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

Н. Я. Великите

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие по изучению дисциплины
для студентов специальности
10.05.03 «Информационная безопасность автоматизированных систем»,
специализация «Безопасность открытых информационных систем»

Калининград
Издательство ФГБОУ ВО «КГТУ»
2025

УДК 004.056.57(076)

Рецензент
кандидат технических наук, доцент кафедры теории машин и механизмов и деталей машин ФГБОУ ВО «Калининградский государственный технический университет» О. С. Витренко

Великите, Н. Я.
Теоретические основы компьютерной безопасности: учебно-методическое пособие для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем», специализация «Безопасность открытых информационных систем» / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2025. – 45 с.

Учебно-методическое пособие является руководством к изучению дисциплины «Теоретические основы компьютерной безопасности» для студентов специальности 10.05.03 «Информационная безопасность автоматизированных систем». В нем представлен тематический план изучения дисциплины, содержание дисциплины по ее разделам и темам, темы практических занятий, указания к изучению каждой темы, рекомендации по выполнению практических заданий. Содержатся требования к текущей и промежуточной аттестации, определены условия получения положительной оценки.
Табл. 2, рис. 4, список лит. – 10 наименований

Учебно-методическое пособие по изучению дисциплины рекомендовано к использованию в учебном процессе в качестве локального электронного методического материала методической комиссией института цифровых технологий 29 апреля 2025 г., протокол № 3

УДК 004.056.57(076)

ОГЛАВЛЕНИЕ

1. ВВЕДЕНИЕ

В данном учебно-методическом пособии изложены основы теории компьютерной безопасности, объединяющие широкий спектр проблем защиты информации в процессе ее преобразования, хранения и передачи в автоматизированных системах обработки данных. Приводится описание основных моделей систем защиты и наиболее существенные результаты их анализа. Также уделено внимание важному понятию компьютерной безопасности – политике безопасности.

Целью освоения дисциплины «Теоретические основы компьютерной безопасности» является: формирование компетенций в области построения и использования моделей безопасности в компьютерных системах, исследования особенностей распределения прав доступа в моделях безопасности.

В результате изучения теоретических основ компьютерной безопасности перед студентом ставятся следующие задачи: студент должен составить представление о компьютерных системах и механизмах их защиты в терминах объектно-субъектных моделей, изучить формальные модели безопасности, политики безопасности, а также уметь использовать теоретические знания моделей механизмов защиты компьютерных систем и критериев, обеспечивающих их защит

В результате освоения дисциплины ожидается, что студенты получат целостное представление о широкой сфере проблем обеспечения теоретических основ компьютерной безопасности в автоматизированных системах и будут:

знать:

– формальные модели, лежащие в основе автоматизированных систем защиты информации.

уметь:

– применять математические модели при проектировании систем защиты информации автоматизированных систем.

владеть:

– навыками исследования формальных моделей систем защиты информации

Дисциплина «Теоретические основы компьютерной безопасности» относится к Модулю «Профессиональный модуль» относится к блоку 1 части, формируемой участниками образовательных отношений.

В учебно-методическом пособии по изучению дисциплины с практическими заданиями 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 потребует 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 промежуточной аттестации – экзамену.

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

2. ТЕМАТИЧЕСКИЙ ПЛАН

Тематический план изучения дисциплины «Теоретические основы компьютерной безопасности» представлен в таблице 1.

Таблица 1 – Тематический план изучения дисциплины «Теоретические основы компьютерной безопасности»

	Раздел (модуль) дисциплины	**Тема**	**Объем аудиторной работы, ч**	**Объем самостоятельной работы, ч**
		Лекции		
1.1	Структура теории компьютерной безопасности	Тема 1 История развития теории и практики обеспечения компьютерной безопасности	4	3
1.2		Тема 2 Основные понятия компьютерной безопасности	4	3
1.3		Тема 3 Анализ угроз компьютерной безопасности	5	3
2.1	Формальные политики безопасности	Тема 4 Понятие формальной политики, доступа и монитора безопасности	5	3
2.2		Тема 5 Основные типы формальных политик безопасности	5	3
2.3		Тема 6 Разработка и реализация формальных политик безопасности	5	3
3.1	Математические модели компьютерной безопасности	Тема 7 Модели безопасности на основе дискреционной политики	5	3
3.2		Тема 8 Модели безопасности на основе мандатной политики	5	3
3.3		Тема 9 Модели безопасности на основе тематической политики	5	3
3.4		Тема 10 Модели безопасности на основе ролевой политики	5	3
			48	**30**
		Практические занятия		

	Раздел (модуль) дисциплины	Тема	Объем аудиторной работы, ч	Объем самостоятельной работы, ч
1.1	Структура теории компьютерной безопасности	Реализация политики информационной безопасности на примере дискреционной модели	4	3
1.2		Изучение уязвимости модели Харрисона-Руззо Ульмана	4	3
1.3		Реализация распространения прав доступа по модели take-grant	4	3
2.1	Формальные политики безопасности	Расширенная модель прав доступа take-grant	4	3
2.2		Нарушение дискреционной политики безопасности программой «Троянский конь»	4	3
2.3		Мандатные политики безопасности	4	3
3.1	Математические модели компьютерной безопасности	Субъектно-объектная модель. Изолированная программная среда	4	4
3.2		Работа с матрицей доступов. Домены безопасности	4	4
			32	**26**
		Рубежный (текущий) и итоговый контроль		
1.	Общие вопросы информационной безопасности	Тестирование (ЭИОС)	8 (РЭ)	
		Экзамен		1,25 (КА)
			56 (СР)	34,75 Контроль

Итого: 180

3. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ И УКАЗАНИЯ К ИЗУЧЕНИЮ

3.1 Раздел 1. Структура теории компьютерной безопасности

3.1.1 Тема 1.1 История развития теории и практики обеспечения компьютерной безопасности

Перечень изучаемых вопросов

1.Введение в предмет компьютерной безопасности (КБ).

2.Основные этапы теории и практики КБ.

3.Отечественная школа КБ.

Методические указания к изучению

В данной теме мы рассмотрим предмет и задачи дисциплины. Рассмотрим специфику, задачи обеспечения безопасности компьютерной информации в автоматизированных системах. Ознакомимся с этапами развития теории КБ. Рассмотрим основополагающие работы зарубежных и отечественных авторов. Покажем, как сформировались три составляющих и, соответственно, три, хотя и взаимосвязанных, но различных направления защиты компьютерной информации – обеспечение конфиденциальности информации, обеспечение целостности данных, обеспечение сохранности и работоспособности данных.

Рекомендуемая литература:

[3, гл. 1, 2]; [2, гл. 1]

Контрольные вопросы для самопроверки

1. Какие ключевые этапы развития компьютерной безопасности вы можете назвать? Какие события стали отправной точкой?

2. Опишите ранние методы защиты компьютерных систем до появления Интернета. Каковы были первые угрозы?

3. Какие изменения произошли в практике информационной безопасности после массового распространения персональных компьютеров?

4. Как повлияло развитие Интернета на развитие методов кибербезопасности?

5. Назовите ключевых исследователей и разработчиков, которые внесли значительный вклад в теорию и практику компьютерной безопасности.

6. В чем заключаются различия между ранними методами шифрования и современными криптографическими стандартами?

7. Какие основные категории угроз существовали в эпоху первых сетей передачи данных? Что изменилось сегодня?

8. Какое влияние оказали государственные программы и инициативы на формирование стандартов кибербезопасности?

9. Опишите эволюцию законодательных актов, регулирующих компьютерную безопасность в разных странах мира.

10. Какие значимые инциденты в области кибератак и утечек данных повлияли на дальнейшее развитие подходов к защите информации?

11. Объясните, почему появились стандарты, такие как ISO/IEC 27001, и как они влияют на современные подходы к обеспечению безопасности?

12. Сравните принципы работы антивирусных программ прошлого и настоящего. Какие новые технологии используются для борьбы с вредоносным ПО?

13. Как появление облачных технологий и интернета вещей (IoT) повлияло на стратегии обеспечения безопасности?

14. Как изменились роли специалистов по кибербезопасности за последние десятилетия? Какие компетенции стали наиболее востребованными?

15. Как теория компьютерных наук и прикладная математика повлияла на развитие современных методов защиты информации?

16. Какие инновационные решения сейчас применяются для предотвращения атак нулевого дня?

17. Какие меры были приняты международными организациями для повышения уровня глобальной киберзащиты?

18. В каких областях деятельности особенно остро ощущается необходимость внедрения новых подходов к кибербезопасности?

