МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ
КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
им. И.РАЗЗАКОВА
БИШКЕКСКИЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ

«Рассмотрено и одобрено» на
Методическом совете БТК
Протокол № 11
от «11» октября 2023г.

Утверждаю
Зам.директора по УР
_____ Досупов М.М.
«___» _____ 2023г.

УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС

по дисциплине

«Операционные системы и среды»

Для специальностей:
230109 «Программное обеспечение вычислительной техники и автоматизированных систем»
230110 «Техническое обслуживание средств вычислительной техники и компьютерных сетей»
230111 «Программное обеспечение в компьютерных системах»

Разработан преподавателем БТК: Мукашов К.Ш.
Рассмотрен и рекомендован к печати на заседании предметно цикловой комиссии специальных дисциплин
Протокол №_7_ от «30» 08 2023 года.
Председатель ЦК_____ Батырбекова.Д.А

РЕЦЕНЗИЯ
НА УЧЕБНО-МЕТОДИЧЕСКИЙ КОМПЛЕКС ДИСЦИПЛИНЫ
“Операционные системы и среды”
Преподавателя Мукашова К.Ш.

Учебно-методический комплекс по дисциплине “Операционные системы и среды” разработан для обеспечения выполнения требований государственного образовательного стандарта СПО КР для общеобразовательного цикла типовых учебных планов к минимуму содержания и подготовки специалистов по всем специальностям.

Учебно-методический комплекс включает в себя следующие элементы:

- Рабочую программу учебной дисциплины;
- Календарно-тематический план;
- Лекционные материалы;
- Задания для текущего контроля знаний студентов;
- Методические рекомендации по планированию организации и проведению практических занятий;

Рабочая программа составлена логично и носит упорядоченный, модульный подход к изучаемым разделам “Операционные системы и среды”. Последовательность тем, предлагаемых изучению, направлена на качественное усвоение учебного материала. Календарно-тематический план соответствует по своему содержанию рабочей программе по соответствующей дисциплине. Методические рекомендации по выполнению практических заданий позволяют углубить полученные теоритическое знания и привить опыт практического применения.

Методические рекомендации по организации самостоятельной работы направлены на закрепление умения поиска, накопления и обработки научной информации. Слайд-сопровождение теоритического материала нуждается в расширении.

Представленный учебно-методический комплекс дисциплины “Операционные системы и среды” имеет практическую направленность, включает достаточное количество разнообразных элементов, направленных на развитие умственных, творческих способностей студентов, приобретение общенаучных, инструментальных, социально-личностных и общекультурных компетенций.

Рекомендуется ввести лабораторные занятий по дисциплине и разделить по сложности индивидуальные задания, расширить количество тестовых контрольных заданий.

Рецензент
Заведующий кафедрой ИСТ
им.А.Жайнакова
к.ф-м.н.доцент

Аманкулова Н.А.

Содержание

СИЛЛАБУС
ДИСЦИПЛИНЫ ДЛЯ СТУДЕНТОВ

1. Краткое описание дисциплины. «Информационная безопасность» в системе подготовки специалистов:

- освоение теоретической и практической базы основ интегрированной среды **Информационная безопасность** для более углубленного понимания информационной безопасность и защиты информации:
- помочь студентам усвоить основы идей информационной безопасности и ориентирован на приобретение знаний и навыков обеспечения информационной безопасности с помощью различных методов и средств защиты информации процессы и явления из области будущей деятельности студентов как специалистов;
- формировать умения и навыки самостоятельного анализа исследования информационных систем, развивать стремление к научному поиску путей совершенствования своей работы.

2. Пререквизиты дисциплины. Для изучения дисциплины **«Информационная безопасность»** студентам необходимо хорошее знание **«Информатики»** в объеме средней школы, **Алгоритмизация и языки программирования, Высокоуровневые методы программирования.**

3. Постреквизиты дисциплины Дисциплина **««Информационная безопасность»** служит базой для изучения таких дисциплин как “Программное обеспечение”, “БиБД”, “Программирование ПО”, “Надежность информационных систем”.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ КЫРГЫЗСКОЙ РЕСПУБЛИКИ
КЫРГЫЗСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ им.И.РАЗЗАКОВА

БИШКЕКСКИЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ

«Согласовано»
_____
«___»_____2023 год.

«Утверждаю»
Зам. директора по УР
_____Долотов М.М.
«___»_____2023 год.

Рабочая программа

По предмету: “**Информационная безопасность”**

Для специальности:
230109 “Программное обеспечение вычислительной техники и автоматизированных систем”
230110 “Техническое обслуживание средств вычислительной техники и компьютерных сетей”

Курс: 3 семестр: 5

Количество часов по учебному плану: 60 часов

Разработан преподавателем БТК КГТУ – Омуралиевой З.М.

Составлен на основании ГОС СПО КР по специальности 230109 “Программное обеспечение вычислительной техники и автоматизированных систем”, утвержденного приказом МОиН КР №567/1 15.05.2019 года (регистрационный №180 от 07.08.2019 года МЮ КР)

Рассмотрена на заседании цикловой комиссии _____

Протокол № _____ от «_____»_____ 2023 года

Председатель ЦК _____ Батырбекова Д.А.

Бишкек 2023 г

СОДЕРЖАНИЕ

1. Паспорт рабочей программы учебной дисциплины «Информационная безопасность»

1.1. Область применения программы

Программа учебной дисциплины «Информационная безопасность» (далее программа) является частью основной профессиональной образовательной программы в соответствии с ГОС СПО по специальности 230109 «Программное обеспечение вычислительной техники и автоматизированных систем», 230110 “Техническое обслуживание средств вычислительной техники и компьютерных сетей” утвержденный приказом Министерства образования и науки КР №567/1 от 15.05.2019 года (регистрационный №180 от 07.06.2019года МЮ КР).

1.2. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина входит в профессиональный цикл дисциплин вариативной части ГОС СПО по специальности 230109 «Программное обеспечение вычислительной техники и автоматизированных систем», 230110 “Техническое обслуживание средств вычислительной техники и компьютерных сетей”.

Цели и задачи дисциплины – требования к результатам освоения дисциплины:

Целью учебной дисциплины - является обеспечение безопасности личных и корпоративных данных. Сохранение структурность и целостность информации. А также обеспечение безопасности от несанкционированного взлома.

Задачи дисциплины – требования к результатам освоения дисциплины

Иметь представление

- о показателях качества и надежности ПО;
- о ресурсосберегающих энергосберегающих технологиях использования вычислительной техники.

Знать:

- виды угроз для информационной безопасности предприятия, организации;
- современные средства для защиты данных и программ, находящихся на компьютерах;
- современные средства для защиты передаваемой информации;
- правовые средства защиты данных;

Уметь:

- организовать комплексную защиту информации на компьютерах предприятия, организации;
- выбирать и использовать современные средства защиты хранимых и передаваемых данных;

Владеть:

- навыками использования программных средств для защиты данных;
- навыками устранения угроз безопасности данных;

Информационная безопасность

Задачи дисциплины – требования к результатам освоения дисциплины

Иметь представление

- о показателях качества и надежности ПО;
- о ресурсосберегающих энергосберегающих технологиях использования вычислительной техники.

Знать:

- виды угроз для информационной безопасности предприятия, организации;
- современные средства для защиты данных и программ, находящихся на компьютерах;
- современные средства для защиты передаваемой информации;
- правовые средства защиты данных;

- законодательный морально-этический, административно-процедурный, физический, аппаратно-программный аспекты обеспечения информационной безопасности; существующие способы защиты информации этапах хранения, обработки, передачи информации в целях сохранения ее необходимых качеств, таких, как доступность, целостность, конфиденциальность, аппелируемость, аутентичность;

Уметь:

- организовать комплексную защиту информации на компьютерах предприятия, организации;
- выбирать и использовать современные средства защиты хранимых и передаваемых данных;
- ориентироваться в методах защиты информации и в том, когда и каким они применяются.

Владеть:

- навыками использования программных средств для защиты данных;
- навыками устранения угроз безопасности данных;
- теоретическими знаниями о существующих способах защиты информации на всех этапах: хранения, обработки, передачи информации в целях сохранения необходимых качеств, таких, как доступность, целостность, конфиденциальность, аппелируемость, аутентичность, навыками организации защиты информационных систем.;

1.4.Перечень формируемых компетенций

В процессе освоения дисциплины у студентов должны формироваться следующие компетенции:

Общие:

ОК1. Уметь организовать собственную деятельность, выбирать методы и способы выполнения профессиональных задач, оценивать их эффективность качество;

ОК2. Решать проблемы, принимать решения в стандартных и нестандартных ситуациях, проявлять инициативу и ответственность;

ОК3. Осуществлять поиск, интерпретацию и использование информации, необходимой для эффективного выполнения профессиональных задач, профессионального и личностного развития;

ОК4. Использовать информационно-коммуникационные технологии в профессиональной деятельности;

ОК 5. Уметь работать в команде, эффективно общаться с коллегами, руководством и клиентами;

ОК 6. Брать ответственность за работу членов команды (подчиненных) и их обучение на рабочем месте, за результат выполнения задания;

ОК7. Управлять собственным личностным и профессиональным развитием, адаптироваться к изменениям условий труда и технологий в профессиональной деятельности;

ОК8. Быть готовым к организационно-управленческой работе с малыми коллективами;

ОК9. Логически верно, аргументированно и ясно строить свою устную и письменную речь на Государственном и официальном языках;

ОК10. Понимать сущность и социальную значимость своей будущей профессии, проявлять к ней устойчивый интерес;

Профессиональные:

К0901. Организовать комплексную защиту информации на ПК предприятия, организации;

К0902. Выбирать и использовать средства защиты хранимых и передаваемых данных, методов защиты информации;

1.4 Рекомендуемое количество часов на освоение рабочей программы учебной дисциплины.

Максимальная учебная нагрузка студентов 60 часов, в т.ч.
Максимальной учебной нагрузки обучающегося - 60 часов, в том числе:

- обязательной аудиторной учебной нагрузки обучающегося - 12 часов;
- лабораторных работ - 18 часов;
- самостоятельной работы обучающегося - 30 часов.

2.Структура и содержание учебной дисциплины.

2.1.Объем учебной дисциплины и виды учебной работы.

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	60
Обязательная аудиторная учебная нагрузка (всего)	30
В том числе:	
Теоретические занятия	12
Лабораторных работ	18
Контрольные работы	
Самостоятельная работа студента (всего)	30
В том числе:	
Индивидуальное задание	
Внеаудиторная самостоятельная работа	30

Структура и примерное содержание учебной дисциплины

№ п/п	Наименование разделов и тем	Количество часов					Уровень освоения
		Всего	СРС	В том числе		Ауд	
				теор	прак		
1	2	3	4	5	6	7	8
Раздел 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И УРОВНИ ЕЕ ОБЕСПЕЧЕНИЯ							
1.1	Понятие «Информационная безопасность»	4	2	2		2	2
1.2	Составляющие информационной безопасности	4	2	2		2	2
1.3	Система формирования режима информационной безопасности	4	2	2		2	2
1.4	Классификация угроз «Информационной безопасности»	4	2	2		2	2
	Итоги по разделу:	**16**	**8**	**8**		**8**	
Раздел 2. КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ							
2.1	Вирусы как угроза информационной безопасности	4	2	2		2	2
2.2	Классификация компьютерных вирусов	4	2	2		2	2
2.3.	Характеристика «Вирусоподобных» программ. Антивирусные программы ***Практическая работа:*** Производить настройки антивирусной программы,	4	2		2	2	2

	проверять различные объекты на наличие вируса. ***Самостоятельная работа:*** Презентация: Характеристика антивирусных программ						
2.4.	Профилактика компьютерных вирусов. Обнаружение неизвестного вируса ***Практическая работа:*** Антивирусная защита (технология тестирования компьютера на наличие вируса и профилактические меры. Знакомство со способами лечения зараженных объектов.) Настроить, режимы работы и сравнение различных антивирусных пакетов. Установить антивирусное программное обеспечение. Выявить компьютерные вирусы ***Самостоятельная работа:*** Презентация: Профилактические меры против вирусов	8	4		4	2	2
	Итоги по разделу:	**20**	**10**	**4**	**6**	**8**	
Раздел 3. ИНФОРМАЦИОННАЯБЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ							
3.1	Особенности обеспечения информационной безопасности в компьютерных сетях ***Практическая работа:*** Поменять учетную запись администратора (Пользователь Администратор с пустым паролем - уязвимость) ***Самостоятельная работа:*** Презентация: Обеспечение безопасности локальной сети	4	2		2	2	2
3.2	Сетевые модели передачи данных. Адресация в глобальных сетях ***Практическая работа:*** Передача данных между двумя соединенными компьютерами. Непосредственная связь двух компьютеров ***Самостоятельная работа:*** Презентация: Повторитель. Концентратор.	4	2		2	2	2
3.3	Классификация удаленных угроз в вычислительных сетях	4	2		2	2	2
3.4	Типовые удаленные атаки и их характеристики. Причины успешной реализации удаленных угроз в вычислительных сетях ***Практическая работа:*** Типовая удаленная атака «отказ в обслуживании». Отсутствие контроля за виртуальными каналами связи между объектами сети; отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений; отсутствие в распределенных вычислительных сетях полной информации о ее объектах; отсутствие в распределенных вычислительных сетях криптозащиты сообщений. ***Самостоятельная работа:*** Презентация: Удаленные угрозы «по цели воздействия»	4	2		2	2	2
3.5	Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация ***Практическая работа:***						

	Защитить информацию в корпоративных сетях, обратить внимание на возможные перебои и нарушения в процессе доступа, способные уничтожить или исказить сведения. *проблемы, связанные с нарушением безопасности в компьютерных сетях, можно условно разделить на несколько типов:* 1. Нарушения работы системного оборудования: разрыв кабелей, перебои в электропитании, сбой в дисковой системе, нарушения функционирования серверов, сетевых карт, рабочих станций, системы архивации. 2. Уничтожение данных вследствие некорректной работы программного обеспечения: ошибки системы, заражение компьютерными вирусами. 3. Следствие несанкционированного доступа: пиратское копирование, устранение или фальсификация данных, работа посторонних с секретными материалами. 4. Неграмотное сохранение архивов. 5. Ошибки технического штата и пользователей сетевого ресурса: случайное искажение либо уничтожение информации, некорректное пользование программными продуктами. 6. Устранить нарушения и усилить систему безопасности компьютерной сети. ***Самостоятельная работа:*** Презентация: Архивирование и дублирование информации	8	4		4	2	2
	Итого по разделу:	**24**	**10**		**12**	**10**	
	Всего по предмету	**60**	**30**	**12**	**18**	**30**	

Для характеристики уровня освоения учебного материала используются следующие обозначения:

1. ***Ознакомительный*** (узнавание ранее изученных объектов, свойств);
2. ***Репродуктивный*** (выполнение деятельности по образцу, инструкции или под руководством);
3. ***Продуктивный*** (планирование и самостоятельное выполнение деятельности, решение проблемных задач)

Содержание

Раздел 1. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ И УРОВНИ ЕЕ ОБЕСПЕЧЕНИЯ

1.1 Понятие информационной безопасность.

Понятие информации. Виды и свойства информации. Структура информационного процесса. Понятие информационной безопасности. Информационные опасности и угрозы. Принципы обеспечения информационной безопасности.

1.2 Составляющие информационной безопасности

Информационная безопасность. Доступности. Целостность. Конфиденциальность.

Лекция №1 «понятие информации. Виды и свойства информации»

Цель: Определить роль и изучить основные понятия информатики.

Основные понятия информации

Введение в информационную безопасность.

Термины "безопасность информации" и "защита информации" отнюдь не являются синонимами. Термин "безопасность" включает в себя не только понятие защиты, но также и аутентификацию, аудит, обнаружение проникновения.

Рассмотрим основные понятия, относящиеся к информационной безопасности, и их взаимосвязь.

Собственник определяет множество **информационных ценностей**, которые должны быть защищены от различного рода атак. Атаки осуществляются противниками или оппонентами, использующими различные уязвимости в защищаемых ценностях. Основными нарушениями безопасности являются раскрытие информационных ценностей (потеря конфиденциальности), их неавторизованная модификация (потеря целостности) или неавторизованная потеря доступа к этим ценностям (потеря доступности).

Собственники информационных ценностей анализируют уязвимости защищаемых ресурсов и возможные атаки, которые могут иметь место в конкретном окружении. В результате такого анализа определяются риски для данного набора информационных ценностей. Этот анализ определяет выбор контрмер, который задается политикой безопасности и обеспечивается с помощью механизмов и сервисов безопасности. Следует учитывать, что отдельные уязвимости могут сохраниться и после применения механизмов и сервисов безопасности. Политика безопасности определяет согласованную совокупность механизмов и сервисов безопасности, адекватную защищаемым ценностям и окружению, в котором они используются.

На рис.1. показана взаимосвязь рассмотренных выше понятий информационной безопасности.

Дадим следующие определения:

Уязвимость - слабое место в системе, с использованием которого может быть осуществлена атака.

Риск - вероятность того, что конкретная атака будет осуществлена с использованием конкретной уязвимости. В конечном счете, каждая организация должна принять решение о допустимом для нее уровне риска. Это решение должно найти отражение в политике безопасности, принятой в организации.

Политика безопасности - правила, директивы и практические навыки, которые определяют то, как информационные ценности обрабатываются, защищаются и распространяются в организации и между информационными системами; набор критериев для предоставления сервисов безопасности.

Рис. 1. Взаимосвязь основных понятий безопасности информационных систем

Атака - любое действие, нарушающее безопасность информационной системы. Более формально можно сказать, что атака - это действие или последовательность связанных между собой действий, использующих уязвимости данной информационной системы и приводящих к нарушению политики безопасности.

Механизм безопасности - программное и/или аппаратное средство, которое определяет и/или предотвращает атаку.

Сервис безопасности - сервис, который обеспечивает задаваемую политикой безопасность систем и/или передаваемых данных, либо определяет осуществление атаки. Сервис использует один или более механизмов безопасности.

Сервисы безопасности

Основными сервисами безопасности являются следующие:

Конфиденциальность - предотвращение пассивных атак для передаваемых или хранимых данных.

Аутентификация - подтверждение того, что информация получена из законного источника, и получатель действительно является тем, за кого себя выдает. В случае передачи единственного сообщения аутентификация должна гарантировать, что получателем сообщения является тот, кто нужно, и сообщение получено из заявленного источника. В случае установления соединения имеют место два аспекта. Во-первых, при инициализации соединения сервис должен гарантировать, что оба участника являются требуемыми. Во-вторых, сервис должен гарантировать, что на соединение не воздействуют таким образом, что третья сторона сможет маскироваться под одну из легальных сторон уже после установления соединения.

Целостность - сервис, гарантирующий, что информация при хранении или передаче не изменилась. Может применяться к потоку сообщений, единственному сообщению или отдельным полям в сообщении, а также к хранимым файлам и отдельным записям файлов.

Невозможность отказа - невозможность, как для получателя, так и для отправителя, отказаться от факта передачи. Таким образом, когда сообщение отправлено, получатель может убедиться, что это сделал легальный отправитель. Аналогично, когда сообщение пришло, отправитель может убедиться, что оно получено легальным получателем.

Контроль доступа - возможность ограничить и контролировать доступ к системам и приложениям по коммуникационным линиям.

Доступность - результатом атак может быть потеря или снижение доступности того или иного сервиса. Данный сервис предназначен для того, чтобы минимизировать возможность осуществления DoS-атак.

Механизмы безопасности

Перечислим основные механизмы безопасности:

Алгоритмы симметричного шифрования - алгоритмы шифрования, в которых для шифрования и дешифрования используется один и тот же ключ или ключ дешифрования легко может быть получен из ключа шифрования.

Алгоритмы асимметричного шифрования - алгоритмы шифрования, в которых для шифрования и дешифрования используются два разных ключа, называемые открытым и закрытым ключами, причем, зная один из ключей, вычислить другой невозможно.

Хэш-функции - функции, входным значением которых является сообщение произвольной длины, а выходным значением - сообщение фиксированной длины. Хэш-функции обладают рядом свойств, которые позволяют с высокой долей вероятности определять изменение входного сообщения.

Основная литература: [1] с.3-7, [2] с.4-:5, [3] с.3-5.

Дополнительная литература: [8] с.13-28, [9] с.35-44.

Контрольные вопросы:

1. Дайте определение информационной безопасности.
2. Дайте определение защите информации.
3. Механизмы безопасности.
4. Собственник информации.
5. Сервисы безопасности.
6. Взаимосвязь основных понятий информационной безопасности.

Большинство ученых в наши дни отказываются от попыток дать строгое определение информации и считают, что информацию следует рассматривать как первичное, неопределимое понятие подобно множества в математике.

Некоторые авторы учебников предлагают следующие определения информации:
Информация – это знания или сведения о ком-либо или о чем-либо.
Информация – это сведения, которые можно собирать, хранить, передавать,обрабатывать, использовать.

Информатика – наука об информации или это наука о структуре и свойствах информации, способах сбора, обработкии передачи информации или информатика, изучает технологию сбора, хранения и переработкиинформации, а компьютер основной инструмент в этой технологии. Термин информация происходит от латинского слова informatio, что означаетсведения, разъяснения, изложение. В настоящее время наука

пытается найти общие свойства и закономерности, присущие многогранному понятию информация, но пока это понятие во многом остается интуитивным и получает различные смысловые наполнения в различных отраслях человеческой деятельности:

1. в быту информацией называют любые данные, сведения, знания, которые кого-либо интересуют. Например, сообщение о каких-либо событиях, о чьей-либо деятельности и т.п.;

2. в технике под информацией понимают сообщения, передаваемые в форме знаков или сигналов (в этом случае есть источник сообщений, получатель (приемник) сообщений, канал связи);

3. в кибернетике под информацией понимают ту часть знаний, которая используется для ориентирования, активного действия, управления, т.е.в целях сохранения, совершенствования, развития системы;

4. в теории информации под информацией понимают сведения об объектах и явлениях окружающей среды, их параметрах, свойствах и состоянии, которые уменьшают имеющуюся о них степень неопределенности, неполноты знаний.

Информация – это отражение внешнего мира с помощью знаков или сигналов. Информационная ценность сообщения заключается в новых сведениях, которые в нем содержатся (в уменьшении незнания).

Свойства информации

Свойства информации следующие:

1. **полнота** — свойство информации исчерпывающе (для данного потребителя) характеризовать отображаемый объект или процесс;

2. **актуальность** — способность информации соответствовать нуждам потребителя в нужный момент времени;

3. **достоверность** — свойство информации не иметь скрытых ошибок. Достоверная информация со временем может стать недостоверной, если устареет и перестанет отражать истинное положение дел;

4. **доступность** — свойство информации, характеризующее возможность ее получения данным потребителем;

5. **релевантность** — способность информации соответствовать нуждам (запросам) потребителя;

6. **защищенность** — свойство, характеризующее невозможность несанкционированного использования или изменения информации;

7. **эргономичность** — свойство, характеризующее удобство формы или объема информации с точки зрения данного потребителя.

Информацию следует считать особым видом ресурса, при этом имеется в виду толкование «ресурса» как запаса неких знаний материальных предметов или энергетических, структурных или каких-либо других характеристик предмета. В отличие от ресурсов, связанных с материальными предметами, информационные ресурсы являются неистощимыми и предполагают существенно иные методы воспроизведения и обновления, чем материальные ресурсы.

С этой точки зрения можно рассмотреть такие свойства информации:

1. **Запоминаемость** — одно из самых важных свойств. Запоминаемую информацию будем называть макроскопической (имея в виду пространственные масштабы запоминающей ячейки и время запоминания). Именно с макроскопической информацией мы имеем дело в реальной практике;

2. **Передаваемость** – способность информации к копированию, т.е. к тому, что она может быть “запомнена” другой макроскопической системой и при этом останется тождественной самой себе. Очевидно, что количество информации не должно возрастать при копировании;

3. **Воспроизводимость** – тесно связана с ее передаваемостью и не является ее независимым базовым свойством. Если передаваемость означает, что не следует считать существенными пространственные отношения между частями системы, между которыми передается информация, то воспроизводимость характеризует неиссякаемость и неистощимость информации, т.е. что при копировании информация остается тождественной самой себе;

4. **Преобразуемость** – фундаментальное свойство информации которое означает, что информация может менять способ и форму своего существования. Копируемость есть разновидность преобразования информации, при котором ее количество не меняется. В общем случае количество информации в процессах преобразования меняется, но возрастать не может.

5. **Стираемость информации** также не является независимым. Оно связано с таким преобразованием информации (передачей), при котором ее количество уменьшается и становится равным нулю.

Данных свойств информации недостаточно для формирования ее меры, так как они относятся к физическому уровню информационных процессов.

Примеры информации могут быть следующими:

1. в неживой природе (например, в геологии или археологии);
2. в биологических системах (например, из жизни животных и растений);
3. в технических устройствах (например, телевидение, телеграфные сообщения);
4. в жизни общества (например, исторические сведения, реклама, средства массовой информации, общение людей).

Информация всегда связана с материальным носителем.

Носителем информации может быть:

1. любой материальный предмет (бумага, камень и т.д.);
2. волны различной природы: акустическая (звук), электромагнитная (свет,радиоволна) и т.д.;
3. вещество в различном состоянии: концентрация молекул в жидком растворе, температура и т.д.
4. Машинные носители информации: CD, DWD, BR, HDD, Flash и т.д.

Сигнал – способ передачи информации. Это физический процесс, имеющий информационное значение. Он может быть непрерывным или дискретным. Сигнал называется дискретным, если он может принимать лишь конечное число значений в конечном числе моментов времени.

Аналоговый сигналы – это сигналы, непрерывно изменяющийся по амплитуде и вовремени. Аналоговые сигналы используют в телефонной связи, радиовещании, телевидении. Дискретные сигналы – это сигналы несущие текстовую, символическую информацию. Дискретный сигнал используется калькуляторами, периферийными устройствами, вычислительными машинами и цифровыми системами. 1.3. Кодирование и единица измерения информации Представление информации с помощью какого-либо языка называют кодированием. Код – набор символов для представления информации. Кодирование – процесс представления информации в виде кода. Знаменитый немецкий ученый Г.В. Лейбниц предложил еще в XVII веке уникальную и простую систему счисления. «Вычисление с помощью двоек…, сведение чисел к простейшим началам (0 и 1)».

Сегодня такой способ представления информации, с помощью языка, содержащего два символа 0 и 1, широко используется в технических устройствах.

Эти два символа 0 и 1 принято называть битами

Бит – наименьшая единица измерения информации и обозначается двоичным числом. Более крупной единицей изменения объема информации принято считать **1 байт**, который состоит из 8 бит. **В 1 байте** содержится **8 битов** (таблица 1).

Таблица 1. Байтовые соотношения информации

1. Килобит Кбит 1 Кбит = 1024 бит = 2 10 бит ≈ 1000 бит

2. Мегабит Мбит 1 Мбит = 1024 Кбит = 2 20 бит ≈ 1 000 000 бит
3. Гигабит Гбит 1 Гбит = 1024 Мбит = 2 30 бит ≈ 1 000 000 000 бит
4. Килобайт Кбайт (Кб) 1 Кбайт = 1024 байт = 2 10 байт ≈ 1000 байт
5. Мегабайт Мбайт (Мб) 1 Мбайт = 1024 Кбайт = 2 20 байт ≈ 1 000 000 байт
6. Гигабайт Гбайт (Гб) 1 Гбайт = 1024 Мбайт = 2 30 байт ≈ 1 000 000 000 байт

Говорить об информации вообще, а не применительно к какому-то ее конкретному виду беспредметно. Классифицировать информацию можно по способу ее восприятия:
1. **Визуальная** — воспринимаемая органами зрения.
2. **Аудиальная** — воспринимаемая органами слуха.
3. **Тактильная** — воспринимаемая тактильными рецепторами.
4. **Обонятельная** — воспринимаемая обонятельными рецепторами.
5. **Вкусовая** — воспринимаемая вкусовыми рецепторами.

По форме представления информация бывает:
1. **Текстовая** — передаваемая в виде символов, предназначенных обозначать лексемы языка;
2. **Числовая** — в виде цифр и знаков, обозначающих математические действия;
3. **Графическая** — в виде изображений, предметов, графиков;
4. **Звуковая** — устная или в виде записи и передачи лексем языка аудиальным путём

По назначению информация бывает:
1. Массовая — содержит тривиальные сведения и оперирует набором понятий, понятным большей части социума;
2. Специальная — содержит специфический набор понятий, при использовании происходит передача сведений, которые могут быть не понятны основной массе социума, но необходимы и понятны в рамках узкой социальной группы, где используется данная информация;
3. Секретная — передаваемая узкому кругу лиц и по закрытым (защищённым) каналам;
4. Личная (приватная) — набор сведений о какой-либо личности, определяющий социальное положение и типы социальных взаимодействий внутри популяции.

Примеры получения информации:
1. динамик компьютера издает специфический звук, хорошо знакомый Васе;
2. пришло новое сообщение по ICQ;
3. с вертолета пожарной охраны в глубине леса замечен густой дым — обнаружен новый лесной пожар;
4. всевозможные датчики, расположенные в сейсмологически неустойчивом районе, фиксируют изменение обстановки, характерное для приближающегося землетрясения.

Основные понятия информатики

Информатика – область человеческой деятельности, связанная с процессами преобразования информации с помощью компьютеров и других средств вычислительной техники.

1. **Информационные ресурсы** — различные формализованные знания (теории, идеи, изобретения), данные (в том числе документы), технологии и средства их сбора, обработки, анализа, интерпретации и применения, а также обмена между источниками и потребителями информации.

2. **Информационный процесс** — последовательность действий (операций) по сбору, передаче, обработке, анализу, выделению и использованию с различной целью информации (и/или её носителей) в ходе функционирования и взаимодействия материальных объектов.

3. **Информационная технология** - совокупность научных дисциплин, занимающихся изучением, созданием и применением методов, способов, используемых для получения новой информации, сбора, обработки, анализа и т.д.

4. **Информационный технологический процесс** — компонент информационной технологии как практического инструмента рецептурной деятельности, часть производственного процесса, состоящая из последовательности согласованных технологических операций, связанных со сбором и обработкой данных как носителей информации, выделением из них необходимых сведений, новостей, знаний, их накоплением, анализом, интерпретацией и применением.

Структура информационного процесса

При переносе информации в виде сигнала от источника к потребителю она проходит последовательно следующие фазы (говорят - фазы обращения), составляющие информационный процесс:

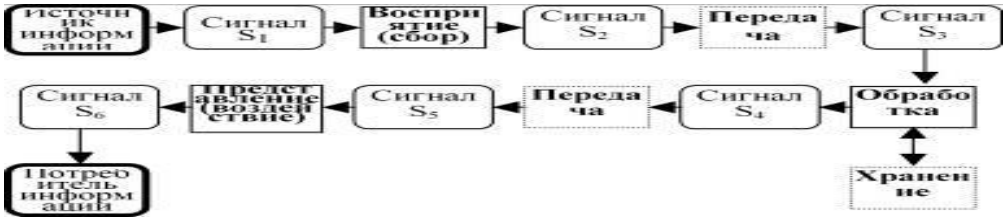
Восприятие (если фаза реализуется технической системой) или **сбор** (если фаза реализуется человеком) - осуществляет отображение источника информации в сигнал. Здесь определяются качественные и количественные характеристики источника, существенные для решения задач потребителя информации, для чего и собирается или воспринимается информация. Совокупность этих характеристик создает образ источника, который фиксируется в виде сигнала на носителе той или иной природы (бумажном, электронном и т.п.).

Передача - перенос информации в виде сигнала в пространстве посредством физических сред любой природы. Включается в информационный процесс, если места выполнения других фаз информационного процесса территориально разобщены.

Обработка - любое преобразование информации с целью решения определенных функциональных задач (они определяются потребителем информации). Данная фаза может включать **хранение** информации как перенос ее во времени.

Представление (если потребителем информации является человек) или воздействие (если потребителем является техническая система). В первом случае выполняется подготовка информации к виду, удобному для потребителя (графики, тексты, диаграммы, таблицы и т.д.). Во втором случае вырабатываются управляющие воздействия на технические средства. Этот случай характерен для выпускников специальности "Автоматизация управления технологическими процессами", а потому здесь не рассматривается

Схематично информационный процесс изображен на рисунке:



Прямоугольниками изображены процедуры (фазы), другие фигуры обозначают объекты. Пунктирные прямоугольники показывают, что эти фазы могут отсутствовать.

Как видно из рисунка, каждая фаза в общем случае преобразует (или отображает) входной сигнал в выходной. Например, при обработке сигнал S_3 преобразуется в сигнал S_4. Это делается для удобства проведения следующей процедуры или, в последнем случае, для удобства потребителя.

Пример 1. Рассмотрим информационный процесс, имеющий место при приеме в ВУЗ абитуриентов, к числу которых в недавнем времени относился и наш читатель (при этом отметим, что подобный информационный процесс, когда решается некоторая задача преобразования информации из конкретной предметной области, называется предметным). Названные на рисунке элементы представлены ниже:

источник информации - абитуриент, сведения о знаниях и других достоинствах которого являются основанием для зачисления в ВУЗ. **Сигнал S_1** - это документы (например, аттестат о среднем образовании), которые сдаются в приемную комиссию;

сбор информации выполняется работниками приемной комиссии, куда стекаются сведения о прошлых успехах абитуриента и результатах вступительных испытаний.

Очевидны качественные и количественные характеристики источника-абитуриента: это баллы в аттестате, различные квалификации, которые он приобрел в результате обучения на дополнительных курсах и факультативах, медицинские справки и т.д. При этом собираемые данные регистрируются, например, записываются в сводные ведомости, где по каждому студенту фиксируются данные о нем. Формируется **сигнал S_2** (в этом случае он носит бумажный характер). Возможно также использование технических систем для регистрации собранных данных. Если приемная комиссия снабжена компьютерной техникой, **сигнал S_2** носит электронный характер. В любом случае, как правило, применяется фиксация информации на бумажном носителе;

передача информации. В простейшем случае это передача данных курьером (работником приемной комиссии) тому лицу, который занимается их обработкой. При этом, очевидно, никаких изменений с данными не происходит (если только курьер их не потеряет), т.е. **сигналы S_2** и **S_3** равны. Если возможно использование технических систем для передачи информации, этот процесс механизирован или автоматизирован (в случае применения ЭВМ). При автоматизации передачи возможно несовпадение **сигналов S_2** и **S_3** по их синтаксическим характеристикам, что связано с особенностями этой процедуры и подробнее рассматривается далее;

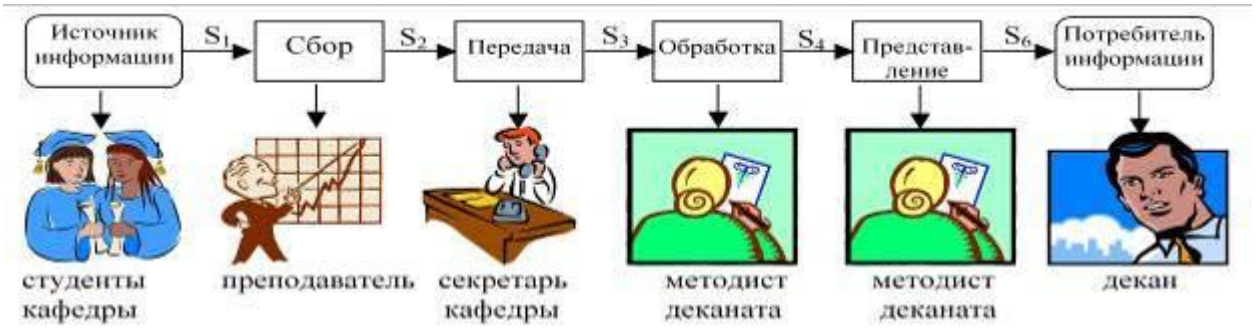
обработка сводится к упорядочению списка абитуриентов в зависимости от качественных и количественных параметров (они назывались выше). Тогда самые достойные на зачисление оказываются в начале списка и первыми включаются затем в приказ. Эту работу выполняют в приемной комиссии (такая задача в несколько упрощенном виде использована ранее). Тогда **сигнал S_4** - это упорядоченный список абитуриентов, разбитый на группы по специальностям. Очевидно, эта фаза может выполняться вручную, но именно для подобных задач используются средства вычислительной техники, и в первую очередь - компьютеры;

передача упорядоченного списка абитуриентов в деканат, занимающийся формированием учебных групп по каждой специальности, аналогично первой процедуре передачи может выполняться как человеком, так и техническими системами. Как отмечалось выше, в первом случае **сигналы S_4** и **S_5** могут совпадать, во втором - могут различаться;

представление списков абитуриентов, разбитых на группы, выполняется деканатами. **Сигнал S_6** имеет вид таблиц, включающих фамилии и инициалы абитуриентов. Каждая из таблиц соотнесена с той или иной учебной группой;

потребитель информации - ректор ВУЗа, который готовит и визирует приказ о зачислении в ВУЗ.

Пример 2. Сформируем схему обращения информации при сдаче студентами сессии:



Сигнал S_1 - это ответы студентов на экзаменах, которые анализируются преподавателем и оцениваются, как правило, по пятибалльной системе (фаза **Сбор**). В результате формируется ведомость сдачи экзамена (сигнал S_2), которая секретарем кафедры (или самим преподавателем) передается в деканат того факультета, к которому "приписаны" студенты (фаза **Передача**). Очевидно, если по дороге не случается фальсификации, сигналы S_2 и S_3 совпадают. В деканате ведомость попадает методисту, который выполняет ее обработку - заполняет специальный журнал успеваемости, где собираются данные об успеваемости каждого студента за все время обучения в Вузе (фаза **Обработка**). Можно сказать, что сам журнал (сигнал S_4)выполняет функцию хранения информации (на рисунке эта фаза не показана). По окончании срока сессии методист готовит для декана справку о результатах сессии по всем учебным группам студентов: списки неуспевающих, списки студентов, претендующих на стипендию, списки тех, кто может получать повышенную (именную) стипендию и т.д. (фаза **Представление**). Эта справка и есть сигнал S_6, который поступает декану для решения типичных для деканата задач: отчисление студентов, перевод на следующий курс или на другую специальность (другое учебное заведение), восстановление и т.п. Следует отметить, что некоторые фазы, в свою очередь, могут рассматриваться как совокупность последовательных операций, среди которых можно выделить операции, аналогичные рассмотренным фазам. Например, в фазе **Обработка,** как будет показано далее, имеет место сбор информации. Это говорит о том, что детализация информационных процессов определяется уровнем их рассмотрения с целью последующей автоматизации, т.е. решения соответствующих задач с помощью компьютера.

Понятие «информационная безопасность»?

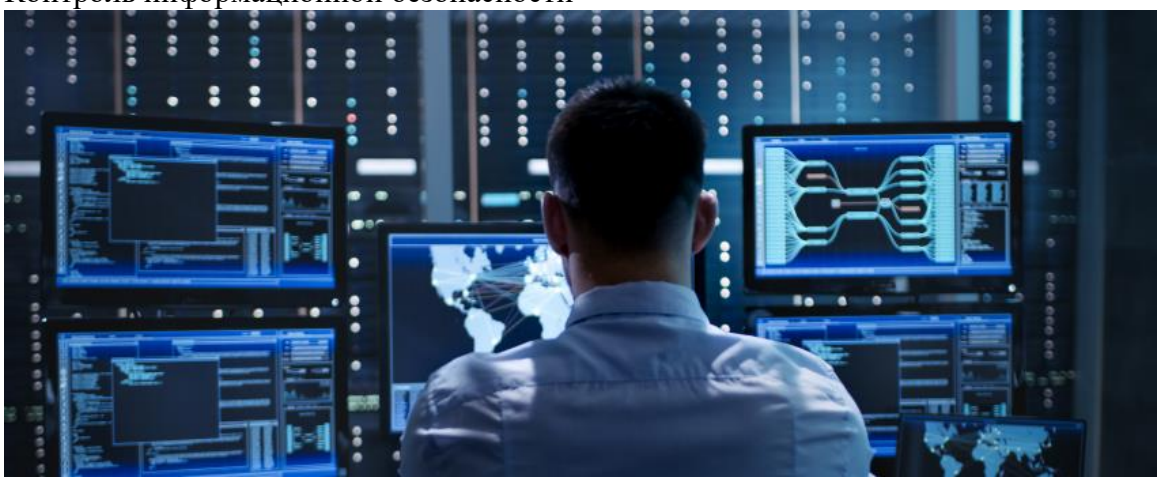
Информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Другими словами, это набор технологий, стандартов и методов управления, которые необходимы для защиты информационной безопасности.

Цель обеспечения информационной безопасности – защитить информационные данные и поддерживающую инфраструктуру от случайного или преднамеренного вмешательства, что может стать причиной потери данных или их несанкционированного изменения. Информационная безопасность помогает обеспечить непрерывность бизнеса.

Для успешного внедрения систем информационной безопасности на предприятии необходимо придерживаться трех главных принципов:

1. **Конфиденциальность.** Это значит ввести в действие контроль, чтобы гарантировать достаточный уровень безопасности с данными предприятия, активами и информацией на разных этапах деловых операций для предотвращения нежелательного или несанкционированного раскрытия. Конфиденциальность должна поддерживаться при сохранении информации, а также при транзите через рядовые организации независимо от ее формата.
2. **Целостность.** Целостность имеет дело с элементами управления, которые связаны с обеспечением того, чтобы корпоративная информация была внутренне и внешне последовательной. Целостность также гарантирует предотвращение искажения информации.
3. **Доступность.** Доступность обеспечивает надежный и эффективный доступ к информации уполномоченных лиц. Сетевая среда должна вести себя предсказуемым образом с целью получить доступ к информации и данным, когда это необходимо. Восстановление системы по причине сбоя является важным фактором, когда речь идет о доступности информации, и такое восстановление также должно быть обеспечено таким образом, чтобы это не влияло на работу отрицательно.

Контроль информационной безопасности



Нужно понимать, что лишь системный и комплексный подход к защите может обеспечить информационную безопасность. В системе информационной безопасности нужно учитывать все актуальные и вероятные угрозы и уязвимости. Для этого необходим непрерывный контроль в реальном времени. Контроль должен производиться 24/7 и охватывать весь жизненный цикл информации – от момента, когда она поступает в организацию, и до ее уничтожения или потери актуальности.

Выбор и внедрение подходящих видов контроля безопасности поможет организации снизить риск до приемлемых уровней. Выделяют следующие виды контроля:

- **Административный.** Административный вид контроля состоит из утвержденных процедур, стандартов и принципов. Он формирует рамки для ведения бизнеса и управления людьми. Законы и нормативные акты, созданные государственными органами, также являются одним из видов административного контроля. Другие примеры административного контроля включают политику корпоративной безопасности, паролей, найма и дисциплинарные меры.
- **Логический.** Логические средства управления (еще называемые техническими средствами контроля) базируются на защите доступа к информационным системам,

программном обеспечении, паролях, брандмауэрах, информации для мониторинга и контроле доступа к системам информации.

- **Физический.** Это контроль среды рабочего места и вычислительных средств (отопление и кондиционирование воздуха, дымовые и пожарные сигнализации, противопожарные системы, камеры, баррикады, ограждения, замки, двери и др.).

Угрозы информационной безопасности

Угрозы информационной безопасности можно разделить на следующие:

- **Естественные** (катаклизмы, независящие от человека: пожары, ураганы, наводнение, удары молнии и т.д.).
- **Искусственные,** которые также делятся на:
  - непреднамеренные (совершаются людьми по неосторожности или незнанию);
  - преднамеренные (хакерские атаки, противоправные действия конкурентов, месть сотрудников и пр.).
- **Внутренние** (источники угрозы, которые находятся внутри системы).
- **Внешние** (источники угроз за пределами системы)

Так как угрозы могут по-разному воздействовать на информационную систему, их делят на пассивные (те, которые не изменяют структуру и содержание информации) и активные (те, которые меняют структуру и содержание системы, например, применение специальных программ).

Наиболее опасны преднамеренные угрозы, которые все чаще пополняются новыми разновидностями, что связано, в первую очередь, с компьютеризацией экономики и распространением электронных транзакций. Злоумышленники не стоят на месте, а ищут новые пути получить конфиденциальные данные и нанести потери компании.

Чтобы обезопасить компанию от потери денежных средств и интеллектуальной собственности, необходимо уделять больше внимания информационной безопасности. Это возможно благодаря средствам защиты информации в лице передовых технологий.

Средства защиты информационной безопасности

Средства защиты информационной безопасности — это набор технических приспособлений, устройств, приборов различного характера, которые препятствуют утечке информации и выполняют функцию ее защиты.

Средства защиты информации делятся на:

- **Организационные.** Это совокупность организационно-технических (обеспечение компьютерными помещениями, настройка кабельной системы и др.) и

организационно-правовых (законодательная база, статут конкретной организации) средств.

- **Программные.** Те программы, которые помогают контролировать, хранить и защищать информацию и доступ к ней.
- **Технические (аппаратные).** Это технические виды устройств, которые защищают информацию от проникновения и утечки.
- **Смешанные аппаратно-программные.** Выполняют функции как аппаратных, так и программных средств.

В связи со стремительным развитием ИТ, все более частыми кибератаками, компьютерными вирусами и другими появляющимися угрозами наиболее распространенными и востребованными на сегодняшний день являются программные средства защиты информации.

Виды средств защиты информации :

- 

Антивирусные программы — программы, которые борются с компьютерными вирусами и возобновляют зараженные файлы.

- 

Облачный антивирус (CloudAV) – одно из облачных решений информационной безопасности, что применяет легкое программное обеспечение агента на защищенном компьютере, выгружая большую часть анализа информации в инфраструктуру провайдера. CloudAV – это также решение для эффективного сканирования вирусов на приспособлениях с невысокой вычислительной мощностью для выполнения самих сканирований. Некоторые образцы облачных антивирусных программ – это Panda Cloud Antivirus, Crowdstrike, Cb Defense и Immunet.

- 

DLP (Data Leak Prevention) решения – это защита от утечки информации. Предотвращение утечки данных (DLP) представляет собой набор технологий, направленных на предотвращение потери конфиденциальной информации, которая происходит на предприятиях по всему миру. Успешная реализация этой технологии

требует значительной подготовки и тщательного технического обслуживания. Предприятия, желающие интегрировать и внедрять DLP, должны быть готовы к значительным усилиям, которые, если они будут выполнены правильно, могут значительно снизить риск для организации.

- **Криптографические системы** – преобразование информации таким образом, что ее расшифровка становится возможной только с помощью определенных кодов или шифров (DES – Data Encryption Standard, AES – Advanced Encryption Standard). Криптография обеспечивает защиту информации и другими полезными приложениями, включая улучшенные методы проверки подлинности, дайджесты сообщений, цифровые подписи и зашифрованные сетевые коммуникации. Старые, менее безопасные приложения, например Telnet и протокол передачи файлов (FTP), медленно заменяются более безопасными приложениями, такими как Secure Shell (SSH), которые используют зашифрованные сетевые коммуникации. Беспроводная связь может быть зашифрована с использованием таких протоколов, как WPA/WPA2 или более старый (и менее безопасный) WEP. Проводные коммуникации (такие как ITU-T G.hn) защищены с использованием AES для шифрования и X.1035 для аутентификации и обмена ключами. Программные приложения, такие как GnuPG или PGP, могут применяться для шифрования информационных файлов и электронной почты.

- **Межсетевые экраны (брандмауэры или файрволы)** – устройства контроля доступа в сеть, предназначенные для блокировки и фильтрации сетевого трафика. Брандмауэры обычно классифицируются как сетевые или хост-серверы. Сетевые брандмауэры на базе сети расположены на шлюзовых компьютерах LAN, WAN и интрасетях. Это либо программные устройства, работающие на аппаратных средствах общего назначения, либо аппаратные компьютерные устройства брандмауэра. Брандмауэры предлагают и другие функции для внутренней сети, которую они защищают, например, являются сервером DHCP или VPN для этой сети. Одним из лучших решений как для малых, так и для больших предприятий являются межсетевые экраны CheckPoint.

- **VPN (Virtual Private Network).** Виртуальная частная сеть (VPN) дает возможность определить и использовать для передачи и получения информации частную сеть в рамках общедоступной сети. Таким образом, приложения, работающие по VPN, являются надежно защищенными. VPN дает возможность подключиться к внутренней сети на расстоянии. С помощью VPN можно создать общую сеть для территориально отдаленных друг от друга предприятий. Что касается отдельных пользователей сети – они также имеют свои преимущества использования VPN, так как могут защищать собственные действия с помощью VPN, а также избегать территориальные ограничения и использовать прокси-серверы, чтобы скрыть свое местоположение.

- **Proxy-server (Прокси-сервер)** – это определенный компьютер или компьютерная программа, которая является связывающим звеном между двумя устройствам, например, такими как компьютер и другой сервер. Прокси-сервер можно установить на одном компьютере вместе с сервером брандмауэра, или же на другом сервере. Плюсы прокси-сервера в том, что его кэш может служить для всех пользователей. Интернет-сайты, которые являются наиболее часто запрашиваемыми, чаще всего находятся в кэше прокси, что несомненно удобно для пользователя. Фиксирование своих взаимодействий прокси-сервером служит полезной функцией для исправления неполадок.

- **Системы мониторинга и управления информационной безопасностью, SIEM.** Чтобы выявлять и реагировать на возникающие угрозы информационной безопасности, используется решение SIEM, которое выполняет сбор и анализ событий из разных источников, таких как межсетевые экраны, антивирусы, IPS, оперативные системы и т.п. Благодаря системе SIEM у компаний появляется возможность централизованно хранить журналы событий и коррелировать их, определяя отклонения, потенциальные угрозы, сбои в работе ИТ-инфраструктуры, кибератаки и т.д.
Отдельное внимание стоит уделять управлению мобильными устройствами на предприятии, так как многие сотрудники часто используют личные смартфоны, планшеты и ноутбуки в корпоративных целях. Внедрение специальных решений, таких как VMware AirWatch, IBM MaaS360, Blackberry Enterprise Mobility Suite, VMware Workspace

One помогут лучше контролировать мобильные устройства сотрудников и защитить данные компании.

