Название учреждения, в котором выполнялась данная диссертационная работа

На правах рукописи

Фамилия Имя Отчество

Название диссертационной работы

Специальность XX.XX.XX ”—
«Название специальности»

Диссертация на соискание учёной степени [1; 2]
кандидата физико-математических наук

Научный руководитель:
уч. степень, уч. звание
Фамилия Имя Отчество

Город ”— 20XX

ЗМІСТ

Список сокращений и условных обозначений 4

Словарь терминов 5

Вступ 6

1 Основы информационной безопасности 7
Теоретические ведомости 7
Практические задания 12
Тест 12

2 Методы защиты информации 13
Теоретические ведомости 13
Задания 18
Пример выполнения работы 18
Варианты 18
Вопросы для контроля 18

3 Методы атаки. Частотная атака 19
Теоретические ведомости 19
Задания 19
Пример выполнения работы 19
Варианты 19
Вопросы для контроля 19

4 Модель системы IDEF0 20
Теоретические ведомости 20
Задания 20
Пример выполнения работы 20
Варианты 20
Вопросы для контроля 20

5 Семинар по теме стандартов в ИБ 21
Требования к знаниям и умениям 21

Термины 21
Темы для обсуждения 22

6 Распределение прав в организациях 23
Теоретические ведомости 23
Задания 23
Пример выполнения работы 23
Варианты 23
Вопросы для контроля 23

7 Сокрытие информации 24
Теоретические ведомости 24
Задания 24
Инструкция к работе с ПО 24
Вопросы для контроля 24

8 Анализ рисков 25
Теоретические ведомости 25
Задания 25
Пример выполнения работы 25
Варианты 25

Заключение 26

Література 27

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

СЛОВАРЬ ТЕРМИНОВ

ВСТУП

Использовать можно в двух системах:

Первый вариант — это выполняются первые 8 работ и получают нужную оценку.

Второй вариант — каждое задание добавляет балы, общая сумма балов определяет итоговую оценку. (Данная система более правильна и гибка, но требует набирать балы за работу)

ПРАКТИЧНА РОБОТА 1

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Мета роботи: Изучение способов и основных концепций ИБ.

Теоретические ведомости

1. Основные понятия информационной безопасности

Прежде чем говорить об обеспечении безопасности персональных данных, необходимо определить, что же такое информационная безопасность. Термин «информационная безопасность» может иметь различный смысл и трактовку в зависимости от контекста. В данном пособии под информационной безопасностью мы будем понимать защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.[1]

Информационная безопасность — это защищённость информации и поддерживающей её инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести ущерб владельцам или пользователям информации.

В ряде случаев понятие «информационная безопасность» подменяется термином «компьютерная безопасность». В этом случае информационная безопасность рассматривается очень узко, поскольку компьютеры только одна из составляющих информационных систем. Несмотря на это, в рамках изучаемого курса основное внимание будет уделяться изучению вопросов, связанных с обеспечением режима информационной безопасности применительно к вычислительным системам, в которых информация хранится, обрабатывается и передаётся с помощью компьютеров. Согласно определению, компьютерная безопасность зависит не только от компьютеров, но и от поддерживающей инфраструктуры, к которой можно отнести системы электроснабжения, жизнеобеспечения, вентиляции, средства коммуникаций, а также обслуживающий персонал.

2. Составляющие информационной безопасности

Обеспечение информационной безопасности в большинстве случаев связано с комплексным решением трёх задач:

1. **Конфиденциальность** – состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право.

2. **Целостность** – состояние информации, при котором отсутствует любое её изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

3. **Доступность** – состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно.

Угрозы информационной безопасности — совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации. [2,3]

Атака — это попытка реализации угрозы. Кто предпринимает такую попытку, называется **злоумышленником**. Потенциальные злоумышленники называются **источниками угрозы**.

Угроза является следствием наличия уязвимых мест или уязвимости в информационной системе. Уязвимости могут возникать по разным причинам, например, в результате непреднамеренных ошибок программистов при написании программ.

Угрозы можно классифицировать по нескольким критериям:

- по свойствам информации (доступность, целостность, конфиденциальность), против которых угрозы направлены в первую очередь;
- по компонентам информационных систем, на которые угрозы нацелены (данные, программы, аппаратура, поддерживающая инфраструктура);
- по способу осуществления (случайные/преднамеренные, действия природного/техногенного характера);
- по расположению источника угроз (внутри/вне рассматриваемой ИС).