19. Какие перспективные направления исследований развиваются в сфере компьютерной безопасности сегодня?

20. Оцените роль социальной инженерии в эволюции киберпреступлений и какие меры противодействия этому виду угроз существуют?

3.1.2 Тема 1.2 Основные понятия компьютерной безопасности

Перечень изучаемых вопросов

1. Иерархия понятий в области ИБ
2. Современное содержание понятия компьютерной безопасности
3. Методологическая база понятия ИБ.

Методические указания к изучению

В рамках данной темы мы познакомимся со следующими понятиями:

– «информационная безопасность» показывает, что ключевыми является следующие аспекты – информационная сфера (объект), угрозы (внутренние и внешние) и состояние защищенности (предмет объекта).

В этой логике сфера понятия «компьютерная безопасность» сужается до объекта, именуемого «компьютерной системой», под которой будем понимать человеко-машинную систему, представляющую совокупность электронно-программируемых технических средств обработки, хранения и представления дан-

ных, программного обеспечения (ПО), реализующего информационные технологии осуществления каких-либо функций, и информации (данных). В развитии этой логики, под компьютерной безопасностью понимается состояние защищенности (безопасность) информации (данных) в компьютерных системах и безотказность (надежность) функционирования компьютерных систем. В результате составляющими компьютерной безопасности выступают безопасность информации (данных), накапливаемых, обрабатываемых в компьютерной системе, и безопасность (безотказность, надежность) функций КС.

Содержательный анализ самого понятия «информация» (сведения (сообщения, данные) независимо от формы их представления), особенностей процессов и технологий ее сбора, обработки, хранения, представления и выдачи показывает, что безотносительно к функционально-содержательной стороне работы с информацией (данными) понятие «безопасность информации» включает три составляющих:

– обеспечение конфиденциальности;

– обеспечение целостности;

– обеспечение доступности.

Рекомендуемая литература: [2, гл. 1].

Контрольные вопросы для самопроверки

1. Что такое информационная безопасность?

2. Какие ключевые уровни иерархии понятий в области ИБ вы можете назвать?

3. Как соотносятся между собой такие понятия, как конфиденциальность, целостность и доступность данных?

4. Приведите пример нарушения конфиденциальности данных и последствия этого инцидента.

5. Объясните, почему обеспечение целостности данных важно для организаций.

6. Каковы основные цели защиты информации на уровне предприятия?

7. Опишите методы обеспечения доступности информационных ресурсов.

8. Какие угрозы информационной безопасности наиболее распространены на современном этапе развития технологий?

9. В чем заключается принцип многоуровневой защиты информации?

10. Назовите основные принципы классификации угроз информационной безопасности.

3.1.3 Тема 1.3 Анализ угроз компьютерной безопасности

Перечень изучаемых вопросов

1. Понятие и классификация угроз.
2. Идентификация и каталогизация угроз.

Методические указания к изучению

Понятие угрозы безопасности является наряду с понятием безопасности информации краеугольным камнем в сфере компьютерной безопасности, поскольку выбор защитных механизмов определяется исходя из целей устранения, нейтрализации угроз, снижения последствий (ущерба) от их возможного проявления и воздействия.

Для того чтобы обеспечить эффективную защиту информации в компьютерной системе, необходимо в первую очередь рассмотреть и проанализировать все факторы, представляющие угрозу информационной безопасности. Рассмотрение понятий: угроза, атака, уязвимость,

Рассмотрена классификация угроз информационной безопасности компьютерных систем по ряду базовых признаков. Понятия классификация, систематизация, каталогизация.

Рекомендуется просмотреть соответствующие ресурсы по ссылкам в ЭИОС, которые обращаются к анализу угроз в компьютерной безопасности.

Рекомендуемая литература: [1, гл. 2].

Контрольные вопросы для самопроверки

1. Назовите две составляющие в информационной системе.
2. Какие процессы называются информационными процессами?
3. Что понимается под понятием «Информационная среда»?
4. Что является объектом защиты информации?
5. Что является предметом защиты в КС?
6. Что понимается под информационной безопасностью?
7. Дайте определение уязвимости КС.
8. Назовите основные угрозы безопасности компьютерной системы.
9. Что представляет собой «защищенная компьютерная система»?
10. Дайте определение безопасности компьютерной системы.
11. Дайте определение угрозе.
12. Дайте определение атаке.
13. Дайте определение уязвимости КС.
14. Назовите основные угрозы безопасности компьютерной системы.
15. Что представляет собой «защищенная компьютерная система»?

3.2. Раздел 2. Формальные политики безопасности

3.2.1 Тема 2.1 Понятие формальной политики, доступа и монитора безопасности

Перечень изучаемых вопросов:

1. Объект, субъект, доступ
2. Монитор безопасности компьютерной системы.

Методические указания к изучению

Фундаментальным понятием в сфере защиты информации компьютерных систем является политика безопасности. Под ней понимают интегральную совокупность норм и правил, регламентирующих процесс обработки информации, выполнение которых обеспечивает состояние защищенности информации в заданном пространстве угроз. Формальное выражение политики безопасности (математическое, схемотехническое, алгоритмическое и т. д.) называют моделью безопасности. Модели безопасности играют важную роль в процессах разработки и исследования защищенных компьютерных систем, так как обеспечивают системотехнический подход, включающий решение следующих важнейших задач:

– выбор и обоснование базовых принципов архитектуры защищенных компьютерных систем (КС), определяющих механизмы реализации средств и методов защиты информации;

– подтверждение свойств (защищенности) разрабатываемых систем путем формального доказательства соблюдения политики безопасности (требований, условий, критериев);

– составление формальной спецификации политики безопасности как важнейшей составной части организационного и документационного обеспечения разрабатываемых защищенных компьютерных систем.

По сути модели безопасности являются исходным связующим элементом в триаде «Заказчик (Потребитель)-Разработчик (Производитель)-Эксперт (Аудитор)». На основе моделей безопасности заказчики могут формулировать те требования к защищенным КС, которые соответствуют политике безопасности, технологическим процессам обработки информации, принятым в своих организациях и предприятиях. Разработчики на основе моделей безопасности формируют технико-технологические требования и программно-технические решения по разрабатываемым системам. В этой теме также рассматриваются понятия: субъект, объект, доступ, монитор безопасности, домен безопасности,

Рекомендуемая литература: [2, гл. 1]; [3, гл. 3].

Контрольные вопросы для самопроверки:

1. Что представляет собой монитор безопасности и какие функции он выполняет?

2. Какие компоненты входят в состав системы мониторинга безопасности?

3. Какие данные собирает и обрабатывает монитор безопасности?

4. Какие технологии используются для построения эффективных систем мониторинга?

5. В чем разница между мониторингом событий и мониторингом поведения пользователей?

6. Как монитор безопасности помогает в выявлении аномалий в работе информационной системы?

7. Какие методы применяются для обнаружения вторжений через монитор безопасности?

8. Приведите пример эффективной архитектуры системы мониторинга безопасности.

9. Какая информация передается в журнал событий, и как она используется?

10. Какие меры предосторожности необходимы для защиты самих журналов событий от несанкционированного доступа?

11. Какими способами осуществляется защита данных, передаваемых монитору безопасности?

3.2.2 Тема 2.2 Основные типы формальных политик безопасности

Перечень изучаемых вопросов

1. Гарантирование выполнения политики безопасности. Изолированная программная среда.

2. Аксиомы защищённости компьютерных систем.

3. Характеристика основных типов формальных политик безопасности.

Методические указания к изучению

Большинство моделей разграничения доступа основывается на представлении КС как совокупности субъектов и объектов доступа.
Приводятся основные положения субъектно-объектной формализации компьютерных систем в аспекте безопасности информации.

Постулируя наличие в КС субъекта, реализующего политику безопасности, рассмотрены описания (на уровне моделей) некоторых известных политик безопасности. Для строгого и однозначного толкования норм и правил политики безопасности обычно дается ее формализованное описание в виде соответствующей модели. Основная цель такого описания – это определение условий, которым должно подчиняться поведение системы, выработка критерия безопасности и проведение формального доказательства соответствия системы этому критерию при соблюдении установленных правил и ограничений. На практике

это означает, что только соответствующим образом уполномоченные пользователи получат доступ к информации и смогут осуществить с ней только санкционированные действия.

Все существующие в настоящее время модели безопасности основаны на следующих базовых представлениях.