Заключение

Информация очень важна для успешного развития бизнеса, следовательно, нуждается в соответствующей защите. Особенно актуально это стало в бизнес-среде, где на передний план вышли информационные технологии. Так как мы живем в эпоху цифровой экономики, без них рост компании просто невозможен.

Информация сейчас подвергается все большему числу угроз и уязвимостей. Хакерские атаки, перехват данных по сети, воздействие вирусного ПО и прочие угрозы приобретают более изощренный характер и набирают огромный темп. Отсюда возникает необходимость внедрять системы информационной безопасности, которые могли бы защитить данные компании.

На выбор подходящих средств защиты информации влияют многие факторы, включая сферу деятельности компании, ее размер, техническую сторону, а также знания сотрудников в области информационной безопасности.

Если у вас есть вопросы по поводу решений информационной безопасности, которые лучше всего подошли бы для вашего предприятия, а также как их внедрять, обращайтесь к специалистам компании «Пирит».

Угрозы информационной безопасности

Угрозы информационной (компьютерной) безопасности — это различные действия, которые могут привести к нарушениям состояния защиты информации. Другими словами, это — потенциально возможные события, процессы или действия, которые могут нанести ущерб информационным и компьютерным системам.

Угрозы ИБ можно разделить на два типа: естественные и искусственные. К естественным относятся природные явления, которые не зависят от человека, например ураганы, наводнения, пожары и т.д. Искусственные угрозы зависят непосредственно от человека и могут быть преднамеренными и непреднамеренными. Непреднамеренные угрозы возникают из-за неосторожности, невнимательности и незнания. Примером таких угроз может быть установка программ, не входящих в число необходимых для работы и в дальнейшем нарушающих работу системы, что и приводит к потере информации. Преднамеренные угрозы, в отличие от предыдущих, создаются специально. К ним можно отнести атаки злоумышленников как извне, так и изнутри компании. Результат реализации этого вида угроз — потери денежных средств и интеллектуальной собственности организации.

Классификация угроз информационной безопасности

В зависимости от различных способов классификации все возможные угрозы информационной безопасности можно разделить на следующие основные подгруппы.

- Нежелательный контент.
- Несанкционированный доступ.
- Утечки информации.
- Потеря данных.
- Мошенничество.
- Кибервойны.
- Кибертерроризм.

Нежелательный контент — это не только вредоносный код, потенциально опасные программы и спам (т.е. то, что непосредственно создано для уничтожения или кражи информации), но и сайты, запрещенные законодательством, а также нежелательные ресурсы с информацией, не соответствующей возрасту потребителя. Источник: международное исследование EY в области информационной безопасности «Путь к киберустойчивости: прогноз, сопротивление, ответная реакция».

Несанкционированный доступ — просмотр информации сотрудником, который не имеет разрешения пользоваться ею, путем превышения должностных полномочий. Несанкционированный доступ приводит к утечке информации. В зависимости от того, каковы данные и где они хранятся, утечки могут организовываться разными способами, а именно через атаки на сайты, взлом программ, перехват данных по сети, использование несанкционированных программ.

Утечки информации можно разделять на **умышленные и случайные**. Случайные утечки происходят из-за ошибок оборудования, программного обеспечения и персонала. Умышленные, в свою очередь, организовываются преднамеренно с целью получить доступ к данным, нанести ущерб.

Потерю данных можно считать одной из основных угроз информационной безопасности. Нарушение целостности информации может быть вызвано неисправностью оборудования или умышленными действиями людей, будь то сотрудники или злоумышленники.

Не менее опасной угрозой является мошенничество с использованием информационных технологий («фрод»). К мошенничеству можно отнести не только манипуляции с кредитными картами («кардинг») и взлом онлайн-банка, но и внутренний фрод. Целями этих экономических преступлений являются обход законодательства, политики безопасности или нормативных актов, присвоение имущества.

Ежегодно по всему миру возрастает террористическая угроза, постепенно перемещаясь при этом в виртуальное пространство. На сегодняшний день никого не удивляет возможность атак на автоматизированные системы управления технологическими процессами (АСУ ТП) различных предприятий. Но подобные атаки не проводятся без предварительной разведки, для чего применяется кибершпионаж, помогающий собрать необходимые данные. Существует также такое понятие, как «информационная война»; она отличается от обычной войны тем, что в качестве оружия выступает тщательно подготовленная информация.

Источник угроз информационной безопасности

Нарушение режима информационной безопасности может быть вызвано как спланированными операциями злоумышленников, так и неопытностью сотрудников. Пользователь должен иметь хоть какое-то понятие об ИБ, вредоносном программном обеспечении, чтобы своими действиями не нанести ущерб компании и самому себе. Такие инциденты, как потеря или утечка информации, могут также быть обусловлены целенаправленными действиями сотрудников компании, которые заинтересованы в получении прибыли в обмен на ценные данные организации, в которой работают или работали.

Основными источниками угроз являются отдельные злоумышленники («хакеры»), киберпреступные группы и государственные спецслужбы (киберподразделения), которые применяют весь арсенал доступных киберсредств, перечисленных и описанных выше. Чтобы пробиться через защиту и получить доступ к нужной информации, они используют слабые места и ошибки в работе программного обеспечения и веб-приложений, изъяны в

конфигурациях сетевых экранов и настройках прав доступа, прибегают к прослушиванию каналов связи и использованию клавиатурных шпионов.

То, чем будет производиться атака, зависит от типа информации, ее расположения, способов доступа к ней и уровня защиты. Если атака будет рассчитана на неопытность жертвы, то возможно, например, использование спам-рассылок.

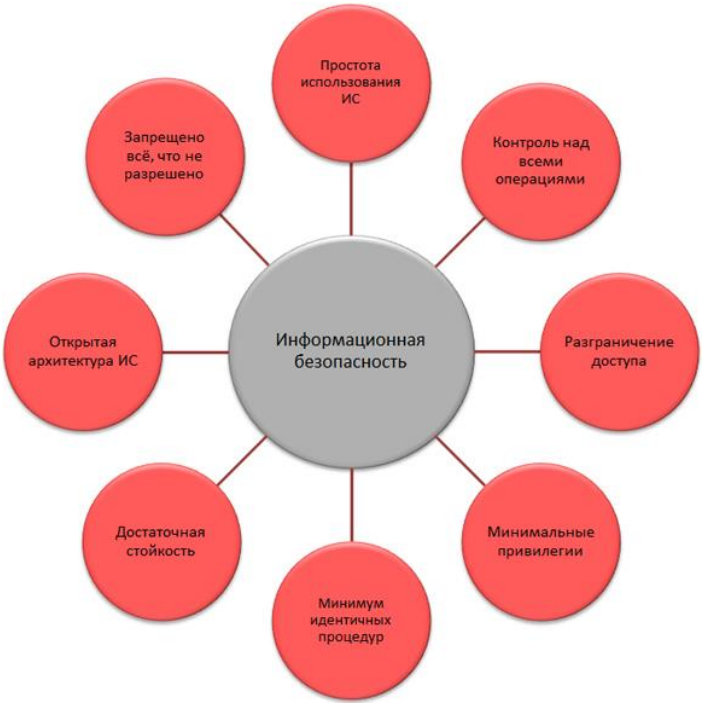
Оценивать угрозы информационной безопасности необходимо комплексно, при этом методы оценки будут различаться в каждом конкретном случае. Так, чтобы исключить потерю данных из-за неисправности оборудования, нужно использовать качественные комплектующие, проводить регулярное техническое обслуживание, устанавливать стабилизаторы напряжения. Далее следует устанавливать и регулярно обновлять программное обеспечение (ПО). Отдельное внимание нужно уделить защитному ПО, базы которого должны обновляться ежедневно. Обучение сотрудников компании основным понятиям информационной безопасности и принципам работы различных вредоносных программ поможет избежать случайных утечек данных, исключить случайную установку потенциально опасного программного обеспечения на компьютер. Также в качестве меры предосторожности от потери информации следует делать резервные копии. Для того чтобы следить за деятельностью сотрудников на рабочих местах и иметь возможность обнаружить злоумышленника, следует использовать DLP-системы.

Организовать информационную безопасность помогут специализированные программы, разработанные на основе современных технологий:

- защита от нежелательного контента (антивирус, антиспам, веб-фильтры, анти-шпионы); сетевые экраны и системы обнаружения вторжений (IPS);
- управление учетными данными (IDM);
- контроль привилегированных пользователей (PUM);
- защита от DDoS;
- защита веб-приложений (WAF);
- анализ исходного кода;
- антифрод;
- защита от таргетированных атак; управление событиями безопасности (SIEM);
- системы обнаружения аномального поведения пользователей (UEBA);
- защита АСУ ТП;
- защита от утечек данных (DLP);
- шифрование;
- защита мобильных устройств;
- резервное копирование;
- системы отказоустойчивости.

Принципы информационной безопасности

Полноценная информационная безопасность базируется на нескольких основополагающих принципах:



Основные принципы информационной безопасности

Рассмотрим принципы ИБ подробно:

1. **Простота использования информационной системы**. Данный принцип информационной безопасности заключается в том, что для минимизации ошибок следует обеспечить простоту использования информационной системы. Во время эксплуатации ИС пользователи и администраторы совершают непреднамеренные ошибки, некоторые из которых могут вести к невыполнению требований политик безопасности и снижению уровня информационной безопасности. Чем более сложны, запутанны и непонятны для пользователей и администраторов совершаемые ими операции, тем больше они делают ошибок. Простота использования ИС является необходимым условием для снижения числа ошибочных действий. При этом следует помнить, что данный принцип информационной безопасности не означает простоту архитектуры и снижение функциональности ИС.

2. **Контроль над всеми операциями**. Этот принцип подразумевает непрерывный контроль состояния информационной безопасности и всех событий, влияющих на ИБ. Необходим контроль доступа к любому объекту ИС с возможностью блокирования нежелательных действий и быстрого восстановления нормальных параметров информационной системы.

3. **Запрещено всё, что не разрешено**. Этот принцип ИБ заключается в том, что доступ к какому-либо объекту ИС должен предоставляться только при наличии соответствующего правила, отраженного, например, в регламенте бизнес-процесса или настройках защитного программного обеспечения. При этом основной функцией системы ИБ является разрешение, а не запрещение каких-либо действий. Данный принцип позволяет допускать только известные безопасные

действия, а не заниматься распознаванием любой угрозы, что очень ресурсоёмко, невозможно в полной мере и не обеспечивает достаточный уровень ИБ.

4. **Открытая архитектура ИС**. Этот принцип информационной безопасности состоит в том, что безопасность не должна обеспечиваться через неясность. Попытки защитить информационную систему от компьютерных угроз путем усложнения, запутывания и скрытия слабых мест ИС, оказываются в конечном итоге несостоятельными и только отсрочивают успешную хакерскую, вирусную или инсайдерскую атаку.

5. **Разграничение доступа**. Данный принцип ИБ заключается в том, что каждому пользователю предоставляется доступ к информации и её носителям в соответствии с его полномочиями. При этом исключена возможность превышения полномочий. Каждой роли/должности/группе пользователей можно назначить свои права на выполнение действий (чтение/изменение/удаление) над определёнными объектами ИС.

6. **Минимальные привилегии**. Принцип минимальных привилегий состоит в выделении пользователю наименьших прав и доступа к минимуму необходимых функциональных возможностей программ. Такие ограничения, тем не менее, не должны мешать выполнению работы.

7. **Достаточная стойкость**. Этот принцип информационной безопасности выражается в том, что потенциальные злоумышленники должны встречать препятствия в виде достаточно сложных вычислительных задач. Например, необходимо, чтобы взлом паролей доступа требовал от хакеров неадекватно больших промежутков времени и/или вычислительных мощностей.

8. **Минимум идентичных процедур**. Этот принцип информационной безопасности состоит в том, что в системе ИБ не должно быть общих для нескольких пользователей процедур, таких как ввод одного и того же пароля. В этом случае масштаб возможной хакерской атаки будет меньше.

Информационные угрозы. Классификация методов защиты информации.

Потенциальные угрозы безопасности информации

При анализе общей проблемы безопасности информации выделяются те направления, в которых преднамеренная или непреднамеренная деятельность человека, а также неисправности технических средств, ошибки программного обеспечения или стихийные бедствия могут привести к разглашению, утечке, несанкционированному доступу, модификации или уничтожению информации.

По-видимому, целесообразно в общем плане различать угрозы безопасности собственно вычислительной системы (информационно-вычислительной или телекоммуникационной сети) и угрозы безопасности находящейся, циркулирующей и обрабатываемой в ней информации.

Под **угрозой безопасности** вычислительной системы понимаются воздействия на систему, которые прямо или косвенно могут нанести ущерб ее безопасности. Разработчики требований безопасности и средств защиты выделяют три вида угроз:

- угрозы нарушения конфиденциальности обрабатываемой информации;
- угрозы нарушения целостности обрабатываемой информации;

- угрозы нарушения работоспособности системы (отказа в обслуживании).

Угрозы конфиденциальности направлены на разглашение секретной или конфиденциальной информации, т.е. информация становится известной лицу, которое не должно иметь к ней доступ. Иногда для обозначения этого явления используется термин **“несанкционированный доступ” (НСД)**, особенно популярный в отечественных литературных источниках, под которым понимается доступ к информации, нарушающий установленные правила разграничения доступа, с использованием штатных средств, предоставляемых средств вычислительной техники (СВТ) или автоматизированных систем (АС). При этом, под штатными средствами понимается совокупность программного, микропрограммного и технического обеспечения СВТ или АС.

Традиционно противостоянию угрозам этого типа уделяется максимальное внимание, и фактически подавляющее большинство исследований и разработок было сосредоточено в этой области, так как она непосредственно относится к защите государственной тайны.

Угрозы целостности представляют собой любое искажение или изменение неуполномоченным на это действие лицом хранящейся в вычислительной системе или передаваемой информации. Целостность информации может быть нарушена как злоумышленником, так и в результате объективных (неумышленных) воздействий со стороны среды эксплуатации системы. Наиболее актуальна эта угроза для систем передачи информации - компьютерных сетей и систем телекоммуникаций.

Угрозы нарушения работоспособности (отказ в обслуживании) направлены на создание ситуаций, когда в результате преднамеренных или непреднамеренных действий снижается работоспособность вычислительной системы, либо ее ресурсы становятся недоступными.

Цель защиты систем обработки информации заключается в противодействии угрозам безопасности. Поэтому систему можно считать безопасной или защищенной, когда она способна успешно и эффективно противостоять угрозам безопасности.

С точки зрения безопасности информации в настоящее время четко обозначились *три аспекта ее уязвимости*:

- опасность несанкционированного (случайного или злоумышленного) получения и использования информации лицом, которому она не предназначалась;
- возможность несанкционированной (случайной или злоумышленной) модификации;
- подверженность физическому уничтожению или искажению.

Появилась новая отрасль компьютерной преступности - *разработка и внедрение компьютерных вирусов*, число типов и видов которых, по оценке отечественных и зарубежных экспертов, приближается к нескольким тысячам. Имеются сведения о том, что рядом государственных и военных научных центров зарубежных государств разрабатываются так называемые “боевые вирусы”, предназначенные для поражения систем управления оружием, войсками и систем связи.

Наиболее широкое распространение получили случаи несанкционированного злоумышленного получения (хищения) информации с использованием различных каналов ее утечки.

Все возможные каналы утечки информации в вычислительных системах и сетях можно классифицировать исходя из типа средства, являющегося основным при получении информации по этим каналам. Различают три типа таких средств: человек, аппаратура, программа. Соответственно, возможные каналы утечки также разбиваются на три группы.

Группу возможных каналов утечки информации, в которых основным средством является человек, составляют:

- хищения носителей информации (магнитных и оптических дисков, магнитных лент, дискет, карт и т.п.);
- чтение информации с экрана посторонними лицами (во время отображения информации на экране законным пользователем или при отсутствии законного пользователя на рабочем месте);
- чтение информации из оставленных без присмотра распечаток и других твердых копий.

В группе возможных каналов утечки информации, в которых основным средством является аппаратура, можно выделить:

- подключения специальных технических средств к устройствам ЭВМ или средствам передачи информации;
- использование специальных технических средств для перехвата электромагнитных излучений.

К группе возможных каналов утечки информации, в которых основным средством является программа, можно отнести:

- несанкционированный доступ программы к данным;
- расшифровку программой зашифрованной информации;
- копирование программой информации с носителей.

Рассмотрим общую схему симметричной, или традиционной, *криптографии*.

Рис. 2. Общая схема симметричного шифрования

В процессе шифрования используется определенный алгоритм шифрования, на вход которому подаются исходное незашифрованное сообщение, называемое также ***plaintext***, и ключ. Выходом алгоритма является зашифрованное сообщение, называемое также ***ciphertext***. Ключ является значением, не зависящим от шифруемого сообщения. Изменение ключа должно приводить к изменению зашифрованного сообщения.

Зашифрованное сообщение передается получателю. Получатель преобразует зашифрованное сообщение в исходное незашифрованное сообщение с помощью алгоритма дешифрования и того же самого ключа, который использовался при шифровании, или ключа, легко получаемого из *ключа шифрования*.

Незашифрованное сообщение будем обозначать P или M, от слов *plaintext* и message. Зашифрованное сообщение будем обозначать C, от слова ciphertext.

Безопасность, обеспечиваемая традиционной *криптографией*, зависит от нескольких факторов.

Во-первых, криптографический алгоритм должен быть достаточно сильным, чтобы передаваемое зашифрованное сообщение невозможно было расшифровать без ключа, используя только различные статистические закономерности зашифрованного сообщения или какие-либо другие способы его анализа.

Во-вторых, безопасность передаваемого сообщения должна зависеть от секретности ключа, но не от секретности алгоритма. Алгоритм должен быть проанализирован специалистами, чтобы исключить наличие слабых мест, при которых плохо скрыта взаимосвязь между незашифрованным и зашифрованным сообщениями. К тому же при выполнении этого условия производители могут создавать дешевые аппаратные чипы и свободно распространяемые программы, реализующие данный алгоритм шифрования.

В-третьих, алгоритм должен быть таким, чтобы нельзя было узнать ключ, даже зная достаточно много пар (зашифрованное сообщение, незашифрованное сообщение), полученных при шифровании с использованием данного ключа.

Клод Шеннон ввел понятия *диффузии* и *конфузии* для описания *стойкости алгоритма* шифрования.

Диффузия - это рассеяние статистических особенностей незашифрованного текста в широком диапазоне статистических особенностей зашифрованного текста. Это достигается тем, что значение каждого элемента незашифрованного текста влияет на значения многих элементов зашифрованного текста или, что то же самое, любой элемент зашифрованного текста зависит от многих элементов незашифрованного текста.

Конфузия - это уничтожение статистической взаимосвязи между зашифрованным текстом и ключом.

Если X - это исходное сообщение и K - криптографический ключ, то зашифрованный передаваемый текст можно записать в виде

$$Y = E_K[X].$$

Получатель, используя тот же ключ, расшифровывает сообщение

$$X = D_K[Y]$$

Противник, не имея доступа к K и X , должен попытаться узнать X, K или и то, и другое.

Основная литература: [1] с.5-11, 36-:43, 76-85.

Дополнительная литература: **[9] с.92-119, 505-527, [10] с.104-134.**

Контрольные вопросы:

1. Какие информационные угрозы существуют.
2. Какие каналы утечки информации существуют.
3. Какие атаки и компьютерные преступления известны.
4. Какие методы защиты информации существуют.
5. Что такое криптография.

1.3 Система формирования режима информационной безопасности

Задачи информационной безопасности общества. Основные положения важнейших законодательных актов КР в области информационной безопасности и защиты информации.

Задачи информационной безопасности общества

Анализ основ информационной безопасности показал, что обеспечение безопасности является задачей комплексной. С одной стороны режима информационной, информационная безопасность предполагает, как минимум, обеспечение трех ее составляющих - доступность, целостность и конфиденциальность данных. И уже с учетом этого проблему информационной безопасности следует рассматривать комплексно. С другой стороны, информацией и информационными системами в буквальном смысле "пронизаны" все сферы общественной деятельности и влияние информации на общество все нарастает, поэтому обеспечение информационной безопасности также требует комплексного подхода.

В этой связи вполне закономерным является рассмотрение проблемы обеспечения информационной безопасности на нескольких уровнях, которые в совокупности обеспечивали бы

защиту информации и информационных систем от вредных воздействий, наносящих ущерб субъектам информационных отношений.

Рассматривая проблему информационной безопасности в широком смысле, можно отметить, что в этом случае речь идет об информационной безопасности всего общества и его жизнедеятельности, при этом на информационную безопасность возлагается задача по минимизации всех отрицательных последствий от всеобщей информатизации и содействия развитию всего общества при использовании информации как ресурса его развития.

В этой связи основными задачами информационной безопасности в широком смысле являются:

защита государственной тайны, т.е. секретной и другой конфиденциальной информации, являющейся собственностью государства, от всех видов несанкционированного доступа, манипулирования и уничтожения;

- защита прав граждан на владение, распоряжение и управление принадлежащей им информацией;
- защита прав предпринимателей при осуществлении ими коммерческой деятельности;
- защита конституционных прав граждан на тайну переписки, переговоров, личную тайну.

Рассматривая проблему информационной безопасности в узком смысле, отметим, что в этом случае речь идет о совокупности методов и средств защиты информации и ее материальных носителей, направленных на обеспечение целостности, конфиденциальности и доступности информации.

Исходя из этого, выделим следующие задачи информационной безопасности:

защита технических и программных средств информатизации от ошибочных действий персонала и техногенных воздействий, а также стихийных бедствий;

защита технических и программных средств информатизации от преднамеренных воздействий.

Основные положения важнейших законодательных актов КР в области информационной безопасности и защиты информации.

Обзор законодательства Республики Кыргызстан в сфере информационной безопасности

Концепция информационной безопасности в Кыргызской Республике

- 1. Общий обзор

До 2001 года в законодательстве Кыргызской Республики не давалось определения понятию безопасность и только с принятием Концепции национальной безопасности Кыргызской Республики появилось нормативное определение этому понятию.

Действующая Концепция национальной безопасности Кыргызской Республики была утверждена указом Президента КР 12 июня 2012 года, в которой заложены и вопросы обеспечения информационной безопасности.

Концепция национальной безопасности КР (далее – Концепция) - официально принятая система взглядов, идей и принципов по защите личности, общества и государства от внешних и внутренних угроз безопасности во всех сферах жизнедеятельности на длительный период.

Интересы личности состоят в реализации конституционных прав и свобод, в обеспечении личной безопасности граждан, в повышении качества и уровня жизни, в физическом, духовном и интеллектуальном развитии человека и гражданина.

Интересы общества состоят в упрочении демократии, в создании правового государства, в достижении и поддержании общественного согласия, в духовно-нравственном обновлении Кыргызской Республики.

Интересы государства состоят в незыблемости конституционного строя, суверенитета и территориальной целостности Кыргызской Республики, в политической, экономической и социальной стабильности, в безусловном обеспечении законности и поддержании правопорядка, в развитии равноправного и взаимовыгодного международного сотрудничества.

В Концепции одной из внутренних угроз национальной безопасности страны определена **недостаточная развитость информационно-коммуникационных технологий и слабая защита информационного пространства страны.**

Принимая во внимание растущее использование сети Интернет с особой остротой встает вопрос защиты информационной инфраструктуры, требующей широкого диапазона мер в области сетей связи и их информационной безопасности, борьбы с кибер-преступностью. Оперативное реагирование и эффективное противодействие противоправным действиям, требует развития сети центров реагирования на компьютерные инциденты и организации их взаимодействия с правоохранительными органами.

Недостаточное внимание уделяется вопросам формирования и реализации единой государственной политики по обеспечению информационной безопасности, координации деятельности органов власти и управления по ее укреплению. Мероприятия, нацеленные на защиту информационной сферы, недостаточно обеспечены финансовыми ресурсами.

Национальные интересы КР в информационной сфере:

1) защита информационных ресурсов от несанкционированного доступа, обеспечение безопасности информационных и телекоммуникационных систем, как уже развернутых, так и создавамых на территории КР;

2) развитие современных ИТ, отечественной ИКТ-индустрии, обеспечение потребностей внутреннего рынка её продукцией и выход этой продукции на мировой рынок, а также обеспечение накопления, сохранения и эффективного использования отечественных информационных ресурсов;

3)информационное обеспечение госполитики КР по доведению до национальной и международнойобщественности достоверной информации и гос.политике КР, с обеспечением доступа к открытым гос.информационным ресурсам;

4)соблюдение прав и свобод человека в информ.сфере, обеспечение духовного обновления в КР, сохранение и укрепление нравственных ценностей общества, традиций патриотизма и гуманизма, культурного и научного потенциала страны.

Виды угроз в информационной сфере:

1) угрозы конституционным правам и свободам человека и гражданина в области духовной жизни и информационной деятельности, индивидуальному, групповому и общественному сознанию, духовному возрождению КР;

2) угрозы информационному обеспечению государственной политики КР;

3)угрозы развитию отечественной индустрии информации, включая индустрию средств информатизации, телекоммуникации и связи, обеспечению потребностей внутреннего рынка в её продукции и выходу этой продукции на мировой рынок, а также обеспечению накопления, сохранности и эффективного использования отечественных информационных ресурсов;

4)угрозы безопасности информационных и телекоммуникационных средств и систем, как уже развернутых, так и создаваемых на территории КР.

Источники угроз в информационной сфере:

Основные внешние источники:

1)деятельность иностранных политических, экономических, военных, разведывательных и инфомационных структур;

2)стремление ряда стран к доминированию и ущемлению интересов КР;

3)обострение международной конкуренции за обладание ИТ и ИР;

4)деятельность международных террористических организаций;

5)увеличение технологического отрыва ведущих стран мира;

6)разработка рядом государств концепций информационных войн.

Внутренние источники:

1)недостаточная разработанность нормативной правовой базы, недостаточная правоприменительная практика

неразвитость институтов гражданского общества;

5) недостаточное бюджетное финансирование мероприятий по обеспечению информ. безопасности КР;

6)недостаточная экономическая мощь государства;

7)недостаточность квалифицированных кадров;

8)отставание от других стран в области создания и внедрения ИКТ, развития индустрии информационных услуг и широкое использование зарубежных программно-аппаратных средств;

9)стремление организованных деструктивных сил к получению доступа к ИР.

В систему обеспечения безопасности личности, общества и государства включено, в первую очередь, совершенствование законодательства в названных направлениях.

К числу перспективных направлений развития законодательства в области национальной безопасности относится **сфера обеспечения информационной безопасности**: создание эффективных государственных механизмов по обеспечению информационной безопасности, а также участия в этой деятельности гражданского общества.

Направления регулирования в сфере информационной безопасности Основными направлениями обеспечения информационной безопасности выступают:

1.правовое обеспечение (применение правовых норм обеспечения безопасности);

2.организационное обеспечение (регламентация деятельности, исключающее нанесение ущерба, наличие соответствующих служб);

3.инженерно-техническое обеспечение (использование технических средств, препятствующих нанесению ущерба, физические, аппаратные, программные и криптографические средства защиты).

Нормативная правовая база обеспечения информационной безопасности формируется из:

1. закона КР «О защите государственных секретов Кыргызской Республики»;
2. закона КР «Об информатизации»;
3. закона КР «О гарантиях и свободе доступа к информации»;
4. закона КР «О Национальном архивном фонде»;
5. закона КР «Об электрической и почтовой связи»;
6. закона КР «Об электронной цифровой подписи»;
7. закона КР «О средствах массовой информации»;
8. закона КР «О правовой охране программ для ЭВМ и баз данных»;
9. закона КР «Об основах технического регулирования в Кыргызской Республике»;
10. закона КР «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления КР» и другие;
11. Гражданского, Семейного, Уголовного и др. кодексов;

других подзаконных актов, регламентирующих общественные отношения в информационной сфере.

Анализ действующего законодательства в сфере информационной безопасности позволяет делать выводы о том, что оно:

в определенной степени остается противоречивым, отражает ведомственные интересы и не подкреплено реальными ресурсами;

не обеспечивает эффективный контроль обеспечения прав субъектов правовых отношений.

- **Ограничение доступа к информации, конфиденциальность и защита информации**

Существует 4 вида информации:

1. информация с ограниченным доступом;
2. информация, доступ к которой не может быть ограничен никаким образом;
3. иная общедоступная информация;
4. информация, не подлежащая распространению как вредная.

В связи с отсутствием в Кыргызской Республике специального закона об информации и её защите, подобная градация находит своё отражение в нескольких нормативно-правовых актах страны.

Законом КР «О защите государственных секретов Кыргызской Республики» разграничены понятия и категории государственных и негосударственных секретов, а также определен правовой режим ограничений и допуска к данной категории информации.

Государственные секреты подразделены на следующие категории: государственная, военная и служебная тайны.

К **негосударственным секретам** относятся: коммерческая тайна, информация для служебного пользования, не для печати, тайна следствия, врачебная, личная и другие виды тайны. Сохранение негосударственных секретов осуществляется их собственником, а также лицами, которым они доверены по службе и роду деятельности.

В законе также определен перечень информации (сведений), которая не может быть засекречена и доступ к которой не может быть ограничен.

Отнесение информации к государственным секретам осуществляется в соответствии с Положением о порядке определения и установления степени секретности сведений, содержащихся в работах, документах и изделиях, на основании Перечня главнейших сведений, составляющих государственные секреты, и Перечня сведений, подлежащих засекречиванию, утверждаемых Правительством КР.

1. Закон КР «О коммерческой тайне» определяет правовые основы защиты коммерческой тайны на территории Кыргызской Республики и порядок доступа к ней.
2. Закон КР «О доступе к информации, находящейся в ведении государственных органов и органов местного самоуправления КР» регулирует отношения, связанные с доступом физических и юридических лиц к находящейся в ведении государственных органов и органов местного самоуправления информации.
3. Закон КР «Об информатизации» дает общее определение понятию **конфиденциальная информация** - это документированная информация, доступ к которой ограничен определенным кругом лиц.

Таким образом, правовой режим **конфиденциальности** устанавливается тем или иным законом, регулирующим определенную сферу использования различных категорий информации.

Персональные данные, личная и семейная тайна

Персональные данные и защита частной жизни в Кыргызской Республике.

В статье 16 Конституции Кыргызской Республики провозглашены основные права граждан в сфере информационной безопасности:

- «Каждый имеет право на тайну переписки, телефонных переговоров, телеграфных, почтовых и иных сообщений.
- Каждый имеет право на неприкосновенность его частной жизни, на уважение и защиту чести и достоинства.
- Не допускается сбор, хранение, использование и распространение конфиденциальной информации о лице без его согласия, кроме случаев, установленных законом.
- Каждому гарантируется судебная защита права опровергать недостоверную информацию о себе и членах своей семьи и права требовать изъятия любой информации, а также право на возмещение материального и морального ущерба, причиненного сбором, хранением и распространением недостоверной информации».

Конституция КР также декларирует, что каждый имеет право знакомиться в органах государственной власти, органах местного самоуправления, учреждениях и организациях со сведениями о себе, не являющимися государственной или иной защищенной законом тайной. Однако существующее законодательство КР не предусматривает механизм реализации этого положения.

В 2008 году был принят закон КР «Об информации персонального характера», направленный на правовое регулирование работы с персональными данными на основе общепринятых международных принципов и норм в соответствии с Конституцией и законами КР в целях обеспечения защиты прав и

свобод человека и гражданина, связанных со сбором, обработкой и использованием персональных данных.

При этом данный закон не распространяется на хранение, обработку и использование персональных данных в связи с личными, семейными или хозяйственными делами физического лица.

Основные понятия

Информация персонального характера (персональные данные) - зафиксированная информация на материальном носителе о конкретном человеке, отождествленная с конкретным человеком или которая может быть отождествлена с конкретным человеком, позволяющая идентифицировать этого человека прямо или косвенно, посредством ссылки на один или несколько факторов, специфичных для его биологической, экономической, культурной, гражданской или социальной идентичности.

К персональным данным относятся биографические и опознавательные данные, личные характеристики, сведения о семейном положении, финансовом положении, состоянии здоровья и прочее.

Обработка персональных данных - любая операция или набор операций, выполняемых независимо от способов держателем (обладателем) персональных данных либо по его поручению, автоматическими средствами или без таковых, в целях сбора, записи, хранения, актуализации, группировки, блокирования, стирания и разрушения персональных данных.

Субъект персональных данных (субъект) - физическое лицо, к которому относятся соответствующие персональные данные.

Держатель (обладатель) массива персональных данных - органы государственной власти, органы местного самоуправления и юридические лица, на которые возложены полномочия определять цели, категории персональных данных и контролировать сбор, хранение, обработку и использование персональных данных в соответствии с настоящим Законом.

В законе также дается определение таким участникам отношений по обработке персональных данных, как обработчик и получатель персональных данных.

Обработчик - физическое или юридическое лицо, определяемое держателем (обладателем) персональных данных, которое осуществляет обработку персональных данных на основании заключенного с ним договора.

Получатель персональных данных - орган государственной власти или органы местного самоуправления, юридические и физические лица, а также субъект персональных данных (субъект), которым передаются и предоставляются персональные данные в соответствии с настоящим Законом.

Для проведения статистических, социологических, исторических, медицинских и других научных и практических исследований держатель (обладатель) массива персональных данных осуществляет **обезличивание** используемых данных, придавая им форму анонимных сведений. При этом режим конфиденциальности, установленный для персональных данных, снимается.

Обезличивание персональных данных - изъятие из персональных данных той их части, которая позволяет отождествить их с конкретным человеком.

Принципы и условия работы с персональными данными

Законом определены следующие **принципы** обработки персональных данных:

- Персональные данные должны быть получены и обработаны в порядке, предусмотренном законом «Об информации персонального характера».
- Персональные данные должны собираться для точно и заранее определенных, объявленных и законных целей, не использоваться в противоречии с этими целями и в дальнейшем не обрабатываться каким-либo образом, несовместимым с данными целями. Первоначальные данные должны быть точными и в случае необходимости обновляться.
- Персональные данные должны храниться не дольше, чем этого требуют цели, для которых они накапливались, и подлежат уничтожению по достижении целей или минованию надобности в них.
- Для персональных данных, сохраняемых более длительные сроки в исторических или иных целях, должны быть установлены необходимые гарантии обеспечения их защиты.
- Не допускается объединение массивов персональных данных, собранных держателями (обладателями) в разных целях, для автоматизированной обработки информации.
- Персональные данные должны храниться и защищаться держателями (обладателями) массивов персональных данных от незаконных доступов, внесений дополнений, изменений и уничтожений.

Основные принципы работы с персональными данными не носят исчерпывающий характер и могут дополняться в соответствии с законодательством КР.

Закон также определяет **случаи**, при которых держатель (обладатель) массива персональных данных может осуществлять работу с персональными данными:

1. если субъект персональных данных дал свое согласие на ее проведение;
2. если она необходима для выполнения органами государственной власти, органами местного самоуправления своей компетенции, установленной законодательством КР;
3. если она нужна для достижения законных интересов держателей (обладателей);
4. когда реализация этих интересов не препятствует осуществлению прав и свобод субъектов персональных данных применительно к обработке персональных данных;
5. когда она необходима для защиты интересов субъекта персональных данных;
6. если обработка персональных данных осуществляется исключительно в целях журналистики либо в целях художественного или литературного творчества при условии, что такие действия будут согласовываться с субъектом персональных данных с соблюдением права на неприкосновенность частной жизни и свободу слова.

В целях информационного обеспечения общества могут создаваться **общедоступные массивы персональных данных** (справочники, телефонные книги, адресные книги и т.п.).

По желанию субъекта для его персональных данных может быть установлен режим общедоступной информации (библиографические справочники, телефонные книги, адресные книги, частные объявления и т.д.). Исключения составляют случаи, когда информация должна носить публичный характер в соответствии с требованиями законодательства КР.

В общедоступные массивы персональных данных с письменного согласия субъекта могут включаться следующие персональные данные: фамилия, имя, отчество, год и место рождения, адрес местожительства, номер контактного телефона, сведения о профессии, иные сведения, предоставленные субъектом и/или полученные из открытых источников, других общедоступных массивов персональных данных, если эти источники сформированы **с согласия субъекта персональных данных.**

В случае если персональные данные получены держателем (обладателем) общедоступного массива персональных данных из открытых источников либо иных общедоступных массивов

персональных данных, держатель (обладатель) общедоступного массива по запросу субъекта информирует в недельный срок о содержании его персональных данных, об источниках получения и цели использования.

Режим конфиденциальности для общедоступных массивов персональных данных не устанавливается.

Законом определены условия обработки **специальной категории персональных данных**.

Так сбор, накопление, хранение и использование персональных данных, раскрывающих расовое или этническое происхождение, национальную принадлежность, политические взгляды, религиозные или философские убеждения, а также касающихся состояния здоровья и сексуальных наклонностей, исключительно в целях выявления этих факторов, не допускаются.

Исключения составляют случаи:

а) если субъект персональных данных дал свое согласие на сообщение и обработку таких данных;

б) если обработка необходима для защиты здоровья и безопасности субъекта данных, иного лица или соответствующей группы лиц.

Принципы сбора, использования **биометрических данных** и порядок биометрической регистрации установлены в законе КР «О биометрической регистрации граждан КР».

К биометрическим данным отнесены:

- цифровое графическое изображение лица;
- графическое строение папиллярных узоров пальцев обеих рук;
- собственноручная подпись.

Сбор, обработка, хранение и использование биометрических данных осуществляются на принципах:

1) обязательной биометрической регистрации;
2) открытости (обеспечения доверия граждан к использованию государством биометрических данных);
3) гарантии законного использования биометрических и персональных данных органами государственной власти, местного самоуправления, наделенными специальными полномочиями в соответствии с законодательством КР;
4) защиты базы биометрических данных;
5) обеспечения безопасности биометрических данных при их сборе, обработке, хранении и использовании в информационных системах и соблюдения требований к материальным носителям.

Несмотря на **принцип обязательности** сдачи биометрических данных, данным законом установлено, что получение информации о биометрических данных осуществляется при наличии согласия в письменной форме субъекта биометрических данных в соответствии с законодательством КР, за исключением случаев, установленных тем же законом.

Получение информации о биометрических данных осуществляется **без согласия субъекта биометрических данных** только в случаях осуществления правосудия и исполнения судебного акта, а также в случаях, предусмотренных законодательством КР о национальной безопасности, о противодействии терроризму и коррупции, об оперативно-розыскной деятельности и иных случаях, определяемых законодательством КР.

При **трансграничной передаче персональных данных** держатель (обладатель) массива персональных данных, находящийся под юрисдикцией Кыргызской Республики, передающий данные,

исходит из наличия международного договора между сторонами, согласно которому получающая сторона обеспечивает адекватный уровень защиты прав и свобод субъектов персональных данных и охраны персональных данных, установленный в Кыргызской Республике.

Кыргызская Республика обеспечивает законные меры охраны находящихся на ее территории или передаваемых через ее территорию персональных данных, исключающие их искажение и несанкционированное использование.

Передача персональных данных в страны, не обеспечивающие адекватный уровень защиты прав и свобод субъектов персональных данных, может иметь место при условии:

- согласия субъекта персональных данных на эту передачу;
- если передача необходима для защиты жизненно важных интересов субъекта персональных данных;
- если персональные данные содержатся в общедоступном массиве персональных данных.

При передаче персональных данных **по глобальной информационной сети (Интернет и т.п.)** держатель (обладатель) массива персональных данных, передающий такие данные, обязан обеспечить передачу необходимыми средствами защиты, соблюдая при этом конфиденциальность информации.

Права субъекта данных и обязанности держателя (обладателя) и обработчика массивов персональных данных. Ответственность

Субъект персональных данных самостоятельно решает вопрос о предоставлении кому-либо любых своих персональных данных, за исключением случаев, предусмотренных законом. Персональные данные предоставляются субъектом лично либо через доверенное лицо.

В целях реализации своих прав и свобод субъект предоставляет данные, а также сведения об их изменениях в соответствующие органы государственной власти, органы местного самоуправления, имеющие право на работу с персональными данными в пределах их компетенции.

Перед предоставлением своих персональных данных субъект должен быть ознакомлен держателем (обладателем) массива персональных данных с **перечнем собираемых данных**, основаниями и целями их сбора и использования, с возможной передачей персональных данных третьей стороне, а также информирован об ином возможном использовании персональных данных.

Субъект персональных данных при отказе в предоставлении своих данных имеет право не указывать причины своего отказа.

Субъект персональных данных имеет право знать о наличии у держателя (обладателя) относящихся к нему персональных данных и иметь к ним доступ. Право на доступ может быть ограничено только в случаях, предусмотренных законом.

Ограничение прав субъекта на предоставление и получение своих персональных данных возможно в отношении:

1) **права предоставления субъектом своих персональных данных держателям (обладателям) массивов персональных данных** - для субъектов персональных данных, допущенных к сведениям, составляющим государственную тайну, - в соответствии с законом КР "О защите государственных секретов Кыргызской Республики";

2) **права доступа субъекта к своим персональным данным**, внесения изменений в свои персональные данные, блокирования своих персональных данных:

а) для персональных данных, полученных в результате оперативно-розыскной деятельности, за исключением случаев, когда эта деятельность проводится с нарушением законодательства КР;

б) для персональных данных субъектов, задержанных по подозрению в совершении преступления либо которым предъявлено обвинение по уголовному делу, либо к которым применена мера пресечения до предъявления обвинения в органах, проводящих указанные действия.
Перечень ограничений прав доступа субъекта к своим персональным данным является **исчерпывающим**.

Держатель (обладатель) массива персональных данных обязан:
а) получать персональные данные непосредственно от субъекта персональных данных, его доверенных лиц;

б) обеспечивать режим конфиденциальности персональных данных в случаях, предусмотренных законодательством КР и законом «Об информации персонального характера»;

в) определить обработчика для обработки персональных данных, предоставляющего гарантии в отношении мер технической безопасности и организационных мер, регулирующих обработку персональных данных, за исключением случаев, когда держатель (обладатель) самостоятельно возлагает на себя функции и обязанности обработчика;

г) обеспечивать сохранность и достоверность персональных данных, а также установленный в нормативном порядке режим доступа к ним;

д) предоставлять персональные данные в недельный срок после поступления запроса от субъекта;

ж) в случае отказа в предоставлении субъекту по его требованию информации о наличии персональных данных о нем, а также самих персональных данных, выдавать письменный мотивированный ответ, в срок, не превышающий одной недели с момента обращения субъекта;

з) представлять по запросам уполномоченного государственного органа или Омбудсмена (Акыйкатчы) Кыргызской Республики в недельный срок информацию, необходимую для исполнения их полномочий;

и) в пределах компетенции разрабатывать в соответствии со спецификой своей деятельности перечни персональных данных и руководствоваться ими;

к) принять к производству заявление субъекта персональных данных (о выявленной недостоверности данных или неправомерности действий с ними держателя (обладателя) массивов) и заблокировать его персональные данные с момента его получения на период проверки заявления;

л) осуществлять действия по блокированию и снятию с блокирования, уничтожению данных в соответствии с требованиями закона «Об информации персонального характера»;

м) информировать субъекта персональных данных об осуществленной передаче его персональных данных третьей стороне в любой форме в недельный срок.

Обработчик персональных данных осуществляет обработку персональных данных на основании договора, заключенного с держателем (обладателем) персональных данных.

Обработчик должен выполнять сбор, запись, хранение, актуализацию, блокирование, уничтожение персональных данных, независимо от способа и средств обработки, по поручению держателя (обладателя) персональных данных.

Лица, которым персональные данные стали известны в силу их служебного положения, принимают на себя обязательства и **несут ответственность** по обеспечению конфиденциальности этих персональных

данных. Такие обязательства остаются в силе и после окончания работы этих лиц с персональными данными в течение срока сохранения режима конфиденциальности, согласно закона.

Субъект персональных данных имеет право на возмещение причиненного ущерба и на компенсацию морального вреда в судебном порядке.

Ответственность за нарушение норм, установленных законом «Об информации персонального характера», наступает в соответствии с действующим законодательством КР.

Конфиденциальность и безопасность персональных данных

Персональные данные, находящиеся в ведении держателя (обладателя), относятся к **конфиденциальной информации**, кроме случаев, определенных законом.

Держатель (обладатель) персональных данных и обработчик обязаны обеспечивать охрану персональных данных во избежание несанкционированного доступа, блокирования, передачи, а равно их случайного или несанкционированного уничтожения, изменения или утраты.

Режим конфиденциальности персональных данных снимается в случаях:

- обезличивания персональных данных;
- по желанию субъекта персональных данных.

Держатель (обладатель) массива персональных данных и обработчик обязаны обеспечить гарантии в отношении **мер технической безопасности и организационных мер**, регулирующих обработку персональных данных.

При обработке персональных данных держатель (обладатель) массива персональных данных и обработчик обязаны:

- исключить доступ посторонних лиц к оборудованию, используемому для обработки персональных данных (контроль за доступом);
- препятствовать самовольному чтению, копированию, изменению или выносу носителей данных (контроль за пользованием носителями данных);
- препятствовать самовольной записи персональных данных и изменению или уничтожению записанных персональных данных (контроль за записью) и обеспечивать возможность установления задним числом когда, кем и какие персональные данные были изменены;
- обеспечить безопасность систем обработки данных, предназначенных для переноса персональных данных независимо от средств передачи данных (контроль за средствами передачи данных);
- обеспечить, чтобы каждый пользователь системы обработки данных имел доступ только к тем персональным данным, к обработке которых он имеет допуск (контроль за допуском);
- обеспечить возможность установления задним числом когда, кем и какие персональные данные вводились в систему обработки данных (контроль за вводом);
- не допускать несанкционированного чтения, копирования, изменения и уничтожения персональных данных при передаче и транспортировке персональных данных (транспортный контроль);
- обеспечить конфиденциальность информации, полученной при обработке персональных данных.

Требования к защите персональных данных и информационной безопасности при их обработке находятся на стадии разработки, которые планируется сформировать в виде подзаконного акта.

Уполномоченный орган

Законом КР «Об информации персонального характера» определено, что государство осуществляет регулирование работы с персональными данными в следующих формах:

- Правительством КР определяется уполномоченный государственный орган Кыргызской Республики;
- ведет учет и регистрацию массивов персональных данных и их держателей (обладателей);
- заключает международные договоры о трансграничной передаче персональных данных, за исключением случаев, противоречащих законодательству КР по защите государственных секретов.

Уполномоченный государственный орган - государственный орган, на который возложены функции по регистрации держателей (обладателей) массива персональных данных, ведению Реестра держателей массива персональных данных и другие задачи, предусмотренные законом.

Однако до настоящего времени данный уполномоченный орган так и не определен.

Государственные секреты

Сведения, составляющие государственные секреты

Правовые основы функционирования системы защиты государственных секретов во всех видах деятельности государственных органов, предприятий, объединений, организаций, независимо от форм собственности, воинских формирований и граждан Кыргызской Республики на всей территории республики и в ее учреждениях за границей регулируются законом КР «О защите государственных секретов КР».

Государственные секреты - информация, хранящаяся и перемещаемая любыми видами носителей, затрагивающая обороноспособность, безопасность, экономические и политические интересы Кыргызской Республики, подконтрольная государству и ограничиваемая специальными перечнями и правилами, разработанными на основе и во исполнение Конституции КР.

Отнесение информации к государственным секретам основывается на **принципах**:

- **законности** - осуществлении засекречивания информации в порядке, установленном действующим законодательством;
- **обоснованности** - определения целесообразности засекречивания информации путем экспертной оценки в интересах государства и граждан;
- **своевременности** - установлении ограничений на распространение сведений с момента их образования.

Государственные секреты КР подразделяются на три категории: государственная, военная и служебная тайны.

К государственной тайне относится информация, разглашение которой может повлечь тяжкие последствия для обороноспособности, безопасности, экономических и политических интересов Кыргызской Республики.

Информации, составляющей государственную тайну, присваиваются ограничительные грифы "особой важности" и "совершенно секретно".

Военную тайну образуют сведения военного характера, разглашение которых может нанести ущерб Вооруженным Силам и интересам КР.

Информации, составляющей военную тайну, присваиваются ограничительные грифы "совершенно секретно" и "секретно".

К **служебной тайне** относится информация, разглашение которой может оказать отрицательное воздействие на обороноспособность, безопасность, экономические и политические интересы КР. Такая информация имеет характер отдельных сведений, относящихся к государственной или военной тайне, и не раскрывает их полностью.

Информации, составляющей служебную тайну, присваивается ограничительный гриф "секретно".

Порядок установления ограничительных грифов секретности на информацию определяется Правительством КР.

Присвоение ограничительных грифов, не предусмотренных законом, не допускается.

Законом определены ограничения на засекречивание информации. **Не подлежат засекречиванию сведения:**

- о стихийных бедствиях и чрезвычайных происшествиях, угрожающих здоровью граждан;
- о катастрофах и их последствиях;
- о положении дел в экологии, использования природных ресурсов, здравоохранения, санитарии, культуре, сельском хозяйстве, образовании, торговли и обеспечения правопорядка;
- о фактах нарушения законности государственными органами и должностными лицами;
- о фактах, посягающих на права и законные интересы граждан, а также создающих угрозу их личной безопасности.

Режим государственной тайны

Основными элементами **системы защиты** государственных секретов являются:

- правила определения и установления степени секретности информации, содержащейся в работах, документах, изделиях и нетрадиционных носителях информации;
- порядок допуска к государственным секретам;
- ограничения для лиц, работающих с государственными секретами;
- порядок обращения с государственными секретами;
- контроль за обеспечением сохранности государственных секретов;
- органы обеспечения защиты государственных секретов;
- ответственность за невыполнение требований по защите государственных секретов.

Отнесение информации к государственным секретам осуществляется в соответствии с Положением о порядке определения и установления степени секретности сведений, содержащихся в работах, документах и изделиях, на основании Перечня главнейших сведений, составляющих государственные секреты, и Перечня сведений, подлежащих засекречиванию, утверждаемых Правительством КР.

