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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ

по выполнению практических работ
по дисциплине «Управление информационной безопасностью»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль)
«Информационная безопасность киберфизических систем»

Ставрополь
2026

Содержание:

Введение

1. Цели и задачи освоения дисциплины:

Основной *целью* изучения дисциплины «Управление информационной безопасностью» является формирование набора общекультурных и профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 Информационная безопасность.

Для достижения указанной цели в процессе изучения данной дисциплины необходимо решить следующие *задачи*:

- приобретение студентами теоретических знаний по системному подходу к управлению информационной безопасностью и практических навыков по их моделированию.

2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесённых с планируемыми результатами освоения образовательной программы

Код, формулировка компетенции	Код, формулировка индикатора	Планируемые результаты обучения по дисциплине (модулю), характеризующие этапы формирования компетенций, индикаторов
ОПК-1 Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ИД-1 ОПК-1 проектирует информационные системы с учетом различных технологий обеспечения информационной безопасности	- формулирует основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности; - выделяет направления развития технологий проектирования информационных, автоматизированных и автоматических систем; - применяет методы проектирования и построения систем информационной безопасности, включая методы тестирования эффективности и

		оценки надёжности
	ИД-3 ОПК-1 разрабатывает и обосновывает критерии оценки эффективности проектируемой системы обеспечения информационной безопасности, оценивает эффективность решений и анализирует показатели деятельности	Полностью оценивает роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства использует современные программные и программно-аппаратные (в том числе криптографические) средства защиты информации в профессиональной деятельности
ОПК-3 Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	ИД-2 ОПК-3 разрабатывает проекты организационно-распорядительной документации по обеспечению информационной безопасности	оперирует основными нормативными правовыми актами в области обеспечения информационной безопасности; нормативными методическими документами ФСБ России в области защиты информации разрабатывает проекты нормативных материалов, регламентирующих работу по защите информации, нормативно-методические материалы по регламентации системы организационной защиты информации, организационно-распорядительную документацию по обеспечению информационной безопасности;
	ИД-3 ОПК-3 проводит технико-экономическое обоснование проектных решений в области построения систем обеспечения информационной безопасности	Выделяет правила построения оптимальной политики безопасности в соответствии с требованиями уровня безопасности, стоимости и сроков реализации анализирует экономическую информацию, возникающую в процессе производственно-хозяйственной деятельности, и вырабатывает рекомендации по

		экономической целесообразности ее защиты, анализировать и классифицирует риски, возникающие при защите информации, выбирает методы их расчётов

ПРАКТИЧЕСКАЯ РАБОТА № 1-2

Стандартизация в сфере управления информационной безопасности

Цель работы:
Применение основ информационной безопасности для имитации действий нарушителя по раскрытию (нарушению конфиденциальности) при использовании одного и того же одноразового блокнота (гаммы) на основе побитового сложения по модулю 2 (взлом двухразового блокнота).
Подготовка и порядок выполнения работы:
Работа состоит из следующих этапов:
1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить соответствующий теоретический материал по курсу «Программирование».
3. Написать на языке Си программу, реализующую поставленную задачу.
4. Проанализировать проделанную работу и предложить свой метод противодействия реализованной атаке.
5. Результат отразить в отчете.
Краткие теоретические сведения
Безопасность для различных сфер жизнедеятельности личности, общества и государства опирается на понятие ограничения доступа к информации.
Шифрование используется как метод усиления таких свойств качественной информации, как конфиденциальность и целостность. Можно легко получить не раскрываемый шифр, но тут имеется одна тонкость. Сначала нужно найти процесс, который может генерировать произвольную бесконечную строку битов, которая называется гаммой. Во-вторых, необходимо преобразовать открытый текст в битовую строку и вычислить побитовое сложение по модулю 2 (операция XOR) открытого текста и ключевой строки. После чего можно послать результирующий зашифрованный текст получателю по незащищенному каналу. Шифрованный текст не может быть раскрыт, поскольку каждая возможная ключевая строка является одинаково вероятным кандидатом; нарушитель не имеет информации. Дополнительно к посылке шифро6. Зашифрованного текста отправитель передает ключевую строку по защищенному каналу получателю так, что получатель может расшифровать текст, обрабатывая XOR шифрованного текста и ключевой строки. Хитрость состоит в том, что нам нужно иметь защищенный канал для посылки ключевой

строки. Более практичный подход для отправителя: сгенерировать эту ключевую строку заранее. Например, отправитель может создать 1000 компакт-дисков, полных произвольных битов, и переправить их получателю на БТР. Хотя еженедельная посылка 1000 дисков и является широкополосной операцией, у нее есть один изъян: ключевой поток должен быть такой же длины, как и данные; если данные на один бит длиннее, чем ожидалось, то появятся проблемы. Строки однократного использования используются иногда на практике (например, однократные пароли).

Обходной путь, часто применяющийся на практике, должен выбрать короткий ключ (скажем, 64 бита) и использовать псевдослучайный генератор чисел, чтобы генерировать ключевую строку из короткого ключа. Теперь нужно послать только 64 бита по защищенному каналу, но придется полагаться на некоторое искусство. А именно: нужен хороший псевдослучайный генератор, для которого по выходу нельзя догадаться о ключе, и для которого один и тот же выход всегда генерируется из данного короткого ключа. Но если нарушитель может управлять входом, то он может восстановить выход произвольного генератора и, возможно, угадать будущие случайные числа!

Из этого следует, что трудно разработать хороший псевдослучайный генератор. Поэтому нужны альтернативные способы шифрования.

Можно ли вычислить, какие два документа зашифровал Борис, используя один и тот же одноразовый блокнот (гамму) – побитовое сложение по модулю 2 (и что собой представляет этот одноразовый блокнот)?

Известна следующая информация:

1. Шифрование использует коды ASCII со 128 возможными символами в любой позиции (хотя некоторые – значительно более вероятны, чем другие).
2. Используемый одноразовый блокнот был произведён псевдослучайным образом, со значениями в пределах от 0 до 127.
3. Использовался один и тот же блокнот, чтобы зашифровать оба исходных текста.

7

4. Если длины исходных текстов не совпадают, то более короткий из них дополняется пробелами.
5. Эти тексты - части относительно известных текстов на английском языке.

Шифр 1:

42 102 120 61 61 67 57 84 117 66 41 33 100 116 15 55 80 16 120 0 54
78 105 113 96 25 43 69 39 82 125 40 40 24 120 94 92 37 114 53 64 63
107 19 82 62 99 81 81 69 103 22 120 123 71 1 113 57 5 50 67 40 2 85
67 11 40 56 22 89 127 95 59 121 27 121 95 121 114 3 1 5 45 103 112
127 62 34 39 13 44 30 80 19 2 60 72 80 56 18 93 31 69 66 45 122 71
33 58 113 12 120 50 63 39 5 110 28 14 48 109 10 68 95 92 88 0 30 107
4 54 92 104 122 5 95 15 118 42 93 75 83 9 35 106 8 13 53 101 93 32
60 53 36 72 101 121 121 121 99 98 89 30 71 87 87 14 107 28 36 42 108
98 95 99 68 2 60

Шифр 2:

34 40 111 117 37 64 32 88 55 74 112 117 103 121 23 54 91 5 116 84 42

79 127 35 114 80 48 67 39 71 53 62 97 12 113 48 47 34 122 57 80 63
122 77 61 93 119 68 71 83 107 87 116 115 2 19 101 112 86 127 78 109 2
89 81 17 85 5 21 94 127 84 59 109 13 42 25 116 126 7 7 18 106 118
113 62 37 63 43 102 69 73 79 14 7 105 70 17 18 25 93 56 7 27 7 84
8 117 50 123 9 44 42 50 98 76 111 6 4 48 117 7 86 88 92 75 29 16
121 65 52 80 107 50 19 8 41 46 10 84 74 95 93 57 106 27 72 125 101
73 97 56 58 51 89 101 108 125 112 99 114 72 18 9 84 30 7 107 89 34
39 103 33 86 36 3 74 104

Программа должна без потерь расшифровывать приведенные файлы (включая список опечаток). Дополнительным заданием может служить создание программы, которая генерирует зашифрованные тексты по заданным открытым текстам.

