

***Разработка программного
средства защиты данных от
несанкционированного доступа
к носителю***

Манько Виктор Юрьевич



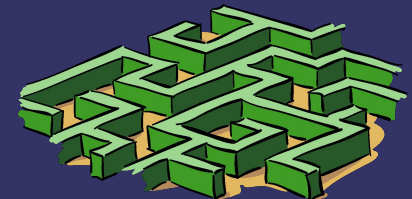
Цель

⇒ Цель – разработать программное средство защиты данных от несанкционированного доступа к носителю.



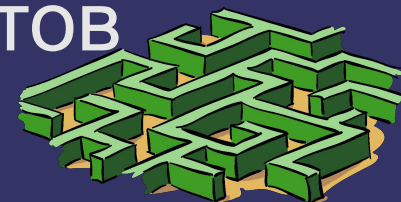
Задачи

- ⇒ Исследование структуры данных при хранении их на отчуждаемых носителях информации;
- ⇒
- ⇒ Исследование технологических методов защиты информации и разработка основных алгоритмов работы программы;
- ⇒
- ⇒ Выбор стандарта шифрования и его использование при разработке программы;
- ⇒
- ⇒ Расчет использования ресурсов носителей информации;
- ⇒
- ⇒ Разработка программной документации.



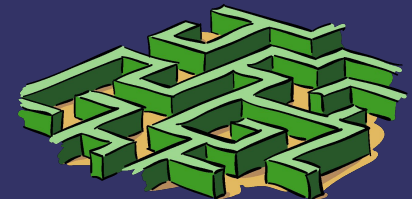
Введение

⇒ Информационная безопасность АС - состояние рассматриваемой автоматизированной системы, при котором она, с одной стороны, способна противостоять дестабилизирующему воздействию внешних и внутренних информационных угроз, а с другой - ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды.



Классификация угроз

- ⇒ По природе возникновения;
- ⇒ По степени преднамеренности проявления;
- ⇒ По непосредственному источнику угроз;
- ⇒ По положению источника угроз;
- ⇒ По степени воздействия на АС;
- ⇒ По способу доступа к ресурсам АС;
- ⇒ По текущему месте расположения информации, хранимой и обрабатываемой в АС.

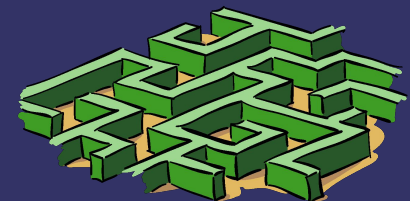


Классификация угроз

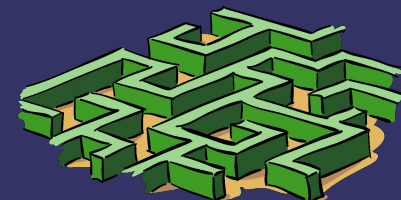
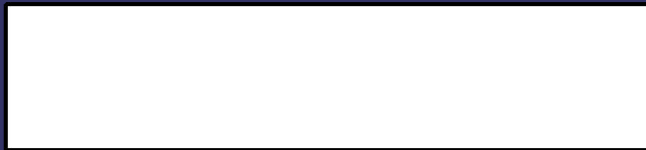
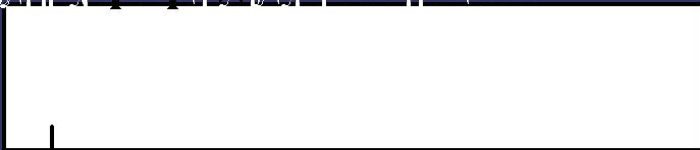


Классификация угроз

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32 33 34 35 36 37 38 39 40 41 42 43 44 45 46 47 48 49 50 51 52 53 54 55 56 57 58 59 60 61 62 63 64 65 66 67 68 69 70 71 72 73 74 75 76 77 78 79 80 81 82 83 84 85 86 87 88 89 90 91 92 93 94 95 96 97 98 99 100



Классификация угроз



Свойства информации

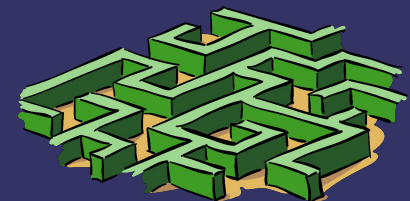
⇒ Конфиденциальность;

⇒

⇒ Целостность;

⇒

⇒ Доступность.



