Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования «Курганский государственный университет»
(КГУ)

Кафедра «Безопасность информационных и автоматизированных систем»

УТВЕРЖДАЮ:
Первый проректор
_____ Т.Р. Змызгова
«31» августа 2023 г.

Рабочая программа учебной дисциплины

МЕТОДЫ КОНТРОЛЯ ЗАЩИЩЕННОСТИ ИНФОРМАЦИИ В ИНФОМАЦИОННЫХ СИСТЕМАХ

образовательной программы высшего образования –
программы специалитета
10.05.03 Информационная безопасность автоматизированных систем

Специализация №5
Безопасность открытых информационных систем

форма обучения – очная

Курган 2023

Рабочая программа дисциплины «Методы контроля защищенности информации в информационных системах» составлена в соответствии с учебными планами по программе специалитета «Информационная безопасность автоматизированных систем» (безопасность открытых информационных систем), утвержденным для очной формы обучения «30» июня 2023 года.

Рабочая программа дисциплины одобрена на заседании кафедры «Безопасность информационных и автоматизированных систем» «31» августа 2023 года, протокол № 1.

Рабочую программу составил:
ст. преподаватель кафедры «БИАС»  В.В. Москвин

Согласовано:

Заведующий кафедрой «БИАС»
канд. тех. наук, доцент  Д.И. Дик

Начальник Управления
образовательной деятельности  И.В. Григоренко

Специалист по учебно-методической
работе Учебно-методического отдела  Г.В. Казанкова

1. ОБЪЕМ ДИСЦИПЛИНЫ

Очная форма обучения

Всего: 3 зачетных единицы трудоемкости (108 академических часа)

Вид учебной работы	На всю дисциплину	семестр
		6
Аудиторные занятия (контактная работа с преподавателем), всего часов в том числе:	**80**	**80**
Лекции	32	32
Лабораторные работы	16	16
Практические работы	32	32
Самостоятельная работа, всего часов в том числе:	**28**	**28**
Подготовка к зачету	18	18
Другие виды самостоятельной работы (подготовка к лабораторным и практическим работам и рубежному контролю)	10	10
Вид промежуточной аттестации	**Зачет**	**Зачет**
Общая трудоемкость дисциплины и трудоемкость по семестрам, часов	**108**	**108**

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

Дисциплина «Методы контроля защищенности информации в информационных системах» относится к дисциплине по выбору к части формируемых участниками образовательных отношений блока 1 учебного плана образовательной программы.

Для освоения дисциплины «Методы контроля защищенности информации в информационных системах» необходимы компетенции, формируемые дисциплинами. «Организация ЭВМ и вычислительных систем», «Технологии и методы программирования», «Теоретические основы компьютерной безопасности».

Компетенции, формируемые дисциплиной «Методы контроля защищенности информации в информационных системах», необходимы для освоения следующих дисциплин: «Программно-аппаратные средства защиты информации», «Защита информации от утечки по техническим каналам», «Разработка и эксплуатация автоматизированных систем в защищенном исполнении».

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Цели и задачи изучения дисциплины

Основная цель изучения дисциплины - освоение принципов и правил работы со средствами и методы контроля защищенности информации в информационных системах.

Задачами дисциплины является изучение нормативно-правовой документации, знакомство со средствами контроля и анализа защищенности, как программных комплексов, так и программно-аппаратных, а также работа по составлению организационных документов (приказов) и ведение журналов учета объектов ИБ.

Формируемые компетенции в результате освоения дисциплины:

- Способен оценивать эффективность систем защиты информации, функционирующих в открытых информационных системах (ПК-8);
- Способен оценивать риски, связанные с осуществлением угроз информационной безопасности (ПК-10);

В результате освоения дисциплины студент должен:

знать:

– Нормативно-правовые документы по обеспечению контроля защищенности в Российской Федерации (для ПК-8, ПК-10);

уметь:

– Разрабатывать организационные документы по учету, контролю и защите носителей информации (для ПК-10);

владеть навыками:

– Установки, настройки и сопровождения средств и систем защиты информации (для ПК-8, ПК-10).

4. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. Учебно-тематический план.