Обеспечение информационной безопасности является сложной задачей, для решения которой требуется комплексный подход.

3. Уровни защиты информации

3.1. Законодательный уровень

Законодательный уровень является основой для построения системы защиты информации, так как даёт базовые понятия предметной области и определяет меру наказания для потенциальных злоумышленников. Этот уровень играет координирующую и направляющую роли и помогает поддерживать в обществе негативное (и карательное) отношение к людям, нарушающим информационную безопасность.

Законодательно-правовой уровень включает комплекс законодательных и иных правовых актов, устанавливающих правовой статус субъектов информационных отношений, субъектов и объектов защиты, методы, формы и способы защиты, их правовой статус. Кроме того, к этому уровню относятся стандарты и спецификации в области информационной безопасности. Система законодательных актов и разработанных на их базе нормативных и организационно-распорядительных документов должна обеспечивать организацию эффективного надзора за их исполнением со стороны правоохранительных органов и реализацию мер судебной защиты и ответственности субъектов информационных отношений. К этому уровню можно отнести и морально-этические нормы поведения, которые сложились традиционно или складываются по мере распространения вычислительных средств в обществе. Морально-этические нормы могут быть регламентированными в законодательном порядке, т. е. в виде свода правил и предписаний. Наиболее характерным примером таких норм является Кодекс профессионального поведения членов Ассоциации пользователей ЭВМ США. Тем не менее, эти нормы большей частью не являются обязательными, как законодательные меры.

3.2. Административный уровень

Это комплекс мер, предпринимаемых локально руководством организации. Включает комплекс взаимокоординируемых мероприятий и технических мер, реализующих практические механизмы защиты в процессе создания и эксплуатации систем защиты информации. Организационный уровень должен охватывать все структурные элементы систем обработки данных на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

Разработка политики безопасности - дело тонкое, поскольку у каждой организации есть своя специфика. Здесь бессмысленно переносить практику режимных государственных организаций на коммерческие структуры, учебные заведения или персональные компьютерные системы. В этой области целесообразно предложить, во-первых, основные принципы разработки политики безопасности, а, во-вторых, - готовые шаблоны для наиболее важных разновидностей организаций.

3.3. Процедурный уровень

К процедурному уровню относятся меры безопасности, реализуемые людьми. В отечественных организациях накоплен богатый опыт составления и реализации процедурных (организационных) мер, однако проблема состоит в том, что они пришли из докомпьютерного прошлого, поэтому нуждаются в существенном пересмотре.

Можно выделить следующие группы процедурных мер:

- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

Для каждой группы в каждой организации должен существовать набор регламентов, определяющих действия персонала. В свою очередь, исполнение этих регламентов следует отработать на практике.

3.4. Программно-технический уровень

Согласно современным воззрениям, включает три подуровня: физический, технический (аппаратный) и программный.

Физический подуровень решает задачи с ограничением физического доступа к информации и информационным системам, соответственно к нему относятся технические средства, реализуемые в виде автономных устройств и систем, не связанных с обработкой, хранением и передачей информации: система охранной сигнализации, система наблюдения, средства физического воспрепятствования доступу (замки, ограждения, решётки и т. д.).

Средства защиты аппаратного и программного подуровней непосредственно связаны с системой обработки информации. Эти средства либо встроены в

аппаратные средства обработки, либо сопряжены с ними по стандартному интерфейсу.К аппаратным средствам относятся схемы контроля информации по четности, схемы доступа по ключу и т. д.

К программным средствам защиты, образующим программный подуровень, относятся специальное программное обеспечение, используемое для защиты информации, например антивирусный пакет и т. д. Программы защиты могут быть как отдельные, так и встроенные. Подчеркнём, что формирование режима информационной безопасности является сложной системной задачей, решение которой в разных странах отличается по содержанию и зависит от таких факторов, как научный потенциал страны, степень внедрения средств информатизации в жизнь общества и экономику, развитие производственной базы, общей культуры общества и, наконец, традиций и норм поведения.

4. Виды информационных угроз

Информационные угрозы могут быть обусловлены:

– естественными факторами (пожар, наводнение, и др.);
– человеческими факторами.