Модель нарушителя

- ⇒ Категория лиц;
- ⇒
- ⇒ Мотив;
- ⇒
- ⇒ Квалификация;
- ⇒
- ⇒ Характер действий.



Сводная информация



Рисунок 1.1 Число утечек информации и объем утекших записей ПДн, скомпрометированных в результате утечек. 2011 - 2015 гг.



Сводная информация

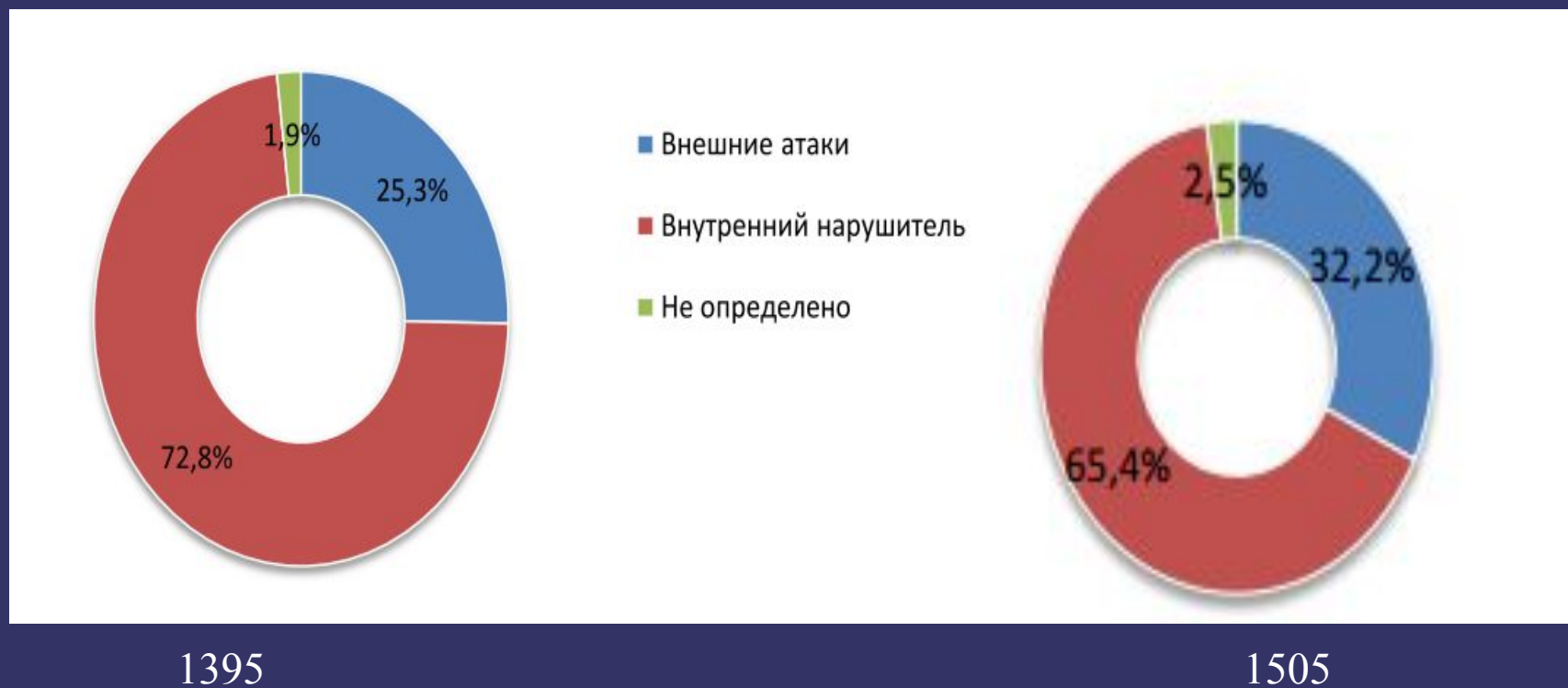
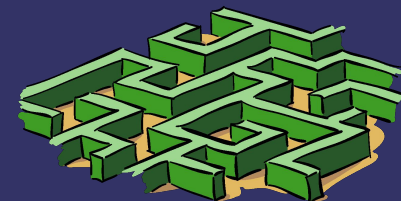