Рубеж	Номер темы	Наименование темы	Количество часов контактной работы с преподавателем		
			Лекции	Лабораторные работы	Практические работы
Рубеж 1	*Тема 1*	Нормативно-правовое регулирование защищенности информации	4	-	4
	Тема 2	Средства контроля и анализа	8	14	-
	Тема 3	Типовые системы контроля защиты	8	2	-
		Рубежный контроль 1	2	-	-
Рубеж 2	*Тема 4*	Методология контроля защищенности информации	8	-	28
		Рубежный контроль 2	2	-	-
Всего:			**32**	**16**	**32**

4.2.Содержание лекционных занятий

Тема №1. Нормативно-правовое регулирование защищенности информации.

Федеральный закон Российской Федерации «Об информации, информационных технологиях и о защите информации» от 27 июля 2006 г. № 149-ФЗ; Федеральный закон Российской Федерации «О персональных данных» от 27.06.2006 г. № 152-ФЗ; Федеральный закон Российской Федерации «О техническом регулировании» от 27.12.2002 № 184-ФЗ; Приказ ФСБ России от 06.05.2019 "Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты"; ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»; ГОСТ Р ИСО/МЭК 13335-1-2006 ИТ. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий; ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения.

Тема №2. Средства контроля и анализа.

Методы и средства контроля защищенности информации: обрабатываемой техническими средствами, от утечки за счет ПЭМИН; акустической речевой информации от утечки по техническим каналам; от НСД. Документирование результатов контроля. Регистрация событий безопасности. Антивирусная защита. Системы обнаружения вторжений (СОВ). Обеспечение целостности информационных систем и информации. Сетевые сканеры безопасности «XSpider», «Ревизор сети», «Сканер-ВС». Средства контроля защищенности информации «ФИКС» и «Ревизор»

Тема №3. Типовые системы контроля защиты.

Типовые системы защиты: от НСД; от угроз вредоносного кода; межсетевого экранирования и защиты каналов связи; обнаружения вторжения; мониторинга событий безопасности. Комплексные системы контроля защищенности: KOMRAD, Enterprise SIEM, АК-ВС 2, ПИК ЭШЕЛОН, RedCheck.

Рубежный контроль № 1.

Тема №4. Методология контроля защищенности информации.

Этапы и подсистемы контроля защищенности. Механизм проведения контроля защищенности информации в средствах и системах информатизации. Создание и ведение документации для обеспечения контроля защищенности. Примеры.

Рубежный контроль № 2.

4.3 Лабораторные работы

№ темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
2	Средства контроля и анализа	*Лабораторная работа №1.* Сравнение функциональных возможностей сетевых сканеров: «Ревизор Сети 2.0» и «XSpider».	4
		Лабораторная работа №2. Установка и настройка средства контроля защищенности для Windows: «Ревизор 2 XP», «ФИКС 2.0.2».	4
		Лабораторная работа №3: Установка и настройка средства контроля защищенности для Unix-систем: «ФИКС-Unix 1.0» и «Ревизор 2 для Linux».	6
3	Типовые системы контроля защиты	*Лабораторная работа №4:* Система контроля RedCheck.	2
Итого			**16**

4.4 Практические работы

№ темы	Наименование темы	Наименование тем лабораторных работ	Норматив времени, час.
1	Нормативно-правовое регулирование защищенности информации	*Практическая работа №1.* Работа с НМД	4
4	Методология контроля защищенности информации	*Практическая работа №2.* Разработка и ведение организационных документов: Приказ «О назначении ответственных лиц» (+инструкции).	3
		Практическая работа №3. Разработка и ведение организационных документов: Инструкция пользователя ИС	2
		Практическая работа №4. Разработка и ведение организационных документов: Приказ о КЗ (+ положение о КЗ).	3

		Практическая работа №5. Разработка и ведение организационных документов: План мероприятий по ИБ и контролю защищенности	2
		Практическая работа №6. Разработка и ведение организационных документов: Журнал учета съемных МНИ	2
		Практическая работа №7. Разработка и ведение организационных документов: Журнал учета СрЗИ.	2
		Практическая работа №8. Разработка и ведение организационных документов: 09 Журнал учета портативных устройств.	2
		Практическая работа №9. Разработка и ведение организационных документов: Журнал инструктажей по ИБ	2
		Практическая работа №10. Разработка и ведение организационных документов: Журнал учета мероприятий по ИБ	2
		Практическая работа №11. Разработка и ведение организационных документов: Приказ об утверждении перечня лиц по ПДн	2
		Практическая работа №12. Разработка и ведение организационных документов: Политика в отношении обработки персональных данных	2
		Практическая работа №13. Разработка и ведение организационных документов: Приказ СКЗИ (+перечень лиц +инструкция +акт уничтожения)	2
		Практическая работа №14. Разработка и ведение организационных документов: Журнал поэкземплярного учета криптосредств.	2
Итого			**32**