Содержание отчета

Отчет должен содержать:

1. Описание атаки.
2. Алгоритм, функциональная схема и функциональный состав программы.

ПРАКТИЧЕСКАЯ РАБОТА № 3-4

Руководитель в системе управления персоналом информационной безопасности.

Цель работы:

Применение принципов организации, проектирования и анализа систем защиты информации и основ их комплексного построения на различных уровнях защиты.

Подготовка и порядок выполнения работы:

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Выполнить работу по аудиту комплексной защиты информации предприятия.
3. Проанализировать проделанную работу и предложить свой метод проведения аудита комплексной защиты информации на предприятии.
4. Результат отразить в отчете.

Краткие теоретические сведения:

Аудит комплексной защиты информации является основой построения системы защиты информации предприятия. Для его проведения и получения достоверных результатов требуется, как правило, привлечение сторонних специализированных организаций.

При создании любой информационной системы (ИС) на базе современных компьютерных технологий неизбежно возникает вопрос о защищенности этой системы от внутренних и внешних угроз безопасности информации.

Но прежде чем решить, как и от кого защищать информацию, необходимо уяснить реальное положение в области обеспечения безопасности информации на предприятии и оценить степень защищенности информационных активов.

Для этого проводится комплексное обследование защищенности ИС

(или аудит безопасности), основанные на выявленных угрозах безопасности информации и имеющихся методах их парирования, результаты которого позволяют:

1. оценить необходимость и достаточность принятых мер обеспечения безопасности информации;
2. сформировать политику безопасности;
3. правильно выбрать степень защищенности информационной системы;
4. выработать требования к средствам и методам защиты;
5. добиться максимальной отдачи от инвестиций в создании и обслуживании СОБИ.

Комплексное обследование (аудит безопасности информации) защищенности представляет собой системный процесс получения и оценки объективных данных о текущем состоянии обеспечения безопасности информации на объектах информатизации, действиях и событиях, происходящих в информационной системе, определяющих уровень их соответствия определенному критерию.

Комплексное обследование защищенности ИС (аудит_____1_-_) позволяет оценить реальное положение в области защиты информации и принять комплекс обоснованных управленческих решений по обеспечению необходимого уровня защищенности информационных активов предприятия.

Аудит защищенности ИС ставит своей целью методологическое обследование процессов, методов и средств обеспечения безопасности информации при выполнении информационной системой своего главного предназначения - информационное обеспечение бизнеса. При этом предполагается, что сама информационная система является оптимальной для решения бизнес - задач.

Результатом аудита защищенности могут быть рекомендации по изменению инфраструктуры сети, когда по экономическим соображениям нецелесообразно или невозможностью достичь требуемого уровня защищенности

информации при существующей инфраструктуре ИС.

Поскольку информационная безопасность должна быть обеспечена не только на техническом, но и на организационно-административном уровне, должный эффект может дать только комплексный подход к обследованию (аудиту), то есть:

1. проверка достаточности принятых программно-аппаратных и технических мер защиты (соответствие установленным требованиям применяемых в ИС программно-аппаратных средств защиты);
2. проверка достаточности инженерно-технических, правовых, экономических и организационных мер защиты (физической защиты, работы с персоналом, регламентации его действий).

Целью проведения работ по комплексному обследованию защищенности ИС является получение объективных данных о текущем состоянии обеспечения безопасности информации на объектах ИС, позволяющих провести минимизацию вероятности причинения ущерба собственнику информационных активов в результате нарушения конфиденциальности, целостности или доступности информации, подлежащей защите, за счет получения несанкционированного доступа к ней, а также выработка комплекса мер, направленных на повышение степени защищенности информации ограниченного доступа.

Процесс комплексного обследования защищенности информационной системы состоит из трех основных частей:

1. сбор необходимых исходных данных и их предварительный анализ (или стадия планирования);
2. оценка соответствия состояния защищенности ИС предъявляемым требованиям и стандартам (стадии моделирования, тестирования и анализа результатов);
3. формулирование рекомендаций по повышению безопасности информации в обследуемой ИС (стадии разработки предложений и документирования полученных результатов).

На разных этапах обследования используются различные методы: технические, аналитические, экспертные, расчетные. При этом, результаты, полученные одними методами, могут дублироваться (дополняться) результатами, полученными другими методами. Совокупность всех применяемых методов позволяет дать объективную оценку состояния обеспечения безопасности информации на обследуемом объекте.

Основными группами методов при обследовании являются:

1. Экспертно-аналитические методы предусматривают проверку соответствия обследуемого объекта установленным требованиям по безопасности информации на основании экспертной оценки полноты и достаточности представленных документов по обеспечению необходимых мер защиты информации, а также соответствия реальных условий эксплуатации оборудования предъявляемым требованиям по размещению, монтажу и эксплуатации технических и программных средств.

3. Моделирование действий злоумышленника («дружественный взлом» системы защиты информации) применяются после анализа результатов, полученных в ходе использования первых двух групп методов, - они необходимы как для контроля данных результатов. Этим методом подтверждаются также реальные возможности потенциальных злоумышленников (как внутренних, легально допущенных к работе с тем или иным уровнем привилегий в ИС, так и внешних - в случае подключения ИС к глобальным информационным сетям). Кроме того, подобные методы могут использоваться для получения дополнительной исходной информации об объекте, которую не удалось получить другими методами.

Важным моментом является то, что применение методов моделирования действий злоумышленника ограниченно. При использовании данных методов необходимо учитывать, что при осуществлении тестовой атаки, используемое в ИС оборудование может быть выведено из строя, информационные ресурсы утрачены или искажены.

Содержание отчета:

Отчет должен содержать:

1. Описание организации проведения Аудита на предприятии.

2. Формальный отчет по результатам Аудита.

3. Вывод, в котором предлагаются методы решения проблемы защиты информации.

Контрольные вопросы:

1. Кратко сформулируйте виды Аудита КЗИ.

2. В чем состоят источники успеха Аудита?

3. Раскройте понятие ѧСюрвейѧ.

4. В чем состоит сложность применения Аудита КЗИ?

ПРАКТИЧЕСКАЯ РАБОТА № 5-6

Деловая игра «Модель нарушителя политики безопасности».

Цель работы:

Изучение основных задач, моделирование и реализация на практике процесса регистрации и учета событий в ОС MS-DOS с целью практического применения основ защиты информации, а также для ознакомления с системой прерываний данной операционной системы. Причины, виды, каналы утечки и искажения информации. Ознакомление с основными методами обработки результатов аудита Осуществление на практике одного из методов обработки аудита клавиатуры с целью более полного представления об алгоритмах работы программ типа «Intrusion Detection».