1. Компьютерная система является совокупностью взаимодействующих сущностей – субъектов и объектов. Объекты можно интуитивно представлять в виде контейнеров, содержащих информацию, а субъектами считать выполняющиеся программы, которые воздействуют на объекты различными способами. При таком представлении безопасность обработки информации обеспечивается путем решения задачи управления доступом субъектов к объектам в соответствии с тем набором правил и ограничений, которые образуют политику безопасности. Считается, что система безопасна, если субъекты не имеют возможности нарушать правила политики безопасности. Таким образом, общим кодом для всех моделей является именно разделение множества сущностей, образующих систему, на множества субъектов и объектов.

2. Все взаимодействия в системе моделируются установлением отношений определенного типа между субъектами и объектами. Множество типов таких отношений определяется в виде набора операций, которые субъекты могут производить над объектами.

3. Все операции между субъектами и объектами, контролируемые монитором взаимодействий, либо запрещаются, либо разрешаются в соответствии с правилами политики безопасности.

4.Политика безопасности задается в виде правил, определяющих все взаимодействия между субъектами и объектами. Взаимодействия, приводящие к нарушению этих правил, пресекаются средствами контроля доступа и не могут быть осуществлены.

5. Совокупность множеств субъектов, объектов и отношений между ними (установившихся взаимодействий) определяет состояние системы. В этом пространстве состояний каждое состояние системы является либо безопасным, либо небезопасным в соответствии с принятым в модели критерием безопасности.

6. Основной элемент модели безопасности – это доказательство того, что система, находящаяся в безопасном состоянии, не может перейти в небезопасное состояние при соблюдении всех установленных правил и ограничений.

Среди моделей политики безопасности можно выделить три основных типа: дискреционные (произвольные), мандатные (нормативные) и ролевые. В основе этих моделей лежат, соответственно, дискреционное управление доступом (Discretionary Access Control – DAC), мандатное управление доступом

(Mandatory Access Control – MAC) и ролевое управление доступом (Role-Based Access Control – RAC).

Рекомендуемая литература: [3, гл. 3].

Контрольные вопросы для самопроверки

1. Что такое изолированная программная среда? Как она помогает обеспечить выполнение политики безопасности?
2. Какие технологии используются для реализации изолированной среды? Приведите примеры.
3. В чём заключается отличие виртуализации от контейнеризации в контексте изоляции программного обеспечения?
4. Какие существуют подходы к обеспечению доверия к программной среде? Объясните принципы доверенной загрузки.
5. Какие угрозы связаны с использованием изолированных сред и как их минимизировать?
6. Как влияет использование изолированных сред на производительность системы?
7. Какие меры применяются для защиты интерфейсов взаимодействия между изолированными средами?
8. Опишите, какие механизмы используются для контроля целостности программной среды после её запуска.
9. Чем отличается изолированная среда для разработки от производственной среды?
10. Какие нормативные требования предъявляются к использованию изолированных сред в государственных информационных системах?
11. Перечислите основные аксиомы защищенности компьютерных систем. Поясните каждую из них.
12. Почему принцип минимального привилегирования является важным элементом в обеспечении информационной безопасности?
13. Что означает аксиома о невозможности проверки всех возможных путей атаки? Как это влияет на проектирование защитных мер?
14. Объясните, почему невозможно создать абсолютно защищённую систему. Какие факторы влияют на эту невозможность?
15. Почему система должна изначально считаться уязвимой до тех пор, пока не доказано обратное?
16. Какие современные методы тестирования систем безопасности соответствуют аксиоме о проверке на наличие слабых мест?
17. Какова роль аудита и мониторинга в рамках соблюдения аксиом защищённости?
18. Приведите пример нарушения одной из аксиом защищённости и последствия такого нарушения.

19. Может ли одна из аксиом нарушаться сознательно ради удобства пользователей? Если да, приведите пример.

20. Какие новые вызовы и угрозы возникают в условиях современных технологий (например, IoT), и как они соотносятся с аксиомами защищённости?

21. Дайте определение формальной политики безопасности. В каких случаях она применяется?

22. Перечислите основные типы формальных политик безопасности (дискреционная, мандатная, ролевая). Объясните различия между ними.

23. Каким образом дискреционные модели доступа обеспечивают гибкость управления доступом?

24. В чём заключаются преимущества и недостатки мандатных моделей доступа?

25. Как реализуется управление ролями в ролевых моделях доступа? Приведите примеры.

26. Какие формальные политики наиболее подходят для корпоративных сетей? Почему?

27. Объясните, каким образом политика безопасности связана с концепциями конфиденциальности, целостности и доступности.

28. В каком случае применение мандатной модели предпочтительнее дискреционной?

29. Какие сложности возникают при внедрении формальных политик безопасности в распределённых вычислительных средах?

30. Как осуществляется мониторинг соответствия действий сотрудников требованиям формальной политики безопасности?

3.2.3 Тема 2.3 Разработка и реализация формальных политик безопасности

Перечень изучаемых вопросов

1. Механизм реализации политики безопасности в локальном сегменте компьютерной системы

2. Управление безопасностью компьютерной системой

Методические указания к изучению

Субъект, который активизируется при возникновении потока информации от любого субъекта (его ассоциированного объекта) к любому объекту называется монитором обращений. В теории компьютерной безопасности различают два вида монитора обращений – индикаторный и содержательный.

Политику безопасности механизма авторизации реализует монитор безопасности объектов (МБО) – монитор обращений, который разрешает поток, принадлежащий только подмножеству легального доступа P1.

В мониторе безопасности объектов реализуется та или иная модель политики безопасности, с помощью которой осуществляется фильтрация потоков, относящихся к множеству потоков легального доступа.

Предполагается, что в локальном сегменте компьютерной системы существуют только попарно корректные субъекты, замкнутые в изолированной программной среде, с контролем целостности порождаемых субъектов. Другими словами, в составе локального сегмента компьютерной системы существует монитор безопасности субъектов (МБС). Кроме того, в локальном сегменте компьютерной системы действует монитор безопасности объектов (МБО), реализующий некоторую политику безопасности.

В защищенной компьютерной системе должна быть создана изолированная программная среда, в состав которой входят монитор безопасности объектов, гарантирующий порождение легальных потоков, и монитор безопасности субъектов, гарантирующий порождение субъектов только для определенных пар субъект-объект.

Монитор безопасности субъектов и монитор безопасности объектов относятся к субъектам защищенной компьютерной системы и, следовательно, имеют ассоциированные с ними объекты-данные, которые содержат необходимые для функционирования субъектов данные.

Объекты – данные, ассоциированные с монитором безопасности субъектов (МБС) и монитором безопасности объектов (МБО) называют объектом управления (ОУ). Совокупность МБО, МБС и ОУ называют ядром безопасности.

Управление безопасностью изучает вопросы формирования и изменения объекта ОУ для субъектов, реализующих политику безопасности (МБО) и субъектов, гарантирующих её выполнение (МБС).

Компьютерная система называется управляемой, если в ней существует субъект, для ассоциированных объектов которого существует поток к объекту управления. Этот субъект называется субъектом администрирования или администрирующим субъектом. Пользователя, который управляет администрирующим субъектом, обычно называют администратором безопасности компьютерной системы.

Можно так же сказать, что только администратор безопасности должен иметь возможность порождения субъекта администрирования. Следовательно, только субъект администрирования должен иметь доступ на запись к объекту управления, а МБО и МБС должны иметь доступ на чтение к объекту управления.

Компьютерная система называется корректно управляемой, если поток к объекту управления существует только для субъекта управления (администрирующего субъекта).

Утверждение (о корректном управлении в ИПС): если в компьютерной системе поддерживается изолированная программная среда с контролем неизменности объектов-источников и существует МБО, который разрешает доступ на запись к объекту управления только субъекту администрирования, то с момента активизации МБО управление в компьютерной системе корректно.

Рекомендуемая литература: [3, гл. 10].

Контрольные вопросы для самопроверки

1. Дайте определение политики безопасности.
2. Дайте определение понятия «Доступа».
3. Назовите основные характеристики системы.
4. Назовите основные типы политики безопасности.
5. Что значит «мандатное управление доступом»?
6. Что является основой мандатной политики безопасности?
7. Что значит «дискреционное управление доступом»?
8. Что является основой ролевой политики безопасности?
9. Что понимается под доменом безопасности?
10. Что называется монитором обращений?
11. Дайте определение монитора безопасности объектов.
12. Что называется методом расщепления прав пользователя?
13. Какая программная среда называется изолированной?
14. Какие два субъекта называются корректными относительно друг друга?
15. Какая программная среда называется замкнутой по порождению объектов?
16. Что называют объектом управления?
17. Что является ядром безопасности?
18. Какая компьютерная система называется корректно управляемой?
19. В чём состоит важность основной аксиомы теории защиты информации?
20. Какие основные виды политик безопасности рассматриваются в теории защиты информации.

