Федеральное агентство по рыболовству
БГАРФ ФГБОУ ВО «КГТУ»
Калининградский морской рыбопромышленный колледж

Утверждаю
Заместитель начальника колледжа
по учебно-методической работе
А.И.Колесниченко

Подписано цифровой подписью: Колесниченко Андрей Игоревич
Причина: Я утвердил этот документ
Дата: 14 Март 2025 г. 20:30:58
DN: E=uc_fk@roskazna.ru, S=77 Москва, ИНН ЮЛ=7710568760, ОГРН=1047797019830, STREET="Большой Златоустинский переулок, д. 6, строение 1", L=г. Москва, C=RU, O=Казначейство России, CN=Федеральное казначейство

ОП.02 АРХИТЕКТУРА АППАРАТНЫХ СРЕДСТВ

Методическое пособие для выполнения самостоятельных работ
по специальности

09.02.06 Сетевое и системное администрирование

МО-09 02 06-ОП.02.СР

РАЗРАБОТЧИК	Халина Е.Н.
ЗАВЕДУЮЩИЙ ОТДЕЛЕНИЕМ	Кругленя В.Ю.
ГОД РАЗРАБОТКИ	2022
ГОД ОБНОВЛЕНИЯ	2025

СОДЕРЖАНИЕ

Введение

Рабочей программой ОП.02. «Архитектура аппаратных средств» предусмотрено выполнение 1 самостоятельной работы.

Самостоятельная работа обучающихся проводится с целью:

-систематизации и закрепления полученных теоретических знаний и практических умений;

- углубления и расширения теоретических знаний;

-формирования умений использовать нормативную, справочную документацию и специальную литературу;

-развития познавательных способностей и активности студентов: творческой инициативы, самостоятельности, организованности;

- формирования самостоятельного мышления;

- развитие исследовательских умений.

Выполнение самостоятельных работ способствует формированию у обучающихся:

ОК 01, 02, ПК 1.1-1.2, ПК 3.1.

Внеаудиторная самостоятельная работа выполняется обучающимися по заданию преподавателя, но без его непосредственного участия.

Критериями оценки результатов внеаудиторной самостоятельной работы обучающихся являются:

- Сформированность общеучебных умений;
- обоснованность и четкость изложения ответа;
- оформление материала в соответствии с требованиями.

Внеаудиторная самостоятельная работа выполняется в отдельных тетрадях. Перед ее выполнением преподаватель проводит инструктаж и знакомит обучающихся с порядком выполнения самостоятельной работы, критериями оценки.

Самостоятельная работа является одним из компонентов комплексной оценки по дисциплине.

Перечень самостоятельных работ

№ п/п	Темы самостоятельной работы	Кол-во часов
1	*Требования к компьютерным сетям. Требования к сетевой безопасности.*	2
	Итого	**2**

Самостоятельная работа №1 Требования к компьютерным сетям. Требования к сетевой безопасности

Работа предусматривает: самостоятельную работу по изучению конспектов занятий, изучению содержания учебной, дополнительной и специальной литературы.

Цель работы:

1. Привитие навыков работы с учебной литературой.
2. Развитие познавательных способностей.

Литература:

Максимов, Н. В. Архитектура ЭВМ и вычислительных систем: учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва: ФОРУМ : ИНФРА-М, 2024. — 511 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-511-0. - Текст: электронный. - URL: https://znanium.com/catalog/product/2083334 – Режим доступа: по подписке.

Колдаев, В. Д. Архитектура ЭВМ : учебное пособие / В.Д. Колдаев, С.А. Лупин. — Москва : ФОРУМ : ИНФРА-М, 2023. — 383 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0868-6. - Текст: электронный. - URL: https://znanium.ru/catalog/product/1896460 – Режим доступа: по подписке.

Теоретический материал

Сетевая безопасность — список требований, рекомендаций и политик, которые используются в сетевой инфраструктуре для повышения ее уровня защиты и отказоустойчивости.

Вторая важная функция анализа работы инфраструктуры компании и предотвращения несанкционированного доступа (НСД) к информационным ресурсам со стороны злоумышленников.

Независимо от масштаба и типа бизнеса (малый, средний или крупный) использование сетевой инфраструктуры подразумевает интеграцию аппаратных и программных решений, которые обеспечивают работоспособность и безопасность сети.