Подготовка и порядок выполнения работы:

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности» на тему «Регистрация и учет событий в вычислительной системе» и «Обработка результатов аудита».
2. Изучить теоретический материал по курсу «Программирование» на тему «Создание резидентных программ», «Работа с файлами», «Ввод данных с клавиатуры» и «Алгоритмы сортировки».
3. Написать на языке Си программу, реализующую протоколирование всех нажатий клавиш в файле аудита клавиатуры, а также времени их нажатия Исключение составляют триггерные клавиши, для них необходимо фиксировать только те нажатия, которые влияют на смену их состояния Программа должна позволять выполнять любые операции операционной системы и не должна мешать работе других программ, то есть она должна работать в так называемом фоновом режиме. Файл аудита клавиатуры должен иметь имя, длиной не более восьми символов, которое должно быть уникальными для каждого пользователя. Необходимо реализовать предотвращение повторного

запуска программы-аудита и отгрузку ее из памяти, то есть управление резидентной частью. Пользователь, выполняющий роль администратора аудита, должен иметь следующие возможности в части запуска и отключения аудита:

- временное отключение аудита;
- определение информации о состоянии аудита (установлен или нет);
- задание идентификационного имени пользователя, для которого необходимо запускать аудит (не должно превышать восьми символов);
- располагать файлы аудита удобным для администратора образом, т.е. файл аудита не должен быть жестко привязан ни к какому конкретному каталогу или диску.

4. Написать на языке Си программу обработки данных аудита клавиатуры, анализирующую содержимое командной строки ОС MS-DOS (или время работы в ОС).
5. Проанализировать проделанную работу с целью нахождения путей применения аудита клавиатуры. В качестве альтернативы можно придумать и реализовать свою программу обработки результатов аудита клавиатуры.
6. Результаты отразить в отчете.

Краткие теоретические сведения:

Мощность современных сетей и причина, по которой они используются, заключаются в способности к быстрой передаче информации. Эта возможность передачи информации представляет также проблему безопасности. Сетевая информация, полученная из базы данных или посланная по электронной почте, может легко выйти из-под контроля. Она может ошибочно оказаться в почтовом ящике другого лица, или может быть собрана из кажущихся безобидными битов данных в критически опасные информационные обзоры, раскрывающие производственные планы, стратегии рынка или бизнес-планы. Поэтому важно контролировать возможности распространения и утечки информации. Для этих целей применяется аудит.

Аудит – это регистрация и учет событий, осуществляемых _____пользовате-

лем в системе. События в данном случае представляют собой нажатия на клавиши. Таким образом, происходит фиксирование информации, введенной пользователем с клавиатуры.

Так как MS-DOS является однозадачной операционной системой, то в определенный момент времени в ней может работать только один пользователь, поэтому в программе аудита должен присутствовать механизм идентификации, позволяющий для каждого пользователя определить идентификационное имя, которое используется для наименования файла аудита. Файл аудита содержит информацию о действиях пользователя в системе:

- время входа с систему (время запуска программы-аудита);
- специальная информация, которая зависит от назначения аудита.

Специальная информация определяется целью аудита. Цель аудита – фиксирование попыток со стороны пользователя осуществить неавторизованные, то есть недозволенные, действия, а также те действия, которые могут повлечь за собой нарушение работоспособности системы Примеры неавторизованных действий:

- работа за терминалом в недозволенное время. Определяется с помощью аудита клавиатуры путем анализа времени протоколирования нажатия на клавишу;
- запуск программ. приводящий к нарушению работоспособности операционной системы. Определяется с помощью аудита клавиатуры, если команда на запуск программы поступает из командной строки, а не с помощью другой программы.

Административные ограничения могут накладываться также на функции создания, удаления, переименование файлов и каталогов. Такие контролирующие действия вынуждают пользователя быть дисциплинированным. Таким образом, аудит – средство, позволяющее проверять выполнение требований, предъявляемых пользователю администратором системы, отвечающим за нормальное функционирование операционной системы и целостность хранящихся в ней данных.

Выполнение программы в фоновом режиме возможно, благодаря возможности создания резидентных программ. Отличительное свойство резидентных программ (TSR – Terminate-but-Stay-Resident) СОСТОИТ В ТОМ, ЧТО ОНИ

после своего завершения остаются в памяти компьютера, а операционная система помечает занятую ими память как используемую. Использование TSR позволяет реализовать так называемое пассивное мультипрограммирование MS-DOS является однопрограммной операционной системой, но активизация TSR вызывает переключение компьютера на резидентную программу. Если активизация TSR выполняется периодически, появляется возможность выполнения программ на фоне других программ.

ПРАКТИЧЕСКАЯ РАБОТА № 7-9

Организация контроля и мотивации выполнения персоналом требований нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.

Цель работы:

Изучение алгоритмов вызова программ в ОС MS DOS, а также принципов действия атак переполнения буфера ("buffer-overflow"). Применение основ информационной безопасности для нахождения путей противодействия угрозе. Реализация на практике модели атаки переполнения буфера в ОС MS DOS.

Подготовка и порядок выполнения работы:

Работа состоит из следующих этапов:

1. Изучить теоретический материал по курсу «Основы информационной безопасности».
2. Изучить теоретический материал по курсу «Программирование» на тему «Передача параметров в программу средствами языка Си++», «Запуск программ-потомков».
3. Написать на языке Си четыре программы:
- программу, подверженную атаке переполнения буфера;
- программу, защищенную от атак данного типа;
- программу, реализующую атаку переполнения буфера;
- программу типа EXPLOIT.
4. Проанализировать проделанную работу и предложить свой метод использования модификации адреса возврата.
5. Результат отразить в отчете.

Краткие теоретические сведения:

Данная ПРАКТИЧЕСКАЯ работа посвящена исследованию атак типа переполнения буфера. Рассматривается одна из тех технологий, которая

сегодня используется все чаще и требует для борьбы с ней понимания работы системы.

Известно, что в результате некорректного обращения к памяти может возникнуть проблема с менеджером памяти или зависание. Как правило, это

20

связано с тем, что программа попыталась получить доступ к не принадлежащей ей области памяти. Это довольно часто случается, если программист забыл, например, проверить размеры строки, заносимой в буфер, и остаток строки попал в какие-то другие данные или даже в код. Это происходит из-за отсутствия контроля за размерами строк и буферов. Логичным следствием является наличие так называемых "buffer-overflow"-программ, которые в защищенных операционных системах используются для нарушения защиты системы и получения привилегий суперпользователя системы (в данной лабораторной работе в качестве модели используется ОС MS DOS).

Рассмотрим две программы, которые подвергаются атакам "bufferoverflow". Их отличие состоит в том, что одна из них подвержена атаке, а другая – нет. Обе программы имеют статически определенный буфер конечного размера и принимают в качестве параметра строку неизвестной длины, которая заносится в этот буфер, признаком конца строки является нулевой символ. Во второй программе присутствует проверка на допустимую длину строки, в первой нет.

Для демонстрации работы этих двух программ необходимо написать специальную "buffer-overflow"-программу, которая вызывает программу-цель в режиме «с возвратом в предок» с параметром-строкой произвольного размера.

Рассмотрим изменение состояния стека в процессе вызова программы-цели. Итак, стек (будем считать, что он растет вверх) перед вызовом функции main() программы-цели выглядит следующим образом (см. рис. 1).

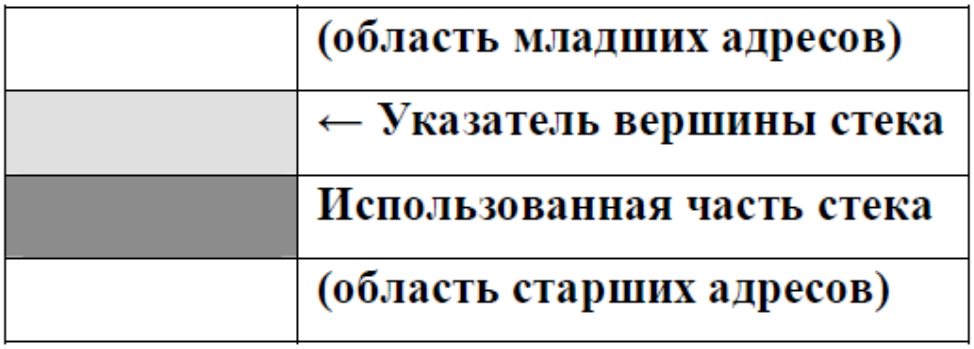

Рис. 1. Состояние стека в процессе вызова программы (шаг 1).

