуск к промежуточной аттестации возможен при следующих условиях:

- наличие всех выполненных, сданных (проверенных, защищенных) лабораторных работ, наличие отчётов по ним;
- наличие показателей приемлемого уровня освоения материалов курса: более 50 % посещений от общего числа требуемых по учебному плану.

Таблица 3. Шкала оценок уровня освоения дисциплины по экзамену

Оценка			
Неудовлетворительный	**Пороговый**	**Углубленный**	**Продвинутый**
«2» (неудовлетворительно)	«3» (удовлетворительно)	«4» (хорошо)	«5» (отлично)
Не знает значительной части программного материала, допускает существенные ошибки, с большими затруднениями выполняет практические задания, задачи	Усвоил только основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала и испытывает затруднения в выполнении практических заданий	Твердо знает программный материал, грамотно и по существу излагает его, не допускает существенных неточностей в ответе на вопрос, может правильно применять теоретические положения и владеет необходимыми умениями и навыками при выполнении практических заданий	Глубоко и прочно усвоил весь программный материал, исчерпывающе, последовательно, грамотно и логически стройно его изложил, не затрудняется с ответом при видоизменении задания, свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, умеет самостоятельно обобщать и излагать материал, не допуская ошибок

4.3. Примерные вопросы к экзамену по дисциплине

1. Основы теории рисков. Состав элементов КОИБАС. Подробно осветить состав организационного элемента и криптографического.
2. Состав элементов КОИБАС. Подробно осветить состав правового, программно-аппаратного элемента и инженерно-технического.
3. Формирование общей структуры КОИБАС.
4. Подробно осветить начальные этапы формирования процесса оценки рисков. Формирование дерева уязвимостей. Формализация оценки рисков.
5. Построение графа компрометации. Указать типы вершин, типы рёбер. Способы формальных вычислений.
6. Использование графа атаки. Расчёты экономических показателей с использованием графа атаки. Оптимизация набора механизмов безопасности с использованием графа атаки.
7. Оптимизация состава КОИБАС на основе модели Клеменса – Хоффмана.
8. Теория уровней (зональная модель) при расчете уязвимости информации.
9. Процедуры оценки защиты КСИ. Схема оценки.
10. Приложение теории надежности к оценке защищенности ИС.
11. Определение уровня защищенности.
12. Особенности определения угроз при построении КОИБАС (по лаб.).
13. Оценка качества защищённости информации методом экспертных структурных вопросов. Этапы морфологического анализа.
14. Определение стоимости потерь.
15. Принципы совмещения элементов КОИБАС. Компоненты формирования КОИБАС.
16. Сетевое планирование и эксплуатационная документация КСИБ.

17. Определение уровня защищённости системы с учётом угроз, рисков и производительности. Привести схему расчётов (ИБАИС).

18. Основы аудита.

19. Особенности применения табличных способов оценки рисков (лабораторная работа).

20. Оценка рисков системы по методу Digital Security (лабораторная работа).

21. Формирование списка угроз для системы с учётом её структуры и информационных потоков (лабораторная работа).

22. Математические методы расчета комп. атак. Перечислить и кратко охарактеризовать.

23. Особенности этапов аудита ИБ организации.

24. Привести информацию, собираемую при обследовании организации.

25. Особенности подбора средств защиты.

5. ЗАКЛЮЧЕНИЕ

В лекциях по предмету излагаются основные знания по курсу дисциплины. Самостоятельная работа имеет особое значение для прочного усвоения материала. Она помогает научиться правильно ориентироваться в научной литературе, самостоятельно мыслить и находить правильные ответы на возникающие вопросы. В ходе всех видов занятий происходит углубление и закрепление знаний студентов, вырабатывается умение правильно излагать свои мысли.

Самостоятельная работа выполняет ряд функций, к которым относятся:

- *развивающая* (повышение культуры умственного труда, приобщение к творческим видам деятельности, обогащение интеллектуальных способностей студентов);
- *информационно-обучающая* (учебная деятельность студентов на аудиторных занятиях, неподкрепленная самостоятельной работой, становится малорезультативной);
- *ориентирующая и стимулирующая* (процессу обучения придается профессиональное ускорение);
- *воспитывающая* (формируются и развиваются профессиональные качества специалиста);
- *исследовательская* (новый уровень профессионально-творческого мышления).

В основе самостоятельной работы студентов лежат принципы: самостоятельности, развивающе-творческой направленности, целевого планирования, личностно-деятельностного подхода.

Самостоятельная работа студентов проводиться с целью:

- систематизации и закрепления полученных теоретических знаний и практических умений студентов;
- углубления и расширения теоретических знаний;
- формирования умений использовать нормативную, правовую, справочную документацию и специальную литературу;
- развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, ответственности и организованности;
- формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации;
- развития исследовательских умений.

Для достижения указанной цели студенты на основе плана самостоятельной работы должны решать следующие задачи:

- изучить рекомендуемые литературные источники;
- изучить основные понятия, представленные в глоссарии;
- ответить на контрольные вопросы;
- решить предложенные задачи, кейсы, ситуации;

- выполнить контрольные и курсовые работы.

Работа студентов в основном складывается из следующих элементов:

1. Изучение и усвоение в соответствии с учебным планом программного материала по всем учебным дисциплинам.
2. Выполнение письменных контрольных и курсовых работ.
3. Подготовка и сдача зачетов, курсовых работ, итоговых экзаменов.
4. Написание и защита дипломной работы.