Принципы построения

Выделяют 4 основных принципа проектирования сетевой безопасности на объекте информатизации:

- Защита оборудования, подключенного к сетевой инфраструктуре. В качестве защитных мер используют антивирусные решения с регулярным обновлением баз, межсетевые экраны с фильтрацией трафика и блокировкой нежелательных абонентов и т. д.
- Оборудование должны быть отказоустойчивым и предусматривать возможность быстрого восстановления. Подразумевается наличие дублирующих компонентов в критически важных узлах.
- Систематический мониторинг всей инфраструктуры компании для обнаружения уязвимых точек. Также система должна предоставлять подробную информацию о любом программном или аппаратном компоненте оборудования.
- Постоянный мониторинг пропускной способности сетевого канала. Это гарантирует своевременную блокировку нежелательного трафику, а также позволяет осуществить балансировку нагрузки в ручном режиме.
- Критически важные узлы инфраструктуры организации должны обеспечивать высокую доступность при любой угрозе либо атаке на компанию. Это достигается за счет создания второй независимой площадки (ЦОДа), которая реплицирует данные с первой в синхронном режиме.

Средства обеспечения сетевой безопасности

Различают 2 вида сетевых атак по статусу действия: активные и пассивные. Они также могут быть внутренними или внешними.

При любом раскладе рекомендуется использовать следующие меры для предотвращения:

- прокси-серверы;
- системы выявления и предотвращения угроз взлома;
- средства защиты от целевых атак;
- межсетевые экраны;
- системы сетевого мониторинга;
- VPN.

Угрозы безопасности информационных систем классифицируются по нескольким признакам (рис. 1).

Рис.1 Классификация угроз информационной безопасности

Угрозы нарушения конфиденциальности направлены на получение (хищение) конфиденциальной информации. При реализации этих угроз информация становится известной лицам, которые не должны иметь к ней доступ. Несанкционированный доступ к информации, хранящейся в информационной системе или передаваемой по каналам (сетям) передачи данных, копирование этой информации является нарушением конфиденциальности информации.

Угрозы нарушения целостности информации, хранящейся в информационной системе или передаваемой посредством сети передачи данных, направлены на изменение или искажение данных, приводящее к нарушению качества или полному уничтожению информации. Целостность информации может быть нарушена намеренно злоумышленником, а также в результате объективных воздействий со стороны среды, окружающей систему (помехи). Эта угроза особенно актуальна для систем передачи информации – компьютерных сетей и систем телекоммуникаций.

Умышленные нарушения целостности информации не следует путать с ее санкционированным изменением, которое выполняется авторизованными пользователями с обоснованной целью.

Угрозы нарушения доступности системы (отказ в обслуживании) направлены на создание таких ситуаций, когда определённые действия либо снижают работоспособность информационной системы, либо блокируют доступ к некоторым её ресурсам.

Причины случайных воздействий:

• аварийные ситуации из-за стихийных бедствий и отключения электроэнергии;

• ошибки в программном обеспечении;

• ошибки в работе обслуживающего персонала и пользователей;

• помехи в линии связи из-за воздействия внешней среды, а также вследствие плотного трафика в системе (характерно для беспроводных решений).

Преднамеренные воздействия связаны с целенаправленными действиями злоумышленника, в качестве которого может выступить любое заинтересованное лицо (конкурент, посетитель, персонал и т.д.). Действия злоумышленника могут быть обусловлены разными мотивами: недовольством сотрудника своей карьерой, материальным интересом, любопытством, конкуренцией, стремлением самоутвердиться любой ценой.

Внутренние угрозы инициируются персоналом объекта, на котором установлена система, содержащая конфиденциальную информацию. Причинами возникновения таких угроз может послужить нездоровый климат в коллективе или неудовлетворенность от выполняемой работы некоторых сотрудников, которые могут предпринять действия по выдаче информации лицам, заинтересованным в её получении.

Также имеет место так называемый "человеческий фактор", когда человек не умышленно, по ошибке, совершает действия, приводящие к разглашению конфиденциальной информации или к нарушению доступности информационной системы. Большую долю конфиденциальной информации злоумышленник (конкурент) может получить при несоблюдении работниками-пользователями компьютерных сетей элементарных правил защиты информации. Это может проявиться, например, в примитивности паролей или в том, что сложный пароль пользователь хранит на бумажном носителе на видном месте или же записывает в текстовый файл на жестком диске и пр. Утечка конфиденциальной информации может происходить при использовании незащищенных каналов связи, например, по телефонному соединению.

Под внешними угрозами безопасности понимаются угрозы, созданные сторонними лицами и исходящие из внешней среды, такие как:

• атаки из внешней сети (например, Интернет), направленные на искажение, уничтожение, хищение информации или приводящие к отказу в обслуживании информационных систем предприятия;

• распространение вредоносного программного обеспечения;

• нежелательные рассылки (спам);

• воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения в информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем;

• перехват информации с использованием радиоприемных устройств;

• воздействие на информацию, осуществляемое путем несанкционированного использования сетей инженерных коммуникаций;

• воздействие на персонал предприятия с целью получения конфиденциальной информации.