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

При прослушивании лекций рекомендуется в конспекте отмечать все важные моменты, на которых заостряет внимание преподаватель, в частности те, которые направлены на качественное выполнение соответствующей лабораторной и практической работы.

Преподавателем запланировано использование при чтении лекций технологии учебной дискуссии. Поэтому рекомендуется фиксировать для себя интересные моменты с целью их активного обсуждения на дискуссии в конце лекции.

Залогом качественного выполнения лабораторных и практических работ является самостоятельная подготовка к ним накануне путем повторения

материалов лекций. Преподавателем запланировано применение на лабораторных и практических работах разбора конкретных ситуаций.

Для текущего контроля успеваемости преподавателем используется балльно-рейтинговая система контроля и оценки академической активности. Поэтому настоятельно рекомендуется тщательно прорабатывать материал дисциплины при самостоятельной работе, участвовать во всех формах обсуждения и взаимодействия, как на лекциях, так и на лабораторных и практических работах в целях лучшего освоения материала и получения высокой оценки по результатам освоения дисциплины.

Выполнение самостоятельной работы подразумевает подготовку к лабораторным и практическим работам, рубежным контролям и зачету.

Рекомендуемая трудоемкость самостоятельной работы представлена в таблице:

Рекомендуемый режим самостоятельной работы

Наименование вида самостоятельной работы	Рекомендуемая трудоемкость, акад. час.
Подготовка к лабораторным работам (по 0,5 часа)	2
Подготовка к практическим работам (по 0,5 часа)	7
Подготовка к рубежным контролям (по 0,5 часу)	1
Подготовка к зачету	**18**
Всего:	**28**

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ АТТЕСТАЦИИ

6.1. Перечень оценочных средств

1. Балльно-рейтинговая система контроля и оценки академической активности студентов в КГУ.
2. Отчеты студентов по лабораторным и практическим работам.
3. Банк тестовых и практических заданий к рубежным контролям № 1, № 2.
4. Вопросы к зачету.

6.2. Система балльно-рейтинговой оценки работы студентов по дисциплине

<table>
<tr><td>№</td><td>Наименование</td><td colspan="8">Содержание</td></tr>
<tr><td rowspan="3">1</td><td rowspan="3">Распределение баллов за семестр по видам учебной работы, сроки сдачи учебной работы (доводятся до сведения студентов на первом учебном занятии)</td><td colspan="8">Распределение баллов</td></tr>
<tr><td>Вид учебной работы:</td><td>Посещение лекций</td><td>Выполнение и защита лабораторных работ</td><td>Выполнение и защита практических работ</td><td>Рубежный контроль №1</td><td>Рубежный контроль №2</td><td>Зачет</td></tr>
<tr><td>Балльная оценка:</td><td>1,5б x14=21б</td><td>3б x 4 =12б</td><td>1,5б x 14 =21б</td><td>6</td><td>10</td><td>30</td></tr>
<tr><td>2</td><td>Критерий пересчета баллов в традиционную оценку по итогам работы в семестре и на экзамене</td><td colspan="8">60 и менее баллов – неудовлетворительно; незачет;
61…73 – удовлетворительно; зачет;
74… 90 – хорошо;
91…100 – отлично</td></tr>
<tr><td>3</td><td>Критерии допуска к промежуточной аттестации, возможности получения автоматически экзаменационной оценки «удовлетворительно» по дисциплине, возможность получения бонусных баллов</td><td colspan="8">Для допуска к промежуточной аттестации по дисциплине за семестр обучающийся должен набрать по итогам текущего и рубежного контроля не менее 51 баллов. В случае если обучающийся набрал менее 51 балла, то к аттестационным испытаниям он не допускается.
Для получения зачета без проведения процедуры промежуточной аттестации обучающемуся необходимо набрать в ходе текущего и рубежных контролей не менее 61 балла. В этом случае итог балльной оценки, получаемой обучающимся, определяется по количеству баллов, набранных им в ходе текущего и рубежного контролей. При этом, на усмотрение преподавателя, бальная оценка обучающегося может быть повышена за счет получения дополнительных баллов за академическую активность.
Обучающийся, имеющий право на получение оценки без проведения процедуры промежуточной аттестации, может повысить ее путем сдачи аттестационного испытания. В случае получения обучающимся на аттестационном испытании 0 баллов итог бальной оценки по дисциплине не снижается.
За академическую активность в ходе освоения дисциплины, участие в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности обучающемуся могут быть начислены дополнительные баллы. Максимальное количество дополнительных баллов за академическую активность составляет 30.
Основанием для получения дополнительных баллов являются:
- выполнение дополнительных заданий по дисциплине; дополнительные баллы начисляются преподавателем;
- участие в течение семестра в учебной, научно-исследовательской, спортивной, культурно-творческой и общественной деятельности КГУ.</td></tr>
</table>