Указанные Положение и Перечни являются документами для служебного пользования, доступ к которым ограничен.

Государственные органы, определяемые Правительством КР, вправе засекречивать и рассекречивать информацию, являющуюся собственностью юридических и физических лиц Кыргызской Республики и отвечающую требованиям закона, с компенсацией убытков собственникам.

Собственники информации вправе обжаловать в суде неправомерные действия по засекречиванию и рассекречиванию информации.

Порядок обращения с государственными секретами осуществляется в соответствии с законом КР «О защите государственных секретов КР» и Инструкцией по обеспечению режима секретности, утверждаемой Правительством КР.

Основанием для передачи секретной информации другому государству являются вступившие в установленном законом порядке в силу международные договоры, участницей которых является

Кыргызская Республика, предусматривающие обязательства сторон по защите передаваемой секретной информации.

Секреты других государств и международных организаций, переданные в установленном порядке Кыргызской Республике, охраняются законом КР «О защите государственных секретов КР» на основе вступивших в установленном законом порядке в силу международных договоров, участницей которых является Кыргызская Республика.

Ответственность за обеспечение сохранности государственных секретов возлагается на руководителей государственных органов, предприятий, учреждений, организаций, объединений.

За разглашение секретных сведений, неправомерное завышение либо занижение степени их секретности, нарушение режима секретности, а также за нарушение требований настоящего Закона, виновные лица, в зависимости от тяжести нанесенного ущерба, привлекаются к уголовной, административной, дисциплинарной ответственности в соответствии с действующим законодательством Кыргызской Республики.

Порядок допуска к государственным секретам:

Гражданам Кыргызской Республики, которым для выполнения служебных обязанностей необходимо работать с государственными секретами, оформляется допуск к этим секретам. При этом, до заключения трудового договора (контракта), в отношении этих граждан, с их добровольного письменного согласия, осуществляются в установленном порядке проверочные мероприятия.

В трудовом договоре (контракте) отражаются: обязанность гражданина соблюдать требования по обеспечению защиты государственных секретов; обязательство о неразглашении этой информации, ограничения, связанные с работой с государственными секретами.

Объем проверочных мероприятий зависит от степени секретности сведений, к которым будет допускаться оформляемое лицо. Устанавливаются три формы допуска граждан к государственным секретам, соответствующие трем степеням секретности сведений, составляющих государственные секреты: к сведениям особой важности, совершенно секретным или секретным. Наличие у граждан допуска к сведениям более высокой степени секретности является основанием для доступа их к сведениям более низкой степени секретности.

Гражданам должна предоставляться только та информация, составляющая государственные секреты, которая необходима им для выполнения служебных обязанностей.

К государственным секретам без согласования с уполномоченным государственным органом, ведающим вопросами национальной безопасности, и **без оформления обязательств о неразглашении допускаются:**

- Президент Кыргызской Республики;
- Торага Жогорку Кенеша КР, его заместители;
- председатель и члены Комитета по обороне и безопасности Жогорку Кенеша КР;
- Премьер-министр, вице-премьер-министры, руководители государственных органов, ведающих вопросами обороны, безопасности, внутренних дел, охраны и защиты государственной границы, и их заместители. Другие члены Правительства, а также приравненные к ним должностные лица и их заместители, определяемые Премьер министром КР по решению руководителя Аппарата Правительства КР;
- депутаты Жогорку Кенеша КР по решению Комитета по обороне и безопасности Жогорку Кенеша КР.

К государственным секретам не допускаются граждане Кыргызской Республики:

- постоянно проживающие за границей или обращающиеся в соответствующие государственные органы с просьбой о выходе из гражданства Кыргызской Республики, получении иностранного гражданства;
- признанные судом недееспособными, ограниченно дееспособными, привлеченные в качестве подозреваемого, обвиняемого, подсудимого за совершение умышленных преступлений, а также при наличии у них неснятой или непогашенной судимости за эти преступления в установленном законом порядке;
- имеющие медицинские противопоказания для работы с государственными секретами, перечень которых утверждается Правительством Кыргызской Республики;
- указавшие заведомо ложные сведения в анкетных данных, влияющие на принятие решения о допуске к государственным секретам;
- имеющие двойное гражданство.

Не допускаются к государственным секретам **иностранцы и лица без гражданства**.

Допуск граждан к секретной информации может быть прекращен по решению руководителя государственного органа, предприятия, учреждения, организации в случаях:

- расторжения трудового договора (контракта) в связи с организационно-штатными мероприятиями;
- грубого или систематического нарушения трудового договора (контракта), связанного с защитой секретной информации.

Прекращение допуска граждан к секретной информации является основанием для расторжения с гражданами трудового договора (контракта).

Прекращение допуска по указанным выше основаниям не освобождает гражданина КР от обязанностей неразглашения известных ему государственных секретов.

Сроки действия секретности информации

Рассекречивание информации производится в сроки, установленные при ее засекречивании, если не принято решение об их продлении в установленном порядке.

Сведения, составляющие государственные секреты, могут быть рассекречены досрочно или сроки их секретности продлены, если этого требуют политические, экономические интересы Кыргызской Республики, а также с появлением факторов, вызывающих необходимость их корректировки.

Решение о рассекречивании и продлении сроков секретности принимается Правительством Кыргызской Республики по представлению заинтересованных министерств, государственных комитетов, административных ведомств, а также предприятий, учреждений, организаций.

Коммерческая тайна

Сведения, составляющие коммерческую тайну

Закон КР «О коммерческой тайне» определяет правовые основы защиты коммерческой тайны на территории Кыргызской Республики.

Под **коммерческой тайной** понимаются не являющиеся государственной тайной сведения, связанные с производством, технологией, управлением, финансовой и другой деятельностью хозяйствующего субъекта, разглашение которых может нанести ущерб его интересам.

Сведения, составляющие коммерческую тайну, являются собственностью субъекта предпринимательства либо находятся в его владении, пользовании, распоряжении в пределах, установленных им в соответствии с законодательством.

Гражданский кодекс КР дает следующее определение служебной и коммерческой тайне, включая её защиту:

- «Гражданским законодательством защищается информация, составляющая служебную или коммерческую тайну, в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

- Лица, незаконными методами получившие такую информацию, а также служащие - вопреки трудовому договору или контрагенты - вопреки гражданско-правовому договору, разгласившие служебную или коммерческую тайну, обязаны возместить причиненный ущерб.»

Сведения, составляющие коммерческую тайну, должны соответствовать следующим требованиям:

а) иметь действительную или потенциальную ценность для субъекта предпринимательства;
б) не являться общеизвестными или общедоступными согласно законодательству;
в) обозначаться соответствующим образом с принятием субъектами предпринимательства надлежащих мер по сохранению их конфиденциальности через систему классификации названных сведений, разработку внутренних правил ограничения пользования, введение соответствующей маркировки документов и иных носителей информации, организации учета, хранения и применение.
К объектам коммерческой тайны не могут относиться:

а) учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности, подлежащей лицензированию (устав, решение о создании предприятия или договор учредителей, регистрационные удостоверения, лицензии, патенты);

б) сведения по утвержденным формам статистической отчетности, а также отчетности о финансово-экономической деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов, а также других обязательных платежей;

в) документы об уплате налогов и других обязательных платежей;

г) документы, удостоверяющие платежеспособность;

е) сведения о численности, составе работников, заработной плате руководителя организации и членов коллегиального исполнительного органа организации, системе оплаты труда, об условиях труда, в том числе об охране труда, о показателях производственного травматизма и профессиональной заболеваемости и наличии свободных рабочих мест;

ж) сведения о загрязнении окружающей среды, нарушении антимонопольного законодательства, несоблюдении правил охраны труда, реализации продукции, причиняющей вред здоровью потребителей, а также о других нарушениях законодательства и размерах причиненного при этом ущерба;

з) сведения об участии должностных лиц государственных предприятий в организациях, занимающихся предпринимательской деятельностью.

Режим коммерческой тайны

Порядок защиты коммерческой тайны определяется субъектом предпринимательства или назначенным им руководителем, который доводит его до работников, имеющих доступ к сведениям, составляющим коммерческую тайну.

Субъектами коммерческой тайны разрабатываются **инструкции, положения по обеспечению сохранности коммерческой тайны**, в которых определяются:

а) состав и объем сведений, составляющих коммерческую тайну;

б) порядок присвоения грифа "Секрет предприятия" сведениям, работам и изделиям и его снятия;

в) процедура допуска работников хозяйствующего субъекта, а также лиц, привлекаемых к его деятельности, к сведениям, составляющим коммерческую тайну;

г) порядок использования, учета, хранения и маркировки документов и иных носителей информации, изделий, сведения о которых составляют коммерческую тайну;

д) организация контроля за порядком использования сведений, составляющих коммерческую тайну;

е) процедура принятия взаимных обязательств хозяйствующими субъектами по сохранению коммерческой тайны при заключении договоров о проведении каких-либо совместных действий;

ж) порядок применения предусмотренных законодательством мер дисциплинарного, материального воздействия на работников, разгласивших коммерческую тайну;

з) возложение ответственности за обеспечение сохранности коммерческой тайны на должностное лицо хозяйствующего субъекта.

Работники хозяйствующего субъекта, имеющие доступ к сведениям, составляющим коммерческую тайну, обязаны:

- сохранять коммерческую тайну, которая станет им известна по работе, и не разглашать ее без разрешения, выданного в установленном порядке, при условии, что сведения, составляющие коммерческую тайну, не были известны им ранее либо не были получены ими от третьего лица без обязательства соблюдать в отношении их конфиденциальность;
- выполнять требования инструкций, положений, приказов по обеспечению сохранности коммерческой тайны;
- в случае попытки посторонних лиц получить от них сведения, составляющие коммерческую тайну, немедленно сообщить об этом соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта;
- сохранять коммерческую тайну хозяйствующих субъектов, с которыми имеются деловые отношения;
- не использовать знание коммерческой тайны для занятий деятельностью, которая в качестве конкурентного действия может нанести ущерб хозяйствующему субъекту;
- в случае увольнения передать все носители информации, составляющие коммерческую тайну (рукописи, черновики, документы, чертежи, магнитные ленты, перфокарты, перфоленты, диски, дискеты, распечатки на принтерах, кино-, фотопленки, модели, материалы и др.), которые находились в их распоряжении, соответствующему должностному лицу или в соответствующее подразделение хозяйствующего субъекта.

Данные обязательства даются в письменной форме при заключении трудового или иного договора либо в процессе его исполнения.

Для обеспечения **защиты коммерческой тайны на хозяйствующих субъектах** могут создаваться специальные режимные подразделения, функции и полномочия которых отражаются в соответствующих инструкциях, положениях, приказах.

Правоохранительные и иные государственные органы оказывают содействие режимным подразделениям хозяйствующих субъектов в выполнении возложенных на них функций.

При осуществлении хозяйствующими субъектами торгово-экономических, научно-технических, валютно-финансовых и других деловых связей, в том числе с иностранными партнерами, договаривающиеся стороны специально оговаривают характер, состав сведений, составляющих коммерческую тайну, а также взаимные обязательства по обеспечению ее сохранности в соответствии с законодательством.

При заключении договора с иностранными партнерами условия конфиденциальности деятельности должны соответствовать законодательству страны, где заключается договор, если иное не предусмотрено межгосударственными соглашениями.

Доступ к коммерческой тайне имеют:

- работники, круг которых определен субъектом предпринимательства;
- государственные контролирующие и правоохранительные органы в соответствии с полномочиями, предоставленными им законодательством по контролю и надзору, имеющие право в пределах своей компетенции на основании письменного запроса знакомиться со сведениями, являющимися коммерческой тайной.

Физические и юридические лица, включая должностных лиц государственных органов контроля и надзора, а также уполномоченного органа по противодействию финансированию терроризма и легализации (отмыванию) доходов, полученных преступным путем, имеющие доступ к коммерческой тайне, обязаны строго соблюдать требования о ее неразглашении, не допускать утечки информации к конкурирующим хозяйствующим субъектам.

За несанкционированное разглашение коммерческой тайны физические и юридические лица привлекаются к **ответственности** в соответствии с законодательством КР.

Работники хозяйствующего субъекта, государственных органов, а также лица, незаконно получившие сведения, составляющие коммерческую тайну, или завладевшие ими, обязаны также возместить ущерб, причиненный хозяйствующему субъекту или субъекту предпринимательства.

Гражданским кодексом КР также регламентировано право на защиту нераскрытой коммерческой информации.

Лицо, правомерно обладающее технической, организационной или коммерческой информацией, в том числе секретами производства (ноу-хау), неизвестной третьим лицам (нераскрытая информация), имеет право на защиту этой информации от незаконного использования, если соблюдены условия, установленные законом для служебной и коммерческой тайны.

Право на защиту нераскрытой информации от незаконного использования возникает независимо от выполнения в отношении этой информации каких-либо формальностей (ее регистрации, получения свидетельств и т.п.).

Лицо, обладающее нераскрытой информацией, может **передать** все или часть сведений, составляющих содержание этой информации, другому лицу по лицензионному договору.

Лицензиат обязан принимать надлежащие меры к охране конфиденциальности информации, полученной по договору, и имеет те же права на ее защиту от незаконного использования третьими лицами, что и лицензиар. Поскольку в договоре не предусмотрено иное, обязанность сохранять конфиденциальность информации лежит на лицензиате и после прекращения лицензионного договора, если соответствующие сведения продолжают оставаться нераскрытой информацией.

Иные виды тайн

Законодательством КР не предусмотрен конкретный перечень видов тайн. Например, законом «О защите государственных секретов КР» определено разделение на государственные и негосударственные секреты.

К негосударственным секретам законом отнесены, помимо коммерческой тайны, информация для служебного пользования, не для печати, тайна следствия, врачебная, личная и другие виды тайны. Таким образом, данный перечень является **неисчерпывающим.**

Перечень тайн, определенных законодательством КР.

Виды тайн	Описание
Банковская тайна	*Банковской тайной* считаются сведения о счетах (вкладах) клиента (корреспондента), ставшие известными банку в связи с его обслуживанием, сведения об операциях (сделках), совершенных по поручению клиента или в его пользу, а также сведения о самом клиенте, сведения о клиентах других банков, ставшие известными в результате обмена информацией между банками, и любые другие сведения, которые были доверены или стали известны банку в процессе отношений между банком и клиентом. Банку, его учредителям, акционерам, членам Совета директоров и правления, исполнительным должностным лицам, сотрудникам банка, а также лицам, которые работают на банк, запрещается раскрывать третьим лицам или использовать в каких-либо целях любую информацию, которая им была доверена или к которой они имели доступ в процессе отношений между банком и клиентами, иначе как по основаниям, предусмотренным законодательством. Данный запрет распространяется и на бывших клиентов банка и касается всей информации, полученной от таких клиентов. Кроме того, запрет касается всех лиц, которым банки оказывали услуги, независимо от того, имеют они счета в банке или нет.
Адвокатская тайна	Адвокатской тайной являются любые сведения, связанные с оказанием адвокатом юридической помощи своему доверителю. Адвокат не вправе использовать в своих интересах или в интересах третьих лиц сведения, составляющие адвокатскую тайну.
Тайна совершения нотариальных действий	Нотариусы и другие должностные лица, уполномоченные совершать нотариальные действия, обязаны хранить в тайне сведения, которые стали им известны в связи с совершением нотариальных действий. Обязанность сохранения тайны совершаемых нотариальных действий распространяется также на лиц, которым о совершенных нотариальных действиях стало известно в связи с исполнением ими служебных обязанностей, в том числе и после прекращения трудового договора.
Врачебная тайна	Информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении, составляют врачебную тайну. Гражданину должна быть подтверждена гарантия конфиденциальности передаваемых им сведений. Не допускается разглашение сведений, составляющих врачебную тайну, лицами, которым они стали известны при обучении, исполнении профессиональных, служебных и иных обязанностей, кроме случаев, установленных частями третьей и четвертой настоящей статьи.
Процессуальная тайна	Данные, полученные в ходе следствия по уголовному делу, не подлежат разглашению (тайна следствия).

	Следователь предупреждает свидетеля, потерпевшего, защитника, гражданского истца, гражданского ответчика или их представителей, эксперта, специалиста, переводчика, понятых и других лиц, присутствующих при производстве следственных действий, о недопустимости разглашения данных следствия и вправе отобрать у них подписку с предупреждением об ответственности. Тайна совещания присяжных заседателей - кроме присяжных заседателей присутствие иных лиц в совещательной комнате не допускается. Присяжные заседатели не вправе разглашать мнения, имевшие место при обсуждении и принятии вердикта, а также сведения, ставшие известными им во время закрытого судебного заседания.
Тайна информации, которая передается средствами связи	Тайна переписки, телефонных переговоров, телеграфных, а также других сообщений, которые передаются средствами связи, охраняется Конституцией и законом «Об электрической и почтовой связи». Предприятия связи всех форм собственности обязаны принимать необходимые организационно-технические меры по защите информации. Ограничение этого права допускается только с санкции прокурора.
Налоговая тайна	Налоговую тайну составляют любые полученные органом налоговой службы или его должностным лицом сведения о налогоплательщике, за исключением сведений: 1) о реквизитах налогоплательщика (наименование или фамилия, имя и отчество налогоплательщика, адрес), а также об идентификационном номере налогоплательщика; 2) о регистрации налогоплательщика в качестве плательщика налога на добавленную стоимость; 3) о счетах-фактурах по налогу на добавленную стоимость и марках акцизного сбора; 4) о сумме налоговой задолженности, признанной налогоплательщиком; 5) о нарушениях налогоплательщиком налогового законодательства КР и мерах ответственности за эти нарушения, установленные вступившим в силу решением суда либо признанные налогоплательщиком; 6) о фактических произведенных налоговых платежах в пользу государственного бюджета юридическими лицами. Налоговая тайна не подлежит разглашению органами налоговой службы, их должностными лицами, за исключением случаев, когда сведения передаются: 1) другим должностным лицам органов налоговой службы, таможенных органов, уполномоченного государственного органа в ходе или в целях исполнения ими своих обязанностей, предусмотренных настоящим Кодексом или законодательством КР в сфере таможенного дела; 2) правоохранительным органам, исключительно в отношении налогоплательщика, по которому возбуждено уголовное дело по факту налогового правонарушения; 3) суду в ходе судебного разбирательства по установлению налоговой задолженности налогоплательщика или его ответственности за налоговые правонарушения; 4) уполномоченному государственному органу по делам о банкротстве, администратору (временному администратору, специальному администратору, консерватору, внешнему управляющему) в целях осуществления ими полномочий, предусмотренных законодательством КР о банкротстве, по тем субъектам, в отношении которых возбужден
	процесс банкротства или в отношении которых вынесено решение об инициировании процесса банкротства; 5) уполномоченному государственному органу по делам государственной службы КР в отношении лиц, обязанных представлять декларацию об имуществе и доходах в соответствии с законодательством КР о государственной службе; 6) депутатам Жогорку Кенеша КР, аппарату Правительства КР, Службе финансовой разведки КР в случаях, установленных законодательством КР, регулирующим их деятельность; 7) налоговым или правоохранительным органам других государств в соответствии с международными договорами о взаимном сотрудничестве между налоговыми или правоохранительными органами, участником которых является Кыргызская Республика; 8) органам государственной статистики в целях осуществления статистической деятельности, предусмотренной законодательством КР.

Тайна страхования	Работники уполномоченного государственного органа в сфере регулирования и надзора за страховой деятельностью не вправе разглашать ставшие известными им в силу должностного положения сведения, составляющие коммерческую тайну страховщика, иную информацию, касающуюся страховщика и его клиентов, кроме случаев, предусмотренных законодательством КР в сфере противодействия финансированию терроризма и легализации (отмыванию) доходов, полученных преступным путем.
Тайна усыновления	Тайна усыновления ребенка охраняется законом. Должностные лица, вынесшие решение об усыновлении ребенка или осуществившие государственную регистрацию усыновления, а также лица, иным образом осведомленные об усыновлении, обязаны сохранять тайну усыновления ребенка.

Криптография

В Кыргызской Республике деятельность в области криптографии (шифровании) регулируется незначительным количеством нормативно-правовых актов.

Существует «Национальный контрольный список Кыргызской Республики контролируемой продукции», утвержденный постановлением Правительства КР от 02.04.2014г. № 197, в который включены в том числе ЭВМ, сопутствующее оборудование и программное обеспечение, выполняющие функции **криптографии, криптоанализа**, сертифицируемой многоуровневой защиты информации или сертифицируемые функции изоляции пользователей либо ограничивающие электромагнитную совместимость (ЭМС).

Законом КР "Об органах национальной безопасности Кыргызской Республики" на **Государственный комитет национальной безопасности КР (ГКНБ КР)** возложены обязанности:

- осуществлять государственный контроль за исполнением требований при обеспечении криптографической и инженерно-технической безопасности информационно-телекоммуникационных систем, систем шифрованной, засекреченной и иных видов специальной связи;

- осуществлять контроль за соблюдением режима секретности при обращении с шифрованной информацией в шифровальных подразделениях государственных органов и организаций на территории Кыргызской Республики и в ее учреждениях, находящихся за ее пределами, а также контроль за обеспечением защиты особо важных объектов (помещений) и находящихся в них технических средств от утечки информации по техническим каналам;

- осуществлять контроль и выдачу разрешений на ввоз в Кыргызскую Республику и вывоз за ее пределы, транзит, а также на разработку, производство, реализацию, приобретение на территории Кыргызской Республики в порядке, установленном Правительством Кыргызской Республики шифровальных средств и нормативно-технической документации к ним.

Ввоз и вывоз шифровальных средств

Законом КР «О лицензионной разрешительной системе в КР» закреплено, что для осуществления ввоза на территорию Кыргызской Республики и вывоза из Кыргызской Республики шифровальных средств (включая шифровальную технику, части для шифровальной техники и пакеты программ для шифрования), нормативно-технической документации к шифровальным средствам (включая конструкторскую и эксплуатационную) требуется получение **разрешения**.

Шифровальные (криптографические) средства внесены в перечень товаров, ввоз/вывоз которых на/с территории Кыргызской Республики **ограничен**.

Так как контроль и выдачу разрешений на ввоз и вывоз шифровальных средств осуществляет ГКНБ КР, имеющиеся подзаконные акты, регламентирующие требования к шифровальным средствам и порядку их ввоза/вывоза, существуют под грифом «для служебного пользования».

Техническая защита информации

Функции по технической защите информации, как и криптографической защите, отнесены к полномочиям органов национальной безопасности. Регулируемые данную область нормативные акты отнесены к документам для служебного пользования, доступ к которым ограничен.

Электронная разведка (прослушка)

Условия проведения оперативно-розыскных мероприятий

Законом КР «Об оперативно-розыскной деятельности» определен следующий перечень оперативно-розыскных мероприятий:

1) опрос граждан;
2) наведение справок;
3) сбор образцов для сравнительного исследования;
4) проверочные закупки;
5) исследование предметов и документов;
6) контролируемые поставки (проверочные поставки);
7) отождествление личности;
8) обследование помещений, зданий, сооружений, участков местности и транспортных средств;
9) контроль почтовых отправлений, телеграфных и иных сообщений;
10) прослушивание и запись переговоров, производящихся по телефону и другим переговорным устройствам;
11) снятие информации с технических каналов связи;
12) создание конспиративных предприятий и организаций;
13) оперативное внедрение;
14) оперативное наблюдение;
15) оперативный эксперимент;
16) оперативная установка;
17) применение технических средств для получения сведений, не затрагивающих охраняемые законом неприкосновенность частной жизни, жилища, личной и семейной тайны, а также тайну личных вкладов и сбережений, переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений;
18) поиск технических средств незаконного снятия информации;
19) оперативный поиск в сетях и на каналах связи;
20) негласное прослушивание и запись разговоров (с использованием видео-, аудиотехники и (или) специальных технических средств);
21) получение информации о соединениях между абонентами и (или) абонентскими устройствами.

Перечень этих действий является исчерпывающим и может быть изменен или дополнен только законом.

Ввоз в Кыргызскую Республику и вывоз за ее пределы, а также разработка, производство, сертификация, реализация, приобретение и использование специальных технических средств, предназначенных для негласного получения информации, осуществляются в порядке, устанавливаемом Правительством Кыргызской Республики. Перечень видов специальных технических средств, предназначенных для негласного получения информации в процессе осуществления оперативно-розыскной деятельности, устанавливается Правительством Кыргызской Республики.

Оперативно-розыскные мероприятия, связанные с использованием сети связи, в интересах решения задач органами, наделенными правом осуществления оперативно-розыскных мероприятий, технически осуществляются органами национальной безопасности в порядке, определяемом Правительством КР.

Проведение оперативно-розыскных мероприятий, затрагивающих охраняемые законом **тайну переписки, телефонных и иных переговоров, телеграфных и иных сообщений, передаваемых по сетям электрической и почтовой связи**, допускается лишь для сбора информации о лицах, подготавливающих или покушающихся на тяжкие и особо тяжкие преступления, совершающих либо совершивших тяжкие и особо тяжкие преступления, по мотивированному постановлению одного из руководителей соответствующего органа, осуществляющего оперативно-розыскную деятельность, исключительно на основании судебного акта с последующим уведомлением надзирающего прокурора в течение 24 часов.

В случае возникновения угрозы жизни, здоровью, собственности отдельных лиц по их заявлению или с их письменного согласия разрешается **прослушивание переговоров, ведущихся с их телефонов или других переговорных устройств**, на основании постановления, утвержденного руководителем органа, осуществляющего оперативно-розыскную деятельность, с обязательным уведомлением соответствующего суда (судьи) и надзирающего прокурора и последующим получением решения суда в течение 24 часов.

Рассмотрение материалов об ограничении конституционных прав граждан **на тайну переписки, телефонных разговоров, почтовых, телефонных и иных сообщений, передаваемых по сетям электрической и почтовой связи**, при проведении оперативно-розыскных мероприятий осуществляется судом, как правило, по месту проведения таких мероприятий или по месту нахождения органа, ходатайствующего об их проведении. Указанные материалы рассматриваются судьей единолично и незамедлительно. Судья не вправе отказать в рассмотрении таких материалов в случае их представления.

Основанием для решения вопроса о проведении оперативно-розыскных мероприятий, ограничивающего конституционные права граждан, является мотивированное постановление одного из руководителей органа, осуществляющего оперативно-розыскную деятельность.

Требования к проведению оперативно-розыскных мероприятий на сетях электросвязи

Закон КР «Об электрической и почтовой связи» определяет круг обязанностей операторов связи при проведении оперативно-розыскных мероприятий на сетях связи.

Операторы связи обязаны предоставлять уполномоченным государственным органам, осуществляющим оперативно-розыскную деятельность в сетях связи, информацию о пользователях услугами связи, а также иную информацию, необходимую для выполнения возложенных на эти органы задач, обеспечивать им организационные и программно-технические возможности проведения оперативно-розыскных мероприятий во всех сетях и на каналах связи, доступ к базам данных, автоматизированным системам оператора связи в случаях, установленных законодательством Кыргызской Республики.

Операторы связи обязаны обеспечивать реализацию установленных Правительством КР **требований к сетям и средствам связи** для проведения оперативно-розыскных мероприятий, а также принимать меры по недопущению раскрытия организационных и тактических приемов проведения указанных мероприятий.

Операторы сотовой связи обязаны вести **реестр идентификационных кодов абонентских устройств**, работающих в их сети, а также в порядке, определяемом Правительством КР, осуществлять сбор и хранение в течение 3 лет данных об абонентах.

Технические требования к сетям связи, специальным техническим средствам, предназначенным для контроля и фиксации получаемых законным путем сведений/информации, передаваемой по техническим каналам связи, порядку взаимодействия при реализации функций системы оперативно-розыскных мероприятий в сетях связи, включая проработку интерфейса (технического регламента), разработку необходимого программного обеспечения, решение вопроса о соединении и каналах доступа, иные вопросы, связанные с обеспечением законности осуществления оперативно-розыскных мероприятий в сетях связи, комплексного решения всех вопросов и проблем, связанных с внедрением и функционированием системы оперативно-розыскных мероприятий в сетях связи, в соответствии с разработанными в этой сфере международными рекомендациями и техническими концепциями, а также требованиями действующего законодательства Кыргызской Республики устанавливаются Правительством Кыргызской Республики.

При проведении уполномоченными государственными органами следственных действий в сетях (на каналах) связи операторы связи оказывают этим органам содействие в соответствии с требованиями уголовно-процессуального законодательства КР.

Приостановление деятельности любых сетей и средств связи, а также оказания услуг связи юридическим и физическим лицам осуществляется операторами связи на основании мотивированного решения в письменной форме одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, в случаях, установленных законами КР.

Операторы мобильной сотовой связи обязаны приостановить работу мобильного устройства, если его международный идентификатор включен в Реестр похищенных мобильных устройств, ведущийся органами внутренних дел КР в порядке, установленном Правительством КР.

Операторы связи обязаны возобновить оказание услуг связи на основании решения суда или мотивированного решения в письменной форме одного из руководителей органа, осуществляющего оперативно-розыскную деятельность, который принял решение о приостановлении оказания услуг связи.

Расходы операторов связи, связанные с обеспечением необходимыми программно-техническими и иными средствами для проведения оперативно-розыскных мероприятий в сетях и на каналах связи, обеспечиваются **за счет средств операторов связи**.

Порядок взаимодействия операторов связи с уполномоченными государственными органами, осуществляющими оперативно-розыскную деятельность, устанавливается «Инструкцией о порядке взаимодействия операторов электросвязи и операторов мобильной сотовой связи с государственными органами Кыргызской Республики, осуществляющими оперативно-розыскную деятельность», утвержденной постановлением Правительства КР.

Борьба с киберпреступностью

Уголовным кодексом КР предусмотрена ответственность за совершение преступлений, связанных с информационными технологиями. К ним относятся:

- Создание программ для ЭВМ или внесение изменение в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами;
- Собирание сведений, составляющих коммерческую или банковскую тайну, путем похищения документов, подкупа и угроз в отношении лиц, владеющих коммерческой или банковской тайной, или их близких, перехвата информации в средствах связи, незаконного проникновения в компьютерную систему или сеть, использования специальных технических средств, а равно иным незаконным способом с целью разглашения либо использования этих сведений;

• Несанкционированное изменение международного идентификатора мобильного устройства, установленного его производителем, а равно подделка международного идентификатора мобильного устройства, совершенные из корыстных побуждений;

• Изготовление с целью сбыта или сбыт поддельных кредитных либо расчетных карт, а также иных платежных документов, не являющихся ценными бумагами;

• Нарушение тайны переписки, телефонных и иных переговоров, почтовых, телеграфных, электронных или иных сообщений граждан , либо то же деяние, совершенное лицом с использованием своего служебного положения или специальных технических средств, предназначенных для негласного получения информации, либо незаконные производство, сбыт или приобретение в целях сбыта специальных технических средств, предназначенных для негласного получения информации.

1.4 Классификация угроз "Иинформационной безопасности"

Безопасность информационных систем. Инфраструктура защиты информации. Двухуровневый подход к проверкам обеспечения безопасности информационных систем. Нисходящий принцип проверки обеспечения безопасности информации. Метод детализации обеспечения безопасности информационных систем. Применение двухуровневого подхода к проверкам информационных систем. Применение метода нисходящей пошаговой детализации в проверке. Метод нисходящей пошаговой детализации. Процесс оценки компьютерной безопасности. Эволюция управления информацией. Управление безопасностью. Служба безопасности. Процесс. Заполнение формы "сообщение об уязвимости информации и определение категории защиты". Заполнение формы "оценка последствий и угроз для деятельности".

Безопасность информационных систем

Понятие безопасности информационных систем знакомо большинству пользователей. Актуальность построения системы информационной безопасности подтверждается постоянным ростом хакерских атак, нападений на банковские, корпоративные сети и компьютеры частных пользователей. Даже устройства «Интернета вещей» несут в себе риски при несанкционированном доступе. Все это порождает особое внимание к построению систем безопасности.

- **Правовое регулирование информационной безопасности**

В основные задачи информационной безопасности установлены в Концепции информационной безопасности, принятой в качестве единой государственной стратегии борьбы с основными видами угроз. Документ, подготовленный на уровне Совета Безопасности, становится основой для разработки новых законов и подзаконных нормативных актов. Деятельность компаний в сфере защиты ИБ он не регламентирует. Если работа государственной или частной организации связана с информационными массивами, защита которых предусмотрена государственной политикой, например, с персональными данными, требования к ИБ, выбору аппаратно-программных и организационных мер защиты будут установлены рекомендациями и нормативными актами регуляторов. Для банков и организаций финансового сектора дополнительные требования разрабатывает Национальный банк.

- **Виды ИБ-угроз**

Информационная безопасность на любом уровне предполагает реализацию трех составляющих:

- конфиденциальность информации или недоступность ее третьим лицам;
- целостность или отсутствие искажений или подмены;
- доступность или постоянная возможность для пользователя иметь доступ к нужным ему данным.

Хакеры могут быть заинтересованы в разрушении любой из этих составляющих в зависимости от целей, которые будут разными у организатора бизнес-шпионажа, злоумышленника, похищающего

номера банковских карт, и иностранного государства, поставившего целью дезорганизовать систему управления противника с применением информационных технологий.

В зависимости от уровня сетей ранжируется и модель угроз. В Концепции информационной безопасности описываются основные типы угроз, стоящие перед государством, а значит, и перед обществом и бизнесом. Это:

- деятельность иностранных технических разведок, способных подорвать безопасность государства;
- международный терроризм, посягающий на информационные системы разных уровней;
- слабость национального кадрового потенциала, призванного решать задачи защиты ИС, и программного обеспечения.

Документ предлагает целостную систему защиты от рисков высшего уровня.

На частном уровне виды угроз конкретизируются. В различных исследованиях называются системные проблемы безопасности информационных систем:

- манипулирование доступом во внутреннее информационное пространство;
- кражи информации из корпоративных сетей и баз данных;
- изменение информации, подлоги документов в электронном виде;
- промышленный шпионаж;
- кражи средств с банковских счетов;
- вирусные угрозы.

Уязвимость программного обеспечения, наличие незадекларированных возможностей позволяют использовать различные способы взлома баз данных. На национальном уровне все чаще преимущество отдается российскому ПО, разрабатываемому с учетом актуальных угроз и не содержащему НД.

- **Составляющие информационной безопасности**

Компания, желающая выстроить эффективную систему информационной безопасности, должна учитывать нарастание степени рисков. Постоянно растет уровень технологий, направленных на совершение нарушений в сфере ИБ, при этом падает квалификация исполнителей. Сейчас выстраивание системы ботнетов, организующих DDoS-атаки, способно обрушить ИС не самого защищенного уровня, а пользование ими доступно школьнику. Риски становятся не единичными, а массовыми, любой интернет-магазин, чья продукция не понравилась покупателю, рискует стать жертвой атаки.

Компания, желающая реализовать целостную концепцию безопасности информационных систем, должна использовать не менее трех уровней защиты:

- административный, предполагающий принятие локальных нормативных актов компании, регулирующих общий подход к задаче, например, называющих ответственное подразделение или утверждающих бюджеты и стратегии;
- организационный, на котором принимаются методики, определяющие частные задачи, например, перечень лиц с различным уровнем допуска к данным;
- технический, где принимаются и реализуются программные и аппаратные решения.

Реализуя эти меры, организация достигает следующих целей:

- защита интеллектуальной собственности и коммерческой тайны компании;
- выполнение требования законодательства о безопасности персональных данных;
- защита информационных ресурсов компании;

- эффективное использование ресурсов организации для решения задач безопасности информационных систем.

Экономия ресурсов становится ключевой задачей для компании. Так, РЖД может позволить себе создавать собственную сеть коммуникаций, Intranet, уровень защищенности которой снимает большинство рисков. Небольшая организация пользуется исключительно Интернетом, неся все последствия, связанные с незащищенностью систем общего доступа.

- **Построение системы ИБ**

Строя работающую структуру безопасности информационных систем, организация должна начать с разработки, которая поможет оптимизировать и систематизировать выбранные меры и средства. Базой для ее построения становятся ответы на вопросы:

- надо ли защищаться чем-то, помимо штатных средств, и какие информационные массивы следует защищать;
- от кого надо защищаться, кто наиболее заинтересован во взломе системы безопасности;
- от чего, от какого типа угроз надо защищаться;
- как надо защищаться, какими средствами и с применением каких технологий, нужно ли применять ПО, сертифицированное для определенных целей;
- что, какие меры и кадровые ресурсы обеспечат эффективность защиты;
- какие финансовые средства необходимы для разработки, внедрения, эксплуатации, сопровождения, обновления и развития систем защиты.

- **Надо ли защищаться и что защищать**

В простых ситуациях, для маленьких компаний задачу безопасности ИС решают штатные средства защиты, встроенные в операционные системы. Это брандмауэры, антивирусы, программы фильтрации электронной почты. Но НИИ окажется заинтересован в сохранности своих архивов от несанкционированного доступа, медицинскому учреждению нужно обеспечить защиту персональных данных клиентов, провайдер интернет-услуг озадачен постоянной доступностью сервера. Модель угроз готовится каждой организацией исходя из того, какие ее информационные ресурсы интересуют злоумышленника.

Вторым шагом станет решение задачи, от какого типа угроз следует защищаться. Необходимо предложить меры, способные:
снять риск нарушения функционирования информационного пространства путем исключения воздействия на информационные системы;
обеспечить защиту от несанкционированного доступа к информации путем обнаружения и ликвидации попыток использования ресурсов информационного пространства, приводящих к нарушению его целостности;

- оберечь от разрушения встраиваемых средств защиты с возможностью доказательства неправомочности действий пользователей и обслуживающего персонала;
- выстроить схему защиты от внедрения вирусов и закладок (незадекларированных возможностей) в программные продукты и технические средства.

- **От кого необходимо защищаться**

Модель угроз окажется индивидуальной в каждом случае. По мнению ИТ-специалистов большинства организаций, основная опасность исходит от хакеров или внешних злоумышленников. И действительно, большинство зафиксированных инцидентов происходит от того, что на информационные системы производятся атаки с внешних ресурсов. И такие риски угрожают не только конфиденциальности информации, они происходят редко и с четко поставленными целями пиара и демонстрации возможностей хакерских группировок. Большая угроза связана с тем, что внешние

злоумышленники нападают на системы управления предприятий, организаций ЖКХ, сайты государственных структур с целью дестабилизации систем управления. Внешние угрозы характерны для банковской сферы, где происходят попытки воровства денег со счетов граждан. Массовые вирусные атаки также носят внешний характер, и их целью становится вымогательство средств за разблокировку ресурса, доступность которого утрачена. Любая информационная система в целях безопасности должна иметь один или несколько встроенных модулей защиты от угроз этого рода.

Но с точки зрения хищения внутренней корпоративной информации или обрабатываемых персональных данных гораздо опаснее оказываются сотрудники. В 70-80 % случаев, как показывают исследования, утечки организовывают сотрудники компании. Существует несколько психологических типов нарушителей:

- работники, недовольные организацией или руководством и желающие нанести ущерб ее интересам;
- сотрудники, финансово заинтересованные в предоставлении информации конкурентам, обычно руководители разных уровней;
- сотрудники, имеющие доступ к персональным данным или иной имеющей ценность в даркнете информации, мотивированные финансовым предложением посредников;
- не задумывающиеся о неправомерности своих действий работники, которые передают данные друзьям или знакомым по их запросам, иногда без финансовой мотивации.

Во многих случаях возможность организации утечки остается у сотрудника и после увольнения, если он сумел сохранить право на удаленный доступ к корпоративной системе. Часто служба информационной безопасности недооценивает эту степень риска. Наибольшую опасность представляет персонал ИТ-подразделений, имеющий доступ ко всем учетным записям и базам данных и способный не только похитить информацию, но и скрыть сведения о своих неправомерных шагах в системе. Даже если настроен аудит действий пользователей, большинство программных продуктов дают возможность затереть их следы в журналах регистрации.

Степень риска невозможно оценить в финансовом отношении, так как большинство компаний и банков, исходя из необходимости сохранения деловой репутации, оставляют в тайне данные о хищении ценной информации, имеющей отношение к клиентам. Чаще всего вскрытие таких инцидентов происходит случайно. В США факт утраты данных клиентов может привести к наложению многомиллионных штрафов на компанию, это служит дополнительной причиной молчания. Утрата конфиденциальных данных говорит о том, что фирма мало времени или средств уделяла работе с персоналом, позволила не менять пароли или иметь несанкционированный доступ к чужим учетным записям, а это значит, что она недостаточно заботится о клиентах.

Часто штатные средства обеспечения безопасности информационных систем не дают возможности разграничить доступ к данным различной степени конфиденциальности на уровне программных средств. Именно этот риск выявился при первом выходе на рынок Windows XP с поддержкой в ней технологии универсальной последовательной шины доступа (Universal Serial Bus, USB). После выявления уязвимости предложенный пользователям вариант обновления Service Pack 2 для Windows XP с множеством улучшений подсистемы безопасности не смог предложить средств разграничения доступа к портам USB и FireWire. Точно так же штатная система аудита действий пользователей, содержащаяся в Windows, не позволяет проводить эффективный поиск по операциям, совершаемым пользователями, и не исключает рисков того, что данные журналов регистрации действий будут удалены системными администраторами.

Эти ситуации приводят к необходимости разрабатывать структуру безопасности, индивидуальную для каждой организации и учитывающую заявленные в модели угроз риски. Возникает необходимость приобретения более сложных, чем встроенные в операционные системы, продуктов безопасности. Часто решением для снятия рисков со стороны инсайдеров становится установка DLP-системы, комплексно решающей задачи организации утечек данных со стороны персонала.

- **От чего защищаться с точки зрения внешних угроз**

При разработке архитектуры системы информационной безопасности необходимо предусмотреть способы защиты, которые минимизируют риски наиболее массовых проблем – вирусов и спама. Решается эта задача установкой:

- сетевых экранов (файрволов);
- антивирусов;
- программ фильтрации электронной почты.

Но если пользователь ненамеренно откроет вложение, содержащее вирус и пришедшее по почте от знакомого корреспондента или от того, чей адрес покажется знакомым, вирус или троянский конь сможет подорвать безопасность всей ИС. Поэтому основными задачами окажутся обучение и подготовка пользователей, установка программных средств, обеспечивающих защиту от непреднамеренных ошибок.

- **Как выстраивать систему безопасности**

Часто руководители, информированные о существовании угроз, идут на поводу у сотрудников ИТ-подразделений и без анализа эффективности приобретают популярные программные продукты. Они не анализируют реальное соответствие предложенного ПО задачам организации.

Построение обоснованной стратегии поможет выбрать и внедрить программные продукты, которые будут соответствовать реальному уровню угроз. Это в наибольшей степени отвечает задачам экономической безопасности, так как затраты окажутся соответствующими угрозам, и компания не понесет дополнительного ущерба из-за неэффективности внедренного ПО.

Но выбор программного обеспечения не единственная задача. Без разработки системы организационных мероприятий ПО окажется бесполезным. Не только исходя из требований регулятора по защите персональных данных, но и опираясь на логику защиты сведений, необходимо определить:

- степени и группы защищаемой информации;
- лиц, ответственных за ее защиту и имеющих права доступа к ней.

В дальнейшем определение этих двух групп позволит соотнести уже на программном уровне, выстраивая степени дифференциации доступа, модель ограничения прав на работу с данными. Такая система выстраивается сначала на уровне принятия локального нормативного акта, далее на уровне программных решений. Но этого недостаточно. В компании необходимо принять и разработать такие документы, как:

1. Политика безопасности по работе с информацией.

2. Правила работы с Интернетом и внешней электронной почтой.

3. Правила обращения с носителями информации, порядок контроля их использования.

4. Правила обращения с бумажными документами, их сохранностью.

В ряде случаев необходимым становится контроль использования систем копирования, принтеров и ксероксов. В каждом из этих случаев современные программные решения позволяют минимизировать риск утечки информации на бумажных носителях. Для операторов персональных данных важны подготовка политики обработки ПД и размещение ее в открытом доступе.

Но чисто технических решений недостаточно, нужно внедрить работающий механизм привлечения нарушителя к ответственности. Для этого необходимо:

- издать в компании приказ о введении режима защиты коммерческой тайны, ознакомить с ним сотрудников;
- разработать перечень информационных ресурсов, относящихся к коммерческой тайне, включив в него персональные данные;
- внести в трудовые договоры с персоналом условие об ответственности за сохранность коммерческой тайны.

При реализации правового механизма обеспечения безопасности информационных систем любой случай преднамеренной или непреднамеренной утечки данных окажется основанием для проведения служебного расследования или привлечения правоохранительных органов. Виновный не только понесет дисциплинарную ответственность, вплоть до увольнения, но и будет обязан возместить причиненный ущерб, а в критичных случаях даже будет привлечен к уголовной ответственности. Убежденность персонала в том, что при любой попытке похитить информацию любой сотрудник понесет наказание, в большинстве случаев снижает степень риска. А если сотрудники будут знать, что все их действия в пределах информационного периметра компании отслеживаются, уровень безопасности информационной системы повысится дополнительно.

- **Технические средства защиты**

Средства контроля за действиями персонала, способные блокировать любые попытки вывести данные за пределы организации, такие как DLP-системы, являются очевидным, но доступным не для всех организаций решением. Но ограничиваться ими нельзя, особенно в ситуации, когда существует риск внешних атак. Потребуются мощные технические средства, например, маршрутизаторы, их установка снизит расходы на брандмауэры.

Программное обеспечение, используемое для сохранения безопасности, должно соответствовать требованиям ФСТЭК РФ, криптографические средства защиты информации должны отвечать рекомендациям ФСБ. Простое шифрование исходящего трафика снимает риски перехвата данных.

Вся концепция работы с безопасностью информационных систем должна соответствовать требованиям регуляторов, а в ряде случаев и превосходить их, так как иногда разрабатываемые рекомендации не отвечают растущему уровню угроз.

Безопасность информационной системы

Безопасность информационной системы — свойство, заключающееся в способности системы обеспечить конфиденциальность и целостность информации.

Угрозы информационным системам можно объединить в следующие группы:

- угроза раскрытия информации;
- угроза нарушения целостности — умышленное несанкционированное или неумышленное изменение (удаление) данных, хранящихся в вычислительной системе или передаваемых из одной системы в другую;
- угроза отказа в обслуживании — блокировка доступа к некоторому ресурсу вычислительной системы.

По природе возникновения угрозы можно разделить на естественные и искусственные.

Естественные угрозы — это угрозы, связанные с воздействиями на ИС объективных физических процессов или природных явлений. Искусственные угрозы — это угрозы информационной системе, связанные с деятельностью человека.

Пользователем ИС могут быть осуществлены следующие непреднамеренные действия, представляющие угрозу безопасности информационной системы:

- доведение до состояния частичного или полного отказа системы, разрушение аппаратных, программных, информационных ресурсов системы (порча оборудования, носителей информации, удаление, искажение файлов с важной информацией или программ, в том числе системных, и т. п.);
- неправомерное включение оборудования или изменение режимов работы устройств и программ;

- запуск сервисных программ, способных при некомпетентном использовании вызывать потерю работоспособности системы или необратимые изменения в системе;
- нелегальное внедрение и использование неучтенных программ, не являющихся необходимыми для выполнения служебных обязанностей, с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти внешних носителей);
- заражение компьютера вирусами;
- разглашение конфиденциальной информации;
- разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т. п.);
- игнорирование организационных ограничений;
- некомпетентное использование, настройка или неправомерное отключение средств защиты информации;
- пересылка данных по ошибочному адресу абонента (устройства);
- ввод ошибочных данных;
- повреждение каналов связи.

Пользователем ИС могут быть осуществлены следующие преднамеренные действия, представляющие угрозу безопасности информационной системы:

- физическое разрушение системы или вывод из строя наиболее важных ее компонентов;
- отключение или вывод из строя подсистем обеспечения функционирования вычислительных систем (электропитания, охлаждения и вентиляции, линий связи и т. п.);
- дезорганизация функционирования системы (изменение режимов работы устройств или программ, создание мощных активных радиопомех и т. п.);
- внедрение агентов в число персонала (в том числе и в службу безопасности), вербовка персонала или отдельных пользователей, имеющих определенные полномочия;
- применение подслушивающих устройств, дистанционная фото и видеосъемка и т. п.;
- перехват побочных электромагнитных, акустических и других излучений устройств и линий связи, а также наводка активных излучений на вспомогательные технические средства, непосредственно не участвующие в обработке информации (телефонные линии, сети питания, отопления и т. п.);
- перехват данных, передаваемых по каналам связи, и их анализ с целью осуществления попыток проникновения в систему;
- хищение носителей информации;
- несанкционированное копирование носителей информации;
- хищение производственных отходов (распечаток, записей, списанных носителей информации и т. п.);
- чтение остатков информации из оперативной памяти и с внешних запоминающих устройств, чтение информации из областей оперативной памяти, используемых операционной системой;
- незаконное получение паролей и других реквизитов разграничения доступа (агентурным путем, используя халатность пользователей, путем подбора, имитации интерфейса системы и т. п.) с последующей маскировкой под зарегистрированного пользователя;
- несанкционированное использование терминалов пользователей, имеющих уникальные физические характеристики;
- вскрытие шифров криптозащиты информации;
- внедрение аппаратных спецвложений, программ "закладок" и "троянских коней".

Следует заметить, что чаще всего для достижения поставленной цели злоумышленник использует не один способ, а их некоторую совокупность.

Формализованное описание или представления комплекса возможностей нарушителя по реализации тех или иных угроз безопасности информации называют моделью нарушителя.

При разработке модели нарушителя делаются предположения:

- о категориях лиц, к которым может принадлежать нарушитель;
- о мотивах действий нарушителя;
- о квалификации нарушителя и его технической оснащенности;
- о характере возможных действий нарушителя.