Компилятор, встречая инструкцию вызова функции main(), заносит в стек смещение следующей после вызова команды. Таким образом, функция

21

main() завершив свою работу, будет знать адрес возврата управления. В результате стек имеет следующий вид (см. рис. 2).

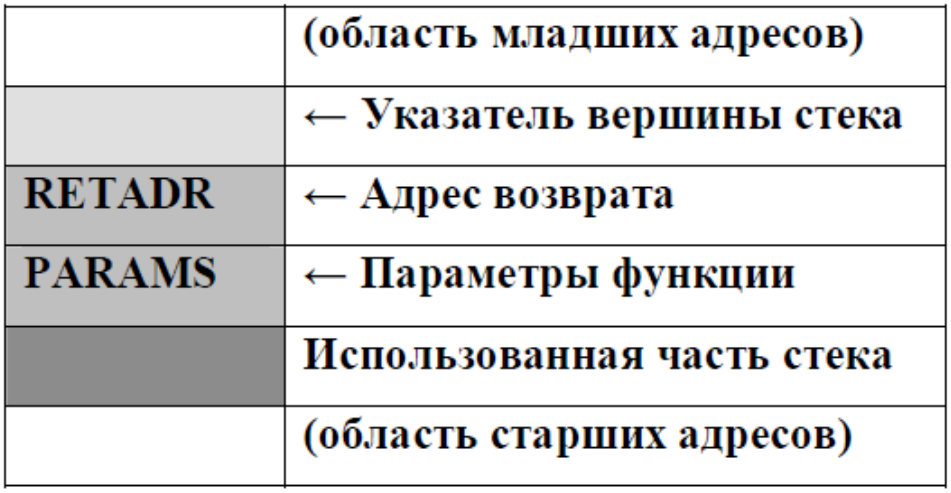

Рис. 2. Состояние стека в процессе вызова программы (шаг 2).

Функции надо запомнить указатель на текущую верхушку стека BP, который будет использоваться в ссылке на параметры. Поэтому, независимо от архитектуры, выполняются следующие две инструкции,

push bp

mov bp, sp

Теперь в верхушке стека лежит предыдущее значение регистра BP, а сам он указывает на верхушку стека и может быть использован в качестве базового регистра при ссылке на параметры. В программах объявлен размер

буфера в SIZE байт – этот буфер будет зарезервирован в стеке. После всех этих операций стек имеет следующий вид (см. рис. 3).__
После всего этого программа работает прекрасно, пока дело не доходит до вызова функции strcpy(). Если длина строки меньше или равна длине буфера, то все пройдет хорошо, функция отработает, освободит зарезервированное пространство, восстановит регистр BP и вернет управление программе, которая очистит стек от переданных параметров. Если же длина строки будет больше размера буфера, то поскольку strcpy() копирует все символы, пока не встретит код конца строки – 0, часть строки затрет верхнюю часть стека и может испортить поле **RETADR**. Это станет заметно не сразу – все будет работать корректно, пока дело не дойдет до вызова return. Управление будет передано по адресу, который хранится в поле **RETADR**, но поскольку адрес испорчен, программа будет продолжать выполняться в некоторой точке адресного пространства, отличающейся от точки вызова. В этом месте воз-
22
никнет исключительная ситуация, и программа будет аварийно прервана, поскольку маловероятно, чтобы адрес возврата указывал на какой-то осмысленный код, причем находящийся в области памяти данной программы.

	(область младших адресов)
	← Указатель вершины стека
?????	**← Начало зарезервированного буфера**
?????	
?????	**← Конец буфера**
OLDBP	**← Старое значение регистра BP**
RETADR	**← Адрес возврата**
PARAMS	**← Параметры функции**
	Использованная часть стека
	(область старших адресов)

Рис. 3. Состояние стека в процессе вызова программы (шаг 3).

Избежать подобной ситуации можно по крайней мере двумя способа-

ми. Первый способ - контроль длины строки, копируемой в буфер. Этот способ необходимо реализовать в программе под номером 2.

Второй способ несколько необычен, но именно он помогает понять действие "buffer-overflow"-программ. Назовем программу, реализующую этот метод **OVERFLOW**. он состоит в следующем:

- файл-цель исследуется с помощью отладчика, например “Turbo Debugger”. Необходимо узнать **BP** и **RETADR**;
- программа OVERFLOW.EXE вызывает программу-цель с параметром – строкой, которая «затирает» поля **BP** и **RETADR** старыми, заранее известными значениями этих полей. Параметром программы OVERFLOW.EXE является имя файла, содержащего имя программы-цели (это поле должно занимать 13 символов), **BP** и **RETADR** (значения должны быть записаны в HEX - формате).

23

На практике для исследования программы-цели применяются так называемые **EXPLOIT**-программы. Их целью является осуществление атаки для формальной проверки исследуемой программы на устойчивость. **EXPLOIT**-программа запускает программу-цель со строкой переменной длины до тех пор, пока программа – цель не зависнет или не сообщит об ошибке. Если программа зависла, это означает, что в ней отсутствует проверка на длину входной строки. Следовательно, данная программа не защищена от атаки переполнения буфера.

Программа должна запускаться с двумя параметрами:

- имя программы-цели;
- предельная длина строки.

В результате работы программы на экран дисплея должно выводится сообщение о текущем размере строки, передаваемой в качестве параметра программе-цели. Если весь вывод перенаправить в файл, то в случае успешной атаки, то есть зависания системы, в этом файле можно будет узнать размер последней строки. Таким образом, можно узнать размер буфера про-

граммы-цели.

Содержание отчета:

1. Описание атаки.

2. Алгоритм, функциональная схема и функциональный состав каждой программы.

3. Вывод должен содержать описание задач, для реализации которых применяются атаки переполнения буфера.

Контрольные вопросы:

1. Каковы основные направления обеспечения информационной безопасности объектов информационной сферы государства?

2. Дайте классификацию методов нарушения конфиденциальности, целостности и доступности информации.

3. В чем заключается атака переполнения буфера?

4. Каковы могут быть последствия атаки в различных операционных системах?

5. Какие алгоритмы противодействия атаке переполнения буфера Вам известны?

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
для обучающихся по организации и проведению практической работы
по дисциплине «Управление информационной безопасностью»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль):
«Информационная безопасность киберфизических систем»

Ставрополь, 2026

Содержание:

ПРАКТИЧЕСКАЯ РОБОТА № 1.

СТАНДАРТИЗАЦИЯ В СФЕРЕ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ.

Цель работы:

Ознакомиться с алгоритмами оценки риска информационной безопасности.

Краткие теоретические сведения:

Риск информационной безопасности – потенциальная возможность использования определенной ***угрозой уязвимостей актива*** или группы активов для причинения вреда организации.

Уязвимость - слабость в системе защиты, делающая возможной реализацию угрозы.

Угроза информационной безопасности - совокупность условий и факторов, которые могут стать причиной нарушений целостности, доступности, конфиденциальности информации.

Информационный актив – это материальный или нематериальный объект, который:

- является информацией или содержит информацию,
- служит для обработки, хранения или передачи информации,
- имеет ценность для организации.

Задание

Загрузите ГОСТ Р ИСО/МЭК ТО 13335-3-2007 «МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Ч а с т ь 3 «Методы менеджмента безопасности информационных технологий»

Ознакомьтесь с **Приложениями C, D** и **E** ГОСТа.

Выберите три различных информационных актива организации (см. вариант).