3.3. Раздел 3. Математические модели компьютерной безопасности

3.3.1 Тема 3.1 Модели безопасности на основе дискреционной политики

Перечень изучаемых вопросов

1. Общая характеристика политики дискреционного доступа.
2. Пятимерное пространство Хартсона.
3. Модели на основе матрицы доступа.
4. Модели распространения прав доступа.

Методические указания к изучению

Модели безопасности, строящиеся на субъектно-объектной модели КС, еще называют моделями конечных состояний. В данных моделях инициализация информационных потоков трактуется как запросы субъектов на доступ к объектам, которые в зависимости от политики безопасности разрешаются или запрещаются. Осуществление субъектом разрешенного доступа к объекту переводит систему в следующий момент времени в другое состояние, рассматриваемое как совокупность состояний субъектов и объектов системы.

Проблема безопасности в КС рассматривается с точки зрения анализа и исследования условий, правил, порядка и т. п. разрешений запросов на доступ, при которых система, изначально находясь в безопасном состоянии, за конечное число переходов перейдет также в безопасное состояние.

Политика дискреционного доступа охватывает самую многочисленную совокупность моделей разграничения доступа, реализованных в большинстве защищенных КС, и исторически является первой, проработанной в теоретическом и практическом плане. Специфика и значение моделей заключается в том, что, исходя из способа представления (описания) области безопасного доступа и механизма разрешений на доступ анализируется и доказывается, что за конечное число переходов система останется в безопасном состоянии. В теоретическом и практическом плане наибольшее развитие и применение получили дискреционные модели, основанные на матрице доступа. В данных моделях область безопасного доступа строится как прямоугольная матрица (таблица), строки которой соответствуют субъектам доступа, столбцы объектам доступа, а в ячейках записываются разрешенные операции соответствующего субъекта над соответствующим объектом. В моделях распространения прав доступа проблема безопасности КС рассматривается с точки зрения анализа возможности или невозможности получения каким-либо субъектом определенных прав доступа к определенному объекту. Иначе говоря, анализируются, прежде всего, изменения прав доступа субъектов к объектам в результате некоторых обусловленных операций (переходов), а не сами процессы осуществления доступов субъектов к объектам.

Рекомендуемая литература: [3, гл. 3, 4].

Контрольные вопросы для самопроверки

1. Что такое дискреционная модель безопасности и в чем ее основные особенности?
2. Какие элементы включает в себя дискреционная модель безопасности?
3. Как реализуется контроль доступа в дискреционной модели безопасности?
4. Какие права доступа могут быть предоставлены пользователям в рамках дискреционной модели?
5. Какие механизмы используются для управления правами доступа в дискреционной модели?
6. Каковы основные преимущества и недостатки дискреционной модели безопасности?
7. Какие существуют примеры реализации дискреционной модели безопасности в операционных системах?
8. Как дискреционная модель безопасности защищает информацию от несанкционированного доступа?
9. Какие угрозы безопасности могут быть связаны с использованием дискреционной модели?
10. Как можно улучшить безопасность в рамках дискреционной модели?

3.3.2 Тема 3.2 Модели безопасности на основе мандатной политики

Перечень изучаемых вопросов

1. Общая характеристика моделей полномочного (мандатного) доступа
2. Модель Белла-ЛаПадулы.
3. Расширения модели Белла-ЛаПадулы.

Методические указания к изучению

Модели безопасности, строящиеся на Мандатное УД (Mandatory Access Control – MAC) – разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах, и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности. Оно основано на сопоставлении атрибутов безопасности субъекта (уровня допуска пользователя) и объекта (грифа секретности информации).

Мандатная модель управления доступом основана на правилах секретного документооборота, принятых в государственных и правительственных учреждениях многих стран. Основным положением данной ПБ, взятым из ре-

альной жизни, является назначение всем участникам процесса обработки защищаемой информации и документам, в которых она содержится, специальной метки, получившей название уровень безопасности (метка безопасности). Метка субъекта описывает его благонадежность, а метка объекта – степень закрытости содержащейся в нем информации. Уровни секретности, поддерживаемые системой, образуют множество, упорядоченное с помощью отношения доминирования. Такое множество может выглядеть следующим образом: сов. секретно, секретно, конфиденциально, несекретно и т. д.

Система в мандатной модели представляется в виде множеств субъектов S, объектов O, решетки уровней безопасности L и матрицы доступа M.

Достоинства мандатного УД:

• экономия памяти, так как элементы матрицы доступа не хранятся, а динамически вычисляются при попытке доступа для конкретной пары субъект-объект на основе их меток;

• удобство корректировки базы данных защиты, то есть модификации меток;

• принудительное УД хорошо согласуется с работой государственных, правительственных и военных организаций, так как переносит общепринятые и хорошо отработанные принципы обращения с бумажными секретами на современную основу работы с документами.

Недостатки мандатного УД:

• затруднено задание прав доступа конкретного субъекта к конкретному объекту;

• каждый субъект и объект должен быть помечен и при любых операциях с данными метки должны оставаться правильными. В особенности это относится к экспорту и импорту данных. Например, печатный документ должен открываться заголовком, содержащим текстовое и/или графическое представление метки безопасности. Аналогично, при передаче файла по каналу связи должна передаваться и ассоциированная с ним метка, причем в таком виде, чтобы удаленная система могла ее правильно трактовать, несмотря на возможные различия в уровнях секретности и наборе категорий.

Наиболее известными мандатными моделями являются ММ Белла-Лападула (Дэвид Белл и Леонардо ЛаПадула), ММ Биба, решетчатая модель Д. Деннинга, ММ совместного доступа с уполномоченными субъектами и т. д.

Рекомендуемая литература: [3, гл. 5].

Контрольные вопросы для самопроверки

1. Что такое мандатная политика безопасности?

2. В чём отличие между мандатной и дискреционной моделями управления доступом?

3. Какие ключевые компоненты включает мандатная модель безопасности?

4. Как классифицируются уровни секретности в мандатной модели?

5. Что означает принцип необходимости знания (need-to-know) в контексте мандатной политики?

6. Опишите механизм работы системы классификации объектов и субъектов в мандатной политике.

7. Какие требования предъявляются к субъекту и объекту для выполнения операций чтения/записи в мандатной модели?

8. Как определяется уровень доверия субъекта в мандатной модели?

9. Чем отличаются уровни конфиденциальности и целостности в мандатной модели?

10. Какие существуют уровни допуска в классической мандатной модели?

11. Приведите пример практического применения мандатной модели в государственных структурах.

12. Какие ограничения накладываются на пользователей в рамках мандатной модели?

13. Каким образом мандатная модель предотвращает утечку конфиденциальной информации?

14. Какие преимущества имеет мандатная модель перед дискреционными политиками?

15. Какие недостатки присущи мандатной модели?

16. Каковы основные цели внедрения мандатной модели безопасности?

17. Какие принципы лежат в основе мандатной политики?

18. Как осуществляется контроль над уровнем допуска в мандатной модели?

19. Почему мандатную политику часто называют моделью Белла-ЛаПадулы?

20. Опишите работу принципа no write down и no read up.

21. Какие современные технологии используют элементы мандатной политики?

22. Можно ли сочетать мандатную и дискреционную модели? Если да, то каким образом?

23. Какие методы используются для проверки корректности реализации мандатной политики?

24. Какая связь существует между мандатной политикой и стандартами безопасности ISO 27001?

25. Как влияет мандатная модель на архитектуру информационных систем?

26. Как мандатная модель помогает обеспечить соответствие требованиям регуляторов?

27. В каких случаях использование мандатной модели неэффективно?

28. Какие практические шаги предпринимаются для аудита соблюдения мандатной политики?

29. В чем заключается разница между многоуровневой и двухуровневой мандатной моделью?

30. Как мандатная модель используется в системах защиты данных в банковской сфере?

3.3.3 Тема 3.3 Модели безопасности на основе тематической политики

Перечень изучаемых вопросов

1. Общая характеристика тематического разграничения доступа
2. Тематическая решетка мультирубрик иерархического рубрикатора
3. Модели тематико-иерархического разграничения доступа

Методические указания к изучению

Важным аспектом, присутствующим в практике разграничения доступа к «бумажным» ресурсам является тематическая «окрашенность» информационных ресурсов предприятий, учреждений по организационно-технологическим процессам и профилям деятельности. Организация доступа сотрудников к информационным ресурсам организации (в библиотеках, архивах, документальных хранилищах) осуществляется на основе тематических классификаторов. Все документы информационного хранилища тематически индексируются, т. е. соотносятся с теми или иными тематическими рубриками классификатора. Сотрудники предприятия согласно своим функциональным обязанностям или по другим основаниям получают права работы с документами определенной тематики. Данный подход, в сочетании с избирательным и мандатным доступом, обеспечивает более адекватную и гибкую настройку системы разграничения доступа на конкретные функционально-технологические процессы, предоставляет дополнительные средства контроля и управления доступом.