4	Формы и виды учебной работы для неуспевающих (восстановившихся на курсе обучения) студентов для получения недостающих баллов в конце семестра	В случае если к промежуточной аттестации (зачету) набрана сумма менее 51 баллов, обучающемуся необходимо набрать недостающее количество баллов за счет выполнения дополнительных заданий, до конца последней (зачетной) недели семестра. Ликвидация академических задолженностей, возникших из-за разности в учебных планах при переводе или восстановлении, проводится путем выполнения дополнительных заданий, форма и объем которых определяется преподавателем.

6.3. Процедура оценивания результатов освоения дисциплины

Рубежный контроль №1 проводится в форме тестирования, рубежный контроль № 2 – в форме выполнения практического задания.

Перед проведением каждого рубежного контроля преподаватель прорабатывает со студентами основной материал соответствующих разделов дисциплины в форме краткой лекции-дискуссии.

Примерные варианты тестовых заданий для рубежного контроля №1 (состоит из 6 вопросов по 1 баллу каждый) и практических заданий для рубежного контроля № 2 (состоит из 1 задания - шаблона журнала и перечня оборудования/съемных носителей, для каждого студента, которое оценивается в 10 баллов) приведены ниже. На каждый рубежный контроль студенту отводится 2 академических часа.

Правильность выполнения рубежного контроля № 2 оценивается с учётом допущенных ошибок при заполнении данных в шаблон журнала.

Преподаватель оценивает в баллах результаты каждого студента и заносит в ведомость учета текущей успеваемости.

Зачет проводится в форме письменного ответа на два вопроса по всем разделам дисциплины. Расчетное время проведения зачета – 1,5 часа. Каждый вопрос оценивается до 15 баллов. Студент, суммарно набравший менее чем 11 баллов за ответ на вопросы, считается не сдавшим зачет.

Результаты текущего контроля успеваемости, зачета заносятся преподавателем в зачетную ведомость, которая сдается в организационный отдел института в день зачета, а также выставляются в зачетную книжку студента.

6.4. Примеры оценочных средств для рубежных контролей и зачета

Примерный перечень вопросов для рубежного контроля №1

1. Какой срок хранения информации о зарегистрированных событиях должен быть обеспечен оператором?

a. не менее месяца, если иное не установлено требования законодательства РФ;

b. не менее трех месяцев, если иное не установлено требования законодательства РФ;

c. не менее полугода, если иное не установлено требования законодательства РФ;

d. не менее года, если иное не установлено требования законодательства РФ.

2. Распределите обязательные и усиленные требования к реализации АНЗ.

a. Обязательные

b. Усиленные

1. выявление (поиск) уязвимостей, связанных с ошибками кода в программном (микропрограммном) обеспечении (общесистемном, прикладном, специальном), а также программном обеспечении СЗИ, правильностью установки и настройки СЗИ, технических средств и программного обеспечения, а также корректностью работы СЗИ при их взаимодействии с техническими средствами и программным обеспечением;

2. оператор должен уточнять перечень сканируемых в информационной системе уязвимостей с установленной им периодичностью, а также после появления информации о новых уязвимостях;

3. оператором должно использоваться тестирование информационной системы на проникновение.