Рисунок 1.2 Распределение утечек по вектору воздействия, 2014-2015 гг.



Сводная информация

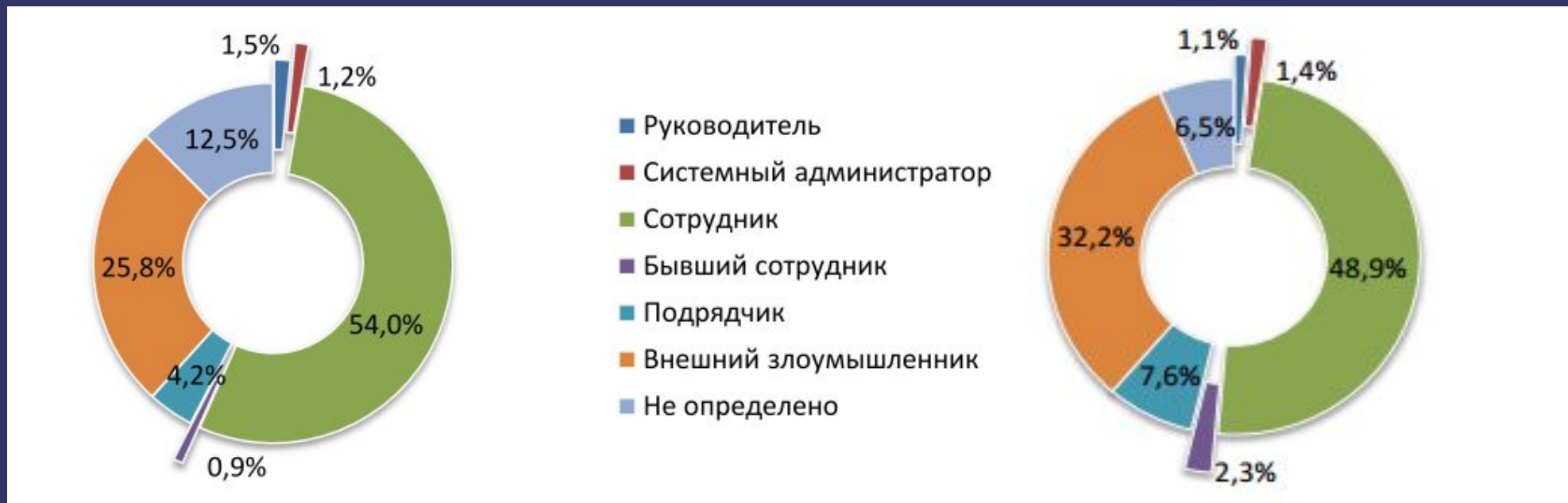
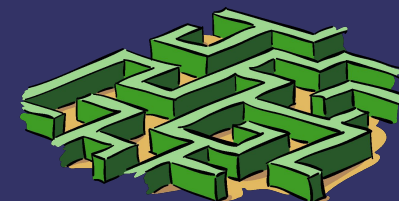


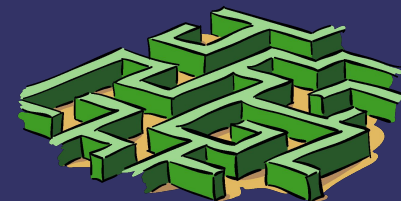
Рисунок 1.3 Распределение утечек по виновнику, 2014-2015 гг.