В современном мире, когда стало возможным применять сервисы и службы с использованием информационной коммуникационной среды (электронные платежи, Интернет-магазины, электронные очереди и т.п.), многократно увеличивается риск именно внешних угроз.

Как правило, несанкционированный доступ, перехват, хищение информации, передаваемой по каналам связи, проводится средствами технической разведки, такими как радиоприемные устройства, средства съема акустической информации, системы перехвата сигналов с компьютерных сетей и контроля телекоммуникаций, средства съема информации с кабелей связи и другие.

Вредоносное программное обеспечение и, прежде всего, компьютерные вирусы представляют очень серьезную опасность для информационных систем. Недооценка этой опасности может иметь серьезные последствия для информации пользователей. В то же время чрезмерное преувеличение угрозы вирусов негативно влияет на использование всех возможностей компьютерной сети. Знание механизмов действия вредоносного программного обеспечения (ПО), методов и средств борьбы с ними позволяет эффективно организовать противодействие вирусам, свести к минимуму вероятность заражения и нанесения вреда машинам и информации.

О наличии вредоносного ПО в системе пользователь может судить по следующим признакам:

• появление сообщений антивирусных средств о заражении или о предполагаемом заражении, "самопроизвольное" отключение антивирусных программных средств;

• явные проявления присутствия вируса, такие как: сообщения, выдаваемые на монитор или принтер, звуковые эффекты, неожиданный запуск программ,

уничтожение файлов и другие аналогичные действия, однозначно указывающие на наличие вируса в системе;

• неявные проявления заражения, которые могут быть вызваны и другими причинами, например, сбоями или отказами аппаратных и программных средств компьютерной системы – увеличение времени обработки той или иной информации (т.н. "задумчивость" ПК), необоснованное уменьшение свободного объёма на дисковых носителях, отказ выполнять программы-сканеры вирусной активности, "зависания" системы и т.п.;

• рассылка писем, которые пользователем не отправлялись, по электронной почте.

Вредоносная программа (Malware, malicious software – злонамеренное программное обеспечение) – это любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа.

Но со временем стремительное развитие вредоносных программ, появление новых платформ и рост числа антивирусных компаний привели к тому, что эта схема фактически перестала использоваться. Ещё более важной причиной отказа от неё стало то, что технологии детектирования систем антивирусных компаний отличаются друг от друга и, как следствие, невозможно унифицировать результаты проверки разными антивирусными программами. Периодически предпринимаются попытки выработать новую общую классификацию детектируемых антивирусными программами объектов. Последним значительным проектом подобного рода было создание стандарта CME (Common Malware Enumeration), суть которого заключается в присвоении одинаковым детектируемым объектам единого уникального идентификатора.

Вопросы для самоконтроля:

1) Какие свойства присущи информации?
2) Дайте понятие объекта защиты информации.
3) Что относят к информационным процессам?
4) Что понимают под информационной системой?
5) Что называют информационными ресурсами?

6) Что понимают под угрозой информации, дайте понятие искусственных и естественных угроз, приведите примеры.

7) Что составляет основу политики безопасности?

8) Сделайте сравнительный анализ избирательной и полномочной политики безопасности.

9) Проанализируйте механизмы и свойства защиты информации

Виды контроля:

1. Устный опрос по теме
2. Проверка письменных ответов на вопросы для самоконтроля.

Список используемой литературы:

Виды источников	Наименование рекомендуемых учебных изданий
Основные	Максимов, Н. В. Архитектура ЭВМ и вычислительных систем : учебник / Н.В. Максимов, Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2024. — 511 с. — (Среднее профессиональное образование). - ISBN 978-5-00091-511-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/2083334 (дата обращения: 24.05.2024). – Режим доступа: по подписке.
Дополнительные	Колдаев, В. Д. Архитектура ЭВМ : учебное пособие / В.Д. Колдаев, С.А. Лупин. — Москва : ФОРУМ : ИНФРА-М, 2023. — 383 с. — (Среднее профессиональное образование). - ISBN 978-5-8199-0868-6. - Текст : электронный. - URL: https://znanium.ru/catalog/product/1896460 (дата обращения: 24.05.2024). – Режим доступа: по подписке.
Интернет-источники	1. Федеральный центр информационно-образовательных ресурсов [Электронный ресурс]. – Режим доступа: http://fcior.edu.ru. 2. Российское образование: федеральный портал [Электронный ресурс]. – Режим доступа: http://www.edu.ru
Электронные образовательные ресурсы	1. ЭБС «Book.ru», https://www.book.ru 2. ЭБС « ЮРАЙТ»https://www.biblio-online.ru 3. ЭБС «Академия», https://www.academia-moscow.ru 4. Издательство «Лань», https://e.lanbook.com 5.Электронно-библиотечная система «Университетская библиотека онлайн»,https://www.biblioclub.ru