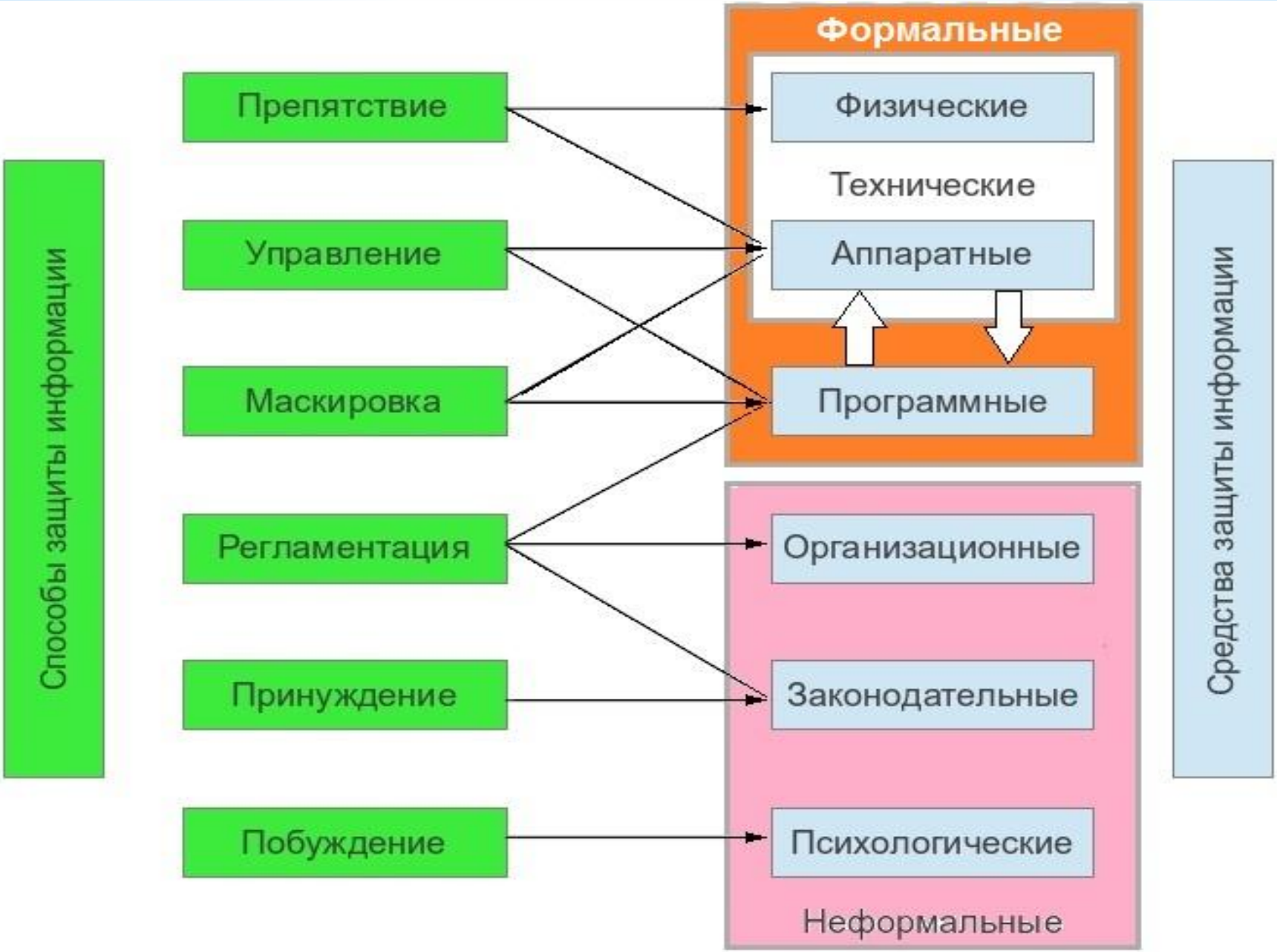
Техническая защита информации

1. Классификация способов защиты информации

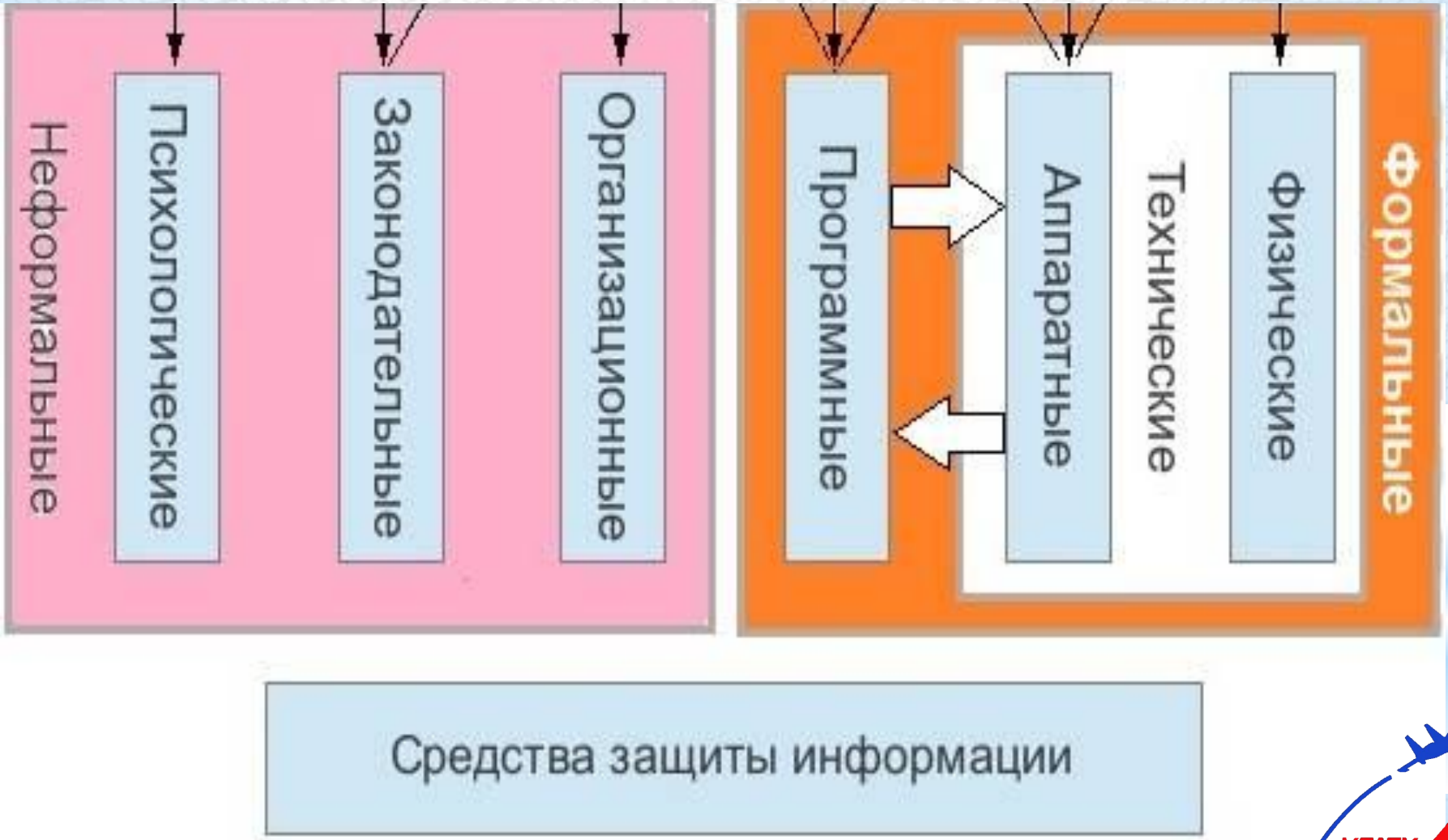
2. Классификация средств защиты информации

3. Классификация технических каналов утечки информации


Способы защиты информации
Препятствие
Управление
Маскировка
Регламентация
Принуждение
Побуждение
Формальные
Физические
Технические
Аппаратные
Программные
Организационные
Законодательные
Психологические
Неформальные
Средства защиты информации