4. Оператором должны осуществляться получение из доверенных источников и установка обновлений базы признаков уязвимостей.

5. Выявление (поиск), анализ и устранение уязвимостей должны проводиться на этапах создания и эксплуатации информационной системы.

6. оператором применяются автоматизированные средства для сравнения результатов сканирования уязвимостей в разные периоды времени для анализа изменения количества и классов (типов) уязвимостей в информационной системе;

3. Распределите обязательные и усиленные требования к реализации РСБ.

a. Обязательные

b. Усиленные

1. Доступ к записям аудита и функциям управления механизмами регистрации (аудита) должен предоставляться только уполномоченным должностным лицам.

2. в информационной системе обеспечивается резервное копирование записей регистрации (аудита);

3. Правила и процедуры защиты информации о событиях безопасности регламентируются в организационно-распорядительных документах оператора по защите информации.

4. в информационной системе обеспечивается резервное копирование записей регистрации (аудита) на носители однократной записи (не перезаписываемые носители информации);

Примерный вид задания для рубежного контроля №2

Перечень имеющихся средств в организации. Заполните свой журнал учёта. Явно неуказанные поля таблицы, при обязательности, нужно заполнить самостоятельно.

1) ФИКС 2.0.1 – сертификат XXFDER14, - 3 шт. инв. № 0000000125, № 0003100700, № 0000005461 – уничтожен по акту № 22– возвращен 10.03.23, выдан пользователю Иванову Д.Д. - кабинет 231, выдан пользователю Смолиной А.Д. – возвращен 25.04.12, выдан пользователю Коневой И.М., 26.04.23, Номер ТС, на которое установлен: 1,2,3.

2) Внешний диск HDD Transcend StoreJet 25M3S TS2TSJ25M3S, 2ТБ, выдан 10.03.23 пользователю Самсонова К.К., параметры для входа: Sa2ms#o4nov@, версия драйвера: 10.0.19041.1, дата последнего тестирования – 01.02.23, уничтожен – 25.12.23, разрешен физический доступ: (системный администратор) Екимова Л.С.

3) SSD Kingston A400 SATA 960 Гб, для создание backup'а системы, не выдан, пользователь Иванов Д.Д. - нет разрешения на вынос за пределы КЗ, пользователь Смолин А.Д – есть разрешение на вынос за пределы КЗ.

4) Смартфон Huawei P Smart 2021 128Gb, S/N. TGFK07421FR014, инв. № 5483310984, пользователь Самсоновой К.К - вынос разрешен за пределы КЗ, выдан пользователю (бухгалтер) Ильину Ф.Ф – нет разрешения на вынос за пределы КЗ, кабинет 43, цель: передача документов.

5) Ревизор 2 XP, - 2 шт. экз. 21, 25– возвращен 10.03.23, пользователь Иванов Д.Д., дата последнего тестирования – 01.02.23, дата следующего тестирования – 01.04.23, Номер ТС, на которое установлен: 142,450.

6) Сетевое хранилище Qnap TS-431P3-4G для HDD 4, разрешен физический доступ: (системный администратор) Екимова Л.С, не выдавался.

7) Флешка USB Kingston DataTraveler Kyson 64ГБ, USB3.1, S/N. TGFH65421FR123, выдан пользователю Иванову Д.Д – нет разрешения на вынос за пределы КЗ, кабинет 231, возвращен 12.05.23, уничтожен по акту №55.

8) Жесткий диск Seagate Barracuda ST2000DM008, 2ТБ, HDD, SATA III Номер ТС, на которое установлен: 4, дата последнего тестирования – 01.02.23, уничтожен – 25.12.23.

9) Карта памяти microSDXC UHS-I Kingston Canvas Select Plus 64 ГБ, 100 МБ/с, Class 10, SDCS2/64GB, 1 шт., переходник SD, цель: передача документов разрешен физический доступ: (системный администратор) Екимова Л.С – нет разрешения на вынос за пределы КЗ

10) Внешний диск HDD Toshiba Canvio Basics HDTB420EK3AA, 2ТБ, дата последнего тестирования – 01.02.23, не выдавался, разрешен физический доступ: (системный администратор) Екимова Л.С

Шаблоны журналов учета, выдаваемые студенту для заполнения: журнал учета стационарных машинных носителей, журнал учета портативных устройств, журнал учета съемных МНИ, журнал учета СрЗИ, журнал периодического тестирования СрЗИ.