Последние, в свою очередь, подразделяются на:

1. Угрозы, носящие случайный, неумышленный характер. Это угрозы, связанные с ошибками процесса подготовки, обработки и передачи информации;

2. Угрозы, обусловленные умышленными, преднамеренными действиями людей. Это угрозы, связанные с несанкционированным доступом к ресурсам АИС.

Умышленные угрозы преследуют цель нанесения ущерба пользователям АИС и, в свою очередь, подразделяются на активные и пассивные. Угрозы также подразделяются на внутренние, возникающие внутри управляемой организации, и внешние.

Под внутренними угрозами понимаются — угрозы безопасности информации инсайдером (исполнителем) которых является внутренний по отношению к ресурсам организации субъект (инсайдер).

Под внешними угрозами понимаются — угрозы безопасности информации инициатором (исполнителем) которых является внешний по отношению к ресурсам организации субъект (удаленный хакер, злоумышленник).

Практические задания

1. Выполнить тестирование.
2. Описать предложенную по варианту ситуацию.

Таблица вариантов по ситуациям. (Какие меры нужно предпринять и на что полагаться)

Тест

1. В чем заключается проблема информационной безопасности?
2. Дайте определение понятию ”информационная безопасность”.
3. Какие определения информационной безопасности приводятся в ”Концепции информационной безопасности сетей связи общего пользования Российской Федерации”?
4. Что понимается под ”компьютерной безопасностью”?
5. Перечислите составляющие информационной безопасности.
6. Приведите определение доступности информации.
7. Приведите определение целостности информации.
8. Приведите определение конфиденциальности информации.
9. Каким образом взаимосвязаны между собой составляющие информационной безопасности? Приведите собственные примеры.
10. Перечислите задачи информационной безопасности общества.
11. Перечислите уровни формирования режима информационной безопасности.
12. Дайте краткую характеристику законодательно-правового уровня.
13. Какие подуровни включает программно-технический уровень?
14. Что включает административный уровень?
15. В чем особенность морально-этического подуровня?

ПРАКТИЧНА РОБОТА 2

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Мета роботи: На практике использовать основные методы криптографической зашиты информации.

Теоретические ведомости

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили уровни защиты информации и вызвали необходимость того, чтобы эффективность защиты информации росла вместе со сложностью архитектуры хранения данных. Постепенно защита информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации; даже проводится ФЗ о защите информации, который рассматривает проблемы и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной системы.

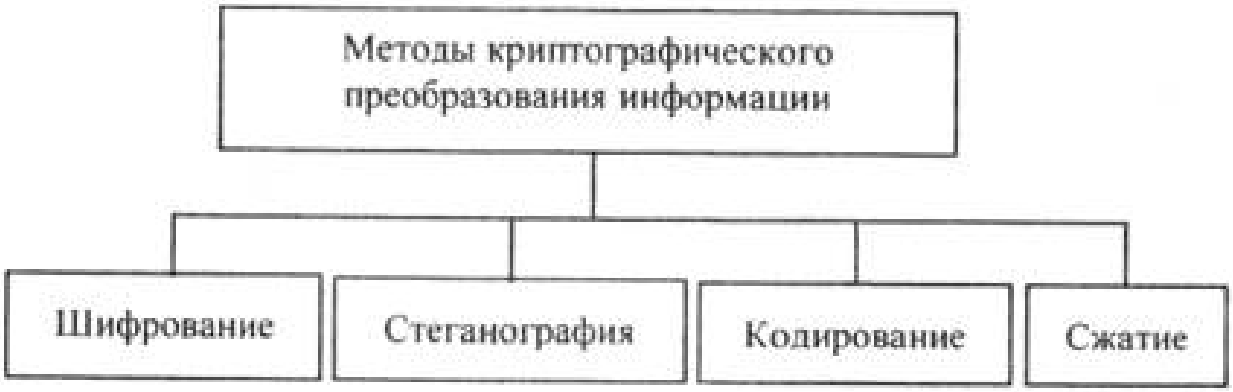


Рисунок 2.1 — Методы криптографического преобразования информации

1. Симметричные криптосистемы

1.1. Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключом в данном случае является размеры таблицы. Например, сообщение «Неясное становится ещё более непонятным» записывается в таблицу из 5 строк и 7 столбцов по столбцам.