Из **Приложения D** ГОСТа подберите три конкретных уязвимости системы защиты указанных информационных активов.

Пользуясь **Приложением С** ГОСТа напишите три угрозы, реализация которых возможна пока в системе не устранены названные в пункте 4 уязвимости.

Пользуясь одним из методов (см. вариант) предложенных в **Приложении Е** ГОСТа произведите оценку рисков информационной безопасности.

Оценку ценности информационного актива производить на основании возможных потерь для организации в случае реализации угрозы.

Содержание отчета

1. Титульный лист
2. Содержание
3. Задание
4. Обоснование выбора информационных активов организации
5. Оценка ценности информационных активов
6. Уязвимости системы защиты информации
7. Угрозы ИБ
8. Оценка рисков
9. Выводы

Варианты

Номер варианта	**Организация**	**Метод оценки риска (см. Приложение Е ГОСТа)**
1	Отделение коммерческого банка	1
2	Поликлиника	2
3	Колледж	3
4	Офис страховой компании	4
5	Рекрутинговое агентство	1
6	Интернет-магазин	2
7	Центр оказания государственных услуг	3
8	Отделение полиции	4

9	Аудиторская компания	1
10	Дизайнерская фирма	2
11	Офис интернет-провайдера	3
12	Офис адвоката	4
13	Компания по разработке ПО для сторонних организаций	1
14	Агентство недвижимости	2
15	Туристическое агентство	3
16	Офис благотворительного фонда	4
17	Издательство	1
18	Консалтинговая фирма	2
19	Рекламное агентство	3
20	Отделение налоговой службы	4
21	Офис нотариуса	1
22	Бюро перевода (документов)	2
23	Научно проектное предприятие	3
24	Брачное агентство	4
25	Редакция газеты	1
26	Гостиница	2
27	Праздничное агентство	3
28	Городской архив	4
29	Диспетчерская служба такси	1
30	Железнодорожная касса	2

ПРАКТИЧЕСКАЯ РАБОТА № 2-3

Руководитель в системе управления персоналом информационной безопасности

Цель работы:

Изучение технологии аутентификации пользователя на основе пароля.

Краткие теоретические сведения:

Аутентификация (Authentication) - процедура проверки подлинности заявленного пользователя, процесса или устройства. Эта проверка позволяет достоверно убедиться, что пользователь (процесс или устройство) является именно тем, кем себя объявляет. При проведении аутентификации проверяющая сторона убеждается в подлинности проверяемой стороны, при этом проверяемая сторона тоже активно участвует в процессе обмена информацией. Обычно пользователь подтверждает свою идентификацию, вводя в систему уникальную, неизвестную другим пользователям информацию о себе (например, пароль или сертификат).

Идентификация и аутентификация являются взаимосвязанными процессами распознавания и проверки подлинности субъектов (пользователей). Именно от них зависит последующее решение системы, можно ли разрешить доступ к ресурсам системы конкретному пользователю или процессу. После идентификации и аутентификации субъекта выполняется его авторизация.

Авторизация (Authorization) - процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

Пароль - это то, что знает пользователь и что также знает другой участник взаимодействия. Для взаимной аутентификации участников взаимодействия может быть организован обмен паролями между ними.

Задание:

Разработать программу, представляющую собой форму доступа к определённым информационным ресурсам на основе пароля:

1. В качестве информационного ресурса использовать любой файл или приложение.

Для справки: работа с текстовым файлом в среде Delphi:

```
var
  myFile : TextFile;
  text : string;

begin
  // Попытка открыть файл Test.txt для записи
  AssignFile(myFile, 'Test.txt');
  ReWrite(myFile);

  // Запись нескольких известных слов в этот файл
  WriteLn(myFile, 'Hello');
  WriteLn(myFile, 'World');

  // Закрытие файла
  CloseFile(myFile);

  // Открытие файла в режиме только для чтения
  FileMode := fmOpenRead;
  Reset(myFile);
```

```
  // Показ содержимого файла
  while not Eof(myFile) do
  begin
    ReadLn(myFile, text);
    ShowMessage(text);
  end;

  // Закрытие файла в последний раз
  CloseFile(myFile);
end;
```

2. Доступ к ресурсу должен быть разрешен только санкционированным пользователям. Для этого в программе должны храниться имена пользователей и их пароли. При попытке доступа пользователя к ресурсу проверяется наличие его идентификатора (имени) в системе и соответствие введенного пароля паролю, который хранится в системе.

Для справки: Пример поиска элемента в массиве (Delphi):

```
// ввод массива for i:=l to SIZE do
a[i] := StrToInt(StringGridl.Cells[i - 1, 0]);
// ввод образца для поиска
obr := StrToInt(edit2.text);
// поиск
found := FALSE; // пусть нужного элемента в массиве нет
i := 1;
repeat
  if a[i] = obr then
    found := TRUE
  else
    i := i + 1;
until (i > SIZE) or (found = TRUE);
```

3. В системе должна храниться следующая информация о пользователе: ID или имя пользователя, пароль, ФИО, дата рождения, место рождения (город) номер телефона.

4. Пользователь должен иметь возможность поменять пароль (ограничения: см. вариант).

Содержание отчета:

1. Титульный лист
2. Содержание
3. Задание
4. Текст программы
5. Пример работы программы
6. Выводы

ПРАКТИЧЕСКАЯ РАБОТА № 4-5

Концепция безопасности предприятия и информационной безопасности .

Цель работы:

Знакомство с основными принципами построения концепции ИБ предприятия, с учетом особенностей его информационной инфраструктуры.

Краткие теоретические сведения:

До начала создания систем информационной безопасности ряд отечественных нормативных документов (ГОСТ Р ИСО/МЭК 15408 ГОСТ Р ИСО/МЭК 27000 ГОСТ Р ИСО/МЭК 17799) и международных стандартов (ISO 27001/17799) прямо требуют разработки основополагающих документов – **Концепции и Политики информационной безопасности.** Если Концепция ИБ в общих чертах определяет, **ЧТО** необходимо сделать для защиты информации, то Политика детализирует положения Концепции, и говорит **КАК**, какими средствами и способами они должны быть реализованы.

Концепция информационной безопасности используется для:

- принятия обоснованных управленческих решений по разработке мер защиты информации;
- выработки комплекса организационно-технических и технологических мероприятий по выявлению угроз информационной безопасности и предотвращению последствий их реализации;
- координации деятельности подразделений по созданию, развитию и эксплуатации информационной системы с соблюдением требований обеспечения безопасности информации;
- и, наконец, для формирования и реализации единой политики в области обеспечения информационной безопасности**.**

Задание:

Используя предложенные образцы, разработать концепцию информационной безопасности компании (см. вариант), содержащую следующие основные пункты (приведен **примерный** план, в который в случае необходимости могут быть внесены изменения):

Общие положения:

Назначение Концепции по обеспечению информационной безопасности.

1.2. Цели системы информационной безопасности

1.3. Задачи системы информационной безопасности.

Проблемная ситуация в сфере информационной безопасности:

2.1. Объекты информационной безопасности.

2.2. Определение вероятного нарушителя.

2.3. Описание особенностей (профиля) каждой из групп вероятных нарушителей.

2.4. Основные виды угроз информационной безопасности Предприятия.

- Классификации угроз.
- Основные непреднамеренные искусственные угрозы.
- Основные преднамеренные искусственные угрозы.

2.5. Общестатистическая информация по искусственным нарушениям информационной безопасности.

2.6. Оценка потенциального ущерба от реализации угрозы (см. Практическую работу № 1).

Механизмы обеспечения информационной безопасности Предприятия:

3.1. Принципы, условия и требования к организации и функционированию системы информационной безопасности.