По отношению к ИС нарушители могут быть внутренними (из числа персонала системы) или внешними (посторонними лицами). Внутренними нарушителями могут быть лица из следующих категорий персонала:

- пользователи системы;

- персонал, обслуживающий технические средства (инженеры, техники);
- сотрудники отделов разработки и сопровождения программного обеспечения (прикладные и системные программисты);
- технический персонал, обслуживающий здание (уборщики, электрики, сантехники и другие сотрудники, имеющие доступ в здание и помещения, где расположены компоненты ИС);
- сотрудники службы безопасности ИС;
- руководители различных уровней должностной иерархии. Посторонние лица, которые могут быть внешними нарушителями:
- клиенты;
- посетители;
- представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации (энерго-, водо-, теплоснабжение и т. п.);
- представители конкурирующих организаций или лица, действующие по их заданию;
- лица, случайно или умышленно нарушившие пропускной режим (без цели нарушения безопасности ИС).

Можно выделить три основных мотива нарушений: безответственность, самоутверждение, корыстный интерес.

Нарушителей можно классифицировать по следующим признакам.

1. По уровню знаний об ИС.
2. По уровню возможностей, различают нарушителей:

- применяющих чисто агентурные методы получения сведений;
- применяющих пассивные средства (технические средства перехвата без модификации компонентов системы);
- использующих только штатные средства и недостатки систем защиты для ее преодоления, а также компактные магнитные носители информации, которые могут быть скрытно пронесены через посты охраны;
- применяющих методы и средства активного воздействия (модификация и подключение дополнительных механических средств, подключение к каналам передачи данных, внедрение программных "закладок" и использование специальных инструментальных и технологических программ).

3. По месту действия нарушители могут быть:

- не имеющие доступа на контролируемую территорию организации;
- действующие с контролируемой территории без доступа в здания и сооружения;
- действующие внутри помещений, но без доступа к техническим средствам ИС;
- действующие с рабочих мест конечных пользователей ИС;
- имеющие доступ в зону данных (баз данных, архивов и т. п.);
- имеющие доступ в зону управления средствами обеспечения безопасности ИС.

Система защиты — это совокупность специальных мер правового и административного характера, организационных мероприятий, программно-аппаратных средств защиты, а также специального персонала, предназначенных для обеспечения информационной безопасности.

Для построения эффективной системы защиты необходимо провести следующие работы:

- определить угрозы безопасности информации;
- выявить возможные каналы утечки информации и несанкционированного доступа (НСД) к данным;
- построить модель потенциального нарушителя;
- выбрать соответствующие меры, методы, механизмы и средства защиты.

Проблема создания системы защиты информации включает две задачи:

- разработка системы защиты информации;
- оценка разработанной системы защиты информации.

Вторая задача решается путем анализа технических характеристик системы с целью установления, удовлетворяет ли система защиты информации комплексу требований. Такая задача в настоящее время решается экспертным путем с помощью сертификации средств защиты информации и аттестации системы защиты информации в процессе ее внедрения.

Основное содержание методов защиты информации:

1. Создание препятствий — методы физического преграждения злоумышленнику пути к защищаемой информации (аппаратуре, носителям информации и т. д.).
2. Управление доступом — метод защиты информации регулированием использования всех ресурсов компьютерной информационной системы (элементов баз данных, программных и технических средств).

3. Защита от несанкционированного доступа к ресурсам компьютера — это комплексная проблема, подразумевающая решение следующих вопросов:

- присвоение пользователю, терминалам, программам, файлам и каналам связи уникальных имен и кодов (идентификаторов);
- выполнение процедур установления подлинности при обращениях к информационной системе, то есть проверка того, что лицо или устройство, сообщившее идентификатор, в действительности ему соответствует;
- проверка полномочий, то есть проверка права пользователя на доступ к системе или запрашиваемым данным;
- автоматическая регистрация в специальном журнале всех как удовлетворенных, так и отвергнутых запросов к информационным ресурсам с указанием идентификатора пользователя, терминала, времени и сущности запроса, то есть ведение аудита.

4. Маскировка — метод защиты информации путем ее криптографического закрытия.

5. Регламентация — метод защиты информации, создающий такие условия автоматизированной обработки, хранения и передачи защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму.

6. Принуждение — метод защиты, при котором пользователи и персонал системы вынуждены соблюдать правила обработки, передачи и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Рассмотренные методы обеспечения безопасности реализуются на практике за счет применения различных средств защиты, таких как технические, программные, организационные, законодательные.

Двухуровневый подход к проверкам обеспечения безопасности информационных систем

В настоящем руководстве представлен двухуровневый подход к проверкам обеспечения безопасности информационных систем. Особо подчеркивается использование здравого смысла в сопоставлении стоимости системы обеспечения безопасности, встраиваемой в систему, и важности информации, используемой этой системой.

В случае ограниченных ресурсов многих высших органов аудита последним предлагается сначала использовать не автоматизированное представление управления безопасностью информации «сверху-вниз». Переход к второму этапу, к детальному анализу, цель которого денежная оценка риска нарушения информации, осуществляется высшими органами аудита, только если руководству нужно точно оценить денежное выражение обеспечения его решений или если оцениваются конкретные технические воздействия. Оба метода включают элементы анализа рисков и управления рисками.

Нисходящий принцип проверки обеспечения безопасности информации

Метод нисходящей пошаговой детализации прост, но в то же время характеризует детальностью. С его помощью высшие органы аудита могут сделать выводы относительно рисков нарушения безопасности информационных систем, рассматриваемых в ходе проверки. Метод использует нисходящий принцип обеспечения безопасности информации, поскольку в его основе лежит точка зрения высшего руководства при определении того, какая информация является ценной для организации, каковы риски и последствия нарушения безопасности и какие рекомендации должны быть выполнены. Такой подход позволяет аудиторам сфокусировать свое внимание на ключевых информационных системах, в частности на тех, которые имеют особое значение при обеспечении безопасности.

Метод нисходящей пошаговой детализации основывается на качественных оценках риска возможных угроз и степени их последствий. Внимание фокусируется на оценке важности информации или данных, передаваемых через информационные системы, для руководства, а не столько на важности собственно технологии. Для каждой информационной системы сначала индивидуально оцениваются важность информации для организации, угрозы и возможные последствия, а затем в целом определяется глобальная степень опасности. Такие оценки являются субъективными и обычно выражаются в терминах высокий, средний и низкий уровень риска, последствий и незащищенности.

Исходя из этих оценок, руководство получает рекомендации о дальнейших действиях или о типе определенных средств контроля и мер обеспечения безопасности, которые следует реализовать. Данные рекомендации являются частью управления рисками.

Метод нисходящей пошаговой детализации имеет ряд преимуществ. Он простой и недорогой. Он не механизирован и может быть применен любым высшим органом аудита, в штате которого имеются сотрудники, осведомленные в вопросах средств контроля управления и информационных и компьютерных систем в целом. Внутренних кадровых ресурсов может оказаться достаточно. Нет необходимости в установке сложных пакетов программного обеспечения для сбора данных о проверяемых информационных системах, для получения обновленных и подходящих статистических данных и для выполнения очень сложных анализов и составления отчетов. В случае использования микрокомпьютера обычно достаточно пакета обработки текстов. Электронные таблицы могут помочь в составлении итоговых таблиц. Для получения большего количества преимуществ можно использовать пакеты, которые обеспечивают функциональность баз данных для сбора информации и последующего составления отчетов по результатам анализа. В предлагаемом двухуровневом подходе к проверке обеспечения безопасности информационных систем метод нисходящей пошаговой детализации рассматривается как точка принятия решения в отношении метода в целом. В зависимости от обстоятельств проверки высшие органы аудита могут быть удовлетворены результатами проверки или могут принять решение о выполнении проверки с применением более сложных процедур в областях особого значения или там, где может потребоваться для руководства привести обоснование введения специальных или дорогостоящих мер обеспечения безопасности.

Метод детализации обеспечения безопасности информационных систем

Методики детализации, используемые на втором уровне подхода, предлагаемого высшим органам аудита, представляют собой анализ и управление рисками хорошо известного типа, основанные на подробном и количественном анализе имущества/ресурсов информационных систем. При их помощи измеряются в чисто денежном выражении последствия рисков нарушения безопасности и внедрения контрмер. Производители по всему миру продают различные пакеты анализа безопасности, которые обеспечивают реализацию такого подхода.

Количественные методы анализа обеспечения безопасности обычно доступны вместе с программным обеспечением микрокомпьютера для аудитора, поскольку ввод данных, расчет рисков нарушения безопасности и составление отчетности по проекту могут на практике оказаться длительным и трудоемким процессом. Такие пакеты управления рисками предоставляются поставщиками вместе с экспертной поддержкой и программой обучения пользователей работе с методом. В третьем томе Руководства описывается неавтоматизированная версия метода детализации обеспечения безопасности информации. Задача тома заключается в том, чтобы познакомить высшие органы аудита с методом, который лучше всего используется при поддержке автоматизированного пакета программного обеспечения.

По сравнению с методом нисходящей пошаговой детализации количественный анализ обеспечения безопасности оценивает в денежном выражении подробно и структурировано все имущество/ресурсы и все возможные угрозы и последствия в отношении информационных систем, находящихся в распоряжении организации. Посредством проведения интервью и опросов выполняется оценка возможных последствий для информации пользователями по шкале от одного до десяти в зависимости от серьезности таких последствий. Затем

рассчитываются показатели ожидаемого ущерба за год путем сложения расходов на замену имущества/ресурсов, вероятностей угроз и весовых коэффициентов последствий.

Большинство методов, имеющихся на рынке, относятся ко второму уровню и отличаются друг от друга способом получения значений вероятностей, расходов и определения показателей ожидаемого ущерба за год. Другие различия могут заключаться в удобстве метода для пользователя и типе поддержки, предоставляемой производителем. Указанный двухуровневый подход занимается некоторыми проблемами.

Применение количественных методов анализа и управления рисками требует изменение таблиц статистических данных рисков и стоимости имущества/ресурсов применительно к обстоятельствам каждой отдельно взятой страны.

Как применяется двухуровневый подход к проверкам информационных систем

Планирование. Планирование проверки обеспечения безопасности является ключом к успеху. Оно должно охватывать следующие основные элементы:

- Знание клиента и среды;

- Пределы проведения проверки: какие информационные системы, какие логические, физические или географические границы?

- Доступные ресурсы: квалифицированный персонал или консультанты, бюджет, сроки;

- Наличие надежных статистических данных об угрозах и показателей стоимости, соответствующих для местных условий; при необходимости, корректировка значений по умолчанию;

- Требования к отчетности: пользователи отчета, обстоятельства проверки (ежегодный отчет, специальный отчет, внутренний, внешний и т.д.), тип необходимых рекомендаций;

- Метод проверки: метод нисходящей пошаговой детализации, подробный анализ или использование обоих методов

Раздел 2. КОМПЬЮТЕРНЫЕ ВИРУСЫ И ЗАЩИТА ОТ НИХ

2.1. Вирусы как угроза информационной безопасности

Компьютерные вирусы и вредоносное ПО. Характерные черты компьютерных вирусов. Классификация вирусов по среде обитания. Классификация вирусов по способу действия. Классификация вирусов по степени влияния. Классификация антивирусных средств.

Компьютерные вирусы и вредоносное ПО

Пользователи компьютеров Windows и Mac, смартфонов и планшетов находятся под постоянно растущей угрозой, исходящей от компьютерных вирусов и вредоносных программ. Принятие мер означает понимание того, с чем вы столкнулись. Рассмотрим основные типы вредоносных программ и их последствия.

Краткий обзор

Термин «вредоносное ПО» используется для описания любой вредоносной программы на компьютере или мобильном устройстве. Эти программы устанавливаются без согласия пользователей и могут вызывать ряд неприятных последствий, таких как снижение производительности компьютера,

извлечение из системы персональных данных пользователя, удаление данных или даже воздействие на работу аппаратных средств компьютера. Поскольку киберпреступники придумывают все более сложные способы проникновения в системы пользователей, рынок вредоносных программ существенно расширился. Давайте рассмотрим некоторые из наиболее распространенных типов вредоносных программ, которые можно встретить в интернете.

1. Вирусы

Компьютерные вирусы получили свое название за способность «заражать» множество файлов на компьютере. Они распространяются и на другие машины, когда зараженные файлы отправляются по электронной почте или переносятся пользователями на физических носителях, например, на USB-накопителях или (раньше) на дискетах. По данным Национального института стандартов и технологий (NIST), первый компьютерный вирус под названием «Brain» был написан в 1986 году двумя братьями с целью наказать пиратов, ворующих ПО у компании. Вирус заражал загрузочный сектор дискет и передавался на другие компьютеры через скопированные зараженные дискеты.

2. Черви

В отличие от вирусов, червям для распространения не требуются вмешательства человека: они заражают один компьютер, а затем через компьютерные сети распространяются на другие машины без участия их владельцев. Используя уязвимости сети, например, недостатки в почтовых программах, черви могут отправлять тысячи своих копий и заражать все новые системы, и затем процесс начинается снова. Помимо того, что многие черви просто «съедают» системные ресурсы, снижая тем самым производительность компьютера, большинство из них теперь содержит вредоносные «составляющие», предназначенные для кражи или удаления файлов.

3. Рекламное ПО

Одним из наиболее распространенных типов вредоносных программ является рекламное ПО. Программы автоматически доставляют рекламные объявления на хост-компьютеры. Среди разновидностей Adware - всплывающие рекламные объявления на веб-страницах и реклама, входящая в состав «бесплатного» ПО. Некоторые рекламные программы относительно безвредны, в других используются инструменты отслеживания для сбора информации о вашем местонахождении или истории посещения сайтов и вывода целевых объявлений на экран вашего компьютера. BetaNews сообщил об обнаружении нового типа рекламного ПО, который может отключить антивирусную защиту. Поскольку Adware устанавливается с согласия пользователя, такие программы нельзя назвать вредоносными: обычно они идентифицируются как «потенциально нежелательные программы».

4. Шпионское ПО

Шпионское ПО делает то, что предполагает его название - следит за вашими действиями на компьютере. Оно собирает информацию (например, регистрирует нажатия клавиш на клавиатуре вашего компьютера, отслеживает, какие сайты вы посещаете и даже перехватывает ваши регистрационные данные), которая затем отправляется третьим лицам, как правило, киберпреступникам. Оно также может изменять определенные параметры защиты на вашем компьютере или препятствовать сетевым соединениям. Как пишет TechEye, новые типы шпионских программ позволяют злоумышленникам отслеживать поведение пользователей (естественно, без их согласия) на разных устройствах.

5. Программы-вымогатели

Программы-вымогатели заражают ваш компьютер, затем шифруют конфиденциальные данные, например, личные документы или фотографии, и требуют выкуп за их расшифровку. Если вы отказываетесь платить, данные удаляются. Некоторые типы программ-вымогателей могут полностью заблокировать доступ к вашему компьютеру. Они могут выдавать свои действия за работу правоохранительных органов и обвинить вас в каких-либо противоправных поступках. В июне 2015 года в Центр приёма жалоб на мошенничество в Интернете при ФБР обратились пользователи, сообщившие о финансовых потерях на общую сумму 18 000 000 долларов в результате деятельности вируса-вымогателя CryptoWall.

6. Боты

Боты - это программы, предназначенные для автоматического выполнения определенных операций. Они могут использоваться для легитимных целей, но злоумышленники приспособили их для своих вредоносных целей. Проникнув в компьютер, боты могут заставить его выполнять определенные команды без одобрения или вообще без ведома пользователя. Хакеры могут также пытаться заразить несколько компьютеров одним и тем же ботом, чтобы создать бот-сеть, которая затем будет использоваться для удаленного управления взломанными машинами - красть конфиденциальные данные, следить за действиями жертвы, автоматически распространять спам или запускать разрушительные DDoS-атаки в компьютерных сетях.

7. Руткиты

Руткиты позволяют третьей стороне получать удаленный доступ к компьютеру и управлять им. Эти программы используются IT-специалистами для дистанционного устранения сетевых проблем. Но в руках злоумышленников они превращаются в инструмент мошенничества: проникнув в ваш компьютер, руткиты обеспечивают киберпреступникам возможность получить контроль над ним и похитить ваши данные или установить другие вредоносные программы. Руткиты умеют качественно маскировать свое присутствие в системе, чтобы оставаться незамеченными как можно дольше. Обнаружение такого вредоносного кода требует ручного мониторинга необычного поведения, а также регулярного внесения корректировок в программное обеспечение и операционную систему для исключения потенциальных маршрутов заражения.

8. Троянские программы

Более известные как троянцы, эти программы маскируются под легитимные файлы или ПО. После скачивания и установки они вносят изменения в систему и осуществляют вредоносную деятельность без ведома или согласия жертвы.

9. Баги

Баги - ошибки в фрагментах программного кода - это не тип вредоносного ПО, а именно ошибки, допущенные программистом. Они могут иметь пагубные последствия для вашего компьютера, такие как остановка, сбой или снижение производительности. В то же время баги в системе безопасности - это легкий способ для злоумышленников обойти защиту и заразить вашу машину. Обеспечение более эффективного контроля безопасности на стороне разработчика помогает устранить ошибки, но важно также регулярного проводить программные корректировки, направленные на устранение конкретных багов.

Мифы и факты

Существует ряд распространенных мифов, связанных с компьютерными вирусами:

- **Любое сообщение об ошибке компьютера указывает на заражение вирусом.** Это неверно: сообщения об ошибках также могут быть вызваны ошибками аппаратного или программного обеспечения.
- **Вирусам и червям всегда требуется взаимодействие с пользователем.** Это не так. Для того чтобы вирус заразил компьютер, должен быть исполнен код, но это не требует участия пользователя. Например, сетевой червь может заражать компьютеры пользователей автоматически, если на них имеются определенные уязвимости.
- **Вложения к электронным письмам от известных отправителей являются безопасными.** Это не так, потому что эти вложения могут быть заражены вирусом и использоваться для распространения заражения. Даже если вы знаете отправителя, не открывайте ничего, что в чем вы не уверены.
- **Антивирусные программы могут предотвратить заражение.** Со своей стороны, поставщики антивирусного ПО делают все возможное, чтобы не отставать от разработчиков вредоносных программ, но пользователям обязательно следует установить на своем компьютере комплексное защитное решение класса Internet security, который включает в себя технологии, специально предназначенные для активного блокирования угроз. Даже при том, что 100-процентной защиты не

существует. Нужно просто осознанно подходить к обеспечению собственной онлайн-безопасности, чтобы уменьшить риск подвергнуться атаке.

- **Вирусы могут нанести физический ущерб вашему компьютеру.** Что если вредоносный код приведет к перегреву компьютера или уничтожит критически важные микрочипы? Поставщики защитных решений неоднократно развенчивали этот миф - такие повреждения просто невозможны.

Между тем, рост количества устройств взаимодействующих друг с другом в Интернете Вещей (IoT), открывает дополнительные интересные возможности: что если зараженный автомобиль съедет с дороги, или зараженная «умная» печь продолжит нагреваться, пока не случится превышение нормальной нагрузки? Вредоносного ПО будущего может сделать такой физический ущерб реальностью.

У пользователей есть ряд неправильных представлений о вредоносных программах: например, многие считают, что признаки заражения всегда заметны и поэтому они смогут определить, что их компьютер заражен. Однако, как правило, вредоносное ПО не оставляет следов, и ваша система не будет показывать каких-либо признаков заражения.

Tweet: Как правило, вредоносное ПО не оставляет следов, и ваша система не будет показывать каких-либо признаков заражения. Твитни это!

Так же не стоит верить, что все сайты с хорошей репутацией безопасны. Они также могут быть взломаны киберпреступниками. А посещение зараженного вредоносным кодом легитимного сайта – еще большая вероятность для пользователя расстаться со своей личной информацией. Именно это, как пишет SecurityWeek, произошло с Всемирным банком. Также многие пользователи считают, что их личные данные - фотографии, документы и файлы - не представляют интереса для создателей вредоносных программ. Киберпреступники же используют общедоступные данные для того, чтобы атаковать отдельных пользователей, или собрать информацию, которая поможет им создать фишинговые письма, чтобы проникнуть во внутренние сети организаций.

1. Стандартные методы заражения

Итак, как же происходит заражение компьютерными вирусами или вредоносными программами? Существует несколько стандартных способов. Это ссылки на вредоносные сайты в электронной почте или сообщениях в социальных сетях, посещение зараженного сайта (известного как drive-by загрузка) и использование зараженного USB-накопителя на вашем компьютере. Уязвимости операционной системы и приложений позволяют злоумышленникам устанавливать вредоносное ПО на компьютеры. Поэтому для снижения риска заражения очень важно устанавливать обновления для систем безопасности, как только они становятся доступными.

Киберпреступники часто используют методы социальной инженерии, чтобы обманом заставить вас делать что-то, что угрожает вашей безопасности или безопасности вашей компании. Фишинговые сообщения являются одним из наиболее распространенных методов. Вы получаете на вид абсолютно легитимное электронное сообщение, в котором вас убеждают загрузить зараженный файл или посетить вредоносный веб-сайт. Цель хакеров - написать сообщение так, чтобы вы нашли его убедительным. Это может быть, например, предупреждение о возможном вирусном заражении или уведомление из вашего банка или сообщение от старого друга.

Конфиденциальные данные, такие как пароли, являются главной целью киберпреступников. Помимо использования вредоносных программ для перехвата паролей в момент их ввода, злоумышленники также могут собирать пароли с веб-сайтов и других компьютеров, которые они взломали. Вот почему так важно использовать уникальный и сложный пароль для каждой учетной записи. Он должен состоять из 15 и более символов, включающих буквы, цифры и специальные символы. Таким образом, если киберпреступникам удастся взломать один аккаунт, они не получат доступ ко всем вашим учетным записям. К сожалению, большинство пользователей имеют очень слабые пароли: вместо того, чтобы придумать труднодоступную комбинацию, они обращаются к standby-паролям типа «123456» или «Password123», которые преступники легко подбирают. Даже контрольные вопросы не всегда могут служить эффективной защитой, потому что многие люди дают один и тот же ответ на вопрос «Ваше любимая еда?», например, если вы находитесь в Соединенных Штатах, то почти наверняка ответ будет - «Пицца».

2. Признаки заражения

Хотя большинство вредоносных программ не оставляет никаких явных следов, и ваш компьютер работает нормально, иногда все же можно заметить признаки возможного заражения. Самый первый из них - снижение производительности, т.е. процессы происходят медленные, загрузка окон занимает больше времени, в фоновом режиме работают какие-то случайные программы. Еще одним настораживающим признаком может считаться измененных домашних интернет-страниц в вашем браузере или более частое, чем обычно, появление всплывающих объявлений. В некоторых случаях вредоносное ПО даже может влиять на базовые функции компьютера: не открывается Windows, нет подключения к Интернету или доступа к более высокоуровневым функциям управления системой более высокого уровня. Если вы подозреваете, что ваш компьютер может быть заражен, немедленно произведите проверку системы. Если заражение не обнаружено, но вы все еще сомневаетесь, получите второе мнение - запустите альтернативный антивирусный сканер.

Компьютерные вирусы и их классификация

Компьютерный вирус - это специально написанная небольшая по размерам программа, имеющая специфический алгоритм, направленный на тиражирование копии программы, или её модификацию и выполнению действий развлекательного, пугающего или разрушительного характера.

Тем или иным способом вирусная программа попадает в компьютер и заражает их. Программа, внутри которой находится вирус, называется **зараженной**. Когда такая программа начинает работу, то сначала управление получает вирус. Вирус находит и заражает другие программы, а также выполняет какие-либо вредоносные действия. Например, портит файлы или таблицу размещения файлов на диске, занимает оперативную память и т.д. После того, как вирус выполнит свои действия, он передает управление той программе, в которой он находится, и она работает как обычно. Тем самым внешне работа зараженной программы выглядит так же, как и незараженной. Поэтому далеко не сразу пользователь узнаёт о присутствии вируса в машине.

Многие разновидности вирусов устроены так, что при запуске зараженной программы вирус остается в памяти компьютера и время от времени заражает программы и выполняет нежелательные действия на компьютере. Пока на компьютере заражено относительно мало программ, наличие вируса может быть практически незаметным.

К числу наиболее характерных **признаков заражения компьютера вирусами** относятся следующие:

- некоторые ранее исполнявшиеся программы перестают запускаться или внезапно останавливаются в процессе работы;

- увеличивается длина исполняемых файлов;
- быстро сокращается объём свободной дисковой памяти;
- на носителях появляются дополнительные сбойные кластеры, в которых вирусы прячут свои фрагменты или части повреждённых файлов;
- замедляется работа некоторых программ;
- в текстовых файлах появляются бессмысленные фрагменты;
- наблюдаются попытки записи на защищённую дискету;
- на экране появляются странные сообщения, которые раньше не наблюдались;
- появляются файлы со странными датами и временем создания (несуществующие дни несуществующих месяцев, годы из следующего столетия, часы, минуты и секунды, не укладывающиеся в общепринятые интервалы и т. д.);
- операционная система перестаёт загружаться с винчестера;
- появляются сообщения об отсутствии винчестера;
- данные на носителях портятся.

Любая дискета, не защищённая от записи, находясь в дисководе заражённого компьютера, может быть заражена. Дискеты, побывавшие в зараженном компьютере, являются разносчиками вирусов. Существует ещё один канал распространения вирусов, связанный с компьютерными сетями, особенно всемирной сетью Internet. Часто источниками заражения являются программные продукты, приобретённые нелегальным путем.

Существует несколько **классификаций компьютерных вирусов**:

1. **По среде обитания** различают вирусы сетевые, файловые, загрузочные и файлово-загрузочные.
2. **По способу заражения** выделяют резидентные и нерезидентные вирусы.
3. **По степени воздействия** вирусы бывают неопасные, опасные и очень опасные;
4. **По особенностям алгоритмов** вирусы делят на паразитические, репликаторы, невидимки, мутанты, троянские, макро-вирусы.

Загрузочные вирусы заражают загрузочный сектор винчестера или дискеты и загружаются каждый раз при начальной загрузке операционной системы.

Резидентные вирусы загружается в память компьютера и постоянно там находится до выключения компьютера.

Самомодифицирующиеся вирусы (мутанты) изменяют свое тело таким образом, чтобы антивирусная программа не смогла его идентифицировать.

Стелс-вирусы (невидимки) перехватывает обращения к зараженным файлам и областям и выдают их в незараженном виде.

Троянские вирусы маскируют свои действия под видом выполнения обычных приложений.

Вирусом могут быть заражены следующие объекты:

1. Исполняемые файлы, т.е. файлы с расширениями имен .com и .exe, а также оверлейные файлы, загружаемые при выполнении других программ. Вирусы, заражающие файлы, называются **файловыми.** Вирус в зараженных исполняемых файлах начинает свою работу при запуске той программы, в которой он находится. Наиболее опасны те вирусы, которые после своего запуска остаются в памяти резидентно - они могут заражать файлы и выполнять вредоносные действия до следующей перезагрузки компьютера. А если они заразят любую программу из автозапуска компьютера, то и при перезагрузке с жесткого диска вирус снова начнет свою работу.

2. Загрузчик операционной системы и главная загрузочная запись жесткого диска. Вирусы, поражающие эти области, называются **загрузочными**. Такой вирус начинает свою работу при начальной загрузке компьютера и становится резидентным, т.е. постоянно находится в памяти компьютера. Механизм распространения загрузочных вирусов - заражение загрузочных записей вставляемых в компьютер дискет. Часто такие вирусы состоят из двух частей, поскольку загрузочная запись имеет небольшие размеры и в них трудно разместить целиком программу вируса. Часть вируса располагается в другом участке диска, например, в конце корневого каталога диска или в кластере в области данных диска. Обычно такой кластер объявляется дефектным, чтобы исключить затирание вируса при записи данных на диск.

3. Файлы документов, информационные файлы баз данных, таблицы табличных процессоров и другие аналогичные файлы могут быть заражены **макро-вирусами**. Макро-вирусы используют возможность вставки в формат многих документов макрокоманд.

Если не принимать мер по защите от вирусов, то последствия заражения могут быть очень серьезными. Например, в начале 1989 г. вирусом, написанным американским студентом Моррисом, были заражены и

выведены из строя тысячи компьютеров, в том числе принадлежащих министерству обороны США. Автор вируса был приговорен судом к трем месяцам тюрьмы и штрафу в 270 тыс. дол. Наказание могло быть и более строгим, но суд учел, что вирус не портил данные, а только размножался.

Средства защиты от вирусов

Для защиты от вирусов можно использовать:

- Общие средства защиты информации, которые полезны также как страховка от физической порчи дисков, неправильно работающих программ или ошибочных действий пользователей;
- профилактические меры, позволяющие уменьшить вероятность заражения вирусом;
- специализированные программы для защиты от вирусов.

Общие средства защиты информации полезны не только для защиты от вирусов. Имеются две основные разновидности этих методов защиты:

- резервное копирование информации, т. е. создание копий файлов и системных областей дисков на дополнительном носителе;
- разграничение доступа, предотвращающее несанкционированное использование информации, в частности, защиту от изменений программ и данных вирусами, неправильно работающими программами и ошибочными действиями пользователей.

Несмотря на то, что общие средства защиты информации очень важны для защиты от вирусов, все же их одних недостаточно. Необходимо применять специализированные программы для защиты от вирусов. Эти программы можно разделить на несколько видов:

1. Программы-**детекторы** позволяют обнаруживать файлы, зараженные одним из нескольких известных вирусов.
2. Программы-**доктора**, или **фаги**, восстанавливают зараженные программы убирая из них тело вируса, т.е. программа возвращается в то состояние, в котором она находилась до заражения вирусом.
3. Программы-**ревизоры** сначала запоминают сведения о состоянии программ и системных областей дисков, а затем сравнивают их состояние с исходным. При выявлении несоответствий об этом сообщается пользователю.
4. **Доктора-ревизоры** - это гибриды ревизоров и докторов, т.е. программы, которые не только обнаруживают изменения в файлах и системных областях дисков, но и могут автоматически вернуть их в исходное состояние.
5. **Программы-фильтры** располагаются резидентно в оперативной памяти компьютера, перехватывают те обращения к операционной системе, которые используются вирусами для размножения и нанесения вреда, и сообщают о них пользователю. Пользователь может разрешить или запретить выполнение соответствующей операции.

Ни один тип антивирусных программ по отдельности не дает полной защиты от вирусов. Поэтому наилучшей стратегией защиты от вирусов является **многоуровневая защита.**

Средствами разведки в защите от вирусов являются программы-детекторы, позволяющие проверять вновь полученное программное обеспечение на наличие вирусов.

На первом уровне защиты находятся резидентные программы для защиты от вируса. Эти программы могут первыми сообщить о вирусной атаке и предотвратить заражение программ и диска.

Второй уровень защиты составляют программы-ревизоры, программы-доктора и доктора-ревизоры. Ревизоры обнаруживают нападение тогда, когда вирус сумел пройти сквозь первый уровень. Программы-доктора применяются для восстановления зараженных программ, если ее копий нет в архиве, но они не всегда лечат правильно. Доктора-ревизоры обнаруживают нападение вируса и лечат зараженные файлы, причем контролируют правильность лечения.

Третий уровень защиты - это средства разграничения доступа. Они не позволяют вирусам и неверно работающим программам, даже если они проникли в компьютер, испортить важные данные.

В **резерве** находятся архивные копии информации и эталонные диски с программными продуктами. Они позволяют восстановить информацию при ее повреждении на жестком диске.

Среди наиболее распространненых российских антивирусных пакетов следует отметить **Kaspersky Antivirus**, **DrWeb**, **Adinf**. Перечисленные средства могут оказать серьёзную помощь в обнаружении вирусов и восстановлении повреждённых файлов, однако не менее важно и соблюдение сравнительно простых **правил антивирусной безопасности.**

1. Следует избегать пользоваться нелегальными источниками получения программ. Наименее же опасен законный способ покупки фирменных продуктов.
2. Осторожно следует относиться к программам, полученным из сети Internet, так как нередки случаи заражения вирусами программ, распространяемых по электронным каналам связи.
3. Всякий раз, когда дискета побывала в чужом компьютере, необходимо проверить дискету с помощью одного или двух антивирусных средств.
4. Необходимо прислушиваться к информации о вирусных заболеваниях на компьютерах в своем районе проживания или работы и о наиболее радикальных средствах борьбы с ними. Атакам нового вируса в первую очередь подвергаются компьютеры образовательных учреждений.
5. При передаче программ или данных на своей дискете её следует обязательно защитить от записи.

Разработка политики информационной безопасности

Политика безопасности определяется как совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов.

При разработке и проведении ее в жизнь целесообразно руководствоваться следующими принципами:

1. Невозможность миновать защитные средства. Все информационные потоки в защищаемую сеть и из нее должны проходить через средства защиты. Не должно быть тайных модемных входов или тестовых линий, идущих в обход защиты.

2. Усиление самого слабого звена. Надежность любой защиты определяется самым слабым звеном, так как злоумышленники взламывать именно его. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

3. Невозможность перехода в небезопасное состояние. Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ.

4. Минимизация привилегий. Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

5. Разделение обязанностей. Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс.

6. Эшелонированность обороны. Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж. Эшелонированная оборона способна по крайней мере задержать злоумышленника и существенно затруднить незаметное выполнение вредоносных действий.

7. Разнообразие защитных средств. Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными, по возможности, несовместимыми между собой навыками.

8. Простота и управляемость информационной системы. Принцип простоты и управляемости гласит, что только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование.

9. Обеспечение всеобщей поддержки мер безопасности. Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или враждебным, то режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное теоретическое и практическое обучение.

Технические, организационные и программные средства обеспечения сохранности и защиты от несанкционированного доступа

Существует **четыре уровня защиты компьютерных и информационных ресурсов:**

Предотвращение предполагает, что только авторизованный персонал имеет доступ к защищаемой информации и технологии.

Обнаружение предполагает раннее раскрытие преступлений и злоупотреблений, даже если механизмы защиты были обойдены.

Ограничение уменьшает размер потерь, если преступление все-таки произошло, несмотря на меры по его предотвращению и обнаружению.

Восстановление обеспечивает эффективное воссоздание информации при наличии документированных и проверенных планов по восстановлению.

Меры защиты - это меры, вводимые руководством, для обеспечения безопасности информации. К мерам защиты относят разработку административных руководящих документов, установку аппаратных устройств или дополнительных программ, основной целью которых является предотвращение преступлений и злоупотреблений.

Формирование режима информационной безопасности - проблема комплексная. Меры по ее решению можно разделить на **четыре уровня**:

- **законодательный:** законы, нормативные акты, стандарты и т. п.;
- **административный:** действия общего характера, предпринимаемые руководством организации;
- **процедурный:** конкретные меры безопасности, имеющие дело с людьми;
- **программно-технический:** конкретные технические меры.

В настоящее время наиболее подробным законодательным документом России в области информационной безопасности является Уголовный кодекс. В разделе "Преступления против общественной безопасности" имеется глава "Преступления в сфере компьютерной информации". Она содержит три статьи - "Неправомерный доступ к компьютерной информации", "Создание, использование и распространение вредоносных программ для ЭВМ" и "Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети". Уголовный кодекс стоит на страже всех аспектов информационной безопасности - доступности, целостности, конфиденциальности, предусматривая наказания за "уничтожение, блокирование, модификацию и копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети".

Рассмотрим некоторые меры защиты информационной безопасности компьютерных систем.

1. Аутентификация пользователей. Данная мера требует, чтобы пользователи выполняли процедуры входа в компьютер, используя это как средство для идентификации в начале работы. Для аутентификации личности каждого пользователя нужно использовать уникальные пароли, не являющиеся комбинациями личных данных пользователей, для пользователя. Необходимо внедрить меры защиты при администрировании паролей, и ознакомить пользователей с наиболее общими ошибками, позволяющими совершиться компьютерному преступлению. Если в компьютере имеется встроенный стандартный пароль, его нужно обязательно изменить.

Еще более надёжное решение состоит в организации контроля доступа в помещения или к конкретному компьютеру сети с помощью идентификационных пластиковых карточек с встроенной микросхемой - так называемых микропроцессорных карточек (smart - card). Их надёжность обусловлена в первую очередь невозможностью копирования или подделки кустарным способом. Установка специального считывающего устройства таких карточек возможна не только на входе в помещения, где расположены компьютеры, но и непосредственно на рабочих станциях и серверах сети.

Существуют также различные устройства для идентификации личности по биометрической информации - по радужной оболочке глаза, отпечаткам пальцев, размерам кисти руки и т.д.

2. Защита пароля.

Следующие правила полезны для защиты пароля:

- нельзя делится своим паролем ни с кем;
- пароль должен быть трудно угадываемым;
- для создания пароля нужно использовать строчные и прописные буквы, а еще лучше позволить компьютеру самому сгенерировать пароль;
- не рекомендуется использовать пароль, который является адресом, псевдонимом, именем родственника, телефонным номером или чем-либо очевидным;
- предпочтительно использовать длинные пароли, так как они более безопасны, лучше всего, чтобы пароль состоял из 6 и более символов;
- пароль не должен отображаться на экране компьютера при его вводе;
- пароли должны отсутствовать в распечатках;
- нельзя записывать пароли на столе, стене или терминале, его нужно держать в памяти;
- пароль нужно периодически менять и делать это не по графику;

- на должности администратора паролей должен быть самый надежный человек;
- не рекомендуется использовать один и тот же пароль для всех сотрудников в группе;
- когда сотрудник увольняется, необходимо сменить пароль;
- сотрудники должны расписываться за получение паролей.

3. Процедуры авторизации.

В организации, имеющей дело с критическими данными, должны быть разработаны и внедрены процедуры авторизации, которые определяют, кто из пользователей должен иметь доступ к той или иной информации и приложениям.

В организации должен быть установлен такой порядок, при котором для использования компьютерных ресурсов, получения разрешения доступа к информации и приложениям, и получения пароля требуется разрешение тех или иных начальников.

Если информация обрабатывается на большом вычислительном центре, то необходимо контролировать физический доступ к вычислительной технике. Могут оказаться уместными такие методы, как журналы, замки и пропуска, а также охрана. Ответственный за информационную безопасность должен знать, кто имеет право доступа в помещения с компьютерным оборудованием и выгонять оттуда посторонних лиц.

4. Предосторожности при работе.

Рекомендуется:

- отключать неиспользуемые терминалы;
- закрывать комнаты, где находятся терминалы;
- разворачивать экраны компьютеров так, чтобы они не были видны со стороны двери, окон и прочих мест, которые не контролируются;
- установить специальное оборудование, ограничивающее число неудачных попыток доступа, или делающее обратный звонок для проверки личности пользователей, использующих телефоны для доступа к компьютеру
- использовать программы отключения терминала после определенного периода неиспользования;
- выключать систему в нерабочие часы;
- использовать системы, позволяющие после входа пользователя в систему сообщать ему время его последнего сеанса и число неудачных попыток установления сеанса после этого. Это позволит сделать пользователя составной частью системы проверки журналов.

5. Физическая безопасность.

В защищаемых компьютерных системах необходимо принимать меры по предотвращению, обнаружению и минимизации ущерба от пожара, наводнения, загрязнения окружающей среды, высоких температур и скачков напряжения.

Пожарная сигнализация и системы пожаротушения должны регулярно проверяться. ПЭВМ можно защитить с помощью кожухов, чтобы они не были повреждены системой пожаротушения. Горючие материалы не должны храниться в этих помещениях с компьютерами.

Температура в помещении может контролироваться кондиционерами и вентиляторами, а также хорошей вентиляцией в помещении. Проблемы с чрезмерно высокой температурой могут возникнуть в стойках периферийного оборудования или из-за закрытия вентиляционного отверстия в терминалах или ПЭВМ, поэтому необходима их регулярная проверка.

Желательно применение воздушных фильтров, что поможет очистить воздух от веществ, которые могут нанести вред компьютерам и дискам. Следует запретить курить, принимать пищу и пить возле ПЭВМ.

Компьютеры должны размещаться как можно дальше источников большого количества воды, например трубопроводов.

6. Защита носителей информации (исходных документов, лент, картриджей, дисков, распечаток).

Для защиты носителей информации рекомендуется:

- вести, контролировать и проверять реестры носителей информации;
- обучать пользователей правильным методам очищения и уничтожения носителей информации;
- делать метки на носителях информации, отражающие уровень критичности содержащейся в них информации;
- уничтожать носители информации в соответствии с планом организации;
- доводить все руководящие документы до сотрудников;
- хранить диски в конвертах, коробках, металлических сейфах;
- не касаться поверхностей дисков, несущих информацию
- осторожно вставлять диски в компьютер и держать их подальше от источников магнитного поля и солнечного света;

- убирать диски и ленты, с которыми в настоящий момент не ведется работа;
- хранить диски разложенными по полкам в определенном порядке;
- не давать носители информации с критической информацией неавторизованным людям;
- выбрасывать или отдавать поврежденные диски с критической информацией только после их размагничивания или аналогичной процедуры;
- уничтожать критическую информацию на дисках с помощью их размагничивания или физического разрушения в соответствии с порядком в организации;
- уничтожать распечатки и красящие ленты от принтеров с критической информацией в соответствии с порядком организации;
- обеспечить безопасность распечаток паролей и другой информации, позволяющей получить доступ к компьютеру.

7. Выбор надежного оборудования.

Производительность и отказоустойчивость информационной системы во многом зависит от работоспособности серверов. При необходимости обеспечения круглосуточной бесперебойной работы информационной системы используются специальные отказоустойчивые компьютеры, т. е. такие, выход из строя отдельного компонента которых не приводит к отказу машины.

На надежности информационных систем отрицательно сказываются и наличие устройств, собранных из комплектующих низкого качества, и использование нелицензионного ПО. Чрезмерная экономия средств на обучение персонала, закупку лицензионного ПО и качественного оборудования приводит к уменьшению времени безотказной работы и значительным затратам на последующее восстановление системы.

8. Источники бесперебойного питания.

Компьютерная система энергоемка, и потому первое условие ее функционирования - бесперебойная подача электроэнергии. Необходимой частью информационной системы должны стать источники бесперебойного питания для серверов, а по возможности, и для всех локальных рабочих станций. Рекомендуется также дублировать электропитание, используя для этого различные городские подстанции. Для кардинального решения проблемы можно установить резервные силовые линии от собственного генератора организации.

9. Разработка адекватных планов обеспечения непрерывной работы и восстановления.

Целью планов обеспечения непрерывной работы и восстановления являются гарантии того, что пользователи смогут продолжать выполнять свои самые главные обязанности в случае невозможности работы по информационной технологии. Обслуживающий персонал должен знать, как им действовать по этим планам.

Планы обеспечения непрерывной работы и восстановления (ОНРВ) должны быть написаны, проверены и регулярно доводиться до сотрудников. Процедуры плана должны быть адекватны уровню безопасности и критичности информации. План ОНРВ может применяться в условиях неразберихи и паники, поэтому нужно регулярно проводить тренировки сотрудников.

10. Резервное копирование.

Одним из ключевых моментов, обеспечивающих восстановление системы при аварии, является резервное копирование рабочих программ и данных. В локальных сетях, где установлены несколько серверов, чаще всего система резервного копирования устанавливается непосредственно в свободные слоты серверов. В крупных корпоративных сетях предпочтение отдается выделенному специализированному архивационному серверу, который автоматически архивирует информацию с жестких дисков серверов и рабочих станций в определенное время, установленное администратором сети, выдавая отчет о проведенном резервном копировании.

Для архивной информации, представляющей особую ценность, рекомендуется предусматривать охранное помещение. Дубликаты наиболее ценных данных, лучше хранить в другом здании или даже в другом городе. Последняя мера делает данные неуязвимыми в случае пожара или другого стихийного бедствия.

11. Дублирование, мультиплексирование и резервирование офисов.

Помимо резервного копирования, которое производится при возникновении внештатной ситуации либо по заранее составленному расписанию, для большей сохранности данных на жестких дисках применяют специальные технологии - зеркалирование дисков и создание RAID-массивов, которые представляют собой объединение нескольких жестких дисков. При записи информация поровну распределяется между ними, так что при выходе из строя одного из дисков находящиеся на нем данные могут быть восстановлены по содержимому остальных.

Технология кластеризации предполагает, что несколько компьютеров функционируют как единое целое. Кластеризуют, как правило, серверы. Один из серверов кластера может функционировать в режиме горячего резерва в полной готовности начать выполнять функции основной машины в случае ее выхода из строя. Продолжением технологии кластеризации является распределенная кластеризация, при которой через глобальную сеть объединяются несколько кластерных серверов, разнесенных на большое расстояние.

Распределенные кластеры близки к понятию резервных офисов, ориентированных на обеспечение жизнедеятельности предприятия при уничтожении его центрального помещения. Резервные офисы делят на холодные, в которых проведена коммуникационная разводка, но отсутствует какое-либо оборудование и горячие, которыми могут быть дублирующий вычислительный центр, получающий всю информацию из центрального офиса, филиал, офис на колесах и т.д.

12. Резервирование каналов связи.

При отсутствии связи с внешним миром и своими подразделениями, офис оказывается парализованным, потому большое значение имеет резервирование внешних и внутренних каналов связи. При резервировании рекомендуется сочетать разные виды связи - кабельные линии и радиоканалы, воздушную и подземную прокладку коммуникаций и т.д.

По мере того, как компании все больше и больше обращаются к Internet, их бизнес оказывается в серьезной зависимости от функционирования Internet-провайдера. У поставщиков доступа к Сети иногда случаются достаточно серьезные аварии, поэтому важно хранить все важные приложения во внутренней сети компании и иметь договора с несколькими местными провайдерами. Следует также заранее продумать способ оповещения стратегических клиентов об изменении электронного адреса и требовать от провайдера проведения мероприятий, обеспечивающих оперативное восстановление его услуг после аварий.

13. Защита данных от перехвата.

Для любой из трех основных технологий передачи информации существует технология перехвата: для кабельных линий - подключение к кабелю, для спутниковой связи – использование антенны приема сигнала со спутника, для радиоволн - радиоперехват. Российские службы безопасности разделяют коммуникации на три класса. Первый охватывает локальные сети, расположенные в зоне безопасности, т. е. территории с ограниченным доступом и заэкранированным электронным оборудованием и коммуникационными линиями, и не имеющие выходов в каналы связи за ее пределами. Ко второму классу относятся каналы связи вне зоны безопасности, защищенные организационно-техническими мерами, а к третьему - незащищенные каналы связи общего пользования. Применение коммуникаций уже второго класса значительно снижает вероятность перехвата данных.

Для защиты информации во внешнем канале связи используются следующие устройства: скремблеры для защиты речевой информации, шифраторы для широковещательной связи и криптографические средства, обеспечивающие шифрование цифровых данных.

Важнейшими характеристиками алгоритмов шифрования являются криптостойкость, длина ключа и скорость шифрования. В настоящее время наиболее часто применяются три основных стандарта шифрования:

- DES;
- ГОСТ 28147-89 - отечественный метод, отличающийся высокой криптостойкостью;
- RSA - система, в которой шифрование и расшифровка осуществляется с помощью разных ключей.

2.2. Классификация компьютерных вирусов

Файловые. Загрузочные. Макро. Сетевые. Файло-загрузочные. Сетевые макро-вирусы. Классификация вирусов по особенностям алгоритма работы. Резидентный. Вирусы, использующие стелс-алгоритмы. Вирусы с самошифрованием и полиморфичностью. Вирусы, использующие нестандартные приемы. Классификация компьютерных вирусов по деструктивным возможностям.

2.3.Характеристика «вирусоподобных» программ. Антивирусные программы

Виды "вирусоподобных" программ. Характеристика "вирусоподобных" программ. Утилиты скрытого администрирования.

Антивирусные программы. Особенности работы антивирусных программ. Методы защиты от вредоносных программ. Факторы, определяющие качество антивирусных программ. Антивирусное программное обеспечение. Угрозы для мобильных устройств. Классификация угроз для мобильных устройств. Защита мобильных устройств.

Практическая работа:

Производить настройки антивирусной программы, проверять различные объекты на наличие вируса.

Самостоятельная работа:

Презентация: характеристика антивирусных программ.

2.4. Профилактика компьютерных вирусов. Обнаружение неизвестного вируса

Классификация компьютерных вирусов. Классификация компьютерных вирусов по среде обитания. Классификация компьютерных вирусов по особенностям алгоритма работы. Классификация компьютерных вирусов по деструктивные возможностям.

Обнаружение неизвестного вируса. Обнаружение загрузочного вируса. Обнаружение файлового вируса. Обнаружение макровируса. Обнаружение резидентного вируса. DOS-вирусы. Вирус в области пользовательских программ. Вирус в области пользовательских программ (UMB). Windows-вирусы. Анализ алгоритма вируса. Восстановление пораженных объектов. Восстановление файлов-документов и таблиц. Восстановление загрузочных секторов.

Практическая работа:

Антивирусная защита (технология тестирования компьютера на наличие вируса и профилактические меры. Знакомство со способами лечения зараженных объектов.)

Настроить, режимы работы и сравнение различных антивирусных пакетов. Установить антивирусное программное обеспечение. Выявить компьютерные вирусы.

Самостоятельная работа:

Презентация: профилактические меры против вирусов.

Раздел 3. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВЫЧИСЛИТЕЛЬНЫХ СЕТЕЙ

3.1. Особенности обеспечения информационной безопасности в компьютерных сетях

Информационная безопасность в компьютерных сетях. Особенности обеспечения информационной безопасности в компьютерных сетях. Общие сведения о безопасности в компьютерных сетях. Целостность данных. Конфиденциальность данных. Доступность данных.

Практическая работа:

Поменять учетную запись администратора (Пользователь Администратор с пустым паролем - уязвимость).

Самостоятельная работа:

Презентация: обеспечение безопасности локальной сети.

3.2. Сетевые модели передачи данных. Адресация в глобальных сетях

Модель взаимодействия открытых систем OSI/ISO. Сравнение сетевых моделей передачи данных TSP/IP и OSI/ISO. Характеристика уровней модели OSI/ISO. Физический уровень. Канального уровень. Сетевой уровень. Маршрутизатор. Транспортный уровень. Сеансовый уровень. Представительный уровень. Прикладной уровень.

Адресация в глобальных сетях. Принципы адресации в глобальных вычислительных сетях, типы адресов и структуру IP-адреса. принципы адресации в современных вычислительных сетях. Классы адресов протокола IP и структуру IP-адреса. Иерархический принцип системы доменных имен. Преобразование двоичного IP-адреса в десятичный. Определение тип сети по IP-адресу. Основы IP-протокола. Классы адресов вычислительных сетей. Система доменных имен.