Таблица 2.1

Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Ё	Е	Н	М

Для получения шифрованного сообщения текст считывается по строкам и группируется по 5 букв:

НОНСБ–НЯЕЕО–ЯОЕТЯ–СВЕЛП–НСТИЩ–ЕОЫНА–ТЕЕНМ

Несколько большей стойкостью к раскрытию обладает метод *одиночной перестановки* по ключу. Он отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы. Используя в качестве ключа слово - ЛУНАТИК, получим следующую таблицу:

Таблица 2.2 — Метод перестановки по ключу

Л	У	Н	А	Т	И	К
4	**7**	**5**	**1**	**6**	**2**	**3**
Н	О	Н	С	Б	Н	Я
Е	Е	О	Я	О	Е	Т
Я	С	В	Е	Л	П	Н
С	Т	И	Щ	Е	О	Ы
Н	А	Т	Е	Е	Н	М

До перестановки

А	И	К	Л	Н	Т	У
1	**2**	**3**	**4**	**5**	**6**	**7**
С	Н	Я	Н	Н	Б	О
Я	Е	Т	Е	О	О	Е
Е	П	Н	Я	В	Л	С
Щ	О	Ы	С	И	Е	Т
Е	Н	М	Н	Т	Е	А

После перестановки

В верхней строке левой таблицы записан ключ, а номера под буквами ключа определены в соответствии с естественным порядком соответствующих букв

ключа в алфавите. Если в ключе встретились бы одинаковые буквы, они бы нумеровались слева направо. Получается шифровка:

СНЯНН–БОЯЕТ–ЕООЕЕ–ПНЯВЛ–СЩОЫС–ИЕТЕН–МНТЕА

Для обеспечения дополнительной скрытности можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины её строк и столбцов отличались от длин строк и столбцов первой таблицы. Лучше всего, если они будут взаимно простыми.

Кроме алгоритмов одиночных перестановок применяются алгоритмы двойных перестановок. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в таблице 2.3.

Таблица 2.3 — Метод перестановки по ключу

	2	**4**	**1**	**3**
4	**П**	Р	И	Е
1	З	Ж	А	Ю
2	-	Ш	Е	С
3	Т	О	Г	**О**

	1	**2**	**3**	**4**
4	И	**П**	Е	Р
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	**О**	О

	1	2	3	4
1	А	З	Ю	Ж
2	Е	-	С	Ш
3	Г	Т	**О**	О
4	И	**П**	Е	Р

Ключом к шифру служат номера столбцов **2413** и номера строк **4123** исходной таблицы. В результате перестановки получена шифровка:

АЗЮЖЕ_СШГТООИПЕР

Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 33 их 36, для 44 их 576, а для $5 \cdot 5$ их 14400.

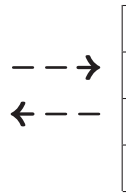
В средние века для шифрования применялись и магические квадраты. Магическими квадратами называются квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Для шифрования необходимо вписать исходный текст по приведённой в квадрате нумерации и затем переписать содержимое таблицы по строкам. В ре-

Таблица 2.4 — Исходный текст с идентификаторами

П	Р	И	Е	З	Ж	А	Ю	_	Ш	Е	С	Т	О	Г	О
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Таблиця 2.5 — Магический квадрат

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1



О	И	Р	Т
З	Ш	Е	Ю
-	Ж	А	С
Е	Г	О	П

зультате получается шифротекст, сформированный благодаря перестановке букв исходного сообщения.

Число магических квадратов очень резко возрастает с увеличением размера его сторон: для таблицы $3 \times 3 \Rightarrow 1$ существует только один квадрат; для таблицы $4 \times 4 \Rightarrow 880$; а для таблицы $5 \times 5 \Rightarrow 250000$.

1.2. Шифры простой замены

0.1. Система шифрования Цезаря. частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на *K* букв. Известная фраза Юлия Цезаря `VENI VINI VICI` – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в `SBKF SFAF SFZF` (при смещении на 4 символа). Греческим писателем Полибием за 100 лет до н.э. был изобретён так называемый полибианский квадрат размером 5×5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже её в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

1.3. Шифры сложной замены

0.1. Шифр Гронсфельда. состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно так же, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

1. пусть в качестве ключа используется группа из трех цифр - 314;
2. тогда Сообщение СОВЕРШЕННО СЕКРЕТНО;
3. Ключ 3143143143143143;
4. Шифровка ФПЖИСЬИОССАХИЛФИУСС.