Анализ библиотечных и других автоматизированных систем документального поиска, основанных на тематическом индексировании содержания документов (текстов), показывает, что определяющее значение в таких системах имеет тематико-классификационная схема, в большинстве случаев именуемая тематическим рубрикатором. Применяются три основных способа тематической классификации:

- перечислительная классификация (дескрипторный подход);
- систематизированная классификация (иерархический подход);
- аналитико-синтетическая классификация (фасетный подход).

Рекомендуемая литература: [3, гл. 4–6].

Контрольные вопросы для самопроверки

1. Что такое тематическая политика в контексте информационной безопасности?

2. Какие существуют основные модели безопасности, основанные на тематической политике? Опишите каждую из них.

3. Какова роль меток конфиденциальности в моделях безопасности на основе тематической политики?

4. Почему модели безопасности на основе тематической политики считаются более строгими по сравнению с моделями на основе дискреционного контроля доступа?

3.3.4 Тема 3.4 Модели безопасности на основе ролевой политики

Перечень изучаемых вопросов

1. Модели ролевого доступа.
2. Модели индивидуально-группового доступа.
3. MMS-модель.

Методические указания к изучению

Анализ различных организационно-управленческих и организационно-технологических схем, показывает, что в реальной жизни сотрудники предприятий, учреждений выполняют определенные функциональные обязанности не от своего личного имени, а в рамках некоторой должности. Должность, которую можно трактовать как определенную роль, представляет некоторую абстрактную, точнее обобщенную сущность, выражающую определенный тип функций и тип положения работника (подчиненность, права и полномочия). Таким образом, в реальной жизни в большинстве организационно-технологических схем права и полномочия предоставляются конкретному сотруднику не лично (непосредственно), а через назначение его на определенную должность (роль), с которой он и получает некоторый типовой набор прав и полномочий.

Еще одним аспектом реальных организационно-технологических и управленческих схем является использование понятий прав и полномочий, как неких процедур над ресурсами системы, отражающих организационно-технологические процессы предметной области КС. Иначе говоря, права и полномочия сотрудникам по их должностям предоставляются не на уровне элементарных операций над ресурсами (читать, изменять, добавлять, удалять, создавать), а на уровне совокупностей элементарных операций, сгруппированных в отдельные логически обобщенные процедуры обработки информации (например, кредитные или дебетные операции над определенными бюджетами).

Таким образом, политика разграничения доступа в компьютерных системах, автоматизирующих те или иные организационно-технологические или организационно-управленческие процессы, должна строиться на основе функционально-ролевых отношений, складывающихся в предметной области КС.

Впервые подобный подход был рассмотрен в конце 70-х – начале 80-х годах в исследованиях по процессам разграничения доступа корпорации IBM и получил название ролевого управления доступом. В начале 80-х годов была представлена модель Лендвера-МакЛина, встречающаяся в литературе также под названием MMS-модели, сочетающая дискреционный и мандатный принципы разграничения доступа с использованием понятия и механизма ролей. Несколько позже появились и формальные выражения ролевых основ управления доступом (Role-Based Access Control –RBAC).

Ролевое УД (Role-Based Access Control – RAC) – универсальная надстройка (каркас), применяемая с дискреционным и мандатным УД и предназначенная для упрощения функций администрирования систем с большим количеством субъектов и объектов.

Суть ролевого УД состоит в том, что между пользователями и их правами доступа к объектам появляются промежуточные сущности – роли. Для каждого пользователя одновременно могут быть активными несколько ролей, каждая из которых дает ему определенные права доступа к объекту и, наоборот, несколько пользователей может выступать в одной роли по отношению к одному объекту. Между ролями могут быть установлены связи, аналогичные отношению наследования в ООП. Таким образом может быть построена иерархия ролей, используя которую можно существенно сократить количество контролируемых (администрируемых) связей.

Рекомендуемая литература: [2, гл. 1]; [4, гл. 8].

Контрольные вопросы для самопроверки

1. Назовите дискреционные модели безопасности.
2. Назовите мандатные модели безопасности.
3. К какому типу моделей политики безопасности относится модель АДЕПТ–50?
4. К какому типу моделей политики безопасности относится модель Харрисона-Руззо-Ульмана?
5. Что рассматривается в модель Харрисона- Руззо-Ульмана?
6. К какому типу моделей политики безопасности относится модель типизированной матрицы доступа?
7. Какая реализация модифицированной типизированной матрицей доступа называется ациклической?
8. Какая реализация модифицированной типизированной матрицей доступа называется циклической?

9. К какому типу моделей политики безопасности относится модель Белла–Лападулы?

10. Что называется уровнем безопасности в модели Белла–Лападулы?

11. Дайте определение решетки уровней безопасности в модели Белла – Лападулы.

12. На какие состояния делятся системы в классической мандатной модели Белла–Лападулы?

13. Назовите основную теорему безопасности (модель Белла–Лападулы).

14. Дайте понятия пользователь и роль в ролевой политики безопасности.

15. Что такое ролевая политика безопасности? В чём её отличие от мандатной модели?

16. Какие ключевые элементы составляют основу ролевой модели безопасности (RBAC)?

17. Чем отличается статическая роль от динамической роли в RBAC?

18. Опишите преимущества ролевой модели перед классической моделью управления доступом (DAC).

19. Какие уровни поддержки ролей существуют в RBAC? Поясните каждый уровень.

20. Каковы основные принципы минимизации привилегий в рамках ролевой политики безопасности?

21. В каких случаях целесообразно использовать ролевые политики безопасности, а когда лучше выбрать другие подходы?

22. Какие основные компоненты входят в архитектуру системы, поддерживающей RBAC?

23. Приведите пример ситуаций, где использование RBAC неэффективно или нежелательно.

24. Почему концепция разделения обязанностей является важной частью ролевой политики безопасности?

25. Объясните понятие иерархии ролей в контексте RBAC. Какие преимущества она даёт?

26. Что такое администрирование ролей в RBAC? Какие виды полномочий могут быть делегированы пользователям?

27. В чём заключается разница между назначением прав доступа непосредственно пользователям и использованием ролей?

28. Перечислите и поясните типы ограничений, которые могут применяться к ролям в RBAC.

29. Как модель RBAC влияет на безопасность в распределённых системах?

4. ПРАКТИЧЕСКИЕ ЗАНЯТИЯ

Практические занятия направлены на углубление знаний и закрепление основных понятий и методов, изучаемых в рамках дисциплины.

Основная цель занятий – научиться применять теоретические знания для решения прикладных задач.

Цель практических занятий по дисциплине: освоение и закрепление на практических занятиях основных положений теории компьютерной безопасности.

Практикум содержит восемь работ.

Практические занятия проводятся в компьютерных классах института цифровых технологий.

В результате выполнения практических занятий ожидается, что студенты приобретут навыки по реализации дискреционной и мандатной политики безопасности, уяснят понятие изолированной среды, домена безопасности и матрицы доступа.

Тематический план практических занятий приведён в таблице 1.

Методические указания к изучению

1. Изучение лекционного материала и конспектов:

– Перед практическими занятиями необходимо проработать соответствующие разделы лекционного материала.

– Рекомендуется вести конспект занятий и дополнительно пересмотреть его перед началом практического занятия.

2. Проработка учебной литературы:

– Используйте основные учебники и методические пособия, рекомендованные преподавателем.

– Для глубокого понимания теории рекомендуется обращаться к дополнительной литературе.

3. Подготовка вопросов:

– Составьте список вопросов по материалу, вызвавшему затруднения.

– Обсуждение этих вопросов на практическом занятии поможет устранить пробелы в знаниях.

4. Вопросы для самоконтроля:

– Перед каждым занятием рекомендуется проверять себя с помощью вопросов для самоконтроля из методических указаний к лекционным занятиям. Это позволит оценить уровень своей подготовки.

Рекомендуется в ходе выполнения задания на практическую работу использовать доступные в компьютерном классе средства компьютеризации и электронного доступа к информационным ресурсам кафедры, сети Интернет.

Подготовка отчета по выполненному практическому занятию осуществляется в соответствии с рекомендованной преподавателем формой отчета.