3.2. Основные направления политики в сфере информационной безопасности.

3.3. Планирование мероприятий по обеспечению информационной безопасности Предприятия.

3.4. Критерии и показатели информационной безопасности Предприятия.

Мероприятия по реализации мер информационной безопасности Предприятия:

4.1. Организационное обеспечение информационной безопасности.

- Задачи организационного обеспечения информационной безопасности.
- Подразделения, занятые в обеспечении информационной безопасности.

- Взаимодействие подразделений, занятых в обеспечении информационной безопасности.

4.2. Техническое обеспечение информационной безопасности Предприятия.

- Общие положения.
- Защита информационных ресурсов от несанкционированного доступа.
- Средства комплексной защиты от потенциальных угроз.
- Обеспечение качества в системе безопасности.
- Принципы организации работ обслуживающего персонала.

4.3. Правовое обеспечение информационной безопасности Предприятия.

- Правовое обеспечение юридических отношений с работниками Предприятия .
- Правовое обеспечение юридических отношений с партнерами Предприятия.
- Правовое обеспечение применения электронной цифровой подписи.

4.4. Оценивание эффективности системы информационной безопасности Предприятия.

Содержание отчета:

1. Титульный лист
2. Содержание
3. Задание
4. Концепция ИБ заданного предприятия по плану, приведенному в задании

ПРАКТИЧЕСКАЯ РАБОТА № 6-7

Деловая игра «Модель нарушителя политики безопасности.»

Цель работы:

Изучить порядок вычисления и проверки ЭЦП (электронной цифровой подписи)

Теоретические сведения:

В настоящее время повсеместное внедрение информационных технологий отразилось и на технологии документооборота внутри организаций и между ними, между отдельными пользователями. Все большее значение в данной сфере приобретает электронный документооборот, позволяющий отказаться от бумажных носителей (или снизить их долю в общем потоке) и осуществлять обмен документами между субъектами в электронном виде. Однако переход от бумажного документооборота к электронному ставит ряд проблем, связанных с обеспечением целостности (подлинности) передаваемого документа и аутентификации подлинности его автора.

Следует отметить, что известные в теории информации методы защиты сообщений, передаваемых по каналам связи, от случайных помех не работают в том случае, когда злоумышленник преднамеренно реализует угрозу нарушения целостности информации. Например, контрольные суммы, используемые для этой цели передатчиком и приемником, могут быть пересчитаны злоумышленником так, что приемником изменение сообщения не будет обнаружено. Для обеспечения целостности электронных документов и установления подлинности авторства необходимо использовать иные методы, отличные от контрольных сумм. Для решения данных задач используют технологию электронно-цифровой подписи.

Электронно-цифровая подпись (ЭЦП) сообщения является уникальной последовательностью, связываемой с сообщением, подлежащей проверке на принимающей стороне с целью обеспечения целостности передаваемого сообщения и подтверждения его авторства.

Процедура установки ЭЦП использует секретный ключ отправителя сообщения, а процедура проверки ЭЦП – открытый ключ отправителя сообщения (рис. 1). Здесь

M – электронный документ, E – электронно-цифровая подпись.

В технологии ЭЦП ведущее значение имеют однонаправленные функции хэширования. Использование функций хэширования позволяет формировать криптографически стойкие контрольные суммы передаваемых сообщений.

Функцией хэширования H называют функцию, сжимающую сообщение произвольной длины M, в значение фиксированной длины H(M) (несколько десятков или сотен бит), и обладающую свойствами необратимости, рассеивания и чувствительности к изменениям. Значение H(M) обычно называют дайджестом сообщения M.

Схема установки ЭЦП (рис. 2):

- Для документа M формируется дайджест H с помощью заданного алгоритма хэширования.
- Сформированный дайджест H шифруют на секретном ключе отправителя сообщения. Полученная в результате шифрования последовательность и есть ЭЦП.
- Сообщение M и его ЭЦП передаются получателю сообщения.

Схема проверки ЭЦП (рис. 3):

- Получатель для проверки ЭЦП должен иметь доступ к самому сообщению M и его ЭЦП.
- Зная алгоритм хэширования, который был использован при установке ЭЦП, получатель получает дайджест H1 присланного сообщения M.
- Зная открытый ключ отправителя, получатель дешифрует ЭЦП, в результате чего получает дайджест H2, сформированный на этапе установки ЭЦП.
- Критерием целостности присланного сообщения M и подтверждения его автора является совпадение дайджестов H1 и H2. Если это равенство не выполнено, то принимается решение о некорректности ЭЦП.

Задание:

Сформировать ЭЦП к сообщению M' (см. вариант) и произвести проверку целостности принятого сообщения.

Порядок выполнения работы:

Разделить лист на две части: слева – сторона отправителя сообщения, справа – получателя.

На стороне отправителя выполнить следующие действия:

Записать сообщение M (см. вариант).

Сформировать профиль сообщения M’ с помощью упрощенной функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения.

Создать ЭЦП шифрованием профиля сообщения h(M’) закрытым ключом отправителя Da (значение ключа (d, n) см. в таблице с вариантами задания), т.е. Da (h(M’)) (см. вариант).

На стороне получателя выполнить следующие действия:

Записать сообщение M (его получает получатель вместе с ЭЦП) и ЭЦП Da (h(M’)).

Сформировать профиль принятого сообщения, M’ с помощью той же функции хэширования h(M’) – перемножения всех цифр кроме нуля этого сообщения (Получателю известен алгоритм хэширования, применяемый на стороне отправителя).

Создать профиль дешифрованием ЭЦП открытым ключем отправителя (Ea (Da (h(M’)) = h(M’)) (значение ключа (e, n) см. в таблице с вариантами задания).

Сравнить два профиля сообщения h(M’) (п.3.2 и 3.3). Убедиться в их совпадении.

Содержание отчета:

- Титульный лист
- Содержание
- Задание
- Лист расчета и проверки ЭЦП
- Выводы

Варианты

Номер варианта	p	q	e	d	M
1	3	11	7	3	5523
3	17	11	7	23	8866
3	13	7	5	29	3565
4	101	113	3533	6597	6546
5	3	11	7	3	8562
6	17	11	7	23	9795
7	13	7	5	29	8462
8	17	11	7	23	7785
9	13	7	5	29	2123
10	101	113	3533	6597	3145
11	7	11	37	13	2566
12	101	113	3533	6597	3782
13	3	11	7	3	3465
14	17	11	7	23	3895
15	13	7	5	29	4132
16	17	11	7	23	5123
17	13	7	5	29	4416
18	101	113	3533	6597	7895
19	3	11	7	3	7459
20	17	11	7	23	5654
21	13	7	5	29	2456

22	17	11	7	23	3585
23	13	7	5	29	2652
24	101	113	3533	6597	5656
25	3	11	7	3	6685
26	17	11	7	23	5566
27	13	7	5	29	4652
28	17	11	7	23	8666
29	13	7	5	29	4556
30	101	113	3533	6597	9266

ПРАКТИЧЕСКАЯ РАБОТА № 8-9

«Организация контроля и мотивации выполнения персоналом требований нормативно-методических и организационно-распорядительных документов по защите информации на предприятии зарубежных странах»

Цель работы:

Ознакомление с основными принципами обеспечения информационной безопасности в ведущих зарубежных странах.

Краткие теоретические сведения:

Обеспечение защиты информации волновало человечество всегда. В процессе эволюции цивилизации менялись виды информации, для её защиты применялись различные методы и средства.