В шифрах *многоалфавитной замены* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (свой алфавит).

В компьютере операция шифрования соответствует сложению кодов ASCII символов сообщения и ключа по модулю 256.

1.4. Гаммирование

Процесс зашифрования заключается в генерации гаммы шифра и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $T(0)_i$ одинаковой длины (по 64 бита). Гамма шифра вырабатывается в виде последовательности блоков Г(с)i аналогичной длины $(c)_i = G(c)_i \oplus T(0)_i$, где $\oplus$ - побитовое сложение, $i = 1 - m$).

Процесс расшифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные $T(0)_i = G(c)_i \oplus (c)_i$.

Исходное сообщение из букв русского алфавита преобразуется в числовое сообщение заменой каждой его буквы числом по следующей таблице:

Таблиця 2.6 — Числовая замена букв

А	Б	В	Г	Д	Е	Ж	З	И	К	Л	М	Н	О	П
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14
Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ь	Ы	Э	Ю	Я
15	16	17	18	19	20	21	22	23	24	25	26	27	28	29

$$\Omega_{i+1} = [(A_i + C_1 – 1) \cdot mod 30] + 1; \tag{2.1}$$

Исходное сообщение ОТДУШКА. Для шифрования числового сообщения используется шифрующий отрезок последовательности А1, А2, ... подходящей длины, начинающийся с A_{100}: $A_{101} \rightarrow 5$, $A_{102} \rightarrow 6$, $A_{103} \rightarrow 17$, $A_{104} \rightarrow 18$, $A_{105} \rightarrow 19$, $A_{106} \rightarrow 3$.

Исходное сообщение	О	Т	Д	У	Ш	К	А
Числовое исходное сообщение	13	17	4	18	23	9	0
Шифрующий отрезок	1	5	6	17	8	19	3
Числовое шифрованное сообщение	14	23	10	5	1	28	3
Шифрованное сообщение	П	Ш	Л	Е	Б	Ю	Г

Задания

(из заданий к экзамену)

Пример выполнения работы

Варианты

Вопросы для контроля

1.
2.
3.

ПРАКТИЧНА РОБОТА 3

МЕТОДЫ АТАКИ. ЧАСТОТНАЯ АТАКА

Мета роботи: Изучение способов атаки на разные уровни системы. Методы подбора и анализ частотной атаки.

Теоретические ведомости

1. Атаки на устарелые алгоритмы

2. Частотная атака

2.1. Защиты от частотной атаки.

Задания

1. Освоить теорию и принципы частотной атаки.
2. Проанализировать представленное ПО
3. Расшифровать текст и предоставить:
   - шифрованное сообщение;
   - перечень замен;
   - расшифрованный текст;
   - предоставить алгоритм дешифровки[1].
4. Выводы к работе

Пример выполнения работы

Варианты

Вопросы для контроля

[1] Задание для дополнительных баллов.

ПРАКТИЧНА РОБОТА 4

МОДЕЛЬ СИСТЕМЫ IDEF0

Мета роботи: Изучение модели IDEF0. Построение структуры системы по модели, анализ возможных атак и альтернативные способы защиты.

Теоретические ведомости

1. **Модели IDEF**
    - **1.1. Виды моделей.**
2. **Модель IDEF0**
3. **Структуры по модели IDEF0**

Задания

1. Чтение материала по варианту.
2. Структурное описание системы.
3. Составление модели IDEF0.

Пример выполнения работы

Варианты

(Разные описания систем, заводов, фирм, компаний, сетей)

Вопросы для контроля

ПРАКТИЧНА РОБОТА 5

СЕМИНАР ПО ТЕМЕ СТАНДАРТОВ В ИБ

Мета: ознакомиться с основными положениями стандартов по обеспечению информационной безопасности в распределённых вычислительных сетях.

Требования к знаниям и умениям

Студент должен знать:

- основное содержание стандартов по информационной безопасности распределённых систем;
- основные сервисы безопасности в вычислительных сетях;
- наиболее эффективные механизмы безопасности;
- задачи администрирования средств безопасности.

Студент должен уметь:

- выбирать механизмы безопасности для защиты распределенных систем.