Рекомендуется прикрепить отчёт по каждому практическому занятию в контейнер в ЭИОС. В этой же системе можно посмотреть требования преподавателя по форме отчёта и по срокам выполнения заданий.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1

Реализация политики информационной безопасности на примере дискреционной модели

Цель работы: изучить формальные модели безопасности; рассмотреть проблемы реализации политик информационной безопасности в компьютерных системах на примере дискреционной модели

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методичке в ЭИОС.

2. Выполнить задание по пункту в методичке в ЭИОС порядок выполнения работы.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– составление графа преобразования прав в соответствии с этапами процесса передачи прав доступа;

– блок-схема алгоритма работы программы.

– ответить на контрольные вопросы.

Контрольные вопросы

1. Что понимается под политикой безопасности в компьютерной системе?

2. В чём заключается модель дискреционной политики безопасности в компьютерной системе?

3. Что должно содержаться в матрице доступов в дискреционной политике безопасности?

4. Какие действия производятся над матрицей доступа, когда субъект передаёт другому субъекту свои права доступа к объекту компьютерной системы?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2

Изучение уязвимости модели Харрисона-Руззо-Ульмана

Цель работы: изучить принципы функционирования политики на основе модели Харрисона-Руззо-Ульмана (HRU), определить уязвимости в модели HRU.

Методические указания и порядок выполнения работы:

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методичке ЭИОС.

2. Выполнить задание по пункту в методичке ЭИОС порядок выполнения работы.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– описание атаки;

– составить матрицы распределения прав доступа начального и конечного состояния системы, отобразить соответствующие последовательности команд перехода и изменений матрицы доступа;

– блок-схема алгоритма работы программы.

– вывод, содержащий предложения по противодействию атаке;

– ответить на контрольные вопросы

Контрольные вопросы

1. Перечислите основные понятия рассматриваемой модели HRU.

2. В чём заключается основной недостаток рассматриваемой модели?

3. Перечислить основные команды рассматриваемой модели.

4. Привести теоремы политики HRU.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3

Реализация распространения прав доступа по модели take-grant

Цель работы: изучить принципы построения политики безопасности по модели take-grant.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методичке ЭИОС.

2. Выполнить задание по пункту в методичке ЭИОС порядок выполнения работы.

3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– составить графы преобразования прав в соответствии с этапами процесса передачи прав доступа;

– блок-схема алгоритма работы программы.

– ответить на контрольные вопросы

Контрольные вопросы

1. Перечислите основные понятия рассматриваемой модели take-grant.
2. В чём заключается основной недостаток данной модели?
3. Перечислите основные правила рассматриваемой модели и обосновать их.
4. Указать условия реализации политики take-grant.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4

Расширенная модель прав доступа take-grant

Цель работы: изучить принципы построения политики безопасности по расширенной модели take-grant.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал и краткие теоретические сведения в методичке ЭИОС.
2. Выполнить задание по пункту в методичке ЭИОС порядок выполнения работы.
3. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– составить графы неявных каналов чтения информации

– блок-схема алгоритма работы программы.

– ответить на контрольные вопросы

Контрольные вопросы

1. Перечислите основные понятия расширенной модели take-grant.
2. В чём заключается основной недостаток изученной модели?
3. Перечислите основные правила рассматриваемой модели и обосновать их.
4. Указать условия реализации расширенной политики take-grant.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5

Нарушение дискреционной политики безопасности программой «Троянский конь»

Цель работы: Закрепление теоретического материала по дискреционной политике безопасности.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал [2, 3].

2. Создать две папки (легальный пользователь, злоумышленник) и назначить к этим папкам доступ штатными средствами операционной системы.

3. Убедиться, что доступ злоумышленника в папку легального пользователя запрещён.

4. Написать программу, реализующую функции «Троянского коня», которая копирует файлы из папки легального пользователя в папку злоумышленника. Записать программу в папку легального пользователя.

5. Запустить программу от имени Злоумышленника и убедиться, что копирование фалов не происходит. Запустить программу от имени Легального пользователя и убедиться, что произошло копирование файлов из папки. Убедиться, что злоумышленник имеет полный доступ к скопированным файлам.

6. Предложить пути усиления защиты.

7. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– описание атаки;

– блок-схема алгоритма работы программы.

– выводы, которые будут содержать предложения по противодействию атаке;

– ответить на контрольные вопросы

Контрольные вопросы

1. Раскройте понятие «Троянский конь»;

2. Как замаскировать действие троянской программы?

3. Расскажите о методах противодействия данной атаке.

4. Каким образом происходить распространение атаки типа «Троянский конь»?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 6

Мандатные политики безопасности

Цель работы: закрепление теоретического материала по мандатной политике безопасности.

Методические указания и порядок выполнения работы

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал. Задание:

Заданы документы с разным уровнем секретности, заданы пользователи с различным уровнем доступа (составить самостоятельно и не менее 3 пользователя и 5 документов)

2. Для каждого пользователя составить список документов, доступных ему для работы при условии, что пользователь не понижает своего уровня допуска.

3. Пусть один из пользователей имеет возможность работать с несколькими документами. На основе этих документов он создаёт новый документ, какой гриф секретности надо присвоить этому документу?

4. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– оформить таблицей уровни доступа и уровни секретности;

– ответить на вопрос в задании к практической работе;

– ответить на контрольные вопросы.

Контрольные вопросы

1. Дайте определение мандатного управления доступом.

2. Перечислите и поясните свойства, которыми должна обладать безопасная система согласно модели Белла-ЛаПадула.

3. Как обобщённо можно сформулировать требования к функциям перехода безопасной системы?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 7

Субъектно-объектная модель. Изолированная программная среда

Цель работы: Закрепление теоретического материала по субъектно-объектной модели политики безопасности, исследование заданной системы на соответствие требованиям заданной политики безопасности.

Методические указания и порядок выполнения работы:

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал. Задание:

2. Для заданной преподавателем КС произвести деление на субъекты, объекты по признаку активности.

3. Выделить в системе специальные объекты МБО, МБС и субъект, который контролирует неизменность субъектов.

4. Определить корректность субъектов относительно друг друга, МБО и МБС.

5. Выделит в множестве субъектов те, которые могут образовать ИПС.

6. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– оформить каждый пункт задания;

– ответить на контрольные вопросы.

Контрольные вопросы

1. Дайте определение субъекта и объекта.

2. При каких условиях субъекты корректны (абсолютно корректны) друг относительно друга.

3. Какова роль МБС и роль МБО в субъектно-объектной модели?

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 8

Работа с матрицей доступов. Домены безопасности

Цель работы: закрепление теоретического материала по дискреционным политикам безопасности., создание матрицы доступа.

Методические указания и порядок выполнения работы:

1. Прийти на занятие подготовленным, а значит заранее изучить предшествующий лекционный материал [2, 3]. Задание:

2. Пусть исследуемая система состоит из множеств субъектов и объектов. Задание индивидуально каждому студенту получить у преподавателя.

3. Необходимо составить множество прав доступа в КС и для заданного множества субъектов и объектов построить матрицу доступов и заполнить её в соответствии с заданной политикой безопасности и с принципом минимизации привилегий.

4. Дополнить матрицу доступов временными доменами для всех возможных комбинаций взаимодействующих субъектов.

5. Оформить отчет по практической работе, разместить его в ЭИОС и защитить преподавателю.

Содержание отчёта:

– название и цель работы;

– оформить каждый пункт задания;

– ответить на контрольные вопросы

Контрольные вопросы

1. В каких случаях в матрицу доступов добавляется временный домен безопасности?

2. Какие существуют правила при формировании прав доступа во временном домене?

3. Дайте определение доменов безопасности.

5. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО САМОСТОЯТЕЛЬНОЙ ПОДГОТОВКЕ

Внеаудиторная самостоятельная работа в рамках данной дисциплины включает в себя:

• подготовку к аудиторным занятиям (лекциям, практическим занятиям) и выполнение соответствующих заданий;

• самостоятельную работу над отдельными темами учебной дисциплины в соответствии с тематическим планом;

• подготовку к экзамену.

Подготовка к лекционным занятиям

При подготовке к лекции рекомендуется повторить ранее изученный материал, что дает возможность получить необходимые разъяснения преподавателя непосредственно в ходе занятия. Рекомендуется вести конспект, главное требование к которому быть систематическим, логически связанным, ясным и кратким. По окончанию занятия обязательно в часы самостоятельной подготовки, по возможности в этот же день, повторить изучаемый материал и доработать конспект.

Подготовка к практическим занятиям

Подготовка к практическим занятиям предусматривает:

• изучение теоретических положений по изучаемой теме;

• детальную проработку учебного материала, рекомендованной литературы и методической разработки на предстоящее занятие.