Процесс развития средств и методов защиты информации можно разделить на три относительно самостоятельных периода:

Наблюдаемые в последние годы тенденции в развитии информационных технологий могут уже в недалеком будущем привести к появлению качественно новых (информационных) форм борьбы, в том числе и на межгосударственном уровне, которые могут принимать форму информационной войны, а сама информационная война станет одним из основных инструментов внешней политики, включая защиту государственных интересов и реализацию любых форм агрессии. Это является одной из причин, почему полезно ознакомиться с основными принципами обеспечения ИБ в ведущих зарубежных странах.

Другая причина заключается в том, что большинство применяемых на территории РФ средств и методов обеспечения ИБ основаны на импортных методиках и строятся из импортных компонентов, которые были разработаны в соответствии с нормами и требованиями по обеспечению ИБ стран-изготовителей. В связи с этим прежде чем приступить к изучению

непосредственно технологий и средств обеспечения ИБ, следует познакомиться с политикой ИБ ведущих зарубежных стран.

Задание:

- Подготовить краткий доклад по заданному вопросу (см. вариант), используя учебное пособие Аверченкова, В.И. ″Системы защиты информации в ведущих зарубежных странах" и другие доступные источники информации.
- Заполнить таблицу " Системы обеспечения ИБ в ведущих зарубежных странах "(см. вариант) на основе подготовленного материала, а также докладов других студентов.
- Провести анализ собранной информации и сделать выводы.

Содержание отчета:

- Титульный лист
- Содержание
- Задание
- Таблица "Системы обеспечения ИБ в ведущих зарубежных странах"
- Выводы

Варианты

Вариант – номер по списку в журнале.

Страна	**Основные принципы обеспечения ИБ**	**Основные документы в области обеспечения ИБ**	**Структура государственных органов обеспечения национальной ИБ**
США	1	2	3
Евросоюз	4	5	6
Великобритания	7	8	9
Швеция	10	11	12
Франция	13	14	15
Германия	16	17	18
Китай	19	20	21

Япония	22	23	24
Швейцария	25	26	27

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

МЕТОДИЧЕСКИЕ УКАЗАНИЯ
для обучающихся по организации и проведению самостоятельной работы
по дисциплине «Управление информационной безопасностью»
для студентов направления подготовки
10.04.01 «Информационная безопасность»
Направленность (профиль):
«Информационная безопасность киберфизических систем

Ставрополь, 2026

СОДЕРЖАНИЕ

Введение

Основной целью изучения дисциплины «Управление информационной безопасностью» является формирование набора общекультурных и профессиональных компетенций будущего магистра по направлению подготовки 10.04.01 Информационная безопасность.

Для достижения указанной цели в процессе изучения данной дисциплины необходимо решить следующие задачи:

- приобретение студентами теоретических знаний по системному подходу к управлению информационной безопасностью и практических навыков по их моделированию.

Компетенции обучающегося, формируемые в результате освоения дисциплины:

№ п/п	Содержание компетенции	Шифр
Общепрофессиональные компетенции		**ОК-(№)**
1.	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание;	ОПК-1
2.	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности;	ОПК-3

В результате освоения дисциплины обучающийся должен:

ЗНАТЬ	– современные подходы к управлению ИБ и направлениях их развития; – основные стандарты, регламентирующие управление ИБ; – принципы построения СУИБ; – принципы разработки процессов управления ИБ;
УМЕТЬ	– анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам управления ИБ; – определять цели и задачи, решаемые разрабатываемыми процессами управления ИБ; – применять процессный подход к управлению ИБ в различных сферах деятельности;
ВЛАДЕТЬ	– навыками управления информационной безопасностью простых объектов; – терминологией и процессным подходом построения систем управления ИБ; – навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках области деятельности СУИБ;

1. Общая характеристика самостоятельной работы студента

Основными видами учебной работы по достижению результатов освоения дисциплины являются лекции, лабораторные, практические занятия и самостоятельная работа студентов (СРС).

На лекциях раскрываются основные положения и понятия курса, формируются знания в области управления информационной безопасностью. На лабораторных занятиях формируются умения и навыки, необходимые для решения задач профессиональной деятельности.

Приступая к изучению учебной дисциплины, необходимо ознакомиться с учебной программой, получить в библиотеке рекомендованные учебные пособия, а также получить у ведущего преподавателя в электронном виде конспекты лекций, методические рекомендации к лабораторным занятиям и тестовые задания, завести новую тетрадь для конспектирования лекций и выполнения практических заданий.

Для изучения дисциплины предлагается список основной и дополнительной литературы. Основная литература предназначена для обязательного изучения, дополнительная – поможет более глубоко освоить отдельные вопросы, подготовить исследовательские задания и выполнить задания для самостоятельной работы.

В ходе лекционных занятий студент обязан осуществлять конспектирование учебного материала, особое внимание обращая на категории, формулировки, раскрывающие содержание тех или иных понятий, физических явлений, процессов, эффектов. В рабочих конспектах желательно оставлять поля, на которых следует делать пометки из рекомендованной литературы, дополнять материал прослушанной лекции, формулировать научные выводы и практические рекомендации. Студент имеет право задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, разрешения спорных ситуаций.

Самостоятельная работа студентов над материалом учебной дисциплины является неотъемлемой частью учебного процесса и должна предполагать углубление знания учебного материала, излагаемого на аудиторных занятиях, и приобретение дополнительных знаний по отдельным вопросам самостоятельно.

Основными видами самостоятельной работы студентов по учебной дисциплине являются:

- самостоятельное изучение учебного материала по заданным темам;
- подготовка к лабораторным и практическим занятиям, оформление отчета по выполненному лабораторной работе и подготовка к собеседованию по результатам

работы.

Основными методами самостоятельной работы студентов являются:

1) для овладения знаниями:

– чтение текста (конспекта лекций, учебника, дополнительной литературы) и конспектирование текста;

– работа с нормативными документами;

– поиск информации в Интернет;

2) для закрепления и систематизации знаний:

– работа с конспектом лекции (обработка текста);

– повторная работа над учебным материалом (учебника, дополнительной литературы, слайдами);

– составление плана и тезисов ответа или графическое изображение структуры ответа;

– составление таблиц для систематизации учебного материала;

– изучение нормативных документов;

– ответы на контрольные вопросы;

3) для формирования умений:

– подготовка к лабораторным занятиям;

– решение задач и практических заданий;

– подготовка отчетов по лабораторным занятиям;

– рефлексивный анализ профессиональных умений.

В случае пропуска учебного занятия студент может воспользоваться содержанием различных блоков учебно-методического комплекса (лекции, практические занятия, контрольные вопросы) для самоподготовки и освоения темы. Для самоконтроля необходимо использовать вопросы и задания, предлагаемые к лабораторным занятиям.

2. Технологическая карта самостоятельной работы обучающихся дисциплине «Управление информационной безопасностью»

Коды реализуемых копетенций, индикаторов	Вид деятельности студентов	Средства и технологии оценки	Обьем часов, в том числе		
			СРС	Контактная работа с преподавателем	Всего
4 семестр					
ИД-2$_{ОПК-3}$ ИД-3$_{ОПК-3}$	Подготовка к лабораторной работе	Собеседование	24.00	2.00	26.00
ИД-1$_{ОПК-1}$, ИД-3 $_{ОПК-1,}$ ИД-2$_{ОПК-3}$ ИД-3$_{ОПК-3}$	Подготовка к экзамену	Вопросы к экзамену	26.00	2.00	28.00
Итого за 4 семестр			48.00	4.00	54.00
Итого			48.00	4.00	54.00

3. Контрольные точки и виды отчетности по ним

По дисциплине предусмотрен текущий контроль на каждом учебном занятии и по каждому разделу учебной дисциплины.

Формы текущего контроля:

- устный опрос;
- защита отчетов по лабораторным занятиям.