Практическая работа:

Передача данных между двумя соединенными компьютерами. Непосредственная связь двух компьютеров.

Самостоятельная работа:

Презентация: Повторитель. Концентратор.

3.3. Классификация удаленных угроз в вычислительных сетях

Классы удаленных угроз и их характеристика. Условию начала осуществления воздействия. Расположению субъекта атаки относительно атакуемого объекта. Уровни модели ISO/OSI, на котором осуществляется воздействие.

3.4. Типовые удаленные атаки и их характеристика. Причины успешной реализации удаленных угроз в вычислительных сетях

Удаленная атака "анализ сетевого трафика". Удаленная атака "подмена доверенного объекта". Удаленная атака "ложный объект". Удаленная атака "отказ в обслуживании".

Причины успешной реализации удаленных угроз «информационной безопасности» в вычислительных сетях. Анализировать причины успеха удаленных атак и принимать меры к их устранению. Причины успешной реализации удаленных угроз в вычислительных сетях. Выявление причин успеха удаленных атак является первым этапом построения защищенных вычислительных сетей.

Практическая работа:

Типовая удаленная атака «отказ в обслуживании». Отсутствие контроля за виртуальными каналами связи между объектами сети; отсутствие в распределенных вычислительных сетях возможности контроля за маршрутом сообщений; отсутствие в распределенных вычислительных сетях полной информации о ее объектах; отсутствие в распределенных вычислительных сетях криптозащиты сообщений.

Самостоятельная работа:

Презентация: удаленные угрозы «По цепи воздействия».

3.5. Принципы защиты распределенных вычислительных сетей. Идентификация и аутентификация

Принципы построения защищенных вычислительных сетей и возможные механизмы защиты. Принципы защиты распределенных вычислительных сетей. Принципы защиты для разработки и реализации механизмов защиты вычислительных селей. Концепция беспарольной идентификации. Ключи и токены вместо логинов и паролей. Структура токена. HTTP-заголовки протокола. Идентификация клиентов сайтами. Авторизация клиентов сайтами. Реализация надежного идентификатора клиентов. Авторизация на сайте глазами пользователя. Смена ключа сайта. Реализация кросс-доменной авторизации. Реализация меж-доменной идентификации. Мобильность учетных записей.

Практическая работа:

Защитить информацию в корпоративных сетях, обратить внимание на возможные перебои и нарушения в процессе доступа, способные уничтожить или исказить сведения.

проблемы, связанные с нарушением безопасности в компьютерных сетях, можно условно разделить на несколько типов:

1. Нарушения работы системного оборудования: разрыв кабелей, перебои в электропитании, сбой в дисковой системе, нарушения функционирования серверов, сетевых карт, рабочих станций, системы архивации.
2. Уничтожение данных вследствие некорректной работы программного обеспечения: ошибки системы, заражение компьютерными вирусами.
3. Следствие несанкционированного доступа: пиратское копирование, устранение или фальсификация данных, работа посторонних с секретными материалами.
4. Неграмотное сохранение архивов.
5. Ошибки технического штата и пользователей сетевого ресурса: случайное искажение либо уничтожение информации, некорректное пользование программными продуктами.
6. Устранить нарушения и усилить систему безопасности компьютерной сети.

Самостоятельная работа:

Презентация: архивирование и дублирование информации.

Криптографические системы.

Проблемой защиты информации путем ее преобразования занимается криптология. Криптология разделяется на два направления – криптографию и криптоанализ. Цели этих направлений прямопротивоположны.

Криптография занимается поиском и исследованием методов преобразования информации с целью скрытия ее содержания.

Сфера интересов криптоанализа - исследование возможности расшифрования информации без

знания ключей.

Современная криптография разделяет криптографические методы на четыре крупных класса.

1. Симметричные криптосистемы.
2. Криптосистемы с открытым ключом.
3. Системы электронной цифровой подписи (ЭЦП).
4. Системы управления ключами.

Основная литература: [1] с.12-13, 92-105, [3] с.5-14.

Дополнительная литература: **[8] с.22-28.**

Контрольные вопросы:

1. Какие языковые средства можно выделить в составе СУБД.
2. Перечислите основные типы полей, применяемые в СУБД.
3. Какая команда позволяет создать или изменить структуру БД.
4. Какие команды позволяют добавлять записи в таблице данных.
5. Какие команды позволяют удалить записи в таблице данных.

Блочные системы шифрования.

Алгоритмы симметричного шифрования различаются способом, которым обрабатывается исходный текст. Возможно шифрование блоками или шифрование потоком.

Блок текста рассматривается как неотрицательное целое число, либо как несколько независимых неотрицательных целых чисел. Длина блока всегда выбирается равной степени двойки. В большинстве блочных алгоритмов симметричного шифрования используются следующие типы операций:

- Табличная подстановка, при которой группа битов отображается в другую группу битов. Это так называемые ***S-box***.
- Перемещение, с помощью которого биты сообщения переупорядочиваются.
- Операция сложения по модулю 2, обозначаемая XOR или $\oplus$.
- Операция сложения по модулю 2^{32} или по модулю 2^{16}.
- Циклический сдвиг на некоторое число битов.

Эти операции циклически повторяются в алгоритме, образуя так называемые ***раунды***. Входом каждого *раунда* является выход предыдущего *раунда* и ключ, который получен по определенному алгоритму из ключа шифрования K. Ключ *раунда* называется ***подключом***. Каждый алгоритм шифрования может быть представлен следующим образом:

Области применения

Стандартный алгоритм шифрования должен быть применим во многих приложениях:

- Шифрование данных. Алгоритм должен быть эффективен при шифровании файлов данных или большого потока данных.
- Создание случайных чисел. Алгоритм должен быть эффективен при создании определенного количества случайных битов.
- Хэширование. Алгоритм должен эффективно преобразовываться в одностороннюю хэш-функцию.

Платформы

Стандартный алгоритм шифрования должен быть реализован на различных платформах, которые, соответственно, предъявляют различные требования.

- Алгоритм должен эффективно реализовываться на специализированной аппаратуре, предназначенной для выполнения шифрования/дешифрования.
- Большие процессоры. Хотя для наиболее быстрых приложений всегда используется специальная аппаратура, программные реализации применяются чаще. Алгоритм должен допускать эффективную программную реализацию на 32-битных процессорах.

- Процессоры среднего размера. Алгоритм должен работать на микроконтроллерах и других процессорах среднего размера.
- Малые процессоры. Должна существовать возможность реализации алгоритма на смарт-картах, пусть даже с учетом жестких ограничений на используемую память.

Дополнительные требования

Алгоритм шифрования должен, по возможности, удовлетворять некоторым дополнительным требованиям.

- Алгоритм должен быть простым для написания кода, чтобы минимизировать вероятность программных ошибок.
- Алгоритм должен иметь плоское пространство ключей и допускать любую случайную строку битов нужной длины в качестве возможного ключа. Наличие слабых ключей нежелательно.
- Алгоритм должен легко модифицироваться для различных уровней безопасности и удовлетворять как минимальным, так и максимальным требованиям.
- Все операции с данными должны осуществляться над блоками, кратными байту или 32-битному слову.

Алгоритм ГОСТ 28147

Алгоритм ГОСТ 28147 является отечественным стандартом для алгоритмов симметричного шифрования. ***ГОСТ 28147*** разработан в 1989 году, является блочным алгоритмом шифрования, длина блока равна 64 битам, длина ключа равна 256 битам, количество *раундов* равно 32. Алгоритм представляет собой классическую сеть Фейштеля.

$L_i = R_{i-1}$

$R_i = L_i \oplus f(R_{i-1}, K_i)$

Функция F проста. Сначала правая половина и i-ый *подключ* складываются по модулю 2^{32}. Затем результат разбивается на восемь 4-битовых значений, каждое из которых подается на вход *S-box*. *ГОСТ 28147* использует восемь различных *S-boxes*, каждый из которых имеет 4-битовый вход и 4-битовый выход. Выходы всех *S-boxes* объединяются в 32-битное слово, которое затем циклически сдвигается на 11 битов влево. Наконец, с помощью XOR результат объединяется с левой половиной, в результате чего получается новая правая половина.

Генерация ключей проста. 256-битный ключ разбивается на восемь 32-битных *подключей*. Алгоритм имеет 32 *раунда*, поэтому каждый *подключ* используется в четырех *раундах* по следующей схеме:

Раунд	1	2	3	4	5	6	7	8
Подключ	1	2	3	4	5	6	7	8
Раунд	9	10	11	12	13	14	15	16
Подключ	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24
Подключ	1	2	3	4	5	6	7	8
Раунд	25	26	27	28	29	30	31	32
Подключ	8	7	6	5	4	3	2	1

Считается, что стойкость *алгоритма ГОСТ 28147* во многом определяется структурой *S-boxes*. Долгое время структура *S-boxes* в открытой печати не публиковалась. В настоящее время известны *S-boxes*, которые используются в приложениях Центрального Банка РФ и считаются достаточно сильными. Напомню, что входом и выходом *S-box* являются 4-битные числа, поэтому каждый *S-box* может быть представлен в виде строки чисел от 0 до 15, расположенных в некотором порядке. Тогда порядковый номер числа будет являться входным значением *S-box*, а само число - выходным значением *S-box*.

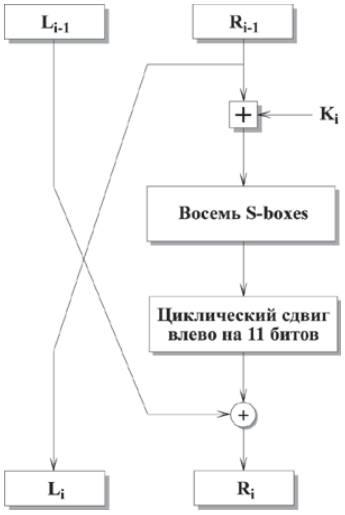


Рис. 3. I-ый раунд ГОСТ 28147

1-ый S-box	4	10	9	2	13	8	0	14
	6	11	1	12	7	15	5	3
2-ой S-box	14	11	4	12	6	13	15	10
	2	3	8	1	0	7	5	9
3-ий S-box	5	8	1	13	10	3	4	2
	14	15	12	7	6	0	9	11
4-ый S-box	7	13	10	1	0	8	9	15
	14	4	6	12	11	2	5	3
5-ый S-box	6	12	7	1	5	15	13	8
	4	10	9	14	0	3	11	2
6-ой S-box	4	11	10	0	7	2	1	13
	3	6	8	5	9	12	15	14
7-ой S-box	13	11	4	1	3	15	5	9
	0	10	14	7	6	8	2	12
8-ой S-box	1	15	13	0	5	7	10	4
	9	2	3	14	6	11	8	12

Режимы выполнения алгоритмов симметричного шифрования

Для любого симметричного блочного алгоритма шифрования определено четыре режима выполнения.

ECB - Electronic Codebook - каждый блок из 64 битов незашифрованного текста шифруется независимо от остальных блоков, с применением одного и того же *ключа шифрования*. Типичные приложения - безопасная передача одиночных значений (например, криптографического ключа).

CBC - Cipher Block Chaining - вход криптографического алгоритма является результатом применения операции XOR к следующему блоку незашифрованного текста и предыдущему блоку зашифрованного текста. Типичные приложения - общая блокоориентированная передача, аутентификация.

CFB - Cipher Feedback - при каждом вызове алгоритма обрабатывается J битов входного значения. Предшествующий зашифрованный блок используется в качестве входа в алгоритм; к J битам выхода алгоритма и следующему незашифрованному блоку из J битов применяется операция XOR, результатом которой является следующий зашифрованный блок из J битов. Типичные приложения - потокоориентированная передача, аутентификация.

OFB - Output Feedback - аналогичен *CFB*, за исключением того, что на вход алгоритма при шифровании следующего блока подается результат шифрования предыдущего блока; только после этого выполняется операция XOR с очередными J битами незашифрованного текста. Типичные приложения - потокоориентированная передача по зашумленному каналу (например, спутниковая связь).

Основная литература: [1] с.105-107, 117-:121, [2] с.20-23, [3] с.15-19, [6] с.82-90.

Контрольные вопросы:

1. Какие системы называются блочными.
2. Что называется блоком текста.
3. Что называется раундом алгоритма.
4. Какова область применения блочных шифров.
5. Требования предъявляемые к блочным шифрам.
6. Чем определяется стойкость *алгоритма ГОСТ 28147*.

Потоковые системы шифрования. Генераторы случайных чисел.

Потоковые шифры представляют собой разновидность гаммирования и преобразуют открытый текст в шифрованный последовательно по 1 биту. Потоковые шифры наиболее пригодны для шифрования непрерывных потоков данных, например, в сетях передачи данных.

В 1946 году в США была запатентована базовая идея самосинхронизирующих потоковых шифров. Она заключается в том, что внутреннее состояние генератора является функцией фиксированного числа предшествующих битов шифрованного текста. Поскольку внутреннее состояние зависит только от n бит шифрованного текста, генератор на приемной стороне войдет в синхронизм с передающей стороной после получения n бит.

Потоковые шифры в которых выходные значения не зависят от исходного или шифрованного текстов называются синхронными. Основная сложность в таких алгоритмах заключается в необходимости синхронизации генераторов ключа на передающей и приемной сторонах.

Алгоритм RC6

RC6 является полностью параметризуемым семейством алгоритмов шифрования. RC6 правильнее указывать как RC6-w/r/b, где w - длина слова в битах, r - число *раундов*, b - длина ключа. Обычно используются значения w = 32 и r = 20.

Алгоритм является *сетью Фейштеля* с 4 ветвями смешанного типа: два четных подблока используются для одновременного изменения содержимого двух нечетных подблоков. Затем производится обычный для *сети Фейштеля* сдвиг на одно слово, что меняет четные и нечетные подблоки местами.

$f(x) = x(2x + 1)$

$a + b$ - сложение целых по модулю 2^w

$a - b$ - вычитание целых по модулю 2^w

$a \oplus b$ - XOR w-битных слов

$a \times b$ - умножение целых по модулю 2^w

$a <<< b$ - ротация влево на b бит w-битного слова a

$a >>> b$ - ротация вправо на b бит w-битного слова a

$S[0, \ldots, 2r + 3]$ - w-битные подключи *раунда*

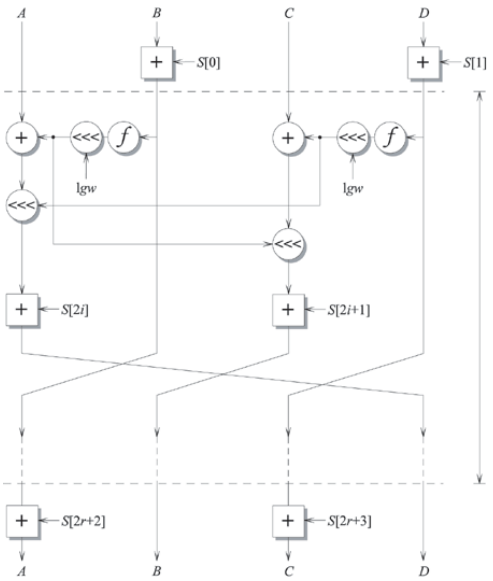


Рис. 5. Алгоритм RC6

Генераторы псевдослучайных чисел

Первой широко используемой технологией создания случайного числа был алгоритм, предложенный Лехмером, который известен как метод линейного конгруента. Этот алгоритм параметризуется четырьмя числами следующим образом:

m	Модуль (основание системы)	m > 0
a	Множитель	$0 \leq a < m$
c	Приращение	$0 \leq c < m$
X0	Начальное значение или зерно (seed)	$0 \leq X_0 < m$

Последовательность случайных чисел $\{X_n\}$ получается с помощью следующего итерационного равенства:

$$X_{n+1} = (a\ X_n + c) \bmod m$$

Если m, a и c являются целыми, то создается последовательность целых чисел в диапазоне $0 \leq X_n < m$.

Выбор значений для a, c и m является критичным для разработки хорошего генератора случайных чисел.

Очевидно, что m должно быть очень большим, чтобы была возможность создать много случайных чисел. Считается, что m должно быть приблизительно равно максимальному положительному целому числу для данного компьютера. Таким образом, обычно m близко или равно 2^{31}.

Существует три критерия, используемые при выборе генератора случайных чисел:

1. Функция должна создавать полный период, т.е. все числа между 0 и m до того, как создаваемые числа начнут повторяться.
2. Создаваемая последовательность должна появляться случайно. Последовательность не является случайной, так как она создается детерминированно, но различные статистические тесты, которые могут применяться, должны показывать, что последовательность случайна.
3. Функция должна эффективно реализовываться на 32-битных процессорах.

Значения a, c и m должны быть выбраны таким образом, чтобы эти три критерия выполнялись. В соответствии с первым критерием можно показать, что если m является простым и c = 0, то при определенном значении a период, создаваемый функцией, будет равен m-1. Для 32-битной арифметики

соответствующее простое значение $m = 2^{31} - 1$. Таким образом, функция создания *псевдослучайных чисел* имеет вид:

$$X_{n+1} = (a\ X_n) \bmod (2^{31} - 1)$$

Только небольшое число значений a удовлетворяет всем трем критериям. Одно из таких значений есть $a = 7^5 = 16807$, которое использовалось в семействе компьютеров IBM 360. Этот генератор широко применяется и прошел более тысячи тестов, больше, чем все другие генераторы *псевдослучайных чисел*.

Сила алгоритма линейного конгруента в том, что если сомножитель и модуль (основание) соответствующим образом подобраны, то результирующая последовательность чисел будет статистически неотличима от последовательности, являющейся случайной из набора 1, 2, ..., m-1. Но не может быть случайности в последовательности, полученной с использованием алгоритма, независимо от выбора начального значения X_0. Если значение выбрано, то оставшиеся числа в последовательности будут предопределены. Это всегда учитывается при криптоанализе.

Если противник знает, что используется алгоритм линейного конгруента, и если известны его параметры ($a = 7^5$, $c = 0$, $m = 2^{31} - 1$), то, если раскрыто одно число, вся последовательность чисел становится известна. Даже если противник знает только, что используется алгоритм линейного конгруента, знания небольшой части последовательности достаточно для определения параметров алгоритма и всех последующих чисел. Предположим, что противник может определить значения X_0, X_1, X_2, X_3. Тогда :

$$X_1 = (a\ X_0 + c\ ) \bmod m$$
$$X_2 = (a\ X_1 + c\ ) \bmod m$$
$$X_3 = (a\ X_2 + c\ ) \bmod m$$

Эти равенства позволяют найти a, c и m.

Таким образом, хотя алгоритм и является хорошим генератором *псевдослучайной последовательности чисел*, желательно, чтобы реально используемая последовательность была непредсказуемой, поскольку в этом случае знание части последовательности не позволит определить будущие ее элементы. Эта цель может быть достигнута несколькими способами. Например, использование внутренних системных часов для модификации потока случайных чисел. Один из способов применения часов состоит в перезапуске последовательности после N чисел, используя текущее значение часов по модулю m в качестве нового начального значения. Другой способ состоит в простом добавлении значения текущего времени к каждому случайному числу по модулю m.

Основная литература: [1] с.111-117, [3] с.23-31.

Контрольные вопросы:

1. Какие шифра называются потоковыми.
2. На каком алгоритме основан алгоритм RC6.
3. Какие критерии используются при выборе генератора случайных чисел.
4. Как можно используя часы разработать генератор случайных чисел.
5. Чем отличаются самосинхронизирующие шифры от синхронных.

Ассиметричные системы шифрования.

Создание *алгоритмов асимметричного шифрования* является величайшим и, возможно, единственным революционным достижением в истории криптографии.

Алгоритмы шифрования с *открытым ключом* разрабатывались для того, чтобы решить две наиболее трудные задачи, возникшие при использовании симметричного шифрования.

Первой задачей является распределение ключа. При симметричном шифровании требуется, чтобы обе стороны уже имели общий ключ, который каким-то образом должен быть им заранее передан. Диффи, один из основоположников шифрования с *открытым ключом*, заметил, что это требование

отрицает всю суть криптографии, а именно возможность поддерживать всеобщую секретность при коммуникациях.

Второй задачей является необходимость создания таких механизмов, при использовании которых невозможно было бы подменить кого-либо из участников, т.е. нужна *цифровая подпись*. При использовании коммуникаций для решения широкого круга задач, например в коммерческих и частных целях, электронные сообщения и документы должны иметь эквивалент подписи, содержащейся в бумажных документах. Необходимо создать метод, при использовании которого все участники будут убеждены, что электронное сообщение было послано конкретным участником. Это более сильное требование, чем аутентификация.

Диффи и Хеллман достигли значительных результатов, предложив способ решения обеих задач, который радикально отличается от всех предыдущих подходов к шифрованию.

Сначала рассмотрим общие черты алгоритмов шифрования с *открытым ключом* и требования к этим алгоритмам. Определим требования, которым должен соответствовать алгоритм, использующий один ключ для шифрования, другой ключ - для дешифрования, и при этом вычислительно невозможно определить дешифрующий ключ, зная только алгоритм шифрования и шифрующий ключ.

Кроме того, некоторые алгоритмы, например RSA, имеют следующую характеристику: каждый из двух ключей может использоваться как для шифрования, так и для дешифрования.

Сначала рассмотрим алгоритмы, обладающие обеими характеристиками, а затем перейдем к алгоритмам *открытого ключа*, которые не обладают вторым свойством.

При описании симметричного шифрования и шифрования с *открытым ключом* будем использовать следующую терминологию. Ключ, используемый в симметричном шифровании, будем называть секретным ключом. Два ключа, используемые при шифровании с *открытым ключом*, будем называть ***открытым ключом*** и ***закрытым ключом***. *Закрытый ключ* держится в секрете, но называть его будем *закрытым ключом*, а не секретным, чтобы избежать путаницы с ключом, используемым в симметричном шифровании. *Закрытый ключ* будем обозначать KR, *открытый ключ* - KU.

Будем предполагать, что все участники имеют доступ к *открытым ключам* друг друга, а *закрытые ключи* создаются локально каждым участником и, следовательно, распределяться не должны.

В любое время участник может изменить свой *закрытый ключ* и опубликовать составляющий пару *открытый ключ*, заменив им старый *открытый ключ*.

Диффи и Хеллман описывают требования, которым должен удовлетворять алгоритм шифрования с *открытым ключом*.

1. Вычислительно легко создавать пару (*открытый ключ* KU , *закрытый ключ* KR).
2. Вычислительно легко, имея *открытый ключ* и незашифрованное сообщение M, создать соответствующее зашифрованное сообщение:
   $C = E_{KU}[M]$
3. Вычислительно легко дешифровать сообщение, используя *закрытый ключ*:
   $M = D_{KR}[C] = D_{KR}[E_{KU}[M]]$
4. Вычислительно невозможно, зная *открытый ключ* KU, определить *закрытый ключ* KR.
5. Вычислительно невозможно, зная *открытый ключ* KU и зашифрованное сообщение C, восстановить исходное сообщение M.

   Можно добавить шестое требование, хотя оно не выполняется для всех алгоритмов с *открытым ключом*:
6. Шифрующие и дешифрующие функции могут применяться в любом порядке:
   $M = E_{KU}[D_{KR}[M]]$

Это достаточно сильные требования, которые вводят понятие *односторонней функции с люком*. ***Односторонней функцией*** называется такая функция, у которой каждый аргумент имеет единственное обратное значение, при этом вычислить саму функцию легко, а вычислить обратную функцию трудно.

$Y = f(X)$ - легко

$X = f^{-1}(Y)$ - трудно

Обычно "легко" означает, что проблема может быть решена за полиномиальное время от длины входа. Таким образом, если длина входа имеет n битов, то время вычисления функции пропорционально n^a, где a - фиксированная константа. Таким образом, говорят, что алгоритм принадлежит классу полиномиальных алгоритмов P. Термин "трудно" означает более сложное понятие. В общем случае будем считать, что проблему решить невозможно, если усилия для ее решения больше полиномиального времени от величины входа. Например, если длина входа n битов, и время вычисления функции пропорционально 2^n, то это считается вычислительно невозможной задачей. К сожалению, тяжело определить, проявляет ли конкретный алгоритм такую сложность. Более того, традиционные представления о вычислительной сложности фокусируются на худшем случае или на среднем случае сложности алгоритма. Это неприемлемо для криптографии, где требуется невозможность инвертировать функцию для всех или почти всех значений входов.

Вернемся к определению ***односторонней функции с люком***, которую, подобно *односторонней функции*, легко вычислить в одном направлении и трудно вычислить в обратном направлении до тех пор, пока недоступна некоторая дополнительная информация. При наличии этой дополнительной информации инверсию можно вычислить за полиномиальное время. Таким образом, *односторонняя функция* с люком принадлежит семейству *односторонних функций* f_k таких, что

$Y = f_k(X)$ - легко, если k и X известны

$X = f_k^{-1}(Y)$ - легко, если k и Y известны

$X = f_k^{-1}(Y)$ - трудно, если Y известно, но k неизвестно

Мы видим, что разработка конкретного алгоритма с *открытым ключом* зависит от открытия соответствующей односторонней функции с люком.

Основными способами использования алгоритмов с *открытым ключом* являются шифрование/дешифрование, создание и проверка подписи и обмен ключа.

Шифрование с *открытым ключом* состоит из следующих шагов:

Рис. 6.1. Шифрование с открытым ключом

1. Пользователь B создает пару ключей KU_b и KR_b, используемых для шифрования и дешифрования передаваемых сообщений.
2. Пользователь B делает доступным некоторым надежным способом свой ключ шифрования, т.е. *открытый ключ* KU_b. Составляющий пару *закрытый ключ* KR_b держится в секрете.
3. Если A хочет послать сообщение B, он шифрует сообщение, используя *открытый ключ* B KU_b .
4. Когда B получает сообщение, он дешифрует его, используя свой *закрытый ключ* KR_b. Никто другой не сможет дешифровать сообщение, так как этот *закрытый ключ* знает только B.

Если пользователь (конечная система) надежно хранит свой *закрытый ключ*, никто не сможет подсмотреть передаваемые сообщения.

***алгоритм RSA*:**

Создание ключей

Выбрать простые p и q

Вычислить $n = p \cdot q$

Выбрать d $\gcd(\Phi(n), d) = 1;\ 1 < d < \Phi(n)$

Вычислить e $e = d^{-1} \bmod \Phi(n)$

Открытый ключ $KU = \{e, n\}$

Закрытый ключ $KR = \{d, n\}$

Шифрование

Незашифрованный текст: $M < n$

Зашифрованный текст: $C = M^e \pmod n$

Дешифрование

Зашифрованный текст: C

Незашифрованный текст: $M = C^d \pmod n$

Рассмотрим конкретный пример:

Выбрать два простых числа: $p = 7,\ q = 17$.

Вычислить $n = p \cdot q = 7 \cdot 17 = 119$.

Вычислить $\Phi(n) = (p - 1) \cdot (q - 1) = 96$.

Выбрать e так, чтобы e было взаимнопростым с $\Phi(n) = 96$ и меньше, чем $\Phi(n)$: $e = 5$.

Определить d так, чтобы $d \cdot e \equiv 1 \bmod 96$ и $d < 96$.

$d = 77$, так как $77 \cdot 5 = 385 = 4 \cdot 96 + 1$.

Результирующие ключи *открытый* $KU = \{5, 119\}$ и *закрытый* $KR = \{77, 119\}$.

Например, требуется зашифровать сообщение $M = 19$.

$19^5 = 66 \pmod{119}$; $C = 66$.

Для дешифрования вычисляется $66^{77} \pmod{119} = 19$.

Основная литература: [1] с.128-132, [2] с.9-16, 26-32, [5] с.12-:19.

Контрольные вопросы:

1. Какие алгоритмы называются ассиметричными.
2. Что такое открытый ключ.
3. Какой ключ является открытым.
4. Какие требования предъявляются к ассиметричным системам шифрования.
5. Из каких этапов состоит шифрование с открытым ключом.

Компьютерные вирусы.

К настоящему времени в мире информатики уже насчитывается достаточное количество фактов, позволяющих провести определенный анализ и классификацию.

Настоящие вирусы (к которым не относятся программы типа “троянский конь”) состоят, по крайней мере, из двух функционально разделенных компонентов. Один из них отвечает за размножение, а второй выполняет задачу по нанесению ущерба. Компонент, ответственный за размножение, включает в себя все те функции, которые необходимы для распространения вируса, в частности поиск неинфицированных программ, внесение в них изменений, внедрение в оперативную память и, наконец, выполнение маскировочных мероприятий.

Компонент, выполняющий задачу по нанесению ущерба, вступает в действие как правило после завершения работы той части вируса, которая отвечает за размножение. Почти всегда для этого компонента четко определяются условия начала его работы (пуска) и предусматривается их проверка при каждой активизации вируса. Если эти условия не соблюдены, то работы данного компонента прекращается и не происходит ничего, чтобы могло бы броситься в глаза. Это объясняет почему

вирусные инфекции очень часто могут оставаться незамеченными на протяжение длительного времени. Вирус “спит” пока не наступит определенный момент.

Если же указанные условия соблюдаются, то вступает в действие компонент, выполняющий разрушительную функцию. Последствия при этом могут быть разными: от невинных эффектов на экране, необъяснимых нарушений работы портов и до полной потери всех данных на жестких дисках или на дискетах. Довольно часто происходит весьма сложное искажение данных так, что ущерб в полной мере можно обнаружить только по истечению значительного времени.

В принципе, все вирусы с технической точки зрения делятся на две большие группы, отличающиеся друг от друга по объекту внедрения: файловые и системные.

ФАЙЛОВЫЕ ВИРУСЫ

Файловые вирусы составляют наиболее многочисленную группу и в свою очередь разделяются по способу воздействия на две подгруппы: вирусы необратимой модификации (ueberschreibende Viren) и вирусы гибкой модификации (nicht ueberschreibende Viren). Вирусы необратимой модификации разрушают программы (файлы) благодаря своему механизму размножения, в результате чего начало программы сразу же заменяется машинным кодом вируса. Измененные программы становятся неработоспособными непосредственно после воздействия на них и поэтому данный тип вирусов быстро обнаруживается и его возможности по распространению и нанесению ущерба ограничен.

Вирусы гибкой модификации, называемые также прикрепляющимися вирусами (link-viruses), более опасны, поскольку их присутствие в системе обнаружить не легко. Такие вирусы “повисают” на программах и, несмотря на произведенные изменения, они способны восстановить прежний вид этих программ непосредственно перед их пуском. Обычно заражение вирусом можно обнаружить только путем сравнения размеров файла с оригиналом.

По способу использования оперативной памяти файловые вирусы бывают резидентные (размещаемые в памяти резидентно) и нерезидентные (удаляются из памяти вместе с выгружаемой инфицированной программой. В специальной терминологии резидентные называются вирусами непрямого действия (indirect action viruses), а нерезидентные - вирусами прямого действия (direct action viruses).

Большинство файловых вирусов (но не все) при вызове зараженных ими программ резидентно инсталлируются в оперативную память, благодаря чему они в той или иной степени могут контролировать систему и, таким образом, эффективно распространяться. Передача инфекции происходит не прямым способом, то есть не в момент загрузки зараженной программы, а в результате последующего функционирования системы, например при последовательной загрузке еще не зараженных программ. Большинство представителей этого подвида заражают программы только при выполнении определенных команд ОС, связанных с загрузкой и запуском программ, в момент обращения к этим командам. Однако некоторые вирусы обладают более сильным и совершенным механизмом, способным распространять инфекцию при выполнении всего перечня файловых команд, осуществляющих открытие, закрытие, копирование и перенос файлов. Поэтому простая проверка программных файлов (путем их открытия для просмотра) на предмет инфекции в этом случае принесет больше вреда, чем пользы.

Другой подвид файловых вирусов (прямого действия) не остается в оперативной памяти резидентно, а только лишь при запуске инфицированной программы такой вирус начинает искать другие программы и пытается их заразить. В этом случае при загрузке неинфицированной программы не происходит ни её заражения, ни дальнейшего распространения инфекции.

СИСТЕМНЫЕ ВИРУСЫ

Системные вирусы работают на более глубоком уровне, внедряясь в дисковую структуры ОС, связанную с базовыми функциями запуска компьютера и ввода/вывода информации.

Активизация этого типа вируса, в отличие от других, происходит только при запуске (перезапуске) компьютера с зараженного диска, после чего вирус резидентно инсталлируется в оперативной памяти и начинает манипулировать пусковым сектором (загрузчиком) и другими элементами дисковой структуры. Распространение инфекции происходит при обращении ОС к другим дискам.

Обнаружить такой вирус и освободиться от него весьма трудно. Это связано, в первую очередь, с тем, что он попадает в оперативную память в процессе запуска компьютера, то есть еще до того как сможет заработать какая-либо антивирусная программа. Единственная возможность обнаружить инфекцию заключается в проверке оперативной памяти сразу же после загрузки. При обнаружении вируса компьютер следует немедленно выключить и загрузить с неинфицированного диска.

В зависимости от конечного объекта внедрения различают два подтипа системных вирусов: вирусы пускового сектора и декомпозиционные вирусы. Разница между ними заключается лишь в том, что вирус пускового сектора “оккупирует” пусковой сектор системного драйва (диска), а декомпозиционный вирус проникает в первый (пусковой) сегмент логического несистемного драйва. Поэтому дальнейшее описание будет сосредоточено на вирусе пускового сектора, являющимся наиболее сложным и эффективным.

Вирусы пускового сектора появились совсем недавно. Вообще раньше считалось, что создать такой, более или менее функционирующий, вирус нельзя, поскольку размер пускового сектора ограничен и там почти невозможно разместить какую-либо действующую программу вместе с пусковой записью (boot-strap record). Однако по мере развития техники программирования был изобретен изощренный механизм, благодаря которому эту задачу удалось решить другим путем.

Детальный механизм работы вируса пускового сектора заключается в том, что сам вирус размещается в первом (пусковом) секторе, замещая пусковую запись своим кодом. Оригинал же пусковой записи он копирует на свободное место на диске. При загрузке ОС загрузчик размещает вирус в оперативной памяти, после чего туда загружается и сам вирус. Данный механизм позволяет создавать вирусы этого типа сложные по структуре и значительно превышающие по размеру пусковой сектор. В этом случае вирус компонуется из двух частей: загрузочной, ограниченной по размеру для размещения в пусковом секторе, и функциональной, размещаемой на свободном дисковом пространстве. После того, как загрузочная часть, попав в оперативную память, берет на себя управление, она находит на диске и загружает в память функциональную часть, затем происходит загрузка пускового записи.

Необходимо особо отметить, что вирус пускового сектора может распространяться не только через системный диск. “Гениальность” описанного выше механизма заключается в том, что пусковой сектор имеется на любом диске единственно, что не все они содержать пусковую запись. Если же пользователь по ошибке пытается запустить компьютер с несистемного (не имеющего пусковую запись) диска, инфицированного вирусом пускового сектора, то компьютер выдаст на экран монитора сообщение об ошибке и попросит сменить диск. Однако считывание пускового сектора происходит в любом случае и, если он содержит вирус, то последний немедленно попадает в оперативную память. После устранения ошибки и смены диска компьютер оказывается зараженным. Существует, правда, простой и надежный способ защиты от попадания вирусов пускового сектора с несистемных дисков: после ошибочной попытки запуска необходимо произвести полную перезагрузку компьютера, то есть очистить оперативную память.

Воздействие системных вирусов чаще всего носит исключительно разрушительный характер. Механизм действия известного всему миру вируса “disk-killer” (разрушитель дисков) основан на последовательном преобразовании двоичных записей дорожек (tracks) с помощью функции XOR, после чего содержание файлов (частей файлов), использующих преобразованные дорожки, превращается в бессмыслицу.

Механизмы вирусной атаки

Все известные вирусы различаются способом размещения в программном обеспечении, методом распространения в вычислительной среде, способом активизации, характером наносимого ущерба [5, 7, 8, 28, 30, 64 и др.].

Компьютерный вирус может находиться в операционной среде, где он сцепляется с программами, расположенными в системной части накопителя на гибком магнитном диске (НГМД) или на жестком магнитном диске (“винчестере”). Его внутренние поля могут располагаться в структуре файлов типа EXE - в области между таблицей адресов и загрузочным модулем программы или в свободной памяти файла за программой, в библиотеках компиляторов - наиболее эффективном варианте размещения вируса, поскольку он при этом может автоматически внедряться в любую программу, составляемую компилятором, в сетевом драйвере (программном обеспечении работы вычислительной сети), в “плохих” или специальных секторах на диске, в постоянном запоминающем устройстве (ПЗУ) в качестве программно-технической закладки, которую обнаружить весьма трудно.

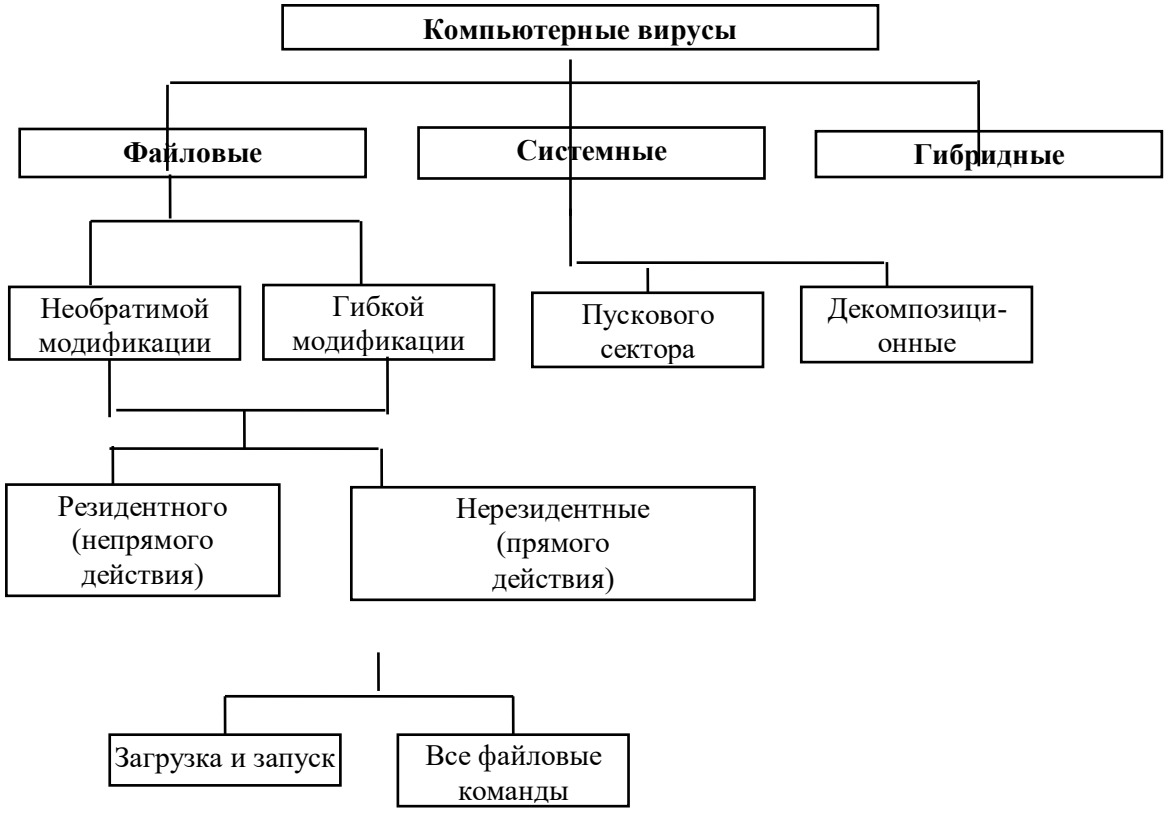


Рис. 7. Классификация компьютерных вирусов

Компьютерный вирус может распространяться транзитно или резидентно. В первом случае, находясь в оперативном запоминающем устройстве (ОЗУ) компьютера, вирус дописывает себя в другие программы, хранимые на диске, во втором случае вирус, введенный в память ЭВМ (в часть, где находятся программы операционной системы (ОС)), при обращениях к ОС “заражает” программы (диски), вызываемые на выполнение.

Активизироваться вирус может: с момента внедрения в средства вычислительной техники, по наступлении определенного события (даты, заданного числа обращений к зараженной программе), случайно (по показанию датчика случайных чисел, содержащегося в вирусе).

Среди вирусов есть такие, которые не создают серьезных помех работе средств вычислительной техники, вызывают нарушения, поддающиеся исправлению, и производят необратимые изменения и разрушения. Наибольшую опасность представляют вирусы, имеющие деструктивную функцию. Эти

вирусы наносят следующие виды ущерба вычислительным средствам: изменение данных в файлах данных, изменение назначенного магнитного диска, в результате чего данные записываются на другой диск. Например, данные могут быть направлены на квазидиск в ОС и потеряны после выключения ЭВМ; уничтожение специальных файлов, содержащих выполняемые программы и данные; уничтожение информации форматированием диска или отдельных треков на нем; уничтожение каталога диска; уничтожение (выключение) программ, постоянно находящихся в ОС; нарушение работоспособности ОС, при которой она не воспринимает внешних воздействий и требует полной загрузки.

Основная литература: [1]с.122-128, [2] с.16-26, [5] с.12-19.

Контрольные вопросы:

1. Что такое компьютерный вирус.
2. Как классифицируются вирусы.
3. Что такое файловый вирус.
4. Какие вирусы называются пусковыми.
5. Какие вирусы относятся к резидентным.

Защита от компьютерных вирусов.

Известно, что нельзя добиться 100 %-ой защиты ПК от компьютерных вирусов отдельными программными средствами. Поэтому для уменьшения потенциальной опасности внедрения компьютерных вирусов и их распространения по корпоративной сети необходим комплексный подход, сочетающий различные административные меры, программно-технические средства антивирусной защиты, а также средства резервирования и восстановления. Делая акцент на программно-технических средствах, можно выделить три основных уровня антивирусной защиты:

1. *Поиск и уничтожение известных вирусов.*
2. *Поиск и уничтожение неизвестных вирусов.*
3. *Блокировка проявления вирусов.*

1. При поиске и уничтожении известных вирусов наиболее распространенным является метод сканирования. Указанный метод заключается в выявлении компьютерных вирусов по их уникальному фрагменту программного кода (сигнатуре, программному штамму). Для этого создается некоторая *база данных сканирования* с фрагментами кодов известных компьютерных вирусов. Обнаружение вирусов осуществляется путем сравнения данных памяти компьютера с фиксированными кодами базы данных сканирования. В случае выявления и идентификации кода нового вируса, его сигнатура может быть введена в базу данных сканирования. В виду того, что сигнатура известна, то существует возможность корректного восстановления (обеззараживания) зараженных файлов и областей. Следует добавить, что некоторые системы хранят не сами сигнатуры, а, например, контрольные суммы или имитоприставки сигнатур.

Антивирусные программы, выявляющие известные компьютерные вирусы, называются *сканерами* или детекторами. Программы, включающие функции восстановления зараженных файлов, называют *полифагами* (фагами), докторами или дезинфекторами. Примером сканера-полифага является знакомая программа Aidstest.

Принято разделять сканеры на следующие:

- транзитные, периодически запускаемые для выявления и ликвидации вирусов,
- резидентные (постоянно находящиеся в оперативной памяти), проверяющие заданные области памяти системы при возникновении связанных с ними событий (например, проверка файла при его копировании или переименовании).

К недостаткам сканеров следует отнести то, что они позволяют обнаружить вирусы, которые уже проникали в вычислительные системы, изучены и для них определена сигнатура. Для эффективной работы сканеров необходимо оперативно пополнять базу данных сканирования. Однако с увеличением

объема базы данных сканирования и числа различных типов искомых вирусов снижается скорость антивирусной проверки. Само собой, если время сканирования будет приближаться ко времени восстановления, то необходимость в антивирусном контроле может стать не столь актуальной.

Некоторые вирусы (мутанты и полиморфные) кодируют или видоизменяют свой программный код. Это затрудняет или делает невозможным выделить сигнатуру, а следовательно, обнаружить вирусы методом сканирования.

Для выявления указанных маскирующихся вирусов используются специальные методы. К ним можно отнести метод эмуляции процессора. Метод заключается в имитации выполнения процессором программы и подсовывания вирусу фиктивных управляющих ресурсов. Обманутый таким образом вирус, находящийся под контролем антивирусной программы, расшифровывает свой код. После этого, сканер сравнивает расшифрованный код с кодами из своей базы данных сканирования.

2. Выявление и ликвидация неизвестных вирусов необходимы для защиты от вирусов, пропущенных на первом уровне антивирусной защиты. Наиболее эффективным методом является контроль целостности системы (обнаружение изменений). Данный метод заключаются в проверке и сравнении текущих параметров вычислительной системы с эталонными, соответствующими ее незараженному состоянию. Понятно, что контроль целостности не являются прерогативой исключительно системы антивирусной защиты. Он обеспечивает защищенность информационного ресурса от несанкционированных модификации и удаления в результате различного рода нелегитимных воздействий, сбоев и отказов системы и среды.

Для реализации указанных функций используются программы, называемые *ревизорами*. Работа ревизора состоит из двух этапов: фиксирование эталонных характеристик вычислительной системы (в основном диска) и периодическое сравнение их с текущими характеристиками. Обычно контролируемыми характеристиками являются контрольная сумма, длина, время, атрибут “только для чтения” файлов, дерево каталогов, сбойные кластеры, загрузочные сектора дисков. В сетевых системах могут накапливаться среднестатистические параметры функционирования подсистем (в частности исторический профиль сетевого трафика), которые сравниваются с текущими.

Ревизоры, как и сканеры, делятся на транзитные и резидентные.

К недостаткам ревизоров, в первую очередь резидентных, относят создаваемые ими всякие неудобства и трудности в работе пользователя. Например, многие изменения параметров системы вызваны не вирусами, а работой системных программ или действиями пользователя-программиста. По этой же причине ревизоры не используют для контроля зараженности текстовых файлов, которые постоянно меняются. Таким образом, необходимо соблюдение некоторого баланса между удобством работы и контролем целостности системы.

Ревизоры обеспечивают высокий уровень выявления неизвестных компьютерных вирусов, однако они не всегда обеспечивают корректное лечение зараженных файлов. Для лечения зараженных файлов неизвестными вирусами обычно используются эталонные характеристики файлов и предполагаемые способы их заражения.

Кроме этого ревизоры не определяют зараженные файлы, создаваемые или копируемые в систему.

Примерами ревизоров являются программы: MSAV ОС MS-DOS и ADinf фирмы “Диалог-Наука”.

Разновидностью контроля целостности системы является метод программного самоконтроля, именуемые вакцинацией. Идея методов состоит в присоединении к защищаемой программе модуля (*вакцины*), контролирующего характеристики программы, обычно ее контрольную сумму.

Помимо статистических методов контроля целостности, для выявления неизвестных и маскирующихся вирусов используются эвристические методы. Они позволяет выявить по известным признакам (определенным в базе знаний системы) некоторые маскирующиеся или новые модифицированные вирусы известных типов. В качестве примера признака вируса можно привести код,

устанавливающий резидентный модуль в памяти, меняющий параметры таблицы прерываний и др. Программный модуль, реализующий эвристический метод обнаружения вирусов, называют *эвристическим анализатором*. Примером сканера с эвристическим анализатором является программа Dr Web фирмы “Диалог-Наука”.

К недостаткам эвристических анализаторов можно отнести ошибки 1-го и 2-го рода: ложные срабатывания и пропуск вирусов. Соотношение указанных ошибок зависит от уровня эвристики.

Понято, что если для обнаруженного эвристическим анализатором компьютерного вируса сигнатура отсутствует в базе данных сканирования, то лечение зараженных данных может быть некорректным.

3. Блокировка проявления вирусов предназначена для защиты от деструктивных действий и размножения компьютерных вирусов, которым удалось преодолеть первые два уровня защиты. Методы основаны на перехвате характерных для вирусов функций. Известны два вида указанных антивирусных средства:

- программы-фильтры,
- аппаратные средства контроля.

Программы-фильтры, называемые также резидентными сторожами и мониторами, постоянно находятся в оперативной памяти и перехватывают заданные прерывания, с целью контроля подозрительной действий. При этом они могут блокировать “опасные” действия или выдавать запрос пользователю.

Действия, подлежащие контролю, могут быть следующими: модификация главной загрузочной записи (MBR) и загрузочных записей логических дисков и ГМД, запись по абсолютному адресу, низкоуровневое форматирование диска, оставление в оперативной памяти резидентного модуля и др. Как и ревизоры, фильтры часто являются “навязчивыми” и создают определенные неудобства в работе пользователя. Примером фильтра является программа Vsafe ОС MS-DOS.

Встроенные аппаратные средства ПК обеспечивают контроль модификации системного загрузчика и таблицы разделов жесткого диска, находящихся в главном загрузочном секторе диска (MBR). Включение указанных возможностей в ПК осуществляется с помощью программы Setup, расположенной в ПЗУ. Следует указать, что программу Setup можно обойти в случае замены загрузочных секторов путем непосредственного обращения к портам ввода-вывода контроллеров жесткого и гибкого дисков.

Наиболее полная защита от вирусов может быть обеспечена с помощью специальных контроллеров аппаратной защиты. Такой контроллер подключается к ISA-шине ПК и на аппаратном уровне контролирует *все* обращения к дисковой подсистеме компьютера. Это не позволяет вирусам маскировать себя. Контроллер может быть сконфигурирован так, чтобы контролировать отдельные файлы, логические разделы, “опасные” операции и т.д. Кроме того, контроллеры могут выполнять различные дополнительные функции защиты, например, обеспечивать разграничение доступа и шифрование.

Примером специальных контроллеров аппаратной защиты является плата Sheriff предприятия ФомСофт.

К недостаткам указанных контроллеров, как ISA-плат, относят отсутствие системы автоконфигурирования, и как следствие, возможность возникновения конфликтов с некоторыми системными программами, в том числе антивирусными.