Вопросы для подготовки к зачету

1) Основные НПА в сфере обеспечения контроля защищённости информации и их краткое описание;

2) Идентификация и аутентификация пользователей, являющихся работниками оператора. Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных;

3) Управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов, средствами аутентификации, в том числе хранение, выдача, инициализация, блокирование и принятие мер в случае утраты и (или) компрометации. Идентификация и аутентификация объектов файловой системы, запускаемых и исполняемых модулей, объектов систем, управление базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, иных объектов доступа;

4) Защита обратной связи при вводе аутентификационной информации. Идентификация и аутентификация пользователей, не являющихся работниками оператора (внешних пользователей);

5) Управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей реализация необходимых методов. Управления доступом (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

6) Назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование информационной системы. Ограничение неуспешных попыток входа в информационную систему;

7) Ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя ИС. Блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу;

8) Поддержка и сохранение атрибутов безопасности, связанных с информацией в процессе ее хранения и обработки. Реализация защищенного удаленного доступа субъектов доступа к объектам доступа через внешние информационно-телекоммуникационные сети;

9) Регламентация и контроль использования в ИС технологий беспроводного доступа. Регламентация и контроль использования в ИС мобильных технических средств, контроль за установкой компонентов программного обеспечения;

10) Установка только разрешенного к использованию ПО и (или) его компонентов. Управление временными файлами, в том числе запрет, разрешение, перенаправление записи, удаление временных файлов;

11) Управление запуском (обращениями) компонентов ПО, в том числе определение запускаемых компонентов, настройка параметров запуска компонентов, контроль за запуском компонентов ПО. Управление установкой компонентов ПО, в том числе определение компонентов, подлежащих установке, настройка параметров установки компонентов;

12) Учет МНИ. Управление доступом к МНИ;

13) Контроль перемещения МНИ за пределы контролируемой зоны. Исключение возможности несанкционированного ознакомления с

содержанием информации, хранящейся на машинных носителях, и (или) использования носителей информации в иных информационных системах;

14) Контроль использования интерфейсов ввода (вывода). Контроль ввода (вывода) информации на МНИ;

15) Контроль подключения МНИ. Уничтожение (стирание) информации на МНИ при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания);

16) Сбор, запись и хранение информации о событиях безопасности в течение установленного времени хранения. Реагирование на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнения объема (емкости) памяти;

17) Мониторинг (просмотр, анализ) результатов регистрации событий безопасности и реагирование на них. Генерирование временных меток и (или) синхронизация системного времени в ИС;

18) Защита информации о событиях безопасности. Обеспечение возможности просмотра и анализа информации о действиях отдельных пользователей в ИС;

19) Обнаружение вторжений. Обновление базы решающих правил;

20) Выявление, анализ и устранение уязвимостей ИС. Контроль установки обновлений программного обеспечения, включая программное обеспечение СЗИ;

21) Контроль работоспособности, параметров настройки и правильности функционирования ПО и СЗИ. Контроль состава технических средств, ПО и СЗИ;

22) Контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС;

23) Типовые системы защиты от НСД и от угроз вредоносного кода;

24) Типовые системы защиты межсетевого экранирования и защиты каналов связи, системы обнаружения вторжения и мониторинга событий безопасности;

25) Комплексные системы контроля защищенности;

26) Этапы и подсистемы контроля защищенности.

6.5. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Полный банк заданий для текущего, рубежных контролей и промежуточной аттестации по дисциплине, показатели, критерии, шкалы оценивания компетенций, методические материалы, определяющие процедуры оценивания образовательных результатов, приведены в учебно-методическом комплексе дисциплины.