Самостоятельная работа включает такие формы работы, как:

- индивидуальное занятие (домашние занятия) – важный элемент в работе студента по расширению и закреплению знаний;
- конспектирование лекций;
- получение консультаций для разъяснений по вопросам изучаемой дисциплины;
- подготовка ответов на вопросы тестов;
- подготовка к экзамену;
- выполнение контрольных, курсовых проектов и дипломных работ;
- подготовка научных докладов, рефератов, эссе;
- анализ деловых ситуаций (миникейсов) и др.

Содержание внеаудиторной самостоятельной работы определяется в соответствии с рекомендуемыми видами заданий в соответствии с *рабочей программой учебной дисциплины*. Распределение объема времени на внеаудиторную самостоятельную работу в режиме дня студента *не* регламентируется расписанием.

Виды заданий для внеаудиторной самостоятельной работы, их содержание и характер могут иметь вариативный и дифференциальный характер, учитывать специфику специальности, изучаемой дисциплины, индивидуальные особенности студента.

Видами заданий для внеаудиторной самостоятельной работы могут быть:

для овладения знаниями:

- чтение текста (учебника, первоисточника, дополнительной литературы);
- составление плана текста;
- конспектирование текста;
- выписки из текста;
- работа со словарями и справочниками;
- исследовательская работа;
- использование аудио- и видеозаписи;
- работа с электронными информационными ресурсами и ресурсами Internet;

для закрепления и систематизации знаний:

- работа с конспектом лекции (обработка текста);
- повторная работа над учебным материалом (учебника, первоисточника, дополнительной литературы, аудио-, видеозаписей);
- составление плана и тезисов ответа;
- выполнение тестовых заданий;
- ответы на контрольные вопросы;
- аннотирование, реферирование, рецензирование текста;
- подготовка сообщений к выступлению на семинаре, конференции; подготовка рефератов, докладов;
- работа с компьютерными программами;
- подготовка к сдаче экзамена;

для формирования умений:

- решение задач и упражнений по образцу;
- решение вариативных задач и упражнений;
- выполнение расчетно-графических работ;
- решение ситуационных производственных (профессиональных) задач;
- участие в научных и практических конференциях;

• проектирование и моделирование разных видов и компонентов профессиональной деятельности;

• создание проспектов, проектов, моделей;

• экспериментальная работа, участие в НИР;

• рефлексивный анализ профессиональных умений с использованием аудио-, видеотехники и компьютерных расчетных программ и электронных практикумов;

• подготовка курсовых проектов и дипломных работ.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет привить студентам умения и навыки в овладении, изучении, усвоении и систематизации приобретаемых знаний в процессе обучения, обеспечивать высокий уровень успеваемости в период обучения, привить навыки повышения профессионального уровня в течение всей трудовой деятельности.

6. ЛИТЕРАТУРА

1. ГОСТ Р ИСО/МЭК 27000-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология.
2. ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.
3. ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.
4. ГОСТ Р ИСО/МЭК 27003-2012 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Руководство по реализации системы менеджмента информационной безопасности.
5. ГОСТ Р ИСО/МЭК 27005-2010 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.
6. ГОСТ Р ИСО/МЭК 27007-2014 Информационная технология. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента информационной безопасности.
7. ГОСТ Р ИСО/МЭК 18045—2013 Информационная технология. Методы и средства обеспечения безопасности. Методология оценки безопасности информационных технологий.
8. ГОСТ Р ИСО 22301-2014 Системы менеджмента непрерывности бизнеса. Общие требования.
9. ГОСТ Р ИСО/МЭК 13335-1-2006 Информационная технология. Методы и средства обеспечения безопасности.
10. ГОСТ Р 55.0.02-2014/ИСО 55001:2014 Управление активами. Национальная система стандартов. Системы менеджмента.
11. Астахов, А.М. Искусство управления информационными рисками. – Эл. изд. – Саратов: Профобразование, 2017. – 312 с., ил.
12. Лившиц, И.И. Оценка степени влияния General Data Protection Regulation на безопасность предприятий РФ // Вопросы кибербезопасности. – 2020. – № 4 (38). – С. 66-74.
13. Лившиц, И.И. Оценка уровня обеспечения информационной безопасности в кредитном предприятии // Стандарты и качество. – 2020. – № 7. – С. 44-49.
14. Лившиц, И.И. Метод оценивания безопасности облачных ИТ-компонент по критериям существующих стандартов // Труды СПИИРАН [SPIIRAS Proceedings]. – 2020. – Т. 19. – № 2 (69). – С. 383-411.
15. Основы управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия – Телеком, 2014.

16. Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия – Телеком, 2014.

17. Технические, организационные и кадровые аспекты управления информационной безопасностью. Учебное пособие для вузов / А.П. Курило, Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая линия. – Телеком, 2014.

18. Мельников, В.П. Методы и средства хранения и защиты компьютерной информации / В.П. Мельников, А.Г. Схиртладзе. – Б. м.: ТНТ, 2018.

19. Аверченков, В.И. Организационно-правовые основы защиты информации / В.И. Аверченков, М.Ю. Рытов, М.Л. Гулак, О.М. Голембиовская, Е.В. Лексиков. – Б. м.: ТНТ, 2021.

20. Клейменов, С.А. Обеспечение информационной безопасности машиностроительных предприятий. Ч. I, Ч II / С. А. Клейменов, В.П. Мельников, А.Г. Схиртладзе, В.П. Борискин, А.И. Петраков – Б. м.: ТНТ, 2017.

Локальный электронный методический материал

Александр Георгиевич Жестовский

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Редактор М. А. Дмитриева

Уч.-изд. л. 0,9. Печ. л. 1,3.

Издательство федерального государственного бюджетного образовательного
учреждения высшего образования
«Калининградский государственный технический университет».
236022, Калининград, Советский проспект, 1