Устный опрос осуществляется на каждом учебном занятии (лекции, лабораторные занятия). Все практические занятия, выполняемые по разделам дисциплины, подлежат оцениванию по результатам проверки отчета и собеседованию.

Критерии оценки для проверки умений при выполнении лабораторных заданий:

- оценка «отлично» выставляется, если студент продемонстрировал высокое умение применять полученные знания на практике через решение конкретной задачи, свободно без затруднений справился с поставленной задачей, показав владение разносторонними приемами и навыками ее выполнения, не допустил ошибок и неточностей;
- оценка «хорошо» выставляется, если студент продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, справился с поставленной задачей, показав владение необходимыми приемами и навыками ее выполнения, при этом допустил не более одной ошибки;
- оценка «удовлетворительно» выставляется, если студент продемонстрировал посредственное умение применять полученные знания на практике через решение конкретной задачи, с трудом справился с поставленной задачей, при этом допустил не более двух ошибок;
- оценка «неудовлетворительно» выставляется, если студент не продемонстрировал умение применять полученные знания на практике через решение конкретной задачи, не справился с поставленной задачей или допустил при ее решении три и более серьезные ошибки.

4. Методические указания по подготовке к лабораторным занятиям

При подготовке к лабораторной работе студенту следует:

- изучить (повторить) теоретический материал, посвящённый теме практического занятия;
- ознакомиться с заданием на лабораторную работу;
- проверить свой уровень подготовки с помощью вопросов и заданий для самоконтроля.

К работе в лаборатории допускаются лица, изучившие правила и меры безопасности, сдавшие зачет по ним и усвоившие порядок выполнения практического занятия.

Требования безопасности перед началом работ:

– ЗАПРЕЩАЕТСЯ: переодеваться, пользоваться огнем, курить, принимать пищу в лаборатории;

– убедиться в целостности электрических розеток и разъемов. В лаборатории необходимо быть в сменной обуви;

– включение компьютера производить только после получения допуска по выполняемой работе и разрешения преподавателя или лаборанта.

Требования безопасности во время работы:

– выполняя лабораторную работу, студенты обязаны использовать только вычислительную технику, периферийное оборудование, соединительные кабели, измерительное оборудование и носители информации, непосредственно относящиеся к данному лабораторной работе;

– подключение и отключение составляющих вычислительного комплекса производить только при полном снятии напряжения со всех составляющих вычислительного комплекса;

– при обнаружении неисправностей в оборудовании немедленно отключить источники питания и доложить об этом руководителю занятий или лаборанту.

Требования безопасности по окончании работы:

– доложить руководителю занятий или лаборанту о завершении работ.

– привести в порядок и сдать рабочее место лаборанту, и доложить руководителю занятий о сдаче.

По результатам выполнения лабораторной работы студенты оформляют и защищают в индивидуальном порядке в форме собеседования результаты выполнения заданий.

При подготовке и выполнении лабораторных работ совместно с оформлением отчетов по лабораторным занятиям позволяет успешно овладеть умениями, необходимыми для дальнейшей учебной и профессиональной деятельности.

Задания, выполняемые по лабораторным занятиям

Раздел 1. Управления ИБ.
ПРАКТИЧЕСКАЯ работа № 1-2. Стандартизация информационной безопасности .

Базовый уровень:

1. Что такое стандартизация ИБ?
2. Приведите виды стандартизации.
3. С чем связана стандартизация ?

Повышенный уровень:

4. Проанализировать регламентирующие различные аспекты реализации использования средств и методов защиты.

ПРАКТИЧЕСКАЯ работа 3-4. Руководитель в системе управления персоналом информационной безопасности ..

Базовый уровень:

4. Кто такой руководитель управления персоналом ИБ персоналом
5. Какая его обязанность и его функции .
6. В чем заключается управление персоналом ИБ

Повышенный уровень:

7. Что такое ИБ ?

Раздел 2. Системы управления информационной безопасности .

ПРАКТИЧЕСКАЯ работа 5-6. Деловая игра «Модель нарушителя политики безопасности».

В чем заключается сущность многокритериального подхода к оценке систем?

8. Кто такой нарушитель?
9. Описание модели нарушителя
10. Чем опасен нарушитель ?

Повышенный уровень:

11. Анализ угроз предприятия
12. Выявление уязвимостей ИБ .

ПРАКТИЧЕСКАЯ работа 7-9. Организация контроля и мотивации выполнения персоналом требований нормативно-методических и организационно-распорядительных документов по защите информации на предприятии.

Базовый уровень:

13. Что такое документ?
14. Угрозы осуществляемы по вине персонала
15. Описать характеристики безопасности системы.

Повышенный уровень:

16. Как осуществляется контроль на предприятии?

5. Примерная тематика заданий для самостоятельной работы студентов

Раздел 1. Управления информационной безопасности

Базовый уровень:

1. Что такое ИБ.
2. Определение информационной системы.
3. Что такое конфиденциальность.
4. Что такое угроза, виды.
5. Уязвимости ИС, виды.
6. Виды ИБ.
7. Структура мер ИБ.

Повышенный уровень:

8. Основные угрозы доступности информации.
9. Сервисы безопасности

Раздел 2. Системы управления информационной безопасности

Базовый уровень:

10. Что такое конфиденциальность.
11. Назовите наиболее эффективное средство для защиты от сетевых атак.
12. Утечка информации это.
13. Виды информации.
14. Причины возникновения ошибок системы.
15. Влияние персонала на предотвращение.
16. Методы повышения входа достоверных данных.
17. Что такое система управления ИБ.

Повышенный уровень:

18. Основные функции управления ИБ.
19. Политика ИБ.
20. Методы защиты информации.

6. Список рекомендуемой литературы

Основная литература:

1. Поздняк, И. С. Управление информационной безопасностью : методические указания / И. С. Поздняк, И. С. Макаров. — Самара : ПГУТИ, 2019. — 43 с.
2. Поздняк, И. С. Планирование и управление информационной безопасностью : учебное пособие / И. С. Поздняк, И. С. Макаров, Л. Р. Чупахина. — Самара : ПГУТИ, 2020. — 69 с.

Дополнительная литература:

1. Галатенко, В.А. Основы информационной безопасности [Электронный ресурс] / В.А. Галатенко. - Изд. 3-е. - М. : Интернет-Университет Информационных Технологий, 2005. - 208 с. - ISBN 5-9556-0052-3. - URL:http://biblioclub.ru/index.php?page=book&id=233063
2. Астахов, А.М. Искусство управления информационными рисками [Электронный ресурс] / А.М. Астахов. - М. : ДМК Пресс, 2010. - 312 с. - ISBN 978-5-94074-574-7. - URL: http://biblioclub.ru/index.php?page=book&id=86481
3. Анисимов, А.А. Менеджмент в сфере информационной безопасности [Электронный ресурс] / А.А. Анисимов. - М. : Интернет-Университет Информационных Технологий, 2009. - 176 с. - ISBN 9778-5-9963-0237-6. - URL: http://biblioclub.ru/index.php?page=book&id=232981
4. Минаев В.А., Фисун А.П. Правовое обеспечение информационной безопасности, Москва, 2008 г. – 368 с.
5. Романов О.А., Бабин С.А., Жданов С.Г. Организационное обеспечение информационной безопасности. – М.: Академия, 2008 г. – 192 стр.

Методическая литература:

- 1.Леонов Г.А. Теория управления. – Санкт-Петербург, 2016. – 234 с.
- 2.Репин В., Елиферов В. Процессный подход к управлению. Моделирование бизнес-процессов. М.: Стандарты и качество, 2014. – 408 с.

Интернет-ресурсы:

- сайт Федеральной службы по техническому и экспортному контролю. – www.fstec.ru;
- сайт Федеральной служба безопасности Российской Федерации. – www.fsb.ru.