7. ОСНОВНАЯ И ДОПОЛНИТЕЛЬНАЯ УЧЕБНАЯ ЛИТЕРАТУРА

7.1. Основная учебная литература

1. Методический документ. Меры защиты информации в государственных информационных системах (утв. ФСТЭК России 11.02.2014) [Электронный ресурс] https://fstek.ru/ сайт. – Электрон. текстовые дан. – Режим доступа: https://fstec.ru/component/attachments/download/675;

2. Михайловская А.С. Методика контроля защищенности конфиденциальной информации в автоматизированной системе от несанкционированного доступа [Электронный ресурс] / А.С. Михайловская // https://moluch.ru/ сайт. – Электрон. текстовые дан. – Режим доступа: https://moluch.ru/archive/116/31904/, свободный. – Загл. с экрана;

3. Скрипник Д. Техническая защита информации. Организация защиты информации ограниченного доступа, не содержащей сведения, составляющие государственную тайну [Электронный ресурс]: курс лекций: учебное пособие: для студентов вузов / Д. Скрипник; Интернет-университет информационных технологий. – Электрон. дан. – М.: Интернет-Университет информационных технологий, 2004. – Режим доступа: https://intuit.ru/studies/courses/3649/891/info, свободный. – Загл. с экрана.

7.2 Нормативно-правовое обеспечение дисциплины:

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

2. Федеральный закон Российской Федерации «О персональных данных» от 27.06.2006 г. № 152-ФЗ;

3. Федеральный закон Российской Федерации «О техническом регулировании» от 27.12.2002 № 184-ФЗ;

4. Приказ ФСБ России от 06.05.2019 "Об утверждении Требований к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты";

5. ГОСТ Р ИСО/МЭК 15408-3-2013 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты доверия к безопасности»;

6. ГОСТ Р ИСО/МЭК 13335-1-2006 ИТ. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий;

7. ГОСТ Р 56939-2016. Защита информации. Разработка безопасного программного обеспечения.

8. РЕСУРСЫ СЕТИ «ИНТЕРНЕТ», НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1) официальный сайт Федеральной службы по техническому и экспортному контролю РФ: http://fstec.ru;

2) официальный сайт ФСБ России: http://www.fsb.ru и т.д.

3) «Консультант-плюс»: http://www.consultant.ru;
4) «Гарант»: http://www.garant.ru;
5) ЭБС «Лань» - https://e.lanbook.com/;
6) ЭБС «Znanium» - https://znanium.com/;
7) ЭБС «Консультант студента» - https://www.studentlibrary.ru;
8) ЭБС IPR BOOKS - http://www.iprbookshop.ru/;
9) национальный Открытый Университет «ИНТУИТ» - https://intuit.ru;
10) сайт КГУ. Научно-исследовательский отдел - http://nio.kgsu.ru/;
11) электронная библиотека КГУ - http://dspace.kgsu.ru/xmlui/;
12) «Кодекс»: http://www.kodeks.ru.

9. ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ИНФОРМАЦИОННЫЕ СПРАВОЧНЫЕ СИСТЕМЫ

1. ЭБС «Лань».
2. ЭБС «Консультант студента».
3. ЭБС «Znanium.com».
4. «Гарант» - справочно-правовая система.

10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Материально-техническое обеспечение по реализации дисциплины осуществляется в соответствии с требования ФГОС ВО по данной образовательной программе.

11. Для студентов, обучающихся с использованием дистанционных образовательных технологий

При использовании электронного обучения и дистанционных образовательных технологий (далее ЭО и ДОТ) занятия полностью или частично проводятся в режиме онлайн. Объем дисциплины и распределение нагрузки по видам работ соответствует п. 4.1. Распределение баллов соответствует п. 6.2 либо может быть изменено в соответствии с решением кафедры, в случае перехода на ЭО и ДОТ в процессе обучения. Решение кафедры об используемых технологиях и системе оценивания достижений, обучающихся принимается с учетом мнения ведущего преподавателя и доводится до сведения обучающихся.

ПРИЛОЖЕНИЕ 1

Аннотация к рабочей программе дисциплины
«Методы контроля защищенности информации в информационных системах»

образовательной программы высшего образования –
программы специалитета
10.05.03 – Информационная безопасность автоматизированных систем
Специализация №5
Безопасность открытых информационных систем

Трудоемкость дисциплины: 3 з.е. (108 академических часа)
Семестр: 6 (очная форма обучения)
Форма промежуточной аттестации: зачет.

Содержание дисциплины

Нормативно-правовое регулирование защищенности информации. Средства контроля и анализа. Типовые системы контроля защиты. Методология контроля защищенности информации.