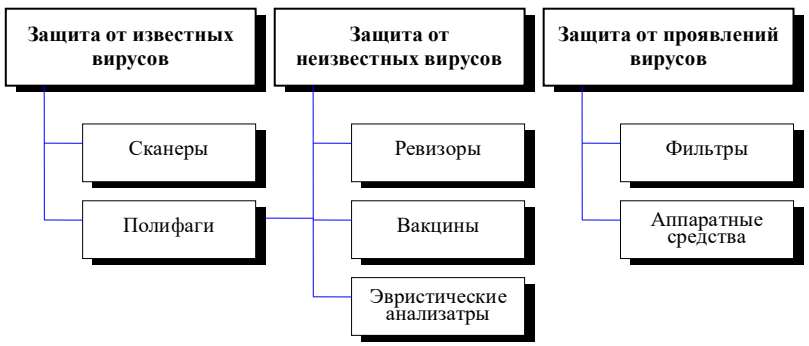


Рис. 8. Уровни и средства антивирусной защиты

Основная литература: [1] с.122-128, [2] с.16-26.

Дополнительная литература: **[9] с.1025-1040.**

Контрольные вопросы:

1. Перечислите уровни антивирусной защиты.
2. Какие программы называются сканерами.
3. Какие функции выполняют полифаги.
4. Что выполняют программы ревизоры.
5. Как работают фильтры.

Идентификация.

Основой любых систем ОБИ являются идентификация и аутентификация, так как все механизмы защиты информации рассчитаны на работу с поименованными субъектами и объектами АС. Напомним, что в качестве субъектов АС могут выступать как пользователи, так и процессы, а в качестве объектов АС — информация и другие информационные ресурсы системы.

Присвоение субъектам и объектам доступа личного идентификатора и сравнение его с заданным перечнем называется *идентификацией.* Идентификация обеспечивает выполнение следующих функций ОБИ:

- установление подлинности и определение полномочий субъекта при его допуске в систему,
- контролирование установленных полномочий в процессе сеанса работы;
- регистрация действий и др.

Аутентификацией (установлением подлинности*)* называется проверка принадлежности субъекту доступа предъявленного им идентификатора и подтверждение его подлинности. Другими словами, аутентификация заключается в проверке: является ли подключающийся субъект тем, за кого он себя выдает.

Общая процедура идентификации и аутентификации пользователя при его доступе в АС представлена на рис. 9. Если в процессе аутентификации подлинность субъекта установлена, то система защиты информации должна определить его полномочия (совокупность прав). Это необходимо для последующего контроля и разграничения доступа к ресурсам.

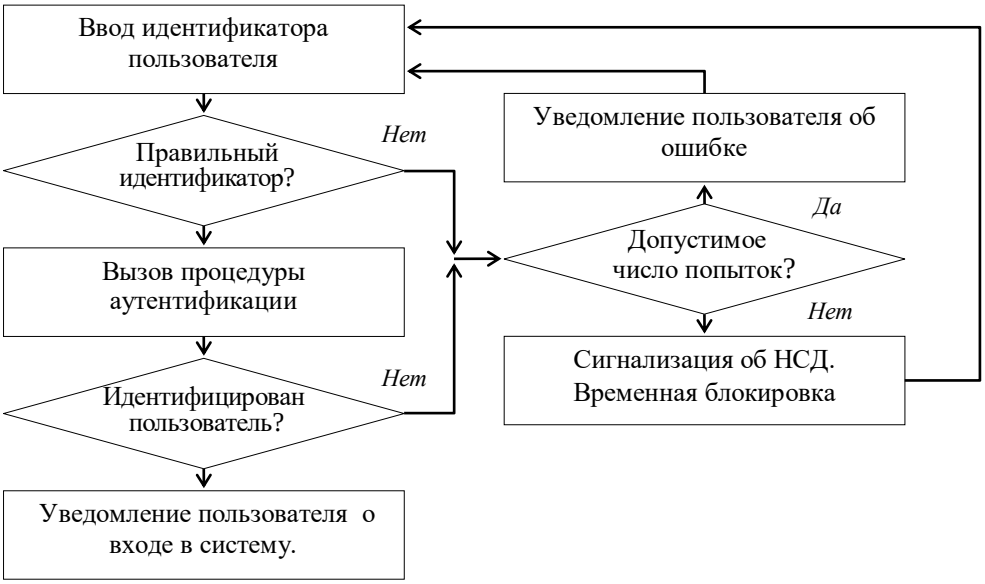


рис. 9. Общая процедура идентификации и аутентификации пользователя

Классическая процедура идентификации и аутентификации

По контролируемому компоненту системы способы аутентификации можно разделить на аутентификацию партнеров по общению и аутентификацию источника данных. Аутентификация партнеров по общению используется при установлении (и периодической проверке) соединения во время сеанса. Она служит для предотвращения таких угроз, как маскарад и повтор предыдущего сеанса связи. Аутентификация источника данных — это подтверждение подлинности источника отдельной порции данных.

По направленности аутентификация может быть односторонней (пользователь доказывает свою подлинность системе, например при входе в систему) и двусторонней (взаимной).

Обычно методы аутентификации классифицируют по используемым средствам. В этом случае указанные методы делят на четыре группы:

1. Основанные на знании лицом, имеющим право на доступ к ресурсам системы, некоторой секретной информации — пароля.
2. Основанные на использовании уникального предмета: жетона, электронной карточки и др.
3. Основанные на измерении биометрических параметров человека — физиологических или поведенческих атрибутах живого организма.
4. Основанные на информации, ассоциированной с пользователем, например с его координатами.

Рассмотрим эти группы.

1. Наиболее распространенными простыми и привычными являются методы аутентификации, основанные на *паролях* — секретных идентификаторах субъектов. Здесь при вводе субъектом своего пароля подсистема аутентификации сравнивает его с паролем, хранящимся в базе эталонных данных в зашифрованном виде. В случае совпадения паролей подсистема аутентификации разрешает доступ к ресурсам АС.

Парольные методы следует классифицировать по степени изменяемости паролей:

- методы, использующие постоянные (многократно используемые) пароли,
- методы, использующие одноразовые (динамично изменяющиеся) пароли.

В большинстве АС используются многоразовые пароли. В этом случае пароль пользователя не изменяется от сеанса к сеансу в течение установленного администратором системы времени его действительности. Это упрощает процедуры администрирования, но повышает угрозу рассекречивания пароля. Известны множество способов вскрытия пароля: от подсмотра через плечо до перехвата сеанса связи. Вероятность вскрытия злоумышленником пароля повышается, если пароль несет смысловую нагрузку (год рождения, имя девушки), небольшой длины, набран на одном регистре, не имеет ограничений на период существования и т.д. Важно, разрешено ли вводить пароль только в диалоговом режиме или есть возможность обращаться из программы. В последнем случае, возможно запустить программу по подбору паролей - “дробилку”.

Более надежный способ — использование одноразовых или динамически меняющихся паролей.

Известны следующие методы парольной защиты, основанные на одноразовых паролях:

- методы модификации схемы простых паролей;
- методы “запрос-ответ”;
- функциональные методы.

В первом случае пользователю выдается список паролей. При аутентификации система запрашивает у пользователя пароль, номер в списке которого определен по случайному закону. Длина и порядковый номер начального символа пароля тоже могут задаваться случайным образом.

При использовании метода “запрос-ответ” система задает пользователю некоторые вопросы общего характера, правильные ответы на которые известны только конкретному пользователю.

Функциональные методы основаны на использовании специальной функции парольного преобразования ***f(x)***. Это позволяет обеспечить возможность изменения (по некоторой формуле) паролей пользователя во времени. Указанная функция должна удовлетворять следующим требованиям:

- для заданного пароля *x* легко вычислить новый пароль ***y = f(x)***;
- зная ***x*** и ***y***, сложно или невозможно определить функцию ***f(x)***.

Методы аутентификации, основанные на измерении биометрических параметров человека, обеспечивают почти 100%-ую идентификацию, решая проблемы утери или утраты паролей и личных идентификаторов. Однако методы нельзя использовать при идентификации процессов или данных (объектов данных), они только начинают развиваться (имеются проблемы со стандартизацией и распространением), требуют пока сложного и дорогостоящего оборудования. Это обусловливает их использование пока только на особо важных объектах и системах, главным образом в МО РФ.

Примерами внедрения указанных методов являются системы идентификации пользователя по рисунку радужной оболочки глаза, отпечаткам ладони, формам ушей, инфракрасной картине капиллярных сосудов, по почерку, по запаху, по тембру голоса и даже по ДНК (см. табл.).

Новым направлением является использование биометрических характеристик в интеллектуальных расчетных карточках, жетонах-пропусках и элементах сотовой связи. Например, при расчете в магазине предъявитель карточки кладет палец на сканер в подтверждение, что карточка действительно его.

Примеры методов биометрии

Физиологические методы	**Поведенческие методы**
• Снятие отпечатков пальцев • Сканирование радужной оболочки глаза • Сканирование сетчатки глаза • Геометрия кисти руки • Распознавание черт лица	• Анализ подписи • Анализ тембра голоса • Анализ клавиатурного почерка

Назовем наиболее используемые биометрические атрибуты и соответствующие системы.

A. Отпечатки пальцев. Такие сканеры имеют небольшой размер, универсальны, относительно недороги. Биологическая повторяемость отпечатка пальца составляет 10^{-5}%. В настоящее время пропагандируются правоохранительными органами из-за крупных ассигнований в электронные архивы отпечатков пальцев.
B. Геометрия руки. Соответствующие устройства используются, когда из-за грязи или травм трудно применять сканеры пальцев. Биологическая повторяемость геометрии руки около 2-х %.
C. Радужная оболочка глаза. Данные устройства обладают наивысшей точностью. Теоретическая вероятность совпадения двух радужных оболочек составляет 1 из 10^{78}.
D. Термический образ лица. Системы позволяют идентифицировать человека на расстоянии до десятков метров. В комбинации с поиском данных по базе данных такие системы используются для опознания авторизованных сотрудников и отсеивания посторонних. Однако при изменении освещенности сканеры лица имеют относительно высокий процент ошибок.
E. Голос. Проверка голоса удобна для использования в телекоммуникационных приложениях. Необходимые для этого 16-разрядная звуковая плата и конденсаторный микрофон стоят менее 25 $. Вероятность ошибки составляет 2-5%. Данная технология подходит для верификации по голосу по телефонным каналам связи, она более надежна по сравнению с частотным набором личного номера. Сейчас развиваются направления идентификации личности и его состояния по голосу — возбужден, болен, говорит правду, не в себе и т.д.
F. Ввод с клавиатуры. Здесь при вводе, например, пароля отслеживаются скорость и интервалы между нажатиями.
G. Подпись. Для контроля рукописной подписи используются дигитайзеры.

Основная литература: [1]с.122-128, [2] с.16-26, [5] с.12-19.

Дополнительная литература: **[9] с.1028-1040.**

Контрольные вопросы:

1. Что называется идентификацией.
2. Как связаны идентификация и аутентификация.
3. Какие способы идентификации существуют.
4. Какой метод идентификации дают максимальный результат.
5. Что относится к биометрическим параметрам.

Хэш-функции и электронно-цифровые подписи.

ТРЕБОВАНИЯ К ХЭШ-ФУНКЦИЯМ

Хэш-функцией называется односторонняя функция, предназначенная для получения *дайджеста* или "отпечатков пальцев" файла, сообщения или некоторого блока данных.

Хэш-код создается функцией H:

$h = H(M)$

Где M является сообщением произвольной длины и h является *хэш-кодом* фиксированной длины.

Рассмотрим требования, которым должна соответствовать *хэш-функция* для того, чтобы она могла использоваться в качестве аутентификатора сообщения. Рассмотрим очень простой пример *хэш-функции*. Затем проанализируем несколько подходов к построению *хэш-функции*.

Хэш-функция H, которая используется для аутентификации сообщений, должна обладать следующими свойствами:

1. *Хэш-функция* H должна применяться к блоку данных любой длины.
2. *Хэш-функция* H создает выход фиксированной длины.
3. H (M) относительно легко (за полиномиальное время) вычисляется для любого значения M.
4. Для любого данного значения *хэш-кода* h вычислительно невозможно найти M такое, что H (M) = h.
5. Для любого данного x вычислительно невозможно найти $y \neq x$, что H (y) = H (x).
6. Вычислительно невозможно найти произвольную пару (x, y) такую, что H (y) = H (x).

Первые три свойства требуют, чтобы *хэш-функция* создавала *хэш-код* для любого сообщения.

Четвертое свойство определяет требование односторонности *хэш-функции*: легко создать *хэш-код* по данному сообщению, но невозможно восстановить сообщение по данному *хэш-коду*. Это свойство важно, если аутентификация с использованием *хэш-функции* включает секретное значение. Само секретное значение может не посылаться, тем не менее, если *хэш-функция* не является односторонней, противник может легко раскрыть секретное значение следующим образом. При перехвате передачи атакующий получает сообщение M и *хэш-код* $C = H(S_{AB} \| M)$. Если атакующий может инвертировать *хэш-функцию*, то, следовательно, он может получить $S_{AB} \| M = H^{-1}(C)$. Так как атакующий теперь знает и M и $S_{AB} \| M$, получить S_{AB} совсем просто.

Пятое свойство гарантирует, что невозможно найти другое сообщение, чье значение *хэш-функции* совпадало бы со значением *хэш-функции* данного сообщения. Это предотвращает подделку аутентификатора при использовании зашифрованного *хэш-кода*. В данном случае противник может читать сообщение и, следовательно, создать его *хэш-код*. Но так как противник не владеет секретным ключом, он не имеет возможности изменить сообщение так, чтобы получатель этого не обнаружил . Если данное свойство не выполняется, атакующий имеет возможность выполнить следующую последовательность действий: перехватить сообщение и его зашифрованный *хэш-код*, вычислить *хэш-код* сообщения, создать альтернативное сообщение с тем же самым *хэш-кодом*, заменить исходное сообщение на поддельное. Поскольку *хэш-коды* этих сообщений совпадают, получатель не обнаружит подмены.

Хэш-функция, которая удовлетворяет первым пяти свойствам, называется ***простой или слабой хэш-функцией***. Если кроме того выполняется шестое свойство, то такая функция называется ***сильной хэш-функцией***. Шестое свойство защищает против класса атак, известных как атака "*день рождения*".

ПРОСТЫЕ ХЭШ-ФУНКЦИИ

Все *хэш-функции* выполняются следующим образом. Входное значение (сообщение, файл и т.п.) рассматривается как последовательность n-битных блоков. Входное значение обрабатывается последовательно блок за блоком, и создается m-битное значение *хэш-кода*.

Одним из простейших примеров *хэш-функции* является побитный XOR каждого блока:

$C_i = b_{i1} \oplus b_{i2} \oplus \ldots \oplus b_{ik}$, где C_i - i-ый бит *хэш-кода*, $1 \leq i \leq n$., k - число n-битных блоков входа, b_{ij} - i-ый бит в j-ом блоке, $\oplus$- операция XOR.

В результате получается *хэш-код* длины n, известный как продольный избыточный контроль. Это эффективно при случайных сбоях для проверки целостности данных.

Часто при использовании подобного продольного избыточного контроля для каждого блока выполняется однобитный циклический сдвиг после вычисления *хэш-кода*. Это можно описать следующим образом.

- Установить n-битный *хэш-код* в ноль.
- Для каждого n-битного блока данных выполнить следующие операции:
  - сдвинуть циклически текущий *хэш-код* влево на один бит;
  - выполнить операцию XOR для очередного блока и *хэш-кода*.

Это даст эффект "случайности" входа и уничтожит любую регулярность, которая присутствует во входных значениях.

Хотя второй вариант считается более предпочтительным для обеспечения целостности данных и предохранения от случайных сбоев, он не может использоваться для обнаружения преднамеренных модификаций передаваемых сообщений. Зная сообщение, атакующий легко может создать новое сообщение, которое имеет тот же самый *хэш-код*. Для этого следует подготовить альтернативное сообщение и затем присоединить n-битный блок, который является *хэш-кодом* нового сообщения, и блок, который является *хэш-кодом* старого сообщения.

Хотя простого XOR или ротационного XOR (RXOR) недостаточно, если целостность обеспечивается только зашифрованным *хэш-кодом*, а само сообщение не шифруется, подобная простая функция может использоваться, когда все сообщение и присоединенный к нему *хэш-код* шифруются. Но и в этом случае следует помнить о том, что подобная *хэш-функция* не может проследить за тем, чтобы при передаче последовательность блоков не изменилась. Это происходит в силу того, что данная *хэш-функция* определяется следующим образом: для сообщения, состоящего из последовательности 64-битных блоков $X_1, X_2, \ldots, X_N$, определяется *хэш-код* C как поблочный XOR всех блоков, который присоединяется в качестве последнего блока:

$$C = X_{N+1} = X_1 \oplus X_2 \oplus \ldots \oplus X_N$$

Затем все сообщение шифруется, включая *хэш-код*, в режиме CBC для создания зашифрованных блоков $Y_1, Y_2, \ldots, Y_{N+1}$. По определению CBC имеем:

$$X_1 = IV \oplus D_K [Y_1]$$

$$X_i = Y_{i-1} \oplus D_K [Y_i]$$

$$X_{N+1} = Y_N \oplus D_K [Y_{N+1}]$$

Но X_{N+1} является *хэш-кодом*:

$$X_{N+1} = X_1 \oplus X_2 \oplus \ldots \oplus X_N =$$

$$(IV \oplus D_K [Y_1]) \oplus (Y_1 \oplus D_K [Y_2]) \oplus \ldots \oplus$$

$$(Y_{N-1} \oplus D_K [Y_N])$$

Так как сомножители в предыдущем равенстве могут вычисляться в любом порядке, следовательно, *хэш-код* не будет изменен, если зашифрованные блоки будут переставлены.

Первоначальный стандарт, предложенный NIST, использовал простой XOR, который применялся к 64-битным блокам сообщения, затем все сообщение шифровалось, используя режим CBC.

Требования к цифровой подписи

Аутентификация защищает двух участников, которые обмениваются сообщениями, от воздействия некоторой третьей стороны. Однако простая аутентификация не защищает участников друг от друга, тогда как и между ними тоже могут возникать определенные формы споров.

Например, предположим, что Джон посылает Мери аутентифицированное сообщение, и аутентификация осуществляется на основе общего секрета. Рассмотрим возможные недоразумения, которые могут при этом возникнуть:

- Мери может подделать сообщение и утверждать, что оно пришло от Джона. Мери достаточно просто создать сообщение и присоединить аутентификационный код, используя ключ, который разделяют Джон и Мери.
- Джон может отрицать, что он посылал сообщение Мери. Так как Мери может подделать сообщение, у нее нет способа доказать, что Джон действительно посылал его.

В ситуации, когда обе стороны не доверяют друг другу, необходимо нечто большее, чем аутентификация на основе общего секрета. Возможным решением подобной проблемы является использование *цифровой подписи*. *Цифровая подпись* должна обладать следующими свойствами:

1. Должна быть возможность проверить автора, дату и время создания подписи.
2. Должна быть возможность аутентифицировать содержимое во время создания подписи.
3. Подпись должна быть проверяема третьей стороной для разрешения споров.

Таким образом, функция *цифровой подписи* включает функцию аутентификации.

На основании этих свойств можно сформулировать следующие требования к *цифровой подписи*:

1. Подпись должна быть битовым образцом, который зависит от подписываемого сообщения.
2. Подпись должна использовать некоторую уникальную информацию отправителя для предотвращения подделки или отказа.
3. Создавать *цифровую подпись* должно быть относительно легко.
4. Должно быть вычислительно невозможно подделать *цифровую подпись* как созданием нового сообщения для существующей *цифровой подписи*, так и созданием ложной *цифровой подписи* для некоторого сообщения.
5. *Цифровая подпись* должна быть достаточно компактной и не занимать много памяти.

Сильная хэш-функция, зашифрованная закрытым ключом отправителя, удовлетворяет перечисленным требованиям.

Существует несколько подходов к использованию функции *цифровой подписи*. Все они могут быть разделены на две категории: *прямые* и *арбитражные*.

Создание и проверка подписи состоит из следующих шагов:

Рис. 10.1. Создание и проверка подписи

1. Пользователь A создает пару ключей KR_A и KU_A, используемых для создания и проверки подписи передаваемых сообщений.
2. Пользователь A делает доступным некоторым надежным способом свой ключ проверки, т.е. *открытый ключ* KU_A. Составляющий пару *закрытый ключ* KR_A держится в секрете.
3. Если A хочет послать подписанное сообщение B, он создает подпись $E_{KRa}[M]$ для этого сообщения, используя свой *закрытый ключ* KR_A.
4. Когда B получает подписанное сообщение, он проверяет подпись $D_{KUa}[M]$, используя *открытый ключ* A KU_A. Никто другой не может подписать сообщение, так как этот *закрытый ключ* знает только A.

Основная литература: [1] с.157-160.

Дополнительная литература: **[9] с.944-960.**

Контрольные вопросы:

1. Что такое хэш-функция.
2. Требования к хэш-функциям.
3. Классификация хэш-функций.
4. Понятие электронно-цифровой подписи.
5. Требования к электронно-цифровым подписям.
6. Этапы создания и проверки подписи.

Аутентификация. Протоколы аутентификации.

При симметричном шифровании два участника, которые хотят обмениваться конфиденциальной информацией, должны иметь один и тот же ключ. Частота изменения ключа должна быть достаточно большой, чтобы у противника не хватило времени для полного перебора ключа. Следовательно, сила любой криптосистемы во многом зависит от технологии распределения ключа. Этот термин означает передачу ключа двум участникам, которые хотят обмениваться данными, таким способом, чтобы никто другой не мог ни подсмотреть, ни изменить этот ключ. Для двух участников A и B распределение ключа может быть выполнено одним из следующих способов.

1. Ключ может быть создан A и физически передан B.
2. *Третья сторона* может создать ключ и физически передать его A и B.
3. A и B имеют предварительно созданный и недолго используемый ключ, один участник может передать новый ключ другому, применив для шифрования старый ключ.
4. Если A и B каждый имеют безопасное соединение с третьим участником C, C может передать ключ по этому безопасному каналу A и B.

Первый и второй способы называются ручным распределением ключа. Это самые надежные способы распределения ключа, однако во многих случаях пользоваться ими неудобно и даже

невозможно. В распределенной системе любой хост или сервер должен иметь возможность обмениваться конфиденциальной информацией со многими аутентифицированными хостами и серверами. Таким образом, каждый хост должен иметь набор ключей, поддерживаемый динамически. Проблема особенно актуальна в больших распределенных системах.

Количество требуемых ключей зависит от числа участников, которые должны взаимодействовать. Если выполняется шифрование на сетевом или IP-уровне, то ключ необходим для каждой пары хостов в сети. Таким образом, если есть N хостов, то необходимое число ключей [N (N - 1)]/2. Если шифрование выполняется на прикладном уровне, то ключ нужен для каждой пары прикладных процессов, которых гораздо больше, чем хостов.

Третий способ распределения ключей может применяться на любом уровне стека протоколов, но если атакующий получает возможность доступа к одному ключу, то вся последовательность ключей будет раскрыта. Более того, все равно должно быть проведено первоначальное распространение большого количества ключей.

Поэтому в больших автоматизированных системах широко применяются различные варианты четвертого способа. В этой схеме предполагается существование так называемого центра распределения ключей (Key Destribution Centre - ***KDC***), который отвечает за распределение ключей для хостов, процессов и приложений. Каждый участник должен разделять уникальный ключ с *KDC*.

Использование центра распределения ключей основано на использовании иерархии ключей. Как минимум используется два типа ключей: *мастер-ключи* и *ключи сессии*.

Для обеспечения конфиденциальной связи между конечными системами используется временный ключ, называемый ***ключом сессии***. Обычно *ключ сессии* используется для шифрования транспортного соединения и затем уничтожается. Каждый *ключ сессии* должен быть получен по сети из центра распределения ключей. *Ключи сессии* передаются в зашифрованном виде, используя *мастер-ключ*, который разделяется между центром распределения ключей и конечной системой.

Эти *мастер-ключи* также должны распределяться некоторым безопасным способом. Однако при этом существенно уменьшается количество ключей, требующих ручного распределения. Если существует N участников, которые хотят устанавливать соединения, то в каждый момент времени необходимо [N (N - 1)]/2 *ключей сессии*. Но требуется только N *мастер-ключей*, по одному для каждого участника.

Время жизни *ключа сессии* как правило равно времени жизни самой сессии.

Чем чаще меняются *ключи сессии*, тем более безопасными они являются, так как противник имеет меньше времени для взламывания данного *ключа сессии*. С другой стороны, распределение *ключей сессии* задерживает начало любого обмена и загружает сеть. Политика безопасности должна сбалансировать эти условия для определения оптимального времени жизни конкретного *ключа сессии*.

Если соединение имеет долгое время жизни, то должна существовать возможность периодически менять *ключ сессии*.

Для протоколов, не поддерживающих соединение, таких как протокол, ориентированный на транзакции, нет явной инициализации или прерывания соединения. Следовательно, неясно, как часто надо менять *ключ сессии*. Большинство подходов основывается на использовании нового *ключа сессии* для каждого нового обмена. Наиболее часто применяется стратегия использования *ключа сессии* только для фиксированного периода времени или только для определенного количества транзакций.

ПРОТОКОЛЫ АУТЕНТИФИКАЦИИ

Рассмотрим основные протоколы, обеспечивающие как взаимную *аутентификацию* участников, так и *аутентификацию* только одного из участников.

Взаимная аутентификация

Данные протоколы применяются для взаимной *аутентификации* участников и для обмена *ключом сессии*.

Основной задачей таких протоколов является обеспечение конфиденциального распределения *ключа сессии* и гарантирование его своевременности, то есть протокол не должен допускать повторного использования старого *ключа сессии*. Для обеспечения конфиденциальности *ключи сессии* должны передаваться в зашифрованном виде. Вторая задача, обеспечение своевременности, важна, потому что существует угроза перехвата передаваемого сообщения и повторной его пересылки. Такие повторения в худшем случае могут позволять взломщику использовать скомпрометированный *ключ сессии*, при этом успешно подделываясь под другого участника. Успешное повторение может, как минимум, разорвать операцию *аутентификации* участников.

Такие повторы называются *replay-атаками*. Рассмотрим возможные примеры подобных *replay-атак*:

1. Простое повторение: противник просто копирует сообщение и повторяет его позднее.
2. Повторение, которое не может быть определено: противник уничтожает исходное сообщение и посылает скопированное ранее сообщение.

Один из возможных подходов для предотвращения *replay-атак* мог бы состоять в присоединении последовательного номера (sequence number) к каждому сообщению, используемому в *аутентификационном* обмене. Новое сообщение принимается только тогда, когда его последовательный номер правильный. Трудность данного подхода состоит в том, что каждому участнику требуется поддерживать значения sequence number для каждого участника, с которым он взаимодействует в данный момент. Поэтому обычно sequence number не используются для *аутентификации* и обмена ключами. Вместо этого применяется один из следующих способов:

1. *Отметки времени*: участник A принимает сообщение как не устаревшее только в том случае, если оно содержит *отметку времени*, которая, по мнению A, соответствует текущему времени. Этот подход требует, чтобы часы всех участников были синхронизированы.
2. Запрос/ответ: участник A посылает в запросе к B случайное число (***nonce*** - number only once) и проверяет, чтобы ответ от B содержал корректное значение этого *nonce*.

Считается, что подход с *отметкой времени* не следует использовать в приложениях, ориентированных на соединение, потому что это технически трудно, так как таким протоколам, кроме поддержки соединения, необходимо будет поддерживать синхронизацию часов различных процессоров. При этом возможный способ осуществления успешной атаки может возникнуть, если временно будет отсутствовать синхронизация часов одного из участников. В результате различной и непредсказуемой природы сетевых задержек распределенные часы не могут поддерживать точную синхронизацию. Следовательно, процедуры, основанные на любых *отметках времени*, должны допускать окно времени, достаточно большое для приспособления к сетевым задержкам, и достаточно маленькое для минимизации возможности атак.

С другой стороны, подход запрос/ответ не годится для приложений, не устанавливающих соединения, так как он требует предварительного рукопожатия перед началом передач, тем самым отвергая основное свойство транзакции без установления соединения. Для таких приложений доверие к некоторому безопасному серверу часов и постоянные попытки каждой из частей синхронизировать свои часы с этим сервером может быть оптимальным подходом.

Основная литература: [1] с.171-178, [6] с.469-486.

Дополнительная литература: **[9] с.958-962**

Контрольные вопросы:

1. Что такое аутентификация.
2. Какие протоколы аутентификации существуют.
3. Какие протоколы относятся к протоколом полного доверия.
4. Какие протоколы являются протоколами неполного доверия.

5. Что такое взаимная аутентификация.

Системы защиты информации (СЗИ).

Система защиты информации (СЗИ) в самом общем виде может быть определена как организованная совокупность всех средств, методов и мероприятий, выделяемых в системах обработки данных для решения в ней выбранных задач защиты [Герасим.§ 8.1].

Помимо общего концептуального требования к СЗИ предъявляется еще целый ряд более конкретных, целевых требований, которые могут быть разделены на функциональные, эргономические, экономические, технические и организационные.

Сформированная к настоящему времени система включает следующий перечень общеметодологических принципов: концептуальное единство; адекватность требованиям; гибкость (адаптируемость); функциональная самостоятельность; удобство использования; минимизация предоставляемых прав; полпота контроля; активность реагирования; экономичность.

Проектирование систем защиты информации заключается в том, чтобы для заданной системы обработки данных создать оптимальные механизмы обеспечении защиты информации и механизмы управления ими.

Выбор той или иной постановки задачи зависит, прежде всего от характера защищаемой информации, вернее - от характера тайны, содержавшейся в защищаемой информации.

Государственные секреты - защищаемые государством сведения, составляющие государственную и служебную тайны, распространение которых ограничивается государством с целью осуществления эффективной военной, экономической, научно-технической, внешнеэкономической, внешнеполитической, разведывательной, контрразведывательной, оперативно-розыскной и иной деятельности, не вступающей в противоречие с общепринятыми нормами международного права.

Государственная тайна - сведения военного, экономического, политического и иного характера, разглашение или утрата которых наносит или может нанести ущерб национальной безопасности Республики Казахстан.

Служебная тайна - сведения, имеющие характер отдельных данных, которые могут входить в состав государственной тайны, разглашение или утрата которых может нанести ущерб национальным интересам государства, интересам государственных органов и организаций Республики Казахстан.

Проектирование СЗИ может осуществляться в различных условиях, причем на различие этих условий определяющее влияние оказывают следующие два параметра: состояние той системы обработки данных, для которой разрабатывается СЗИ, и уровень затрат, которые могут быть допущены на создание СЗИ. Что касается первого параметра, то, очевидно, можно выделить три различных состояния СОД: система функционирует, имеется готовый проект системы, система еще только проектируется.

В соответствии с общеизвестной методологией проектирования больших систем последовательность разработки индивидуального проекта СЗИ представлена на рис. Рассмотрим общее содержание выделенных этапов проектирования.

Этап 1. Обоснование требований и анализ условий защиты информации: формирование факторов, влияющих на защиту информации в СОД; выбор и обоснование требований по защите информации; анализ условий защиты информации в СОД.

Этап 2. Определение функций защиты информации - обоснование перечня тех функций защиты, осуществление которых позволит обеспечить требуемый уровень защиты.

Этап 3. Определение перечня потенциально возможных каналов несанкционированного получения информации; классификация каналов; определение характеристик каналов.

Этап 4. Обоснование перечня подлежащих решению задач защиты: определение перечня задач защиты информации, перекрывающих все потенциально возможные каналов несанкционированного получения информации; классификация задач защиты информации; определение эффективности

решении задач защиты с точки зрения перекрытия каналов несанкционированного получения информации; выбор подлежащих решению задач защиты информации.

Этап 5. Выбор средств, достаточных для решения выбранных задач защиты информации: определение перечня типовых проектных решений, которые могут быть использованы для решения задач защиты информации; классификация типовых проектных решений; определение эффективности использования выбранных типовых проектных решений; определение оптимального набора типовых проектных решений, необходимых для решения задач защиты информации с заданной эффективностью;

Этап 6. Оценка эффективности защиты информации в условиях выбранных задач защиты информации: оценка защищенности информации в условиях решений выбранных задач выбранными средствами; сравнение полученных оценок защищенности с требуемой (при этом учитываются и стоимостные расходы на обеспечение защиты).

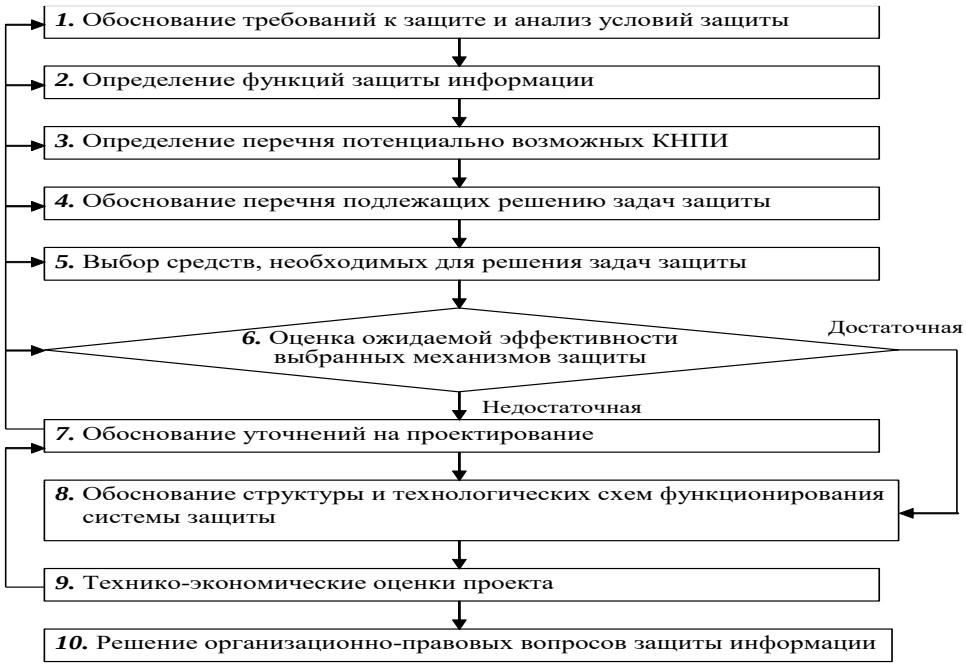
Этап 7. Обоснование уточнений задания на проектирование: определение причин недостаточного обеспечения защиты информации; выбор рационального варианта уточнения задания на проектирование СЗИ.

Этап 8. Обоснование структуры и технологии функционирования СЗИ: определение общей структуры СЗИ, ее подсистем и ядра защиты информации; определение состава ТО, МО, ПО, ИО, ОО и ЛО, нормативно-правовых актов и организационно-технических мероприятий по защите информации; обоснование структуры компонентов и архитектуры СЗИ; обоснование технологических схем функционирования СЗИ во всех режимах автоматизированной обработки информации; обоснование технологии оперативно-диспетчерского управления защитой информации; обоснование схемы обеспечения повседневной деятельности СЗИ.

Этап 9. Технико-экономические оценки проекта: оценка надежности выполнения функций защиты информации; оценка живучести СЗИ, т.е. способности выполнять свои функции в экстремальных условиях функционирования СОД; экономические оценки СЗИ; оценка степени влияния СЗИ на временные характеристики СОД при автоматизированной обработке информации.

Этап 10. Решение организационно-правовых вопросов защиты информации: определение прав и обязанностей по защите информации всех подразделений и лиц, участвующих в процессах функционирования СОД; разработка правил осуществления всех процедур и мероприятий по защите информации; обучение всех лиц, участвующих в процессах функционирования СОД, выполнению правил обеспечения защиты информации; обеспечение всех подразделений и лиц необходимыми руководящими и методическими материалами (документами); разработка правил и порядка контроля функционирования СЗИ; определение мер ответственности за нарушение правил защиты информации; разработка порядка разрешения спорных и конфликтных ситуаций, относящихся к вопросам обеспечения защиты информации.

Проектирование корпоративной системы защиты информации. Цель функционирования корпоративной СЗИ - обеспечение защиты информации, обрабатываемой, передаваемой, хранимой в ИС, от преднамеренного или непреднамеренного разрушения, искажения и несанкционированного доступа, а также пресечение попыток нарушения целостности информации и работоспособности ИС.



Последовательность и содержание проектирования СЗИ

Основные функции корпоративной СЗИ:

- управление доступом и защита корпоративной ЛВС от несанкционированного доступа изнутри и извне (из общедоступных сетей, Интернета и т.д.);
- комплексная система антивирусной защиты, в том числе на уровне шлюзов и почтовых серверов;
- content - фильтрация;
- защищенный доступ пользователей ЛВС в общедоступные сети и Интернет;
- обнаружение атак;
- защита информационных потоков между ЛВС, рабочими станциями и серверами, а также в сетях Интернет/Интранет;
- идентификация и аутентификация пользователей ИС;
- обеспечение доступности сетевых сервисов и серверов;
- криптографическая защита информации;
- защита рабочих станций и серверов от несанкционированного доступа;
- защита общесистемного и прикладного ПО, файловых и почтовых серверов;
- защита электронного документооборота и корпоративных почтовых систем;
- системы оперативного восстановления после сбоев и катастроф.

Основная литература: [1] с.160-163,178:189, [4] с.4-34.

Контрольные вопросы:

1. Дайте определение системе защиты информации.
2. Перечислите общеметодологические принципы построения СЗИ
3. Каков порядок проектирования и разработки СЗИ?
4. Общее содержание этапов проектирования больших систем
5. Назовите основные функции корпоративной СЗИ

Политика информационной безопасности предприятия.

Применение технических средств может обеспечить эффективную защиту только в совокупности с организационными мероприятиями Под ***политикой информационной безопасности*** предприятия в

общем случае будем понимать совокупность распорядительных документов, регламентирующих все аспекты обработки информации на предприятии

Прежде всего, необходимо определиться с тем, какая информация обрабатывается на предприятии и как она может быть классифицирована (секретная, конфиденциальная, служебная тайна, ограниченного доступа и др.). Не определив, что защищать, невозможно в принципе решать вопрос о том, как защищать. При классификации информации необходимо учитывать формализованные признаки ее отнесения к какой-либо категории, например, к секретной или конфиденциальной.

Концепция обеспечения информационной безопасности предприятия техническими мерами защиты. Концепция обеспечения информационной безопасности задает основные принципы обработки информации на предприятии и ее технической защиты. В общем случае эта концепция должна включать:

1. Порядок обработки защищаемой информации - определяется, какая информация обрабатывается вручную, какая с использованием средств вычислительной техники, какая информация предназначена для внутреннего использования, какая предполагает обмен вне предприятия и т.д.

2. Характеристику вычислительных средств, применяемых для обработки информации, требующей защиты. Сюда относятся архитектурные принципы построения корпоративной сети, используемые информационные технологии, ОС, приложения и т.д.

3. Характеристику предполагаемого использования вычислительных средств для обработки защищаемой информации - где хранится, где и как обрабатывается, каким образом вводится и выводится, как передается по сети и т.д. Таким образом, эта характеристика позволяет выявить объекты корпоративной сети (компьютеры, информационные потоки и т.д.), требующие защиты. Результатом этого будут сформулированные требования к распределению ресурсов защищаемых объектов (компьютеров) между субъектами доступа - разграничительная политика доступа к ресурсам.

4. Характеристику распределения всей совокупности задач управления функционированием корпоративной сети, каким-либо образом влияющих на безопасность защищаемой информации: задачи защиты информации, задачи системного и иного администрирования, задачи инсталляции ПО, задачи обработки информации и т.д.

Здесь концептуально должно быть задано распределение задач между всеми субъектами доступа к защищаемой информации: сотрудники службы безопасности, администраторы (безопасности, системный, приложений, сети и т.д.), пользователи, сотрудники службы эксплуатации, начальники подразделений и т.д.

В рамках решения данной совокупности задач определяется потенциальный злоумышленник, т.е., от кого же следует защищать информацию. Данные субъекты должны исключаться из схемы управления функционированием корпоративной сети, прежде всего, из схемы управления информационной безопасностью. Результатом должна быть разработка концепции администрирования информационной безопасности корпоративной сети предприятия. При этом должны быть определены субъекты (сотрудники службы безопасности, администратор безопасности и т.д.) и объекты (рабочие станции, серверы, информационные технологии и т.д.) администрирования.

5. Требования к технологии защиты информации, включающие:

• требования к механизмам защиты в части реализации заданной разграничительной политики доступа к ресурсам;

• требования к механизмам защиты в части противодействия НСД определенных потенциальных злоумышленников. Данные требования должны выдвигаться с учетом существующей статистики и потенциальных возможностей осуществления угроз, создаваемых определенными потенциальными злоумышленниками;

• требования к механизмам, реализующим выбранную схему управления (администрирования) техническими средствами защиты информации.

6. Характеристику взаимодействия субъектов с целью формирования, задания и контроля разграничительной политики доступа к ресурсам. При этом определяется:

- порядок назначения и изменения прав доступа субъекта к ресурсу;
- порядок их задания в конфигурационных файлах средств технической защиты;
- порядок контроля за выполнением субъектами заданных разграничений и порядок принятия решений при обнаружении фактов НСД;
- порядок проведения регламентных работ, инсталляции ПО и т.д.

7. Инструкции всех субъектов для доступа к конфиденциальной информации, где должны быть определены их права, обязанности, ответственность за нарушение разграничительной политики доступа. Данные инструкции должны быть доведены (за подписью) до каждого субъекта доступа к защищаемой информации.

Концепция обеспечения информационной безопасности организационными мерами защиты. В рамках данного документа регламентируются все организационные мероприятия, реализуемые с целью защиты информации: порядок контроля доступа в помещения, порядок работы с внешними носителями (выдача пользователям, хранение, утилизация) и др. Организационные меры должны рассматриваться в совокупности с возможностями (требованиями) средств технической защиты и соответствующим образом их дополнять.

Разработка политики информационной безопасности. Политика информационной безопасности - это основополагающий документ, регламентирующий все мероприятия, реализуемые на предприятии с целью обеспечения компьютерной безопасности. Политика информационной безопасности – это та основа, без которой невозможно приступать ни к выбору, ни к проектированию средств защиты информации.

Разработка политики информационной безопасности в общем случае является итерационной процедурой, состоящей из выполнения следующих шагов.

Первый шаг – разработка гипотетически идеальной для предприятия политики, куда закладываются те требования, которые идеально подходят для данного предприятия – формулируется некий идеальный профиль защиты.

Второй шаг – выбор (либо разработка) системы защиты, максимально обеспечивающей выполнение требований гипотетически идеальной политики информационной безопасности.

Третий шаг – определение требований политики информационной безопасности, которые не выполняются системой защиты.

Далее возможны следующие пути:

- осуществление доработки выбранного средства защиты в части выполнения ими сформулированных требований;
- выполнение (по возможности) данных требований организационными мерами;
- пересмотр политики информационной безопасности (если это возможно) с учетом возможностей выбранного средства защиты информации. Сделано это должно быть таким образом, чтобы не выполняемые системой защиты требования не выдвигались в качестве основных требований к обеспечению информационной безопасности.

Основная литература: [1] с.163-170.

Дополнительная литература: **[8] с.159-164, [9] с. 81-83,792-794.**

Контрольные вопросы:

1. Какие аспекты должны найти свое отражение в политике безопасности предприятия?
2. Что должна включать концепция обеспечения информационной безопасности предприятия техническими мерами защиты?
3. Шаги (этапы) разработки политики информационной безопасности?

Служба информационной безопасности.

Служба информационной безопасности (СИБ) представляет собой нештатную, функционально-ориентированную группу специалистов, в состав которой входят:

1. заместитель Директора по безопасности и защите информации;
2. администратор безопасности АС;
3. администратор системы;
4. администраторы групп.

СИБ создается для непосредственной организации и обеспечения эффективного функционирования системы защиты информации.

Основными задачами СИБ являются:

- формирование требований к системе защиты в процессе создания АС;
- участие в проектировании системы защиты, ее испытаниях и приемке в эксплуатацию;
- планирование, организация и обеспечение функционирования системы защиты АС;
- распределение между пользователями необходимых реквизитов защиты;
- контроль функционирования системы защиты и ее элементов;
- тестирование системы защиты;
- обучение пользователей АС правилам безопасной обработки информации;
- принятие мер реагирования на попытки НСД к информации и нарушения правил функционирования системы защиты;
- выполнение восстановительных процедур после фактов нарушения безопасности;
- устранения слабостей в системе защиты и совершенствование механизмов защиты.

Для обеспечения эффективной работы СИБ необходимо отразить основные организационные вопросы принятой политики безопасности в соответствующих Инструкциях и Распоряжениях. В них в первую очередь должны быть определены:

- должностные обязанности групп пользователей;
- правила доступа к информации;
- правила разграничения доступа к информации;
- мероприятия по обеспечению контроля и функционирования системы защиты информации;
- меры реагирования на нарушение режима безопасности;
- планирование и организация восстановительных работ.

Разработка сетевых аспектов политики безопасности

При разработке и проведении политики безопасности в жизнь целесообразно руководствоваться следующими принципами:

- невозможность миновать защитные средства;
- усиление самого слабого звена;
- невозможность перехода в небезопасное состояние;
- минимизация привилегий;
- разделение обязанностей;
- эшелонированность обороны;
- разнообразие защитных средств;
- простота и управляемость информационной системы;
- обеспечение всеобщей поддержки мер безопасности.

Поясним смысл перечисленных принципов.

Принцип невозможность миновать защитные средства. Если у злоумышленника или недовольного пользователя появится возможность миновать защитные средства, он, разумеется, так и сделает. Применительно к межсетевым экранам данный принцип означает, что все информационные

потоки в защищаемую сеть и из нее должны проходить через экран. Не должно быть «тайных» модемных входов или тестовых линий, идущих в обход экрана.

Принцип усиление самого слабого звена. Надежность любой обороны определяется самым слабым звеном. Часто самым слабым звеном оказывается не компьютер или программа, а человек, и тогда проблема обеспечения информационной безопасности приобретает нетехнический характер.

Принцип невозможности перехода в небезопасное состояние означает, что при любых обстоятельствах, в том числе нештатных, защитное средство либо полностью выполняет свои функции, либо полностью блокирует доступ. Образно говоря, если в крепости механизм подъемного моста ломается, мост должен оставаться в поднятом состоянии, препятствуя проходу неприятеля.

Принцип минимизации привилегий предписывает выделять пользователям и администраторам только те права доступа, которые необходимы им для выполнения служебных обязанностей.

Принцип разделения обязанностей предполагает такое распределение ролей и ответственности, при котором один человек не может нарушить критически важный для организации процесс. Это особенно важно, чтобы предотвратить злонамеренные или неквалифицированные действия системного администратора.

Принцип эшелонированности обороны предписывает не полагаться на один защитный рубеж, каким бы надежным он ни казался. За средствами физической защиты должны следовать программно-технические средства, за идентификацией и аутентификацией - управление доступом и, как последний рубеж, - протоколирование и аудит. Эшелонированная оборона способна по крайней мере задержать злоумышленника, а наличие такого рубежа, как протоколирование и аудит, существенно затрудняет незаметное выполнение злоумышленных действий.

Принцип разнообразия защитных средств рекомендует организовывать различные по своему характеру оборонительные рубежи, чтобы от потенциального злоумышленника требовалось овладение разнообразными и, по возможности, несовместимыми между собой навыками (например, умением преодолевать высокую ограду и знанием слабостей нескольких операционных систем).

Принцип простоты и управляемости информационной системы в целом и защитных средств в особенности. Только для простого защитного средства можно формально или неформально доказать его корректность. Только в простой и управляемой системе можно проверить согласованность конфигурации разных компонентов и осуществить централизованное администрирование. В этой связи важно отметить интегрирующую роль Web-сервиса, скрывающего разнообразие обслуживаемых объектов и предоставляющего единый, наглядный интерфейс. Соответственно, если объекты некоторого вида (скажем таблицы базы данных) доступны через Web, необходимо заблокировать прямой доступ к ним, поскольку в противном случае система будет сложной и трудноуправляемой.

Принцип всеобщей поддержки мер безопасности носит нетехнический характер. Если пользователи и/или системные администраторы считают информационную безопасность чем-то излишним или даже враждебным, режим безопасности сформировать заведомо не удастся. Следует с самого начала предусмотреть комплекс мер, направленный на обеспечение лояльности персонала, на постоянное обучение, теоретическое и, главное, практическое.

Анализ рисков - важнейший этап выработки политики безопасности. При оценке рисков, которым подвержены Internet-системы, нужно учитывать следующие обстоятельства:

• новые угрозы по отношению к старым сервисам, вытекающие из возможности пассивного или активного прослушивания сети. Пассивное прослушивание означает чтение сетевого трафика, а активное - его изменение (кражу, дублирование или модификацию передаваемых данных). Например, аутентификация удаленного клиента с помощью пароля многократного использования не может считаться надежной в сетевой среде, независимо от длины пароля;

• новые (сетевые) сервисы и ассоциированные с ними угрозы.

Ниже приведен примерный список вопросов для оказания помощи в определении политики безопасности предприятия для данной среды. Сами по себе вопросы достаточно прямые. Именно ответы могут стать сложными из-за неизвестного риска для информации, находящейся под угрозой. Во-первых, необходимо выполнить общую оценку в масштабах компании с последующим уточнением деталей для составных частей: внутреннего комплекса, внешнего подключения удаленного допуска и внешней сети Интернет.

- Какая информация является конфиденциальной и должна быть защищена?
- Как эта информация будет защищена?
- Будет ли эта конфиденциальная информация зашифрована?
- Будет ли существовать ограниченный доступ к информации?
- Кто может обратиться к информации и внести в ней изменения?
- Кто может аннулировать доступ к информации?

Кто имеет право настроить и задать конфигурацию инфраструктуры сети?

Основная литература: [1] с. 7-11.