Сводная информация

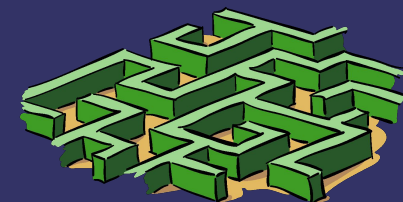


Рисунок 1.4 Распределение утечек по каналам, 2014 - 2015 гг.

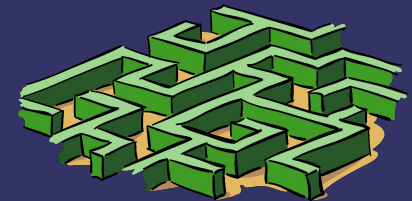
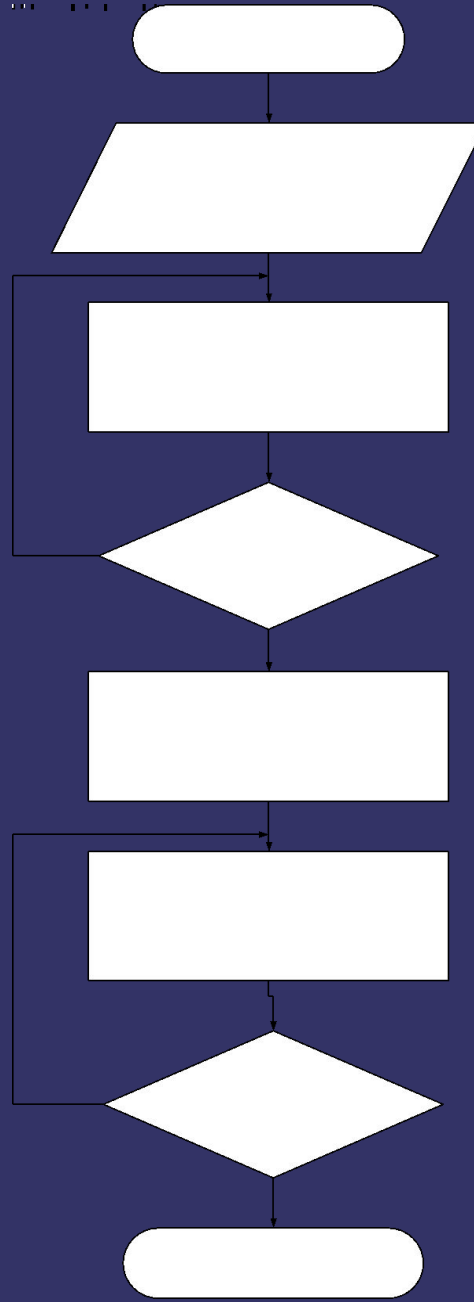


Сравнительные характеристики алгоритмов

| Показатель | ГОСТ28147-89 | ГОСТ Р34.12-2015 | Rijndael |
|---|--|--|---|
| Размер блока, бит | 64 | 128 | 128, 192, 256 |
| Размер ключа, бит | 256 | 256 | 128, 192, 256 |
| Архитектура | Однородная сбалансированная сеть Файстеля | SP-сеть | «Квадрат» (Square) |
| Число раундов | 32 | 10 | 10, 12, 14 ² |
| Часть блока, шифруемая за один раунд, бит | 32 (полблока) | 128 (полный блок) | 128, 192, 256 (полный блок) |
| Размер раундового ключевого элемента, бит | 32 (половина размера блока) | 128 (равен размеру блока) | 128, 192, 256 (равен размеру блока) |
| Структура раунда | Простая | Сложная | Более сложная |
| Используемые на раунде операции | Только аддитивные операции, подстановки и сдвиги | Нелинейное и линейное преобразование, операции наложения ключа | Широкое использование операций над конечными полями |
| Эквивалентно | С точностью до | С точностью до | С точностью до |



Общая схема программного средства



Спасибо
за внимание.