Самостоятельная работа над отдельными темами учебной дисциплины: При организации самостоятельного изучения ряда тем лекционного курса обучаемый работает в соответствии с указаниями, выданными преподавателем. Указания по изучению теоретического материала курса составляются дифференцированно по каждой теме и включают в себя следующие элементы: название темы; цели и задачи изучения темы; основные вопросы темы; характеристику основных понятий и определений, необходимых обучаемому для усвоения данной темы; список рекомендуемой литературы; наиболее важные фрагменты текстов рекомендуемых источников, в том числе таблицы, рисунки, схемы и т. п.; краткие выводы, ориентирующие обучаемого на определенную совокупность сведений, основных идей, ключевых положений, систему доказательств, которые необходимо усвоить; контрольные вопросы, предназначенные для самопроверки знаний.

Подготовка к экзамену

При подготовке к экзамену большую роль играют правильно подготовленные заранее записи и конспекты. В этом случае остается лишь повторить

пройденный материал, учесть, что было пропущено, восполнить пробелы, закрепить ранее изученный материал.

В ходе самостоятельной подготовки к экзамену при анализе имеющегося теоретического и лабораторного материала студенту также рекомендуется проводить постановку различного рода задач по изучаемой теме, что поможет в дальнейшем выявлять критерии принятия тех или иных решений, причины совершения определенного рода ошибок. При ответе на вопросы, поставленные в ходе самостоятельной подготовки, обучающийся вырабатывает в себе способность логически мыслить, искать в анализе событий причинно-следственные связи.

Рекомендуемая литература

1. Мошак, Н. Н. Защищенные информационные системы: учеб. пособие / Н. Н. Мошак, Л. К. Птицына. – Санкт-Петербург: СПбГУТ им. М. А. Бонч-Бруевича, 2020. – 216 с. – URL: https://e.lanbook.com/book/180099. – ~Б. ц. – Текст: электронный.

2. Шаньгин, В. Ф. Информационная безопасность и защита информации [Электронный ресурс] / В. Ф. Шаньгин. – Электрон. текстовые дан. – Москва: ДМК Пресс, 2014. – 702 с. – Режим доступа: http://www.iprbookshop.ru/2

3. Защита информации. Инсайд: информационно-методический журнал. – Санкт-Петербург: ООО «Изд. Дом «Афина»».

4. Безопасность информационных технологий: научно-технический журнал. – Москва: Изд-во журнала «Безопасность информационных технологий». 3. Информационно-управляющие системы = Informatsionno-upravliaiushchie sistemy: науч. журн./ учредитель: «Информационно-управляющие системы»; гл. ред. Михаил Сергеев. – Санкт-Петербург: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 2002. – 29 с. – Перевод заглавия: Informatsion and control systems. – Срок хранения 5 лет. – Выходит раз в два месяца. Гл. ред.: Сергеев М. Б. - ISSN 1684-8853. – Текст: непосредственный. Держатели документа: НТБ КГТУ: 236022, г. Калининград, Советский пр., д. 1

Вопросы и задачи для самопроверки

ЗАДАЧА 1. «Разработка политики безопасности Монитора безопасности объекта с использованием дискреционных моделей»

Цель: моделирование политики безопасности МБО.

Задание

При разработке политики безопасности МБО использовать формальную модель Харрисона-Руззо-Ульмана (например, добавление субъекта в матрицу прав доступа с учетом критерия безопасности). Проанализировать состояния компьютерной системы при выполнении следующих процессов:

– пользователь 1 разрабатывает на языке программирования C++ код приложения Структура и запускает его на выполнение, затем текст кода приложения Структура записывает в файл, созданный текстовым процессором Word, и выводит текст на печатающее устройство;

– пользователь 2 запускает на выполнение код приложения Структура, разрабатывает на языке программирования C++ код приложения и записывает его в файл 5, выводит на печатающее устройство файлы 9 и A5 и с помощью субъекта 3 запускает на выполнение файл 4.

Права доступа:

1 read 1, код приложения Структура

write 1, 9

execute код приложения, 9, 1, A5, Visual C++, текстовый процессор Word

2 read 5, 9, код приложения,

write код приложения Структура, A5

execute код приложения Структура, 4, Vis-ual C++, текстовый процессор Word.

Индивидуальное задание и пример выполнения можно посмотреть в системе ЭИОС.

ЗАДАЧА 2. Разработка политики безопасности Монитора безопасности объекта с использованием мандатных моделей»

Цель: моделирование политики безопасности МБО.

Задание

1. При разработке политики безопасности МБО использовать формальную модель Белла-ЛаПадулы (моделирование безопасной функции перехода Мак-Лина по чтению, алгоритм).

Определение субъекта, имеющего наименьшее количество доступов типа write и read к объектам матрицы доступа.

Составление списка пользователей, которые вошли в систему и ни разу не обратились к матрице прав доступа.

2. Проанализировать состояния компьютерной системы при выполнении следующих процессов:

– пользователь H1 запускает на выполнение Excel и сохраняет созданный файл с именем Список1, затем читает файл Список2 и запускает его на выполнение;

– пользователь H2 запускает на выполнение Access и создает две таблицы Таблица1 и Таблица2, затем с помощью объекта Формы заполняет таблицы конкретными данными и сохраняет их под теми же именами;

– пользователь Н3 запускает на выполнение файлы Поиск1.с и Поиск2.с. Данные для отладки кодов приложений задать самостоятельно по следующей схеме в соответствии с выполняемыми процессами:

Объекты:
Пользователи: Н1, Н2, Н3
Права доступа:
Н1 read
write
execute
Н2 read
write
execute
Н3 read
write
execute.

ЗАДАЧА 3. Модель Take-Grant

Для заданной задачи (рисунок 1) показать последовательность команд, которая позволяет субъекту S1 в санкционированном режиме получить право r на объект X.

Задание 1

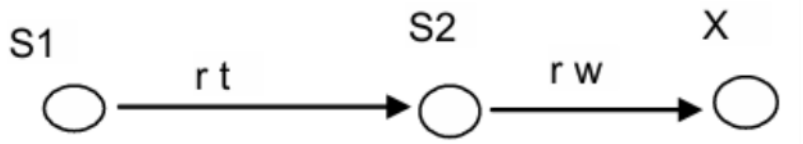

Рисунок 1 – Начальные условия

Для заданной задачи (рисунок 2) показать последовательность команд, которая позволяет субъекту S1 в санкционированном режиме получить право r на объект X.

Задание 2

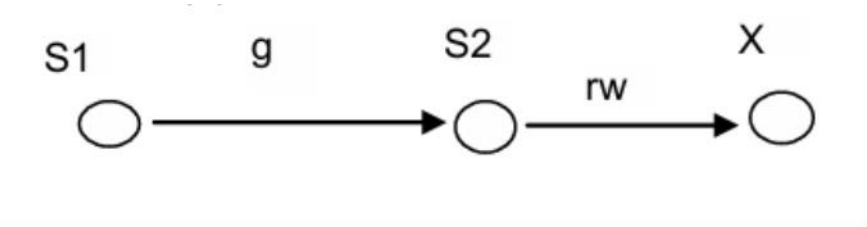

Рисунок 2 – Начальные условия

Для заданной задачи (рисунок 3) показать последовательность команд, которая позволяет субъекту S1 в санкционированном режиме получить право r на объект X.

Задание 3

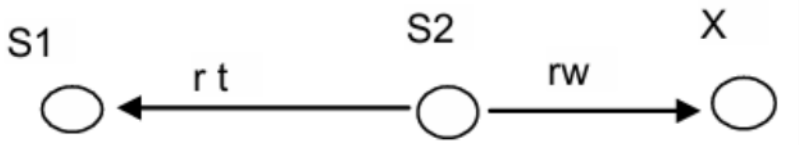

Рисунок 3 – Начальные условия

Для заданной задачи (рисунок 4) показать последовательность команд, которая позволяет субъекту S1 в санкционированном режиме получить право r на объект X.

Задание 4

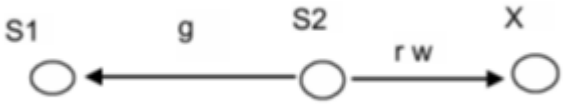

Рисунок 4 – Начальные условия

Вопросы для самоподготовки

1. Каково назначение модели Take-Grant, для каких систем применима данная модель.

2. Какие средства используются в модели take-Grant для описания системы.

3. Каково назначение прав доступа take и grant, какие возможности предоставляются субъекту, обладающему такими правами.