Дополнительная литература: **[8] с. 28-36, [9] с. 65-88.**

Контрольные вопросы:

4. Кто входит в состав службы информационной безопасности (СИБ)?
5. Какие основные задач СИБ?
6. Какие основные организационные вопросы принятой ПБ должны быть отражены в соответствующих инструкциях и распоряжениях ?
7. При разработке и проведении политики безопасности в жизнь какими принципами целесообразно руководствоваться?
8. Что означает принцип невозможность миновать защитные средства применительно к межсетевым экранам?
9. Что предписывает принцип минимизации привилегий?
10. Какой примерный список вопросов для оказания помощи в определении политики безопасности предприятия?

Защита в сетях. Заключение.
КЛАССИФИКАЦИЯ СЕТЕВЫХ АТАК

В общем случае существует информационный поток от отправителя (файл, пользователь, компьютер) к получателю (файл, пользователь, компьютер):

Рис. 15.1. Информационный поток

Все атаки можно разделить на два класса: пассивные и активные.

I. Пассивная атака

Пассивной называется такая атака, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

Рис. 15.2. Пассивная атака

II. Активная атака

Активной называется такая атака, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. Различают следующие типы активных атак:

1. **Отказ в обслуживании** - DoS-атака (Denial of Service)

Отказ в обслуживании нарушает нормальное функционирование сетевых сервисов. Противник может перехватывать все сообщения, направляемые определенному адресату. Другим примером подобной атаки является создание значительного трафика, в результате чего сетевой сервис не сможет обрабатывать запросы законных клиентов. Классическим примером такой атаки в сетях TCP/IP является SYN-атака, при которой нарушитель посылает пакеты, инициирующие установление TCP-соединения, но не посылает пакеты, завершающие установление этого соединения. В результате может произойти переполнение памяти на сервере, и серверу не удастся установить соединение с законными пользователями.

Рис. 15.3. DoS-атака

2. **Модификация потока данных** - атака "man in the middle"

Модификация потока данных означает либо изменение содержимого пересылаемого сообщения, либо изменение порядка сообщений.

Рис. 15.4. Атака "man in the middle"

3. **Создание ложного потока (фальсификация)**

Фальсификация (нарушение аутентичности) означает попытку одного субъекта выдать себя за другого.

Рис. 15.5. Создание ложного потока

4. **Повторное использование**

Повторное использование означает пассивный захват данных с последующей их пересылкой для получения несанкционированного доступа - это так называемая replay-атака. На самом деле replay-атаки являются одним из вариантов фальсификации, но в силу того, что это один из наиболее

распространенных вариантов атаки для получения несанкционированного доступа, его часто рассматривают как отдельный тип атаки.

Рис. 15.6. Replay-атака

Перечисленные атаки могут существовать в любых типах сетей, а не только в сетях, использующих в качестве транспорта протоколы TCP/IP, и на любом уровне модели OSI. Но в сетях, построенных на основе TCP/IP, атаки встречаются чаще всего, потому что, во-первых, Internet стал самой распространенной сетью, а во-вторых, при разработке протоколов TCP/IP требования безопасности никак не учитывались.

МОДЕЛЬ СЕТЕВОГО ВЗАИМОДЕЙСТВИЯ

Модель безопасного сетевого взаимодействия в общем виде можно представить следующим образом:

Сообщение, которое передается от одного участника другому, проходит через различного рода сети. При этом будем считать, что устанавливается логический информационный канал от отправителя к получателю с использованием различных коммуникационных протоколов (например, TCP/IP).

Средства безопасности необходимы, если требуется защитить передаваемую информацию от противника, который может представлять угрозу конфиденциальности, аутентификации, целостности и т.п. Все технологии повышения безопасности имеют два компонента:

1. Относительно безопасная передача информации. Примером является шифрование, когда сообщение изменяется таким образом, что становится нечитаемым для противника, и, возможно, дополняется кодом, который основан на содержимом сообщения и может использоваться для аутентификации отправителя и обеспечения целостности сообщения.
2. Некоторая секретная информация, разделяемая обоими участниками и неизвестная противнику. Примером является ключ шифрования.

Рис. 15.7. Модель сетевой безопасности

Кроме того, в некоторых случаях для обеспечения безопасной передачи бывает необходима третья доверенная сторона (third trusted party - TTP). Например, третья сторона может быть ответственной за распределение между двумя участниками секретной информации, которая не стала бы

доступна противнику. Либо третья сторона может использоваться для решения споров между двумя участниками относительно достоверности передаваемого сообщения.

Из данной общей модели вытекают три основные задачи, которые необходимо решить при разработке конкретного сервиса безопасности:

1. Разработать алгоритм шифрования/дешифрования для выполнения безопасной передачи информации. Алгоритм должен быть таким, чтобы противник не мог расшифровать перехваченное сообщение, не зная секретную информацию.
2. Создать секретную информацию, используемую алгоритмом шифрования.
3. Разработать протокол обмена сообщениями для распределения разделяемой секретной информации таким образом, чтобы она не стала известна противнику.

Основная литература: [1] с.26-35.

Дополнительная литература: **[8] с.56-70, [9] с.56-58.**

Контрольные вопросы:

1. Перечислите основные сетевые атаки.
2. Какая атака считается активной.
3. Какая атака относится к пассивной.
4. Как работает атака «повторное использование».
5. Что входит в модель сетевого взаимодействия.
6. Какие задачи нужно решить при разработке сервиса безопасности.

Контрольные вопросы

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию "информационная безопасность".
3. Перечислите составляющие информационной безопасности.
4. Приведите определение доступности информации.
5. Приведите определение целостности информации.
6. Приведите определение конфиденциальности информации.
7. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
8. Перечислите задачи информационной безопасности общества.
9. Перечислите уровни формирования режима информационной безопасности.
10. Дайте краткую характеристику законодательно-правового уровня.
11. Какие подуровни включает программно-технический уровень?
12. Что включает административный уровень?
13. В чем особенность морально-этического подуровня?
14. Перечислите основополагающие документы по информационной безопасности.
15. Понятие государственной тайны.
16. Что понимается под средствами защиты государственной тайны?
17. Цели и задачи административного уровня обеспечения информационной безопасности.
18. Содержание административного уровня.
19. Дайте определение политики безопасности.
20. Направления разработки политики безопасности.
21. Перечислите составные элементы автоматизированных систем.
22. Субъекты информационных отношений и их роли при обеспечении информационной безопасности.
23. Перечислите классы угроз информационной безопасности.
24. Назовите причины и источники случайных воздействий на информационные системы.
25. Дайте характеристику преднамеренным угрозам.
26. Перечислите каналы несанкционированного доступа.
27. В чем особенность "упреждающей" защиты в информационных системах.
28. Характерные черты компьютерных вирусов.
29. Дайте определение программного вируса.
30. Какие трудности возникают при определении компьютерного вируса?
31. Когда появился первый вирус, который самостоятельно дописывал себя в файлы?
32. В чем особенность компьютерного вируса "Чернобыль"?
33. Какой вид вирусов наиболее распространяемый в распределенных вычислительных сетях?
34. Перечислите классификационные признаки компьютерных вирусов.
35. Охарактеризуйте файловый и загрузочный вирусы.
36. В чем особенности резидентных вирусов?
37. Сформулируйте признаки стелс-вирусов.
38. Перечислите деструктивные возможности компьютерных вирусов.
39. Поясните самошифрование и полиморфичность как свойства компьютерных вирусов.
40. Перечислите виды "вирусоподобных" программ.
41. Поясните механизм функционирования "троянской программы" (логической бомбы).
42. В чем заключаются деструктивные свойства логических бомб?
43. Как используются утилиты скрытого администрирования и их деструктивные возможности?

44. Охарактеризуйте "intended"- вирусы и причины их появления.
45. Для чего используются конструкторы вирусов?
46. Для создания каких вирусов используются полиморфик - генераторы?
47. Поясните понятия "сканирование налету" и "сканирование по запросу".
48. Перечислите виды антивирусных программ.
49. Охарактеризуйте антивирусные сканеры.
50. Принципы функционирования блокировщиков и иммунизаторов.
51. Особенности CRC-сканеров.
52. В чем состоят особенности эвристических сканеров?
53. Какие факторы определяют качество антивирусной программы.

Условия реализации учебной дисциплины.
Методические указания:

Для выполнения практических работ;

- Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2017.

- Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ,

Наглядные пособия

- Таблицы. (Таблицы антивирусных угроз взятых с интернета Казаков Б.Н. Словарь научных терминов: Справочное пособие. — Казань: КГУ, 2017. — 32 с.)
- Поисковые Интернет - сервера.
- 1. www.cyberpol.ru Компьютерная преступность и способы борьбы.
- 2. www.iso27000.ru Информационный портал, посвященный вопросам управления информационной безопасностью.
- 3. www.itsec.ru Интернет-журнал «Информационная безопасность».
- 4. www.inside-zi.ru Информационно-методический журнал «Защита информации. Инсайд».
- 5. www.kaspersky.ru Лаборатория Касперского.
- 6. www.comss.ru.
- 7. www.drweb.com.
- 8. www.esethod32.ru.
- 9. www.kaspersky.ru.
- 10. http://free.avg.com
- 11. www.kaspersky.ru/removaltools
- 12. www.freedrweb.com/cureit/
- 13. www.computerologia.ru
- 14. www.free-av.com
- 15. www.mcafee.com
- 16. http://www.viruslab.ru/
- 17. www.bitdefender.com.

Справочный материал.

- Толковый словарь терминов взятый из интернета
- Черемушкин А. В. Информационная безопасность. Глоссарий. Под ред. С. Пазизина. – М.: «АВАНГАРД ЦЕНТР», 2017. – 322 стр.

Технические средства обучения

- Компьютер
- Проектор
- Интерактивная доска

3. Контроль и оценка результатов освоения учебной дисциплины. Критерии оценки выполнения студентами отчетных работ

Оценка «5» (отлично) ставится в том случае, если студент показывает правильное понимание сущности изучаемых ситуаций и закономерностей, методов и принципов; дает точное определение и истолкование основных понятий, принципов и методов; указывает все свойства тех или иных объектов изучения; выполняет работу полностью, без ошибок и недочетов, с указанием всех необходимых свойств, законов, пояснений; схемы, графики, диаграммы выполнены точно; сделаны необходимые выводы.

Оценка «4» (хорошо) ставится, если работа студента удовлетворяет основным требованиям к работе на оценку «5», но в ней допущены одна ошибка или не более двух недочетов; допущены ошибки в диаграммах; работа выполнена небрежно; выводы из полученных расчетных данных сделаны недостаточно полно.

Оценка «3» (удовлетворительно) ставится, если студент правильно понимает сущность изучаемых методов, понятий, теорем, законов, но в знаниях имеются пробелы, не мешающие выполнению основных требований, предусмотренных программой; если студент правильно выполнил не менее 2/3 всей работы или допустил не более одной грубой ошибки и двух недочетов, не более одной грубой и одной негрубой ошибки, не более трех негрубых ошибок, одной негрубой ошибки и трех недочетов, при наличии четырех-пяти недочетов.

Оценка «2» (неудовлетворительно) ставится, если студент выполнил менее 2/3 работы или допустил больше ошибок и недочетов, чем необходимо для оценки «3»; не усвоил основные закономерности и понятия по курсу учебной дисциплины.

4. Перечень рубежных точек контроля

Наименование точки рубежного контроля (тема, раздел)	Форма проведения
Классификация компьютерных вирусов	Контрольная работа по вариантам
Профилактика компьютерных вирусов	Контрольная работа по вариантам

Литература

1. Аверченков В.И. Аудит информационной безопасности [электронный ресурс]: учебное пособие/ В.И. Аверченков. М.: Флинта, 2017 – 269с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=93245&sr=1 2
2. Бирюков А.А. Информационная безопасность: защита и нападение [электронный ресурс]: учебник / Бирюков А.А. – М. Изд. «ДМК Пресс», 2018. – 474с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=39990
3. Анисимов А.А. Менеджмент в сфере информационной безопасности \ курс лекций [электронный ресурс]. М.: Интернет университет информационных технологий, 2017 -176с. Режим доступа: http://biblioclub.ru/index.php?page=book&id=232981&sr=1
4. Беломойцев Д.Е., Волосатова Т.М., Радионов С.В. Основные методы криптографической обработки данных [электронный ресурс]: учебное пособие / Беломойцев Д.Е. – М. Изд. МГТУ им. Н.Э. Баумана (Московский государственный технический университет имени Н.Э. Баумана), 2018– 76с. Режим доступа: http://e.lanbook.com/books/element.php?pl1_id=58438

Дополнительная литература

1. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2014.
2. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. – М: Яхтсмен, 2010.
3. Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2013.
4. Галатенко В. А. Стандарты информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2014.
5. *www.jetinfo.ru*.
6. Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2013.
7. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2011.
8. Галатенко В. А. Стандарты информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2014.
9. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. – М: Яхтсмен, 2016.
10. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2011.
11. Карпов Е. А., Котенко И. В., Котухов М. М., Марков А. С., Парр Г. А., Рунеев А. Ю. Законодательно-правовое и организационно-техническое обеспечение информационной безопасности автоматизированных систем и информационно-вычислительных сетей / Под редакцией И. В.Котенко. – СПб.: ВУС, 2010.
12. Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2013.
13. Галатенко В. А. Стандарты информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2014.
14. Лаборатория Касперского [электронный ресурс]: http://www.kaspersky.ru 2 Information Security / Информационная безопасность. Журнал [электронный ресурс]: http://www.itsec.ru/main.php 3 Энциклопедия хакера [электронный ресурс]: http://www.inattack.ru 4 Консультант плюс [электронный ресурс]: http://www.consultant.ru/online/

Темы для самостоятельной работы
Вариант 1

№	Тема задания	Содержание задания	Литература
1.	Стандарты информационной безопасности	Изучить стандарты информационной безопасности	[1] с.184-185, [6] с. 73-74, 15-28
2.	Классификация информационных угроз	Изучить классификацию информационных угроз.	[1] с. 94-105, [3] с. 7-17, [3] с. 5-14
3.	Стеганография.	Изучить принципы построения стеганографических систем	[1] с. 105-107, [3] с. 21-24, [3] с.15-19
4.	Стандарт шифрования IDEA	Изучить стандарт шифрования	[1] с. 117-121, [3] с. 50-51, [3] с. 20-23
5.	Стандарт SHA	Изучить стандарт	[1] с. 111-117, [3] с. 43-45, [3] с. 23-32
6.	Стандарт шифрования DH	Изучить стандарт	[1] с. 122-133, [2] с. 26-29]
7.	Гибридные вирусы	Изучить работу и строение гибридных вирусов.	[2] с. 16-26, [9] с. 1028-1037
8.	Антивирусные программы	Изучить работу антивирусных программ и провести сравнительный анализ их работы.	[2] с. 16-26, [9] с. 1028-1037
9.	Эвристический поиск	Изучить работу антивирусных программ с эвристическим поиском	[2] с. 16-26, [9] с. 1028-1037
10.	Биометрические параметры аутентификации	Изучить биометрические параметры, их свойства и принцип их использования.	[1] с. 194-201, [7] с. 97-115
11.	Стандарт MD1-MD4	Изучить стандарт	[7] с. 124-128, 132,155,162,384-385
12.	Протокол KERBEROS	Изучить работу протокола в различных режимах.	[1] с. 201-207, [7] с. 277-295
13.	Протокол IPSEC	Изучить работу протокола в различных режимах.	[1] с. 207-210, [7] с. 39-56
14.	Политика безопасности.	Создать политику безопасности для аудитории.	[7] с. 531-548
15.	Брандмауэры	Изучить работу	[6] с. 56-89, [9] с. 56-58

Вариант 2

№	Тема занятия	Содержание задания	Литература
1.	Шифр Бофора	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[11] с. 18-25
2.	Шифр Полибий	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с.5-11, 36-43, 76-85, **[10] с.104-134.**
3.	Дробный шифр	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1]с.94-105,[3] с. 7-17, [3] с. 5-14
4..	Шифр Трисемуса.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с. 105-107,[3] с. 21-24,[3] с.15-19
5.	Шифр Гронсфельда.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с. 117-121, [3] с.50-51, [3] с. 20-23
6.	Шифр Альбама.	Изучить шифр, выбрать текст, ключ и провести	[1] с.92-117,[3] с.4-

		шифрование. Затем провести дешифрование	48
7.	Шифр Фальконера.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с. 122-133,[2] с. 26-29
8.	Шифр Плэйфера	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[2] с. 16-26, [9] с. 1028-1037
9.	Код Хоффмана.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[2] с. 16-26, [9] с. 1028-1037
10.	Сложный шифр Виженера.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[2] с. 16-26, [9] с. 1028-1037
11.	Сложный шифр транспозиции.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с. 194-201, [7] с.97-115
12.	Обратный шифр Бофора	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с. 194-201, [7] с. 97-132
13.	Шифр с автоключом.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с. 201-207,[7] с.277-295
14.	Шифр Эль-Гамаля.	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[1] с.207-210,[7] с.39-56
15.	Шифр Диффи-Хелмана	Изучить шифр, выбрать текст, ключ и провести шифрование. Затем провести дешифрование	[6] с. 56-89, [9] с. 56-58

Тематика и краткое описание практических работ

Разработка программы шифра простой замены
1. Работать ключ.
2. Выбрать текст.
3. Разработать программу шифрования и зашифровать текст.
4. Расшифровать зашифрованный текст с помощью ключа и проверить правильность полученного текста.

Разработка программы шифра транспозиции
1. Выбрать период для транспозиции.
2. Создать ключ для транспозиции.
3. Разработать программу и зашифровать текст.
4. Расшифровать текст и проверить правильность полученного текста.

Разработка программы шифра Цезаря
1. Выбрать ключ.
2. Определить длину алфавита.
3. Разработать программу и зашифровать текст.
4. Расшифровать текст т проверить правильность полученного текста

Разработка программы шифра Виженера
1. Выбрать ключ.
2. Определить длину алфавита.
3. Разработать программу и зашифровать текст.
4. Расшифровать текст т проверить правильность полученного текста

Изучение работы антивирусной программы
1. Рассмотреть режимы работы антивирусных программ.
2. Рассмотреть антивирусные базы.
3. Рассмотреть процесс удаления вирусов.
Методические рекомендации: Использовать любую антивирусную программу.

Разработать программу демонстрирующую работу протокола аутентификации неполного доверия
1. Выбрать протокол.
2. Выбрать алгоритм шифрования

3. Разработать программу.
4. Объяснить работу программы.

Разработать программу демонстрирующую работу протокола аутентификации полного доверия
1. Выбрать протокол.
2. Выбрать алгоритм шифрования
3. Разработать программу.
4. Объяснить работу программы.

Разработать программу генератора случайных чисел на регистрах сдвига
1. Выбрать регистр сдвига.
2. Выбрать первоначальное состояние генератора.
3. Разработать программу и получить случайные числа.

Методические рекомендации:

Тесты

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Модуль 1

1.Под информационной безопасностью понимается

А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре**

Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия

В) нет правильного ответа

Г) преднамеренные воздействия

2.Защита информации – это

А) **комплекс мероприятий, направленных на обеспечение информационной безопасности**

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей

В) небольшая программа для выполнения определенной задачи

Г) нет правильного ответа

3.От чего зависит информационная безопасность

А) нет правильного ответа

Б) от поддерживающей инфраструктуры

В) от информации

Г) от антивирусов

4.Основные составляющие информационной безопасности

А) вирусы

Б) защиты

В) конфиденциальность

Г) противоречивости

5. Доступность – это

А) **возможность за приемлемое время получить требуемую информационную услугу**
Б) логическая независимость
В) нет правильного ответа
Г) программа

6.Целостность – это

А) информация
Б) непротиворечивость информации
В) разрушения
Г**)** нет правильного ответа

7.Конфиденциальность – это

А) **защита от несанкционированного доступа к информации**
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур
Г) нет правильного ответа

8.Для чего создаются информационные системы

А) **получения определенных информационных услуг**
Б) обработки информации
В) нет правильного ответа
Г) обработки модулей

9.Целостность можно подразделить

А) финансовую
Б) динамичную
В) структурную
Г) информационную

10.Где применяются средства контроля динамической целостности

А) **анализе потока финансовых сообщений**
Б) обработке данных
В) при утечке информации
Г) нет правильного ответа

11.Какие трудности возникают в информационных системах при конфиденциальности

А) сведения о технических каналах утечки информации являются закрытыми
Б) отвечает на текущее состояние разработки требованиям данного этапа
В) нет правильного ответа
Г) окно опасности

12.Угроза – это

А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа
Г) разработка специального программного обеспечения, используемого для осуществления неправомерного доступа

13. Атака – это
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.
Г) использование специальных программ для ведения работы на компьютере жертвы, а также дальнейшего распространения (это вирусы и черви).

14.Источник угрозы – это
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа
Г) червь

15.Окно опасности – это
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
Г) отслеживание окон опасности должно производится постоянно, а выпуск заплат - оперативно

16.Какие события должны произойти за время существования окна опасности
А) решения задач определенного класса конкретной предметной области
Б) должны быть выпущены соответствующие заплаты
В) внутренний отказ информационной системы
Г) необходимость установить обновления защищаемой ИС

17. Угрозы можно классифицировать по нескольким критериям
А) отслеживание окон опасности
Б) по способу осуществления
В) по компонентам И.С
Г) несанкционированное использование информационных ресурсов

18.По каким компонентам классифицируется угрозы доступности
А) нет правильного ответа
Б) отказ поддерживающей инфраструктуры
В) ошибка в программе
Г) внутренний отказ информационной системы; отказ поддерживающей инфраструктуры

19.Основными источниками внутренних отказов являются
А) отступление от установленных правил эксплуатации
Б) отказ поддерживающей инфраструктуры
В) нет правильного ответа
Г) ошибки при (пере) конфигурировании системы

20. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы

А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа
Г) внутренний отказ информационной системы

21.Какие существуют грани вредоносного П.О
А) вредоносная функция
Б) специализированная
В) нет правильного ответа
Г) повреждение или даже разрушение оборудования

22.По механизму распространения П.О. различают
А) вирусы
Б) виды модуляции
В) атаки
Г) нет правильного ответа

23.Вирус – это
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи
Г) нет правильного ответа

24.Черви – это
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами
Г) программа-вирус, которая часто распространяется как вложение в электронные письма, заражающее файлы на локальных компьютерах и распространяющее себя по локальной сети

25.Конфиденциальную информацию можно разделить
А) нет правильного ответа
Б) служебную
В) глобальную
Г) специализированную

26.Природа происхождения угроз
А) нет правильного ответа
Б) преднамеренные
В) природные
Г) случайные

27.Предпосылки появления угроз
А) нет правильного ответа
Б) субъективные
В) преднамеренные

Г) несанкционированный доступ к ресурсам ЭВМ

28.К какому виду угроз относится присвоение чужого права
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда
Г) хищение носителей информации

29.Отказ, ошибки, сбой – это
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы
Г) Ошибки конструкции, технологии производства оборудования, пуско-наладки, условий эксплуатации

30.Отказ - это
А) **нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов
Г) нет правильно ответа

31.Ошибка – это
А) **неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния**
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу
Г) Диспетчер устройств не отображает неподключенные устройства

32.Сбой – это
А) **такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод
Г) нет правильного ответа

33.Побочное влияние – это
А) **негативное воздействие на систему в целом или отдельные элементы**
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций

Г) доступ (чтение или запись) к объекту, определённому с модификатором

34.СЗИ (система защиты информации) делится
А) **ресурсы автоматизированных систем**
Б) нет правильного ответа
В) техническое обеспечение
Г) системы защиты информации для повышения защищенности от угроз нарушения информационной безопасности

35.Что относится к человеческому компоненту СЗИ
А) **системные порты**
Б) техническое обеспечение
В) программное обеспечение
Г) Классификация защищенности средств вычислительной техники

36.Что относится к ресурсам А.С. СЗИ
А) программное обеспечение
Б) техническое обеспечение
В) нет правильного ответа
Г) Классы защищенности средств вычислительной техники

37.По уровню обеспеченной защиты все системы делят
А) **сильной защиты**
Б) особой защиты
В) слабой защиты
Г) нет правильного ответа

38.По активности реагирования СЗИ системы делят
А) **пассивные**
Б) активные
В) полупассивные
Г) стратегические и текущие задачи

39.Правовое обеспечение безопасности информации – это
А) **совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа
Г) состояние защищенности личности, общества и государства, их интересов, прав и свобод в информационном пространстве

40.Правовое обеспечение безопасности информации делится

А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные
Г) экономические нормы

41.Информацию с ограниченным доступом делят
А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию
Г) Коммерческая тайна

42.Что относится к государственной тайне
А) **сведения, защищаемые государством в области военной, экономической … деятельности**
Б) документированная информация
В) нет правильного ответа
Г) защита

43.Вредоносная программа - это
А) **программа, специально разработанная для нарушения нормального функционирования систем**
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение
Г) нет правильного ответа

44.Основополагающие документы для обеспечения безопасности внутри организации
А) **трудовой договор сотрудников**
Б) должностные обязанности руководителей
В) коллективный договор
Г**)** нет правильного ответа

45.К организационно - административному обеспечению информации относится
А) **взаимоотношения исполнителей**
Б) подбор персонала
В) регламентация производственной деятельности
Г) административному обеспечению

46.Что относится к организационным мероприятиям
А) **хранение документов**
Б) проведение тестирования средств защиты информации
В) **пропускной режим**
Г) оформление работ нарядом-допуском (далее - наряд), распоряжением, перечнем работ, выполняемых в порядке текущей эксплуатации

47.Какие средства используется на инженерных и технических мероприятиях в защите информации

А) **аппаратные**

Б) криптографические

В) физические

Г) допуск к работе

48.Программные средства – это

А) **специальные программы и системы защиты информации в информационных системах различного назначения**

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

Г) обеспечение безопасности

49. Криптографические средства – это

А) **средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования**

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

Г) нет правильного ответа

50. **Дискреционная политика доступа**

а) **Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)**

б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности

в) Является алгоритмом формирования матрицы доступа

г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

51. **Мандатная политика доступа**

а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)

б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов

в) Является алгоритмом формирования матрицы доступа

г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

52. **Виртуальный защищённый канал строится**

а) Путём шифрации информации, проходящей через открытые глобальные сети

б) Для передачи видео и аудио информации в привилегированном, защищённом от задержек и прерываний режиме

в) Для имитации использования системы защиты информации с целью ввести в заблуждение возможного злоумышленника

Г) нет правильного ответа

53. **Какое утверждение верно**

а) Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов

б) ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак

в) Защиту от вирусов гарантирует использование только лицензионного программного обеспечения

Г) все ответы правильные

54. **Компьютерным вирусом называется**

а**) Программа, способная внедряться в другие программы, с возможностью самовоспроизводства**

б) Вид бактерий, разрушающий микросхемы

в) Процесс разрушения информации на неисправном жёстком диске

Г) биологический вирус

55. **Монитор безопасности это**

а) Личный терминал системного администратора.

б) Совокупность резидентных программ, реализующих политику безопасности

в) Программа контроля данных аудита

Г) класс защищённости

56. **Программная система защиты информации отвечает за**

а) Сохранность всей введённой в информационную систему информации

б) Реализацию заданной политики безопасности

в) Корректное поведение пользователей.

Г) нет правильного ответа

57. **Цифровая подпись это**

а) Ключевое слово или набор цифр в конце электронного документа, известное только отправителю и получателю

б) Цифровое представление графического изображения персональной подписи человека.

в) Результат применения специальной функции к содержимому документа с ключом, известным только отправителю, и который можно проверить с помощью ключа, известного всем получателям

Г) электронная подпись

58.Аутентификация это

а) Подтверждение заявленного идентификатора

б) Процесс ввода текста без отображения на экране

в) Ввод сведений личного характера

Г) нет правильного ответа

Модуль 2

1) К правовым методам, обеспечивающим информационную безопасность, относятся

А. Разработка аппаратных средств обеспечения правовых данных

Б. Разработка и установка во всех компьютерных правовых сетях журналов учета действий

В. Разработка и конкретизация правовых нормативных актов обеспечения безопасности

Г. Нет правильного ответа

2) Основными источниками угроз информационной безопасности являются все указанное в списке

А. Хищение жестких дисков, подключение к сети, инсайдерство

Б. Перехват данных, хищение данных, изменение архитектуры системы

В. Хищение данных, подкуп системных администраторов, нарушение регламента работы

Г. Нет правильного ответа

3) Виды информационной безопасности

А. Персональная, корпоративная, государственная

Б. Клиентская, серверная, сетевая

В. Локальная, глобальная, смешанная

Г. Нет правильного ответа

4) Цели информационной безопасности – своевременное обнаружение, предупреждение

А. несанкционированного доступа, воздействия в сети

Б. инсайдерства в организации

В. чрезвычайных ситуаций

Г. Нет правильного ответа

5) Основные объекты информационной безопасности

А. Компьютерные сети, базы данных

Б. Информационные системы, психологическое состояние пользователей

В. Бизнес-ориентированные, коммерческие системы

Г. Нет правильного ответа

6) Основными рисками информационной безопасности являются

А. Искажение, уменьшение объема, перекодировка информации

Б. Техническое вмешательство, выведение из строя оборудования сети

В. Потеря, искажение, утечка информации

Г. Нет правильного ответа

7) К основным принципам обеспечения информационной безопасности относится
А. Экономической эффективности системы безопасности
Б. Многоплатформенной реализации системы
В. Усиления защищенности всех звеньев системы
Г. Нет правильного ответа

8) Основными субъектами информационной безопасности являются
А. руководители, менеджеры, администраторы компаний
Б. органы права, государства, бизнеса
В. сетевые базы данных, фаерволлы
Г. Нет правильного ответа

9) К основным функциям системы безопасности можно отнести все перечисленное
А. Установление регламента, аудит системы, выявление рисков
Б. Установка новых офисных приложений, смена хостинг-компании
В. Внедрение аутентификации, проверки контактных данных пользователей
Г. Нет правильного ответа

10) Принципом информационной безопасности является принцип недопущения
А. Неоправданных ограничений при работе в сети (системе)
Б. Рисков безопасности сети, системы
В. Презумпции секретности
Г. Нет правильного ответа

11) Принципом политики информационной безопасности является принцип
А. Невозможности миновать защитные средства сети (системы)
Б. Усиления основного звена сети, системы
В. Полного блокирования доступа при риск-ситуациях
Г. Нет правильного ответа

12) Принципом политики информационной безопасности является принцип
А. Усиления защищенности самого незащищенного звена сети (системы)
Б. Перехода в безопасное состояние работы сети, системы
В. Полного доступа пользователей ко всем ресурсам сети, системы
Г. Нет правильного ответа

13) Принципом политики информационной безопасности является принцип
А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Б. Одноуровневой защиты сети, системы
В. Совместимых, однотипных программно-технических средств сети, системы
Г. Нет правильного ответа

14) К основным типам средств воздействия на компьютерную сеть относится
А. Компьютерный сбой
Б. Логические закладки («мины»)
В. Аварийное отключение питания
Г. Нет правильного ответа

15) Когда получен спам по e-mail с приложенным файлом, следует

А. Прочитать приложение, если оно не содержит ничего ценного – удалить
Б. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
В. Удалить письмо с приложением, не раскрывая (не читая) его
Г. Нет правильного ответа

16) Принцип Кирхгофа
А. Секретность ключа определена секретностью открытого сообщения
Б. Секретность информации определена скоростью передачи данных
В. Секретность закрытого сообщения определяется секретностью ключа
Г. Нет правильного ответа

17) ЭЦП – это
А. Электронно-цифровой преобразователь
Б. Электронно-цифровая подпись
В. Электронно-цифровой процессор
Г. Нет правильного ответа

18) Наиболее распространены угрозы информационной безопасности корпоративной системы
А. Покупка нелицензионного ПО
Б. Ошибки эксплуатации и неумышленного изменения режима работы системы
В. Сознательного внедрения сетевых вирусов
Г. Нет правильного ответа

19) Наиболее распространены угрозы информационной безопасности сети
А. Распределенный доступ клиент, отказ оборудования
Б. Моральный износ сети, инсайдерство
В. Сбой (отказ) оборудования, нелегальное копирование данных
Г. Нет правильного ответа

20) Наиболее распространены средства воздействия на сеть офиса
А. Слабый трафик, информационный обман, вирусы в интернет
Б. Вирусы в сети, логические мины (закладки), информационный перехват
В. Компьютерные сбои, изменение администрирования, топологии
Г. Нет правильного ответа

21) Утечкой информации в системе называется ситуация, характеризуемая
А. Потерей данных в системе
Б. Изменением формы информации
В. Изменением содержания информации
Г. Нет правильного ответа

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются
А. Целостность
Б. Доступность
В. Актуальность
Г. Нет правильного ответа

23) Угроза информационной системе (компьютерной сети) – это
А. Вероятное событие

Б. Детерминированное (всегда определенное) событие
В. Событие, происходящее периодически
Г. Нет правильного ответа

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется
А. Регламентированной
Б. Правовой
В. Защищаемой
Г. Нет правильного ответа

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке
А. Программные, технические, организационные, технологические
Б. Серверные, клиентские, спутниковые, наземные
В. Личные, корпоративные, социальные, национальные
Г. Нет правильного ответа

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет
А. Владелец сети
Б. Администратор сети
В. Пользователь сети
Г. Нет правильного ответа

27) Политика безопасности в системе (сети) – это комплекс
А. Руководств, требований обеспечения необходимого уровня безопасности
Б. Инструкций, алгоритмов поведения пользователя в сети
В. Нормы информационного права, соблюдаемые в сети
Г. Нет правильного ответа

28) Наиболее важным при реализации защитных мер политики безопасности является
А. Аудит, анализ затрат на проведение защитных мер
Б. Аудит, анализ безопасности
В. Аудит, анализ уязвимостей, риск-ситуаций
Г. Нет правильного ответа

29. Под информационной безопасностью понимается
А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре**
Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
В) нет правильного ответа
Г) преднамеренные воздействия

30.Защита информации – это
А) **комплекс мероприятий, направленных на обеспечение информационной безопасности**

Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи
Г) нет правильного ответа

31.От чего зависит информационная безопасность
А) **от компьютеров**
Б) от поддерживающей инфраструктуры
В) от информации
Г) от антивирусов

32.Основные составляющие информационной безопасности
А) целостность
Б) достоверность
В) конфиденциальность
Г) доступность

33.Доступность – это
А) **возможность за приемлемое время получить требуемую информационную услугу**
Б) логическая независимость
В) нет правильного ответа
Г) программа

34.Целостность – это
А) информация
Б) программа
В) защищенность от разрушения
Г**)** нет правильного ответа

35.Конфиденциальность – это
А) **защита от несанкционированного доступа к информации**
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур
Г) нет правильного ответа

36.Для чего создаются информационные системы
А) **получения определенных информационных услуг**
Б) обработки информации
В) нет правильного ответа
Г) обработки модулей

37.Целостность можно подразделить

А) **статическую, динамичную**
Б) нет правильного ответа
В) структурную
Г) информационную

38.Где применяются средства контроля динамической целостности
А) **анализе потока финансовых сообщений**
Б) обработке данных
В) в системе программных языковых организационных и технических средств
Г) нет правильного ответа

39.Какие трудности возникают в информационных системах при конфиденциальности
А) сведения о технических каналах утечки информации являются закрытыми
Б) многочисленные технические проблемы
В) нет правильного ответа
Г) окно опасности

40.Угроза – это
А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа
Г) разработка специального программного обеспечения, используемого для осуществления неправомерного доступа

41.Атака – это
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.
Г) использование специальных программ для ведения работы на компьютере жертвы, а также дальнейшего распространения (это вирусы и черви).

42.Источник угрозы – это
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа
Г) червь

43.Окно опасности – это
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется**

Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
Г) отслеживание окон опасности должно производится постоянно, а выпуск заплат - оперативно

44.Какие события должны произойти за время существования окна опасности
А) **должно стать известно о средствах использования пробелов в защите**
Б) должны быть выпущены соответствующие заплаты
В) заплаты должны быть установлены в защищаемой И.С
Г) Необходимость установить обновления защищаемой ИС

45. Угрозы можно классифицировать по нескольким критериям
А) **по спектру И.Б**
Б) по способу осуществления
В) по компонентам И.С
Г) несанкционированное использование информационных ресурсов

46.По каким компонентам классифицируется угрозы доступности
А) **отказ пользователей, отказ поддерживающей инфраструктуры**
Б) нет правильного ответа
В) ошибка в программе
Г) внутренний отказ информационной системы; отказ поддерживающей инфраструктуры

47.Основными источниками внутренних отказов являются
А) отступление от установленных правил эксплуатации, разрушение данных
Б) внутренний отказ информационной системы
В) все ответы правильные
Г) ошибки при (пере) конфигурировании системы

49. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа
Г) внутренний отказ информационной системы

50.Какие существуют грани вредоносного П.О
А) **вредоносная функция, внешнее представление**
Б) внутренний отказ информационной системы
В) нет правильного ответа
Г) повреждение или даже разрушение оборудования

51.По механизму распространения П.О. различают
А) вирусы
Б) черви
В) атаки
Г) все ответы правильные

52.Вирус – это
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи
Г) нет правильного ответа

53.Черви – это
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами
Г) программа-вирус, которая часто распространяется как вложение в электронные письма, заражающее файлы на локальных компьютерах и распространяющее себя по локальной сети

54.Конфиденциальную информацию можно разделить
А**) предметную**
Б) служебную
В) глобальную
Г) специализированную

55.Природа происхождения угроз
А) **случайные**
Б) преднамеренные
В) природные
Г) случайные

56.Предпосылки появления угроз
А) **объективные**
Б) субъективные
В) преднамеренные
Г) несанкционированный доступ к ресурсам ЭВМ

57.К какому виду угроз относится присвоение чужого права
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда

Г) хищение носителей информации

58.Отказ, ошибки, сбой – это
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы
Г) Ошибки конструкции, технологии производства оборудования, пуско-наладки, условий эксплуатации

59.Отказ - это
А) **нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов
Г) нет правильно ответа

60.Ошибка – это
А) **неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния**
Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу
Г) Диспетчер устройств не отображает неподключенные устройства

61.Сбой – это
А) **такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод
Г) нет правильного ответа

62.Побочное влияние – это
А) **негативное воздействие на систему в целом или отдельные элементы**
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Г) доступ (чтение или запись) к объекту, определённому с модификатором

63.СЗИ (система защиты информации) делится
А) **ресурсы автоматизированных систем**
Б) организационно-правовое обеспечение
В) человеческий компонент

Г) системы защиты информации для повышения защищенности от угроз нарушения информационной безопасности

64.Что относится к человеческому компоненту СЗИ
А) **системные порты**
Б) администрация
В) программное обеспечение
Г) Классификация защищенности средств вычислительной техники

65.Что относится к ресурсам А.С. СЗИ
А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные
Г) Классы защищенности средств вычислительной техники

66.По уровню обеспеченной защиты все системы делят
А) **сильной защиты**
Б) особой защиты
В) слабой защиты
Г) нет правильного ответа

67.По активности реагирования СЗИ системы делят
А) **пассивные**
Б) активные
В) полупассивные
Г) стратегические и текущие задачи

68.Правовое обеспечение безопасности информации – это
А) **совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа
Г) состояние защищенности личности, общества и государства, их интересов, прав и свобод в информационном пространстве

69.Правовое обеспечение безопасности информации делится
А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные
Г) экономические нормы

70.Информацию с ограниченным доступом делят

А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию
Г) Коммерческая тайна

71.Что относится к государственной тайне
А) **сведения, защищаемые государством в области военной, экономической … деятельности**
Б) документированная информация
В) нет правильного ответа
Г) защита

72.Вредоносная программа - это
А) **программа, специально разработанная для нарушения нормального функционирования систем**
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение
Г) нет правильного ответа

73.Основополагающие документы для обеспечения безопасности внутри организации
А) **трудовой договор сотрудников**
Б) должностные обязанности руководителей
В) коллективный договор
Г**)** нет правильного ответа

74.К организационно - административному обеспечению информации относится
А) **взаимоотношения исполнителей**
Б) подбор персонала
В) регламентация производственной деятельности
Г) административному обеспечению

75.Что относится к организационным мероприятиям
А) **хранение документов**
Б) проведение тестирования средств защиты информации
В) **пропускной режим**
Г) оформление работ нарядом-допуском (далее - наряд), распоряжением, перечнем работ, выполняемых в порядке текущей эксплуатации

76.Какие средства используется на инженерных и технических мероприятиях в защите информации
А) **аппаратные**
Б) криптографические
В) физические
Г) допуск к работе

77.Программные средства – это

А) **специальные программы и системы защиты информации в информационных системах различного назначения**

Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла

В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними

Г) обеспечение безопасности

78. Криптографические средства – это

А) **средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования**

Б) специальные программы и системы защиты информации в информационных системах различного назначения

В) механизм, позволяющий получить новый класс на основе существующего

Г) нет правильного ответа

79. **Дискреционная политика доступа**

а) **Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)**

б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности

в) Является алгоритмом формирования матрицы доступа

г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

80. **Мандатная политика доступа**

а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)

б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов

в) Является алгоритмом формирования матрицы доступа

г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

81. **Виртуальный защищённый канал строится**

а) Путём шифрации информации, проходящей через открытые глобальные сети

б) Для передачи видео и аудио информации в привилегированном, защищённом от задержек и прерываний режиме

в) Для имитации использования системы защиты информации с целью ввести в заблуждение возможного злоумышленника
Г) нет правильного ответа

82. **Какое утверждение верно**
а) Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов
б) ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак
в) Защиту от вирусов гарантирует использование только лицензионного программного обеспечения
Г) все ответы правильные

83. **Компьютерным вирусом называется**
а**) Программа, способная внедряться в другие программы, с возможностью самовоспроизводства**
б) Вид бактерий, разрушающий микросхемы
в) Процесс разрушения информации на неисправном жёстком диске
Г) биологический вирус

84. **Монитор безопасности это**
а) Личный терминал системного администратора.
б) Совокупность резидентных программ, реализующих политику безопасности
в) Программа контроля данных аудита
Г) класс защищённости

85. **Программная система защиты информации отвечает за**
а) Сохранность всей введённой в информационную систему информации
б) Реализацию заданной политики безопасности
в) Корректное поведение пользователей.
Г) нет правильного ответа

86. **Цифровая подпись это**
а) Ключевое слово или набор цифр в конце электронного документа, известное только отправителю и получателю
б) Цифровое представление графического изображения персональной подписи человека.
в) Результат применения специальной функции к содержимому документа с ключом, известным только отправителю, и который можно проверить с помощью ключа, известного всем получателям
Г) электронная подпись

87.Аутентификация это
а) Подтверждение заявленного идентификатора

б) Процесс ввода текста без отображения на экране
в) Ввод сведений личного характера
Г) нет правильного ответа

88.Основная масса угроз информационной безопасности приходится на
а) Троянские программы
б) Шпионские программы
в) Черви
Г) нет правильного ответа

89.Какой вид идентификации и аутентификации получил наибольшее распространение
а) системы PKI
б) постоянные пароли
в) одноразовые пароли
Г) нет правильного ответа

90. Под какие системы распространение вирусов происходит наиболее динамично
а) Windows
б) Mac OS
в) Android
Г) нет правильного ответа

91. Какие угрозы безопасности информации являются преднамеренными
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ
Г) нет правильного ответа

92.Какие вирусы активизируются в самом начале работы с операционной системой
а) загрузочные вирусы
б) троянцы
в) черви
Г) нет правильного ответа

93. Под информационной безопасностью понимается
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) комплекс мероприятий, направленных на обеспечение информационной безопасности
Г) нет правильного ответа

94.Информационная безопасность зависит от

а) компьютеров, поддерживающей инфраструктуры

б) пользователей

в) информации

Г) нет правильного ответа

95.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности

а) хакеры

б) контрагенты

в) сотрудники

Г) нет правильного ответа

96.Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены

а) владельцы данных

б) руководство

в) администраторы

Г) нет правильного ответа

97. Процедурой называется

а) пошаговая инструкция по выполнению задачи

б) обязательные действия

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

Г) нет правильного ответа

98. Какая из приведенных техник является самой важной при выборе конкретных защитных мер

а) анализ рисков

б) результаты ALE

в) анализ затрат / выгоды

Г) нет правильного ответа

99. Что такое политика безопасности

а) детализированные документы по обработке инцидентов безопасности

б) широкие, высокоуровневые заявления руководства

в) общие руководящие требования по достижению определенного уровня безопасности

Г) нет правильного ответа

Итоговый модуль

1) К правовым методам, обеспечивающим информационную безопасность, относятся

А. Разработка аппаратных средств обеспечения правовых данных

Б. Разработка и установка во всех компьютерных правовых сетях журналов учета действий

В. Разработка и конкретизация правовых нормативных актов обеспечения безопасности
Г. Нет правильного ответа

2) Основными источниками угроз информационной безопасности являются все указанное в списке
А. Хищение жестких дисков, подключение к сети, инсайдерство
Б. Перехват данных, хищение данных, изменение архитектуры системы
В. Хищение данных, подкуп системных администраторов, нарушение регламента работы
Г. Нет правильного ответа

3) Виды информационной безопасности
А. Персональная, корпоративная, государственная
Б. Клиентская, серверная, сетевая
В. Локальная, глобальная, смешанная
Г. Нет правильного ответа

4) Цели информационной безопасности – своевременное обнаружение, предупреждение
А. несанкционированного доступа, воздействия в сети
Б. инсайдерства в организации
В. чрезвычайных ситуаций
Г. Нет правильного ответа

5) Основные объекты информационной безопасности
А. Компьютерные сети, базы данных
Б. Информационные системы, психологическое состояние пользователей
В. Бизнес-ориентированные, коммерческие системы
Г. Нет правильного ответа

6) Основными рисками информационной безопасности являются
А. Искажение, уменьшение объема, перекодировка информации
Б. Техническое вмешательство, выведение из строя оборудования сети
В. Потеря, искажение, утечка информации
Г. Нет правильного ответа

7) К основным принципам обеспечения информационной безопасности относится
А. Экономической эффективности системы безопасности
Б. Многоплатформенной реализации системы
В. Усиления защищенности всех звеньев системы
Г. Нет правильного ответа

8) Основными субъектами информационной безопасности являются
А. руководители, менеджеры, администраторы компаний
Б. органы права, государства, бизнеса
В. сетевые базы данных, фаерволлы
Г. Нет правильного ответа

9) К основным функциям системы безопасности можно отнести все перечисленное
А. Установление регламента, аудит системы, выявление рисков
Б. Установка новых офисных приложений, смена хостинг-компании
В. Внедрение аутентификации, проверки контактных данных пользователей

Г. Нет правильного ответа

10) Принципом информационной безопасности является принцип недопущения
А. Неоправданных ограничений при работе в сети (системе)
Б. Рисков безопасности сети, системы
В. Презумпции секретности
Г. Нет правильного ответа

11) Принципом политики информационной безопасности является принцип
А. Невозможности миновать защитные средства сети (системы)
Б. Усиления основного звена сети, системы
В. Полного блокирования доступа при риск-ситуациях
Г. Нет правильного ответа

12) Принципом политики информационной безопасности является принцип
А. Усиления защищенности самого незащищенного звена сети (системы)
Б. Перехода в безопасное состояние работы сети, системы
В. Полного доступа пользователей ко всем ресурсам сети, системы
Г. Нет правильного ответа

13) Принципом политики информационной безопасности является принцип
А. Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
Б. Одноуровневой защиты сети, системы
В. Совместимых, однотипных программно-технических средств сети, системы
Г. Нет правильного ответа

14) К основным типам средств воздействия на компьютерную сеть относится
А. Компьютерный сбой
Б. Логические закладки («мины»)
В. Аварийное отключение питания
Г. Нет правильного ответа

15) Когда получен спам по e-mail с приложенным файлом, следует
А. Прочитать приложение, если оно не содержит ничего ценного – удалить
Б. Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
В. Удалить письмо с приложением, не раскрывая (не читая) его
Г. Нет правильного ответа

16) Принцип Кирхгофа
А. Секретность ключа определена секретностью открытого сообщения
Б. Секретность информации определена скоростью передачи данных
В. Секретность закрытого сообщения определяется секретностью ключа
Г. Нет правильного ответа

17) ЭЦП – это
А. Электронно-цифровой преобразователь
Б. Электронно-цифровая подпись
В. Электронно-цифровой процессор
Г. Нет правильного ответа

18) Наиболее распространены угрозы информационной безопасности корпоративной системы
А. Покупка нелицензионного ПО
Б. Ошибки эксплуатации и неумышленного изменения режима работы системы
В. Сознательного внедрения сетевых вирусов
Г. Нет правильного ответа

19) Наиболее распространены угрозы информационной безопасности сети
А. Распределенный доступ клиент, отказ оборудования
Б. Моральный износ сети, инсайдерство
В. Сбой (отказ) оборудования, нелегальное копирование данных
Г. Нет правильного ответа

20) Наиболее распространены средства воздействия на сеть офиса
А. Слабый трафик, информационный обман, вирусы в интернет
Б. Вирусы в сети, логические мины (закладки), информационный перехват
В. Компьютерные сбои, изменение администрирования, топологии
Г. Нет правильного ответа

21) Утечкой информации в системе называется ситуация, характеризуемая
А. Потерей данных в системе
Б. Изменением формы информации
В. Изменением содержания информации
Г. Нет правильного ответа

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются
А. Целостность
Б. Доступность
В. Актуальность
Г. Нет правильного ответа

23) Угроза информационной системе (компьютерной сети) – это
А. Вероятное событие
Б. Детерминированное (всегда определенное) событие
В. Событие, происходящее периодически
Г. Нет правильного ответа

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется
А. Регламентированной
Б. Правовой
В. Защищаемой
Г. Нет правильного ответа

25) Разновидностями угроз безопасности (сети, системы) являются все перечисленное в списке
А. Программные, технические, организационные, технологические
Б. Серверные, клиентские, спутниковые, наземные
В. Личные, корпоративные, социальные, национальные
Г. Нет правильного ответа

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет
А. Владелец сети
Б. Администратор сети
В. Пользователь сети
Г. Нет правильного ответа

27) Политика безопасности в системе (сети) – это комплекс
А. Руководств, требований обеспечения необходимого уровня безопасности
Б. Инструкций, алгоритмов поведения пользователя в сети
В. Нормы информационного права, соблюдаемые в сети
Г. Нет правильного ответа

28) Наиболее важным при реализации защитных мер политики безопасности является
А. Аудит, анализ затрат на проведение защитных мер
Б. Аудит, анализ безопасности
В. Аудит, анализ уязвимостей, риск-ситуаций
Г. Нет правильного ответа

29. Под информационной безопасностью понимается
А) **защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре**
Б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
В) нет правильного ответа
Г) преднамеренные воздействия

30.Защита информации – это
А) **комплекс мероприятий, направленных на обеспечение информационной безопасности**
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи
Г) нет правильного ответа

31.От чего зависит информационная безопасность
А) **от компьютеров**
Б) от поддерживающей инфраструктуры
В) от информации
Г) от антивирусов

32.Основные составляющие информационной безопасности
А) целостность
Б) достоверность
В) конфиденциальность
Г) доступность

33.Доступность – это

А) **возможность за приемлемое время получить требуемую информационную услугу**

Б) логическая независимость

В) нет правильного ответа

Г) программа

34.Целостность – это

А) информация

Б) программа

В) защищенность от разрушения

Г**)** нет правильного ответа

35.Конфиденциальность – это

А) **защита от несанкционированного доступа к информации**

Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов

В) описание процедур

Г) нет правильного ответа

36.Для чего создаются информационные системы

А) **получения определенных информационных услуг**

Б) обработки информации

В) нет правильного ответа

Г) обработки модулей

37.Целостность можно подразделить

А) **статическую, динамичную**

Б) нет правильного ответа

В) структурную

Г) информационную

38.Где применяются средства контроля динамической целостности

А) **анализе потока финансовых сообщений**

Б) обработке данных

В) в системе программных языковых организационных и технических средств

Г) нет правильного ответа

39.Какие трудности возникают в информационных системах при конфиденциальности

А) сведения о технических каналах утечки информации являются закрытыми

Б) многочисленные технические проблемы

В) нет правильного ответа

Г) окно опасности

40.Угроза – это

А) **потенциальная возможность определенным образом нарушить информационную безопасность**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) процесс определения отвечает на текущее состояние разработки требованиям данного этапа
Г) разработка специального программного обеспечения, используемого для осуществления неправомерного доступа

41.Атака – это
А) **попытка реализации угрозы**
Б) потенциальная возможность определенным образом нарушить информационную безопасность
В) программы, предназначенные для поиска необходимых программ.
Г) использование специальных программ для ведения работы на компьютере жертвы, а также дальнейшего распространения (это вирусы и черви).