Термины

Распределённая информационная система — совокупность аппаратных и программных средств, используемых для накопления, хранения, обработки, передачи информации между территориально удалёнными пользователями.

Сервис *(Сервисная деятельность)* — это вид деятельности, направленный на удовлетворение потребностей социальных субъектов посредством оказания услуг.

Сервис безопасности — это деятельность государственных и частных организаций, а также отдельных специалистов, направленная на удовлетворение потребностей социальных субъектов в безопасности.

Цель сервиса безопасности − удовлетворение потребностей в безопасности индивидуальных и групповых социальных субъектов. **Сущность сервиса безопасности** состоит в оказании услуг, направленных на обеспечение безопасности. **Услуга безопасности** – это деятельность субъекта безопасности, направленная на удовлетворение потребности заказчика в безопасности, а также результат взаимодействия исполнителя и заказчика услуги безопасности, выраженный в виде полезного эффекта.

Темы для обсуждения

1. Механизмы безопасности.
2. Сервисы безопасности в вычислительных сетях.
3. Функций и механизмов безопасности.
4. Администрирование средств безопасности.
5. Международные стандарты.
6. Стандарты ГОСТ и ДСТУ.

Ссылки на литературу: 1. Щербаков А. Ю. Введение в теорию и практику компьютерной безопасности. – М.: Издательство Молгачева С. В., 2001.2. Теория и практика обеспечения информационной безопасности / Под ред. П. Д. Зегжды. – М: Яхтсмен, 1996.3. Галатенко В. А. Основы информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2003.4. Галатенко В. А. Стандарты информационной безопасности. – М: Интернет-Университет Информационных Технологий – ИНТУИТ. РУ, 2004.5. www.iso.ch – Web-сервер Международной организации по стандартизации.

ПРАКТИЧНА РОБОТА 6

РАСПРЕДЕЛЕНИЕ ПРАВ В ОРГАНИЗАЦИЯХ

Мета роботи: Научиться определять потребности в системах по моделям IDEF0, предоставление полномочий для разных классов сотрудников.

Теоретические ведомости

1. **Права в информационной безопасности**
2. **Распределение прав**
3. **Использование модели IDEF0**

Задания

1. Выбрать предприятие, структуру из табл.
2. Построение модели IDEF0.
3. Распределить права между сотрудниками, их полномочия и средства защиты.
4. Определить технологии защиты от несанкционированного доступа.
5. Предоставить результаты в отчёте.

Пример выполнения работы

Варианты

Вопросы для контроля

ПРАКТИЧНА РОБОТА 7

СОКРЫТИЕ ИНФОРМАЦИИ

Мета роботи: Изучить методы, факторы и риски при сокрытии информации.

Теоретические ведомости

1. Методы сокрытия информации

1.1. Использование шума.

2. Методы обнаружения информации

Обнаружения информации в файлах.

Задания

Цель практической части работы состоит в получении максимально коэф. сокрытия информации.

1. Изучить теорию, быть готовым к опросу.
2. Сокрыть информацию с помощью предоставленного ПО:
    а) в тесте;
    б) в изображении;
    в) в музыке.
3. Сравнение методов и выводы к работе.

Инструкция к работе с ПО

(ф-ции программы, методы и т.д.)

Вопросы для контроля

1. Какие есть способы сокрытия информации?
2. В каких файлах лучше скрывать информацию?
3. Что такое шум?
4. Риски потери и дешифровка информации.

ПРАКТИЧНА РОБОТА 8

АНАЛИЗ РИСКОВ

Мета роботи: Изучение анализа рисков. Формирование навыка определения угроз и защита.

Теоретические ведомости

Риски в информационной безопасности
Анализ стойкости системы
Правила определения угроз и защиты информации

Задания

1. Защита объекта по варианту из табл..
2. Оценка качества защиты.

Пример выполнения работы

Варианты

РЕКОМЕНДАЦІЇ

ЛІТЕРАТУРА

1. *Покровский*, *А. В.* Устранимые особенности решений эллиптических уравнений : дис. ... д-ра физ.-мат. наук : 01.01.01 / А. В. Покровский. — М., 2008. — 178 с.
2. *Фамилия*, *И. О.* название тезисов конференции / И. О. Фамилия // Название сборника. — 2015.