4. При каких условиях согласно модели Take-Grant, возможна передача прав доступа в санкционированном режиме.

5. При каких условиях согласно модели Take-Grant, возможна передача прав доступа в режиме похищения прав доступа.

ЗАДАЧА 4. Мандатная политика безопасности

Заданы документы с различным уровнем секретности, заданы пользователи с различным уровнем доступа (список документов и пользователей и их уровни доступа/секретности составить самостоятельно. Не менее 5 пользователей и 5 документов).

Задание

Для каждого пользователя составить список документов, доступных ему для работы при условии, что пользователь не понижает своего уровня допуска.

Для одного из пользователей составить список документов, доступных ему для работы при условии, что пользователь может понизить свой уровень доступа на один уровень.

Показать на примере одного из пользователей, что мандатная политика безопасности не может быть нарушена программой типа "Троянский конь"

Вопросы для самоподготовки

1. Дайте определение мандатного управления доступом.

2. Объясните, почему системы, реализующие мандатное управление доступом устойчивы к атакам с помощью программ типа «Троянский конь».

3. Перечислите и поясните свойства, которыми должна обладать безопасная система согласно модели Белла-ЛаПадула.

4. Как обобщенно можно сформулировать требования к функциям перехода безопасной системы.

ЗАДАЧА 5. Реализация политики информационной безопасности на примере дискреционной модели

Порядок выполнения

1. Реализовать программный модуль, формирующий матрицу доступов субъектов к объектам компьютерной системы, используя таблицу 2, либо самостоятельно сформировать таблицу с правами доступов, но не меньше 3 субъектов, которые имеют доступы к объектам компьютерной системы тоже не менее 3.

Таблица 2. Задание

Объект/Субъект	Объект 1	Объект 2	Объект 3
root	r, w, e	r, w, e	r, w, e
User 1	-	r	r
User 2	r, передача прав	r, w	r, w, e

2. При реализации матрицы доступа необходимо, чтобы один из пользователей субъектов (root) обладал всеми возможными правами доступа ко всем объектам системы. Пользователи User могут иметь несколько прав к некоторому объекту компьютерной системы.

3. Реализовать программный модуль, демонстрирующий работу пользователя в дискреционной модели политики безопасности. Данный модуль должен выполнять следующие функции:

– аутентификации пользователей системы

– при успешной идентификации каждого из пользователей предполагается вывод списка всех объектов системы с указанием прав доступа идентифицированного пользователя к данным объектам. Вывод можно отображать в виде таблицы, либо таким образом, чтобы были отображены тип объекта, права доступа, владелец, имя объекта.

4. После вывода на экран перечня прав доступа пользователя к объектам КС, программа должна ждать указаний пользователя на осуществление действий над объектами в КС. После получения команды от пользователя на экран должно выводиться сообщение об успешности либо не успешности выполнения операции.

5. При выполнении операции передачи прав (grant), если она есть в вашей матрице доступа матрица должна модифицироваться.

6. Ваша программа должна поддерживать операцию выхода из системы (quit), после которой должен запрашиваться другой идентификатор пользователя.

6. КОНТРОЛЬ И АТТЕСТАЦИЯ

К оценочным средствам текущего контроля успеваемости относятся:

– тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

– экзаменационные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов.

Критерии оценки результатов освоения дисциплины

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100-балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 2).

Таблица 2 – Система оценок и критерии выставления оценки

Система оценок / Критерий				
	–40 %	**–60 %**	**–80 %**	**–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
Системность и полнота знаний в отношении изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно-корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом на изучаемый объект
2 Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные источники информации в рамках поставленной задачи
3 Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно-корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно-корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовлекает в исследование новые релевантные по-

Система оценок / Критерий				
	–40 %	**–60 %**	**–80 %**	**–100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
			релевантные задаче данные	ставленной задаче данные, предлагает новые ракурсы поставленной задачи
4 Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/не зачтено («зачтено» – 41–100 % правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» – менее 40 % правильных ответов; оценка «удовлетворительно» – от 41 до 60 % правильных ответов; оценка «хорошо» – от 61 до 80 % правильных ответов; оценка «отлично» – от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

Задание открытого и закрытого типа приведены в ФОС (приложении к рабочему модулю).

Типовые контрольные задания и иные материалы, необходимые для оценки результатов освоения дисциплин модуля (в том числе в процессе освоения), а также методические материалы, определяющие процедуры этой оценки приводятся в приложении к рабочей программе модуля. Оценивание результатов обучения проводится с применением электронного обучения, дистанционных образовательных технологий.

7. СПИСОК ЛИТЕРАТУРЫ

Основная литература

1. Мошак, Н. Н. Защищенные информационные системы: учеб. пособие / Н. Н. Мошак, Л. К. Птицына. – Санкт-Петербург: СПбГУТ им. М. А. Бонч-Бруевича, 2020. – 216 с. – URL: https://e.lanbook.com/book/180099. – ~Б. ц. – Текст: электронный.

2. Нестеров, С. А. Основы информационной безопасности / С. А. Нестеров. – 3-е изд., стер. – Санкт-Петербург: Лань, 2024. – 324 с. – Режим доступа: для авториз. пользователей. -–Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/370967 (дата обращения: 09.10.2024). – ISBN 978-5-507-49077-6. – Текст : электронный.

3. Богульская, Н. А. Модели безопасности компьютерных систем: учеб. пособие / Н. А. Богульская, М. М. Кучеров. – Красноярск: СФУ, 2019. – 206 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/157578 (дата обращения: 11.10.2024). – ISBN 978-5-7638-4008-7. – Текст : электронный

Дополнительная литература

4. Горкуш, С. В. Защита конфиденциальной информации. Практикум: учеб. пособие / С. В. Горкуш, О. Г. Савка. – Москва: РТУ МИРЭА, 2022. – 87 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/311156 (дата обращения: 09.10.2024). – Текст : электронный.

5. Петренко, В. И. Защита персональных данных в информационных системах. Практикум: учеб. пособие для вузов / В. И. Петренко, И. В. Мандрица. – 6-е изд., стер. – Санкт-Петербург: Лань, 2025. – 108 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/437192 (дата обращения: 09.10.2024). – ISBN 978-5-507-50458-9. – Текст : электронный.

6. Основы защиты информации: учеб. пособие для студентов специальности 090105.65 «Комплекс. обеспечение информ. безопасности автоматиз. Систем» всех форм обучения / А. В. Кузнецов, В. А. Иванов, О. П. Пономарев, И. А. Ветров; Федер. агентство по рыболовству [и др.]. – Калининград: БГАРФ, 2014. – 179 с. – ISBN 978-5-7481-0268-1 (в обл.). – Текст : непосредственный.

Учебно-методические пособия по дисциплинам, нормативная литература

7. Великите, Н. Я. Теоретические основы компьютерной безопасности: учеб.-метод. пособие по изучению дисциплины для студ. специальности 10.05.03 «Информационная безопасность автоматизированных систем» / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2023. – 23 с. –

URL: https://klgtu.ru/vikon/sveden/files/rij/UMP_Teoreticheskie_osnovy_kompyyuternoi_bezopasnosti.pdf (дата обращения: 09.10.2024). – Текст : электронный.

8. Великите, Н. Я. Учебно-методическое пособие по выполнению лабораторных работ по дисциплине «Теоретические основы компьютерной безопасности» / Н. Я. Великите. – Калининград: Изд-во ФГБОУ ВО «КГТУ», 2022. – 11 с. – Режим доступа: для авториз. пользователей. – URL: https://eios.klgtu.ru/course/view.php?id=9340 (дата обращения: 09.10.2024). – Текст : электронный.

9. Семыкина, Н. А. Математические модели в информационной безопасности: учебно-методическое пособие / Н. А. Семыкина. – Тверь: ТвГУ, 2020. – 126 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/217946 (дата обращения: 09.12.2024). – ISBN 978-5-7609-1573-3. – Текст : электронный.

10. Исследование способов доступа в информационные системы: учебно-методическое пособие / С. И. Журавлев, В. В. Кадомкин, О. В. Трубиенко [и др.]. – Москва: РТУ МИРЭА, 2023. – 58 с. – Режим доступа: для авториз. пользователей. – Лань : электронно-библиотечная система. – URL: https://e.lanbook.com/book/368651 (дата обращения: 09.12.2024). – ISBN 978-5-7339-1774-0. – Текст : электронный

Локальный электронный методический материал

Наталья Яронимо Великите

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Редактор С. Кондрашова
Корректор Т. Звада

Уч.-изд. л. 3,2. Печ. л. 2,8.

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