42.Источник угрозы – это
А) **потенциальный злоумышленник**
Б) злоумышленник
В) нет правильного ответа
Г) червь

43.Окно опасности – это
А) **промежуток времени от момента, когда появится возможность слабого места и до момента, когда пробел ликвидируется**
Б) комплекс взаимосвязанных программ для решения задач определенного класса конкретной предметной области
В) формализованный язык для описания задач алгоритма решения задачи пользователя на компьютере
Г) отслеживание окон опасности должно производится постоянно, а выпуск заплат - оперативно

44.Какие события должны произойти за время существования окна опасности
А) **должно стать известно о средствах использования пробелов в защите**
Б) должны быть выпущены соответствующие заплаты
В) заплаты должны быть установлены в защищаемой И.С
Г) Необходимость установить обновления защищаемой ИС

45. Угрозы можно классифицировать по нескольким критериям
А) **по спектру И.Б**
Б) по способу осуществления
В) по компонентам И.С
Г) несанкционированное использование информационных ресурсов

46.По каким компонентам классифицируется угрозы доступности

А) **отказ пользователей, отказ поддерживающей инфраструктуры**
Б) нет правильного ответа
В) ошибка в программе
Г) внутренний отказ информационной системы; отказ поддерживающей инфраструктуры

47.Основными источниками внутренних отказов являются
А) отступление от установленных правил эксплуатации, разрушение данных
Б) внутренний отказ информационной системы
В) все ответы правильные
Г) ошибки при (пере) конфигурировании системы

49. По отношению к поддерживающей инфраструктуре рекомендуется рассматривать следующие угрозы
А) **невозможность и нежелание обслуживающего персонала или пользователя выполнять свои обязанности**
Б) обрабатывать большой объем программной информации
В) нет правильного ответа
Г) внутренний отказ информационной системы

50.Какие существуют грани вредоносного П.О
А) **вредоносная функция, внешнее представление**
Б) внутренний отказ информационной системы
В) нет правильного ответа
Г) повреждение или даже разрушение оборудования

51.По механизму распространения П.О. различают
А) вирусы
Б) черви
В) атаки
Г) все ответы правильные

52.Вирус – это
А) **код обладающий способностью к распространению путем внедрения в другие программы**
Б) способность объекта реагировать на запрос сообразно своему типу, при этом одно и то же имя метода может использоваться для различных классов объектов
В) небольшая программа для выполнения определенной задачи
Г) нет правильного ответа

53.Черви – это
А) **код способный самостоятельно, то есть без внедрения в другие программы вызывать распространения своих копий по И.С. и их выполнения**
Б) код обладающий способностью к распространению путем внедрения в другие программы
В) программа действий над объектом или его свойствами

Г) программа-вирус, которая часто распространяется как вложение в электронные письма, заражающее файлы на локальных компьютерах и распространяющее себя по локальной сети

54.Конфиденциальную информацию можно разделить
А**) предметную**
Б) служебную
В) глобальную
Г) специализированную

55.Природа происхождения угроз
А) **случайные**
Б) преднамеренные
В) природные
Г) случайные

56.Предпосылки появления угроз
А) **объективные**
Б) субъективные
В) преднамеренные
Г) несанкционированный доступ к ресурсам ЭВМ

57.К какому виду угроз относится присвоение чужого права
А) **нарушение права собственности**
Б) нарушение содержания
В) внешняя среда
Г) хищение носителей информации

58.Отказ, ошибки, сбой – это
А) **случайные угрозы**
Б) преднамеренные угрозы
В) природные угрозы
Г) Ошибки конструкции, технологии производства оборудования, пуско-наладки, условий эксплуатации

59.Отказ - это
А) **нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций**
Б) некоторая последовательность действий, необходимых для выполнения конкретного задания
В) структура, определяющая последовательность выполнения и взаимосвязи процессов
Г) нет правильно ответа

60.Ошибка – это
А) **неправильное выполнение элементом одной или нескольких функций происходящее в следствии специфического состояния**

Б) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
В) негативное воздействие на программу
Г) Диспетчер устройств не отображает неподключенные устройства

61.Сбой – это
А) **такое нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент**
Б) неправильное выполнение элементом одной или нескольких функций происходящее в следствие специфического состояния
В) объект-метод
Г) нет правильного ответа

62.Побочное влияние – это
А) **негативное воздействие на систему в целом или отдельные элементы**
Б) нарушение работоспособности какого-либо элемента системы в следствии чего функции выполняются неправильно в заданный момент
В) нарушение работоспособности элемента системы, что приводит к невозможности выполнения им своих функций
Г) доступ (чтение или запись) к объекту, определённому с модификатором

63.СЗИ (система защиты информации) делится
А) **ресурсы автоматизированных систем**
Б) организационно-правовое обеспечение
В) человеческий компонент
Г) системы защиты информации для повышения защищенности от угроз нарушения информационной безопасности

64.Что относится к человеческому компоненту СЗИ
А) **системные порты**
Б) администрация
В) программное обеспечение
Г) Классификация защищенности средств вычислительной техники

65.Что относится к ресурсам А.С. СЗИ
А) лингвистическое обеспечение
Б) техническое обеспечение
В) все ответы правильные
Г) Классы защищенности средств вычислительной техники

66.По уровню обеспеченной защиты все системы делят
А) **сильной защиты**
Б) особой защиты
В) слабой защиты

Г) нет правильного ответа

67.По активности реагирования СЗИ системы делят
А) **пассивные**
Б) активные
В) полупассивные
Г) стратегические и текущие задачи

68.Правовое обеспечение безопасности информации – это
А) **совокупность законодательных актов, нормативно-правовых документов, руководств, требований, которые обязательны в системе защиты информации**
Б) система программных языковых организационных и технических средств, предназначенных для накопления и коллективного использования данных
В) нет правильного ответа
Г) состояние защищенности личности, общества и государства, их интересов, прав и свобод в информационном пространстве

69.Правовое обеспечение безопасности информации делится
А) международно-правовые нормы
Б) национально-правовые нормы
В) все ответы правильные
Г) экономические нормы

70.Информацию с ограниченным доступом делят
А) **государственную тайну**
Б) конфиденциальную информацию
В) достоверную информацию
Г) Коммерческая тайна

71.Что относится к государственной тайне
А) **сведения, защищаемые государством в области военной, экономической … деятельности**
Б) документированная информация
В) нет правильного ответа
Г) защита

72.Вредоносная программа - это
А) **программа, специально разработанная для нарушения нормального функционирования систем**
Б) упорядочение абстракций, расположение их по уровням
В) процесс разделения элементов абстракции, которые образуют ее структуру и поведение
Г) нет правильного ответа

73.Основополагающие документы для обеспечения безопасности внутри организации

А) **трудовой договор сотрудников**
Б) должностные обязанности руководителей
В) коллективный договор
Г**)** нет правильного ответа

74.К организационно - административному обеспечению информации относится
А) **взаимоотношения исполнителей**
Б) подбор персонала
В) регламентация производственной деятельности
Г) административному обеспечению

75.Что относится к организационным мероприятиям
А) **хранение документов**
Б) проведение тестирования средств защиты информации
В) **пропускной режим**
Г) оформление работ нарядом-допуском (далее - наряд), распоряжением, перечнем работ, выполняемых в порядке текущей эксплуатации

76.Какие средства используется на инженерных и технических мероприятиях в защите информации
А) **аппаратные**
Б) криптографические
В) физические
Г) допуск к работе

77.Программные средства – это
А) **специальные программы и системы защиты информации в информационных системах различного назначения**
Б) структура, определяющая последовательность выполнения и взаимосвязи процессов, действий и задач на протяжении всего жизненного цикла
В) модель знаний в форме графа в основе таких моделей лежит идея о том, что любое выражение из значений можно представить в виде совокупности объектов и связи между ними
Г) обеспечение безопасности

78. Криптографические средства – это
А) **средства специальные математические и алгоритмические средства защиты информации, передаваемые по сетям связи, хранимой и обрабатываемой на компьютерах с использованием методов шифрования**
Б) специальные программы и системы защиты информации в информационных системах различного назначения
В) механизм, позволяющий получить новый класс на основе существующего
Г) нет правильного ответа

79. **Дискреционная политика доступа**

а) **Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)**
б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности
в) Является алгоритмом формирования матрицы доступа
г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

80. **Мандатная политика доступа**
а) Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)
б) Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа субъектов и меток конфиденциальности объектов
в) Является алгоритмом формирования матрицы доступа
г) Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

81. **Виртуальный защищённый канал строится**
а) Путём шифрации информации, проходящей через открытые глобальные сети
б) Для передачи видео и аудио информации в привилегированном, защищённом от задержек и прерываний режиме
в) Для имитации использования системы защиты информации с целью ввести в заблуждение возможного злоумышленника
Г) нет правильного ответа

82. **Какое утверждение верно**
а) Последние версии антивирусных программ и регулярное обновление ОС гарантируют защиту от вирусов
б) ОС с грамотно реализованной системой защиты от несанкционированного доступа лучше защищена от вирусных атак
в) Защиту от вирусов гарантирует использование только лицензионного программного обеспечения
Г) все ответы правильные

83. **Компьютерным вирусом называется**
а**) Программа, способная внедряться в другие программы, с возможностью самовоспроизводства**
б) Вид бактерий, разрушающий микросхемы
в) Процесс разрушения информации на неисправном жёстком диске
Г) биологический вирус

84. **Монитор безопасности это**

а) Личный терминал системного администратора.
б) Совокупность резидентных программ, реализующих политику безопасности
в) Программа контроля данных аудита
Г) класс защищённости

85. **Программная система защиты информации отвечает за**
а) Сохранность всей введённой в информационную систему
информации
б) Реализацию заданной политики безопасности
в) Корректное поведение пользователей.
Г) нет правильного ответа

86. **Цифровая подпись это**
а) Ключевое слово или набор цифр в конце электронного документа,
известное только отправителю и получателю
б) Цифровое представление графического изображения персональной подписи человека.
в) Результат применения специальной функции к содержимому документа с ключом, известным только отправителю, и который можно проверить с помощью ключа, известного всем получателям
Г) электронная подпись

87.Аутентификация это
а) Подтверждение заявленного идентификатора
б) Процесс ввода текста без отображения на экране
в) Ввод сведений личного характера
Г) нет правильного ответа

88.Основная масса угроз информационной безопасности приходится на
а) Троянские программы
б) Шпионские программы
в) Черви
Г) нет правильного ответа

89.Какой вид идентификации и аутентификации получил наибольшее распространение
а) системы PKI
б) постоянные пароли
в) одноразовые пароли
Г) нет правильного ответа

90. Под какие системы распространение вирусов происходит наиболее динамично
а) Windows
б) Mac OS
в) Android
Г) нет правильного ответа

91. Какие угрозы безопасности информации являются преднамеренными
а) ошибки персонала
б) открытие электронного письма, содержащего вирус
в) не авторизованный доступ
Г) нет правильного ответа

92.Какие вирусы активизируются в самом начале работы с операционной системой
а) загрузочные вирусы
б) троянцы
в) черви
Г) нет правильного ответа

93. Под информационной безопасностью понимается
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) комплекс мероприятий, направленных на обеспечение информационной безопасности
Г) нет правильного ответа

94.Информационная безопасность зависит от
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации
Г) нет правильного ответа

95.Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности
а) хакеры
б) контрагенты
в) сотрудники
Г) нет правильного ответа

96.Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены
а) владельцы данных
б) руководство
в) администраторы
Г) нет правильного ответа

97. Процедурой называется
а) пошаговая инструкция по выполнению задачи

б) обязательные действия

в) руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах

Г) нет правильного ответа

98. Какая из приведенных техник является самой важной при выборе конкретных защитных мер

а) анализ рисков

б) результаты ALE

в) анализ затрат / выгоды

Г) нет правильного ответа

99. Что такое политика безопасности

а) детализированные документы по обработке инцидентов безопасности

б) широкие, высокоуровневые заявления руководства

в) общие руководящие требования по достижению определенного уровня безопасности

Г) нет правильного ответа

Перечень программных вопросов по пройденному курсу и соответствующих итоговым тестам

1. Дайте определение информационной безопасности.
2. Дайте определение защите информации.
3. Механизмы безопасности.
4. Собственник информации.
5. Сервисы безопасности.
6. Взаимосвязь основных понятий информационной безопасности.
7. Какие информационные угрозы существуют.
8. Какие каналы утечки информации существуют.
9. Какие атаки и компьютерные преступления известны.
10. Какие методы защиты информации существуют.
11. Что такое криптография.
12. Какие языковые средства можно выделить в составе СУБД.
13. Перечислите основные типы полей, применяемые в СУБД.
14. Какая команда позволяет создать или изменить структуру БД.
15. Какие команды позволяют добавлять записи в таблице данных.
16. Какие команды позволяют удалить записи в таблице данных.
17. Какие системы называются блочными.
18. Что называется блоком текста.
19. Что называется раундом алгоритма.
20. Какова область применения блочных шифров.
21. Требования предъявляемые к блочным шифрам.
22. Чем определяется стойкость *алгоритма ГОСТ 28147*.
23. Какие шифра называются потоковыми.
24. На каком алгоритме основан алгоритм RC6.
25. Какие критерии используются при выборе генератора случайных чисел.
26. Как можно используя часы разработать генератор случайных чисел.
27. Чем отличаются самосинхронизирующие шифры от синхронных.
28. Какие алгоритмы называются ассиметричными.
29. Что такое открытый ключ.
30. Какой ключ является открытым.
31. Какие требования предъявляются к ассиметричным системам шифрования.
32. Из каких этапов состоит шифрование с открытым ключом.

33. Что такое компьютерный вирус.
34. Как классифицируются вирусы.
35. Что такое файловый вирус.
36. Какие вирусы называются пусковыми.
37. Какие вирусы относятся к резидентным.
38. Перечислите уровни антивирусной защиты.
39. Какие программы называются сканерами.
40. Какие функции выполняют полифаги.
41. Что выполняют программы ревизоры.
42. Как работают фильтры.
43. Что называется идентификацией.
44. Как связаны идентификация и аутентификация.
45. Какие способы идентификации существуют.
46. Какой метод идентификации дают максимальный результат.
47. Что относится к биометрическим параметрам.
48. Что такое хэш-функция.
49. Требования к хэш-функциям.
50. Классификация хэш-функций.
51. Понятие электронно-цифровой подписи.
52. Требования к электронно-цифровым подписям.
53. Этапы создания и проверки подписи.
54. Что такое аутентификация.
55. Какие протоколы аутентификации существуют.
56. Какие протоколы относятся к протоколом полного доверия.
57. Какие протоколы являются протоколами неполного доверия.
58. Что такое взаимная аутентификация.
59. Дайте определение системе защиты информации.
60. Перечислите ообще методологические принципы построения СЗИ
61. Каков порядок проектирования и разработки СЗИ?
62. Общее содержание этапов проектирования больших систем
63. Назовите основные функции корпоративной СЗИ

Глоссарий

Авторизация - процесс определения того, какие типы действий разрешены. Обычно авторизация выполняется в контексте аутентификации после того, как пользователь аутентифицирован, он может получить право (авторизацию) на доступ или действия различного типа.

Администратор системы защиты - Субъект доступа, ответственный за защиту автоматизированной системы от НСД.

Антивирус – Программа, обнаруживающая и удаляющая вирусы. Если вирус удалить не удается, то зараженная программа должна быть уничтожена.

Антивирусная программа – Обслуживающая программа, предназначенная для поиска, диагностики, профилактики и лечения файлов, зараженных компьютерным вирусом. В процессе поиска и диагностики определяются зараженные файлы и тип вируса. Профилактика позволяет предотвратить заражение. Лечение подразумевает удаление вируса, восстановление поврежденных файлов и т. п.

Аутентификация - процесс определения идентичности пользователя, пытающегося получить доступ к системе.

Доступ к информации – Ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности. Итак, защита информации - комплекс мероприятий, проводимых в целях предотвращения утечки, хищения, утраты, несанкционированного уничтожения, изменения, модификации (подделки), несанкционированного копирования, блокирования информации. Включает в себя организационные, программные и технические методы и средства, направленные на удовлетворение ограничений, установленных для типов данных в системе обработки данных.

Идентификация – Присвоение объектам и субъектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с перечнем присвоенных идентификаторов.

Несанкционированный доступ к информации (НСД) – Получение защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации.

Пароль – Идентификатор субъекта доступа, который является его (субъекта) секретом. Строка или последовательность символов, недоступных для посторонних и предназначенных для идентификации и аутентификации субъектов или объектов между собой.

Политика безопасности – Набор законов, правил и норм поведения, определяющих, как организация обрабатывает, защищает и распространяет информацию. В частности, правила определяют, в каких случаях пользователь имеет право оперировать с определенными наборами данных. Политика безопасности - это активный компонент защиты, включающий в себя анализ возможных угроз и выбор мер противодействия.

Санкционированный доступ к информации – Доступ к информации, не нарушающий правила разграничения доступа.

Субъект доступа - Лицо или процесс, действия которых регламентируются правилами разграничения доступа.

Средство криптографической защиты информации – Средство вычислительной техники, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

Система защиты информации (СЗИ) - Комплекс организационных мер и программно-технических (в том числе криптографических) средств обеспечения безопасности информации в автоматизированных системах.

Методические рекомендации
Методические указания преподавателю

Дисциплина «Информационная безопасность» является профессиональной дисциплиной, базирующейся на изученных ранее дисциплинах «Информатика» и «Вычислительные системы, сети и телекоммуникации». Предполагается, что студенты имеют представление о месте технических средств в автоматизированных информационных системах, владеют терминологией и классификацией технических средств.

Подготовка к лекционным занятиям требует от преподавателя детального изучения современных архитектур и конструкций процессоров, чипсетов, оперативной и внешней памяти, периферийных устройств.

Основной материал по последним разработкам может быть получен из периодических изданий, таких как: журналы «КомпьютерПресс» и «Мир ПК», а также из сети Интернет.

При проведении лабораторных работ основной упор необходимо делать на правильное выполнение студентами операций по подготовке, сборке и техническом обслуживании компьютера и периферийной техники. При защите отчетов по практическим работам студенты должны показать знания о конкретных моделях технических средств, их устройстве и принципах работы.

5.1.1. Организация занятий и контроля знаний

Преподавание дисциплины «Информационная безопасность» предусматривает:

- проведение лекций;
- проведение практических занятий;
- проведение лабораторных занятий;
- выполнение домашних заданий;
- проведение контрольных работ по разделам;
- аналитический обзор литературы определенной тематики
- проведение зачетных испытаний
- самостоятельная работа студентов (изучение теоретического материала, подготовка к практическим занятиям, выполнение домашних лабораторных заданий, реферирование, составление сводной таблицы, подготовка к контрольной работе).

В рамках изучения дисциплины «Информационная безопасность» необходимо предусмотреть развитие форм самостоятельной работы студентов.

Пакет базовых заданий для самостоятельной работы (индивидуальные типовые расчеты во время лабораторно-практических заданий, вопросы для подготовки к зачету, тематику контрольных работ, тематику и вопросы для подготовки рефератов) следует выдавать в начале семестра, определив предельные сроки выполнения и сдачи. Задания для самостоятельной работы желательно составлять из базовой и дополнительной частей. Организуя самостоятельную работу, необходимо постоянно обучать студентов методам такой работы.

Содержание лекции должно отвечать следующим дидактическим требованиям:

- изложение материала от простого к сложному, от известного к неизвестному;
- логичность, четкость и ясность в изложении материала;
- возможность проблемного изложения, дискуссии, диалога с целью активизации деятельности студентов;
- связь теоретических положений и выводов с практикой

Преподаватель, читающий лекционные курсы в колледже, должен знать существующие в педагогической науке и используемые на практике варианты лекций, их дидактические и воспитывающие возможности, а также их методическое место в структуре процесса обучения.

Преподаватель должен рекомендовать студентам изучать разделы дисциплины путем прослушивания и конспектирования лекций и материалов практических занятий, а также путем самостоятельной работы с рекомендуемой учебной литературой.

Лекции по курсу «Информационная безопасность» целесообразно читать в аудитории, оснащённой проекционной аппаратурой для демонстрации заранее подготовленных компьютерных презентаций. Презентации должны содержать опорный материал для конспектирования: отражать логику изложения в виде иерархической структуры, содержать основные определения, табличный и графический

иллюстрационный материал. Определяющим требованием к презентации является её способность привить базовые навыки отражения смысла изучаемых процессов, а также дать необходимые основы для выполнения заданий лабораторного практикума.

В начале каждой лекции и практического занятия рекомендуется кратко напомнить основные положения материала предыдущего занятия, а в конце - обобщить изложенный материал и ответить на вопросы студентов. При проведении практических занятий с разбором решений типовых задач целесообразно акцентировать внимание студентов на распространенных ошибках и пояснять причины их возникновения.

Самостоятельная работа по курсу используется:

- для проработки конспектов лекций и обязательной учебной литературы по курсу;
- при необходимости - для ознакомления с рекомендуемой литературой;
- для написания реферата, предусмотренного данной рабочей программой;
- для выполнения расчётного задания по теме;
- для выполнения тех заданий лабораторного практикума, которые, как правило, не вызывают затруднений у студентов и потому могут быть выполнены в отсутствие преподавателя;

Выполнение контрольной работы, выполнение и защита индивидуальных типовых расчетов и рефератов являются необходимым условием положительной оценки промежуточной и итоговой аттестации студента по дисциплине.

Порядок подготовки и защиты индивидуальных типовых расчетов изложен в методических указаниях для студентов.

При защите индивидуальных типовых расчетов, выполненных во время лабораторно- практических занятий, можно использовать следующие критерии (показатели) оценки ответов:

1. полнота и конкретность ответа, его обоснованность и доказательность;
2. последовательность и логика изложения;
3. уровень культуры речи (при защите в форме собеседования);
4. при выполнении практического задания: умение правильно определить возможные методы и способы решения задачи и выбрать из них наиболее оптимальный.

Также рекомендуется давать подобную оценку по результатам защиты рефератов, выполнения контрольной работы и в конце каждого практического занятия со студентами.

При изложении материала важно помнить, что почти половина информации на лекции передается через интонацию. Учитывать тот факт, что первый кризис внимания студентов наступает на 15-20- й минутах, второй - на 30-35-й минутах.

При проведении аттестации студентов важно всегда помнить, что систематичность, объективность, аргументированность - главные принципы, на которых основаны контроль и оценка знаний студентов. Проверка, контроль и оценка знаний студента, требуют учета его индивидуального стиля в осуществлении учебной деятельности. Знание критериев оценки знаний обязательно для преподавателя и студента.

Характеристика используемых форм, методов и технологий контроля учебной работы (аттестации) студента

Порядок проведения текущего контроля и промежуточной аттестации должен проводится в строгом соответствии с положением о проведении текущего контроля успеваемости и промежуточной аттестации студентов в колледже. Требования к итоговой аттестации, определяются требованиями к итоговой аттестации.

Промежуточная аттестация.

Промежуточная аттестация проводится по результатам выполнения домашних заданий

1. Домашние задания.

На каждом практическом занятии студент получает домашнее задание — набор заданий.

2. Выполнение контрольной работы.

Контрольная работа выполняется на аудиторном занятии. Примерный вариант заданий для контрольной работы приведен в разделе «Рубежный контроль».

3. Выполнение и защита индивидуальных типовых расчетов.

Индивидуальные типовые расчеты выполняются студентами на аудиторных лабораторно-практических занятиях (в рамках самостоятельной работы). Защита индивидуальных типовых расчетов проводится только после правильного выполнения всех заданий. При защите индивидуальных типовых

расчетов студенту задают два вопроса по теоретическим материалам соответствующего раздела дисциплины

4. Итоговая аттестация по дисциплине (дифференцированный зачет).

Итоговой аттестацией по дисциплине является дифференцированный зачет. Для его проведения имеются контрольно-оценочные средства (представлены в разделе «Итоговый контроль по дисциплине»

- 5.1.2. Организация и контроль самостоятельной работы

В современный период востребованы высокий уровень знаний, академическая и социальная мобильность, профессионализм специалистов, готовность к самообразованию и самосовершенствованию. В связи с этим должны измениться подходы к планированию, организации учебно-воспитательной работы, в том числе и самостоятельной работы студентов.

Прежде всего, это касается изменения характера и содержания учебного процесса, переноса акцента на самостоятельный вид деятельности, который является не просто самоцелью, а средством достижения глубоких и прочных знаний, инструментом формирования у студентов активности и самостоятельности.

Целью методических рекомендаций является повышение эффективности учебного процесса, в том числе благодаря самостоятельной работе, в которой студент становится активным субъектом обучения, что означает:

- способность занимать в обучении активную позицию;
- готовность мобилизовать интеллектуальные и волевые усилия для достижения учебных целей;
- умение проектировать, планировать и прогнозировать учебную деятельность;
- привычку инициировать свою познавательную деятельность на основе внутренней положительной мотивации;
- осознание своих потенциальных учебных возможностей и психологическую готовность составить программу действий по саморазвитию.

- Организация и контроль самостоятельной работы

Для успешного выполнения самостоятельной работы студентов необходимо планирование и контроль со стороны преподавателей.

Аудиторная самостоятельная работа выполняется студентами на лекциях, лабораторно-практических занятиях, и, следовательно, преподаватель должен заранее выстроить систему самостоятельной работы, учитывая все ее формы, цели, отбирая учебную и научную информацию и средства (методических) коммуникаций, продумывая роль студента в этом процессе и свое участие в нем.

Вопросы для самостоятельной работы студентов, указанные в рабочей программе дисциплины, предлагаются преподавателями в начале изучения дисциплины. Студенты имеют право выбирать дополнительно интересующие их темы для самостоятельной работы.

Внеаудиторная самостоятельная работа студентов (далее самостоятельная работа) -планируемая учебная, учебно-исследовательская, научно-исследовательская деятельность студентов, осуществляемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Она включает в себя:

- подготовку к аудиторным занятиям (лекциям, практическим, семинарским, лабораторным работам и др.) и выполнение соответствующих заданий;
- самостоятельную работу над отдельными темами учебных дисциплин в соответствии с учебно-тематическими планами;
- написание рефератов, докладов, эссе;
- подготовку ко всем видам практики и выполнение предусмотренных ими заданий;
- выполнение письменных контрольных работ;
- подготовку ко всем видам контрольных испытаний, в том числе к экзаменам;
- работу в студенческих научных обществах, кружках, семинарах и др.;
- участие в работе факультативов, спецсеминаров и т.п.;
- участие в научных и научно-практических конференциях, семинарах, конгрессах и т.п.;
- другие виды деятельности, организуемой и осуществляемой колледжем.

Выполнение любого вида самостоятельной работы предполагает прохождение студентами следующих этапов:

- определение цели самостоятельной работы;
- конкретизация познавательной (проблемной или практической) задачи;
- самооценка готовности к самостоятельной работе по решению поставленной или выбранной задачи;
- выбор адекватного способа действий, ведущего к решению задачи (выбор путей и средств для ее решения);
- планирование (самостоятельно или с помощью преподавателя) самостоятельной работы по решению задачи;
- реализация программы выполнения самостоятельной работы.

Методические рекомендации для студентов по организации самостоятельной работы
Методические рекомендации по работе с литературой

Важной составляющей самостоятельной внеаудиторной подготовки является работа с литературой ко всем видам занятий: лекционным, практическим, при подготовке к зачетам, экзаменам, тестированию, участию в научных конференциях.

Умение работать с литературой означает научиться осмысленно пользоваться источниками. Прежде чем приступить к освоению научной литературы, рекомендуется чтение учебников и учебных пособий.

Существует несколько методов работы с литературой.

Один из них -самый известный - ***метод повторения**:* прочитанный текст можно заучить наизусть. Простое повторение воздействует на память механически и поверхностно. Полученные таким путем сведения легко забываются.

Наиболее эффективный метод ***- метод кодирования:*** прочитанный текст нужно подвергнуть большей, чем простое заучивание, обработке.

Чтобы основательно обработать информацию и закодировать ее для хранения, важно произвести целый ряд мыслительных операций:

- прокомментировать новые данные;
- оценить их значение;
- поставить вопросы;
- сопоставить полученные сведения с ранее известными.

Для улучшения обработки информации очень важно устанавливать осмысленные связи, структурировать новые сведения.

Изучение научной, учебной и иной литературы требует ведения рабочих записей.

Форма записей может быть весьма разнообразной: простой или развернутый план, тезисы, цитаты, конспект.

План - первооснова, каркас какой-либо письменной работы, определяющие последовательность изложения материала.

План является наиболее краткой и потому самой доступной и распространенной формой записей содержания исходного источника информации По существу, это перечень основных вопросов, рассматриваемых в источнике. План может быть простым и развернутым. Их отличие состоит в степени детализации содержания и, соответственно, в объеме.

Преимущество плана состоит в следующем. Во-первых, план позволяет наилучшим образом уяснить логику мысли автора, упрощает понимание главных моментов произведения.

Во-вторых, план позволяет быстро и глубоко проникнуть в сущность построения произведения и, следовательно, гораздо легче ориентироваться в его содержании.

В-третьих, план позволяет - при последующем возвращении к нему - быстрее обычного вспомнить прочитанное.

В-четвертых, с помощью плана гораздо удобнее отыскивать в источнике нужные места, факты, цитаты и т. д.

Выписки - небольшие фрагменты текста (неполные и полные предложения, отдельные абзацы, а также дословные и близкие к дословным записи об излагаемых в нем фактах), содержащие в себе квинтэссенцию содержания прочитанного.

Выписки представляют собой более сложную форму записей содержания исходного источника информации. По сути, выписки - не что иное, как цитаты, заимствованные из текста. Выписки позволяют в концентрированной форме и с максимальной точностью воспроизвести в произвольном (чаще последовательном) порядке наиболее важные мысли автора, статистические и даталогические

сведения. В отдельных случаях - когда это оправданно с точки зрения продолжения работы над текстом - вполне допустимо заменять цитирование изложением, близким к дословному.

Тезисы - сжатое изложение содержания изученного материала в утвердительной (реже опровергающей) форме.

Отличие тезисов от обычных выписок состоит в следующем.

Во-первых, тезисам присуща значительно более высокая степень концентрации материала.

Во-вторых, в тезисах отмечается преобладание выводов над общими рассуждениями.

В-третьих, чаще всего тезисы записываются близко к оригинальному тексту, т. е. без использования прямого цитирования.

Исходя из сказанного, нетрудно выявить основное преимущество тезисов: они незаменимы для подготовки глубокой и всесторонней аргументации письменной работы любой сложности, а также для подготовки выступлений на защите, докладов и пр.

Аннотация - краткое изложение основного содержания исходного источника информации, дающее о нем обобщенное представление.

К написанию аннотаций прибегают в тех случаях, когда подлинная ценность и пригодность исходного источника информации исполнителю письменной работы окончательно неясна, но в то же время о нем необходимо оставить краткую запись с обобщающей характеристикой. Для указанной цели и используется аннотация.

Характерной особенностью аннотации наряду с краткостью и обобщенностью ее содержания является и то, что пишется аннотация всегда после того, как (хотя бы в предварительном порядке) завершено ознакомление с содержанием исходного источника информации. Кроме того, пишется аннотация почти исключительно своими словами и лишь в крайне редких случаях содержит в себе небольшие выдержки оригинального текста.

Резюме - краткая оценка изученного содержания исходного источника информации, полученная, прежде всего, на основе содержащихся в нем выводов.

Резюме весьма сходно по своей сути с аннотацией. Однако, в отличие от последней, текст резюме концентрирует в себе данные не из основного содержания исходного источника информации, а из его заключительной части, прежде всего выводов.

Но, как и в случае с аннотацией, резюме излагается своими словами -выдержки из оригинального текста в нем практически не встречаются.

Конспект - сложная запись содержания исходного текста, включающая в себя заимствования (цитаты) наиболее примечательных мест в сочетании с планом источника, а также сжатый анализ записанного материала и выводы по нему.

Для работы над конспектом следует:

- определить структуру конспектируемого материала, чему в значительной мере способствует письменное ведение плана по ходу изучения оригинального текста;
- в соответствии со структурой конспекта произвести отбор и последующую запись наиболее существенного содержания оригинального текста — в форме цитат или в изложении, близком к оригиналу;
- выполнить анализ записей и на его основе - дополнение записей собственными замечаниями, соображениями, "фактурой", заимствованной из других источников и т. п. (располагать все это следует на полях тетради для записей или на отдельных листах-вкладках);
- завершить формулирование и запись выводов по каждой из частей оригинального текста, а также общих выводов.

Систематизация изученных источников позволяет повысить эффективность их анализа и обобщения. Итогом этой работы должна стать логически выстроенная система сведений по существу исследуемого вопроса.

Необходимо из всего материала выделить существующие точки зрения на проблему, проанализировать их, сравнить, дать им оценку.

Кстати, этой процедуре должны подвергаться и материалы из Интернета во избежание механического скачивания готовых текстов. В записях и конспектах студенту очень важно указывать названия источников, авторов, год издания. Это организует его, а главное, пригодится в последующем обучении. Безусловно, студент должен взять за правило активно работать с литературой в библиотеке не только, но и в других библиотеках, используя, в том числе, их компьютерные возможности (электронная библиотека в сети Интернет).

Методические рекомендации по подготовке к контрольным работам, тестам, зачетам, экзаменам

Приступая к изучению новой учебной дисциплины, студенты должны ознакомиться с учебной программой, учебной, научной и методической литературой, имеющейся в библиотеке колледжа, получить в библиотеке рекомендованные учебники и учебно-методические пособия, завести новую тетрадь для конспектирования лекций и работы с первоисточниками.

Помимо учебной, научной литературы студентами должны активно использоваться хрестоматии - сборники текстов, иллюстрирующих содержание учебника, а также словари, справочники. В хрестоматиях собраны материалы, которые позволяют расширить кругозор. При подготовке к занятиям, зачетам, экзаменам следует в полной мере использовать академический курс учебника, рекомендованного преподавателем. Они дают более углубленное представление о проблемах, получивших систематическое изложение в учебнике. Работа с хрестоматией позволит студенту самостоятельно изучить документы, фрагменты источников, другие произведения, разъясняющие сущность изучаемого вопроса.

Студентам рекомендуется самостоятельно выполнять доклады, индивидуальные письменные задания и упражнения, предлагаемые при подготовке к занятиям. Работа, связанная с решением этих задач и упражнений, представляет собой вид интеллектуальной практической деятельности. Она способствует выработке умения и привычки делать что-либо правильно, а также закреплению навыков и знаний по проблеме.

Доклад - это вид самостоятельной работы студентов, заключающийся в разработке студентами темы на основе изучения литературы и развернутом публичном сообщении по данной проблеме. Отличительными признаками доклада являются:

- передача в устной форме информации;
- публичный характер выступления;
- стилевая однородность доклада;
- четкие формулировки и сотрудничество докладчика и аудитории;
- умение в сжатой форме изложить ключевые положения исследуемого вопроса и сделать выводы.

В ходе самостоятельной подготовки к семинарским занятиям, особенно по гуманитарным дисциплинам, студентами может использоваться, к примеру, так называемый метод контрфактического моделирования событий, который научит их самостоятельно рассуждать о минувших, а также современных событиях, покажет мотивы принятия людьми решений, причины совершенных ошибок.

Такая работа, в процессе которой студенту приходится сравнивать, сопоставлять, выявлять логические связи и отношения, применять методы анализа и синтеза, позволит успешно в дальнейшем подготовиться к зачетам, экзаменам и тестированию. Тестирование ориентировано в целом на проверку блоков проблем, способствует систематизации изученного материала, проверке качества его усвоения.

Серьезная и методически грамотно организованная работа по подготовке к семинарским занятиям, написанию письменных работ значительно облегчит подготовку к экзаменам и зачетам. Основными функциями экзамена, зачета являются: обучающая, оценочная и воспитательная. Экзамены и зачеты позволяют выработать ответственность, трудолюбие, принципиальность. При подготовке к зачету, экзамену студент повторяет, как правило, ранее изученный материал. В этот период сыграют большую роль правильно подготовленные заранее записи и конспекты.

Студенту останется лишь повторить пройденное, учесть, что было пропущено, восполнить пробелы при подготовке к семинарам, закрепить ранее изученный материал.

Методические рекомендации по написанию письменных работ студентов

Написание письменных научно - исследовательских работ студентов решает ряд задач:

- обучение студентов самостоятельному поиску и отбору учебной и специальной научной литературы по предмету;
- привитие навыков реферирования научных статей по проблематике изучаемых дисциплин;
- выработка умения подготовки рефератов, докладов, выступлений и сообщений;
- приобретение опыта выступления с докладами
- систематизация, закрепление и расширение теоретических и практических знаний и навыков по изучаемым дисциплинам;
- приобщение студентов к решению проблемных вопросов по избранной теме работы;
- обучение студентов излагать материал в виде стройной системы теоретических положений, связанных логической последовательностью и подкрепленных примерами из практики.

Участие студентов в работе.

Участие в научной работе позволяет студентам реализовать творческий потенциал в процессе учебы в колледже. Их вклад в научно-исследовательскую деятельность может выражаться в самых разнообразных формах: выполнение курсовых работ и дипломных проектов в форме НИР; производственная и др.

В общем виде НИР студентов (НИРС) состоит из следующих элементов:

- работа в научных кружках;
- участие в конкурсах научных работ;
- участие в выставках научных работ;
- участие в студенческих конференциях;
- подготовка студенческих публикаций.

Процесс обучения способствует развитию у студентов задатков к научным исследованиям - памяти, наблюдательности, воображения, самостоятельности суждений и выводов. Каждый из перечисленных компонентов необходим для самостоятельной исследовательской работы.

Наряду с выполнением научных исследований студенты принимают участие в сборе и обработке статистических данных, составлении и подготовке различной компьютерной продукции. Результаты научных исследований студенты представляют на конференциях, научных семинарах и т.д. При подготовке к докладу или выступлению на конференции студент получает опыт систематизации и обобщения материала, приобретает навыки научного творчества и, наконец, овладевает очень важным искусством публичного выступления, аргументированной полемики.

В этой связи необходимо запомнить несколько правил, характеризующих культуру полемики, дискуссии.

Дискуссия - это соревнование интеллектов, здесь оружие - аргументы.

Необходимо найти надежные аргументы в пользу своей точки зрения и проверять имеющиеся на надежность. Не недооценивайте оппонента. Самыми ценными являются документальные аргументы, ссылки на документы и надежно установленные факты, противоречащие утверждению оппонента.

Следует тщательно проанализировать свои аргументы; пофантазируйте над тем, что можно им противопоставить и как можно их повернуть.

Дискуссия похожа на игру в шахматы: и там и тут очень важно предвидеть возможное развитие событий, только события - ходы заменены более сложными событиями - аргументами, а правила движения фигур - правилами логического мышления.

Необходимо строго следовать логике.

Вкупе с надежными аргументами она обеспечит вам победу. Любой логический промах может быть использован оппонентом, чтобы поставить под сомнение всю вашу конструкцию! Побеждая в дискуссии, следует быть великодушным. Ваши оппоненты не единственные, кто придерживается этой точки зрения, так им легче будет пережить горечь поражения.

Выступление с докладом и публикации материалов позволят студентам приобрести к тому же общественное признание в среде профессионалов -преподавателей колледжа, других вузов, представителей общественности.

Методические рекомендации по работе над рефератом

Реферат - краткое изложение содержания документа или его части, научной работы, включающее основные фактические сведения и выводы, необходимые для первоначального ознакомления с источниками и определения целесообразности обращения к ним.

Современные требования к реферату-точность и объективность в передаче сведений, полнота отображения основных элементов как по содержанию, так и по форме.

Цель реферата - не только сообщить о содержании реферируемой работы, но и дать представление о вновь возникших проблемах соответствующей отрасли науки.

В учебном процессе реферат представляет собой краткое изложение в письменном виде или в форме публичного доклада содержания книги, учения, научного исследования и т.п.

Иначе говоря, это доклад на определенную тему, освещающий её вопросы на основе обзора литературы и других источников.

Рефераты в рамках учебного процесса в вузе оцениваются по следующим основным критериями:

- актуальность содержания, высокий теоретический уровень, глубина и полнота анализа фактов, явлений, проблем, относящихся к теме;
- информационная насыщенность, новизна, оригинальность изложения вопросов;

- простота и доходчивость изложения;
- структурная организованность, логичность, грамматическая правильность и стилистическая выразительность;
- убедительность, аргументированность, практическая значимость и теоретическая обоснованность предложений и выводов.

Составление списка использованной литературы.

В соответствии с требованиями, предъявляемыми к реферату, докладу, необходимо составить список литературы, использованной в работе над ним.

Основные этапы работы над рефератом

В организационном плане написание реферата-процесс, распределенный во времени по этапам. Все этапы работы могут быть сгруппированы в три основные: подготовительный, исполнительский и заключительный.

Подготовительный этап включает в себя поиски литературы по определенной теме с использованием различных библиографических источников; выбор литературы в конкретной библиотеке; определение круга справочных пособий для последующей работы по теме.

Исполнительский этап включает в себя чтение книг (других источников), ведение записей прочитанного.

Заключительный этап включает в себя обработку имеющихся материалов и написание реферата, составление списка использованной литературы.

Написание реферата.

Определен список литературы по теме реферата.

Изучена история вопроса по различным источникам, составлены выписки, справки, планы, тезисы, конспекты. Первоначальная задача данного этапа -систематизация и переработка знаний. Систематизировать полученный материал - значит привести его в определенный порядок, который соответствовал бы намеченному плану работы.

- Структура реферата

Введение

Введение - это вступительная часть реферата, предваряющая текст. Оно должно содержать следующие элементы:

а) очень краткий анализ научных, экспериментальных или практических достижений в той области, которой посвящен реферат;

б) общий обзор опубликованных работ, рассматриваемых в реферате;

в) цель данной работы;

г) задачи, требующие решения.

Объем введения при объеме реферата 10-15 может составлять одну страницу.

Основная часть.

В основной части реферата студент дает письменное изложение материала по предложенному плану, используя материал из источников. В этом разделе работы формулируются основные понятия, их содержание, подходы к анализу, существующие в литературе, точки зрения на суть проблемы, ее характеристики. В соответствии с поставленной задачей делаются выводы и обобщения. Очень важно не повторять, не копировать стиль источников, а выработать свой собственный, который соответствует характеру реферируемого материала.

Заключение

Заключение подводит итог работы. Оно может включать повтор основных тезисов работы, чтобы акцентировать на них внимание читателей (слушателей), содержать общий вывод, к которому пришел автор реферата, предложения по дальнейшей научной разработке вопроса и т.п. Здесь уже никакие конкретные случаи, факты, цифры не анализируются.

Заключение по объему, как правило, должно быть меньше введения.

Список использованных источников

В строго алфавитном порядке размещаются все источники, независимо от формы и содержания: официальные материалы, монографии и энциклопедии, книги и документы, журналы, брошюры и газетные статьи.

Список использованных источников оформляется в той же последовательности, которая указана в требованиях к оформлению рефератов, курсовых, дипломных работ.

Порядок сдачи и защиты рефератов.

1.Реферат сдается на проверку преподавателю за 1-2 недели до зачетного занятия.

2.При защите реферата преподаватель учитывает:

- качество
- степень самостоятельности студента и проявленную инициативу
- связность, логичность и грамотность составления
- оформление в соответствии с требованиями ГОСТ.

3.Защита тематического реферата может проводиться на выделенном одном занятии в рамках часов учебной дисциплины или конференции или по одному реферату при изучении соответствующей темы, либо по договоренности с преподавателем.

4.Защита реферата студентом предусматривает

•доклад по реферату не более 5-7 минут

•ответы на вопросы оппонента.

На защите запрещено чтение текста реферата.

Требования к оформлению рефератов, курсовых работ

Работа должна быть выполнена с помощью ПК через 1,5 интервала. Тексты работ печатают с соблюдением размеров полей: справа не менее 2 см, слева 3 см, снизу, сверху-2 см, размер шрифта TimesNewRoman-14.

Расстояние между заголовками и текстом должно быть в одну пустую строку. Абзацы начинаются отступами в 1,5 см.

Страницы нумеруются арабскими цифрами, нумерация страниц должна быть сквозной. Титульный лист включается в общую нумерацию, однако номер на нем не ставится. Иллюстрации и таблицы, расположенные на отдельных листах, а также все приложения включают в общую нумерацию страниц работы. Номер страницы проставляется внизу посередине.

Иллюстрации (графики, схемы, диаграммы) располагаются непосредственно после текста, в котором они упоминаются впервые, или на следующей странице. Все иллюстрации обозначаются словом «Рисунок» и в тексте на них делаются ссылки. Иллюстрации нумеруются арабскими цифрами или двумя цифрами (напр. 2.1), где 1-я цифра указывает номер главы, 2-я -номер рисунка, но сквозной нумерацией в пределах всей работы.

Если ссылки приводятся в конце страницы, используются знаки сносок, как правило, цифры, в том месте, где заканчивается мысль автора. Например, в тексте: Речевой период, который некоторые называют синтаксической конструкцией, создается по принципу кругообразно замыкающихся и ритмически организованных частей.

В сноске:

Ефимов А.И. О мастерстве речи пропагандиста. -М., 1997. Изд-во Юрайт, с. 42.

Цифровой материал рекомендуется оформлять в виде таблиц, каждую из которых размещают после упоминания о ней. Таблица должна иметь номер (арабскими цифрами) и заголовок, написанный с заглавной буквы.

Слово «Таблица» помещается с красной строки с номером, затем ставится пробел, тире, пробел и заголовок таблицы с прописной буквы без кавычек.

Тексты желательно иллюстрировать графиками, диаграммами, рисунками. При ссылке на таблицы и рисунки указывают их полный номер.

Список использованных источников оформляется в определенной последовательности. Вначале приводятся:

1. Законы, указы Президента, постановления Правительства, нормативные материалы, изданные органами власти и управления различных уровней.

2. Монографии, научные сборники, журнальные статьи в алфавитном порядке, с указанием ф.и.о. авторов; названия; года издания; издательства; номеров журналов, номеров страниц начала и окончания статьи. Для научной и учебной литературы -общее число страниц.

Основная учебная литература

1. Павлов А. Защита информации. Краткий взгляд на методы технических средств защиты информации. // Журнал депонированных рукописей.- №11.– 2001. С. 43-55.
2. Шеннон К. Работы по теории информации и кибернетики. – М.: Иностранная литература, 1963.
3. Пшенин Е.С. Теоретические основы защиты информации. – Алматы. КазНТУ, 2000
4. Иванов М.А. Теория кодирования и криптографии - М.:КУДИЦ – ОБРАЗ, 2002. – 167 с.
5. Алферов А.П., Зубков А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. 2-ое изд. – М., 2002
6 Смарт Н. Мир программирования. Криптография: Техносфера. – М., 2005
7. Лукацкий А. В. Комплексный подход к обеспечению компьютерной безопасности. // Системы безопасности, связи и телекоммуникаций. - №1. – 1998. С. 10-25.

Дополнительная учебная литература

1. Павлов А. Защита информации. Краткий взгляд на методы технических средств защиты информации. // Журнал депонированных рукописей.- №11.– 2001. С. 43-55.
2. Шеннон К. Работы по теории информации и кибернетики. – М.: Иностранная литература, 1963.
3. Семенов Г. Не только шифрование, или Обзор криптотехнологий.
4. Стуленков А. Безопасность компьютерных систем на базе NT.

Перечень Интернет-ресурсов

http://ru.wikipedia.org/
http://catalog.iot.ru/
http://catalog.ivs.kz