1. Классификация способов защиты информации

2.Классификация средств защиты информации



Классификация
ТСЗИ по используемым средствам

3. Классификация технических каналов утечки информации

Утечки информации в 2018 году*

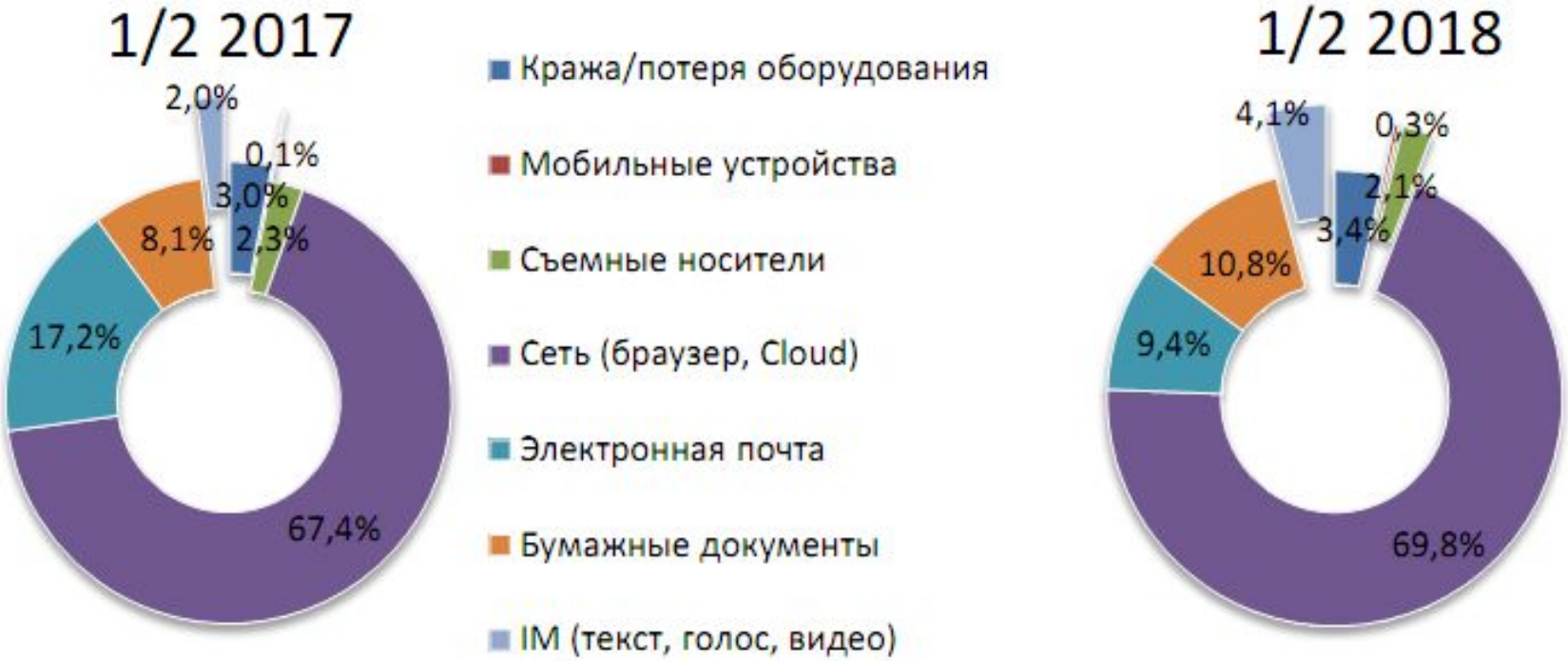


Рисунок 6. Распределение утечек по каналам, ½ 2017 – ½ 2018 гг.

* - по данным исследования Аналитического центра Infowatch

Утечки информации в 2018 году*

Основные риски бизнеса в настоящее время связаны не с внешним воздействием, а с внутренними утечками. Речь идет как о ненамеренных ошибках, так и о злоумышленных действиях сотрудников и руководителей компаний, направленных на компрометацию охраняемых данных, манипулирование информацией ограниченного доступа (в том числе инсайдерской информацией), корыстное использование полученных данных в мошеннических целях.

Учитывая отмеченную в 2017 году тенденцию на укрупнение корпоративных и государственных хранилищ данных, развитие технологий обработки больших объемов информации, не стоит удивляться, что конкретные факты применения таких технологий в ущерб владельцам данных все чаще становятся достоянием общественности. Это выводит на первый план проблему юридического регулирования режима больших пользовательских данных, ставит вопрос о том, кому же принадлежит собранная база данных и знания, извлеченные на основе ее анализа, кто отвечает за утечку данных, если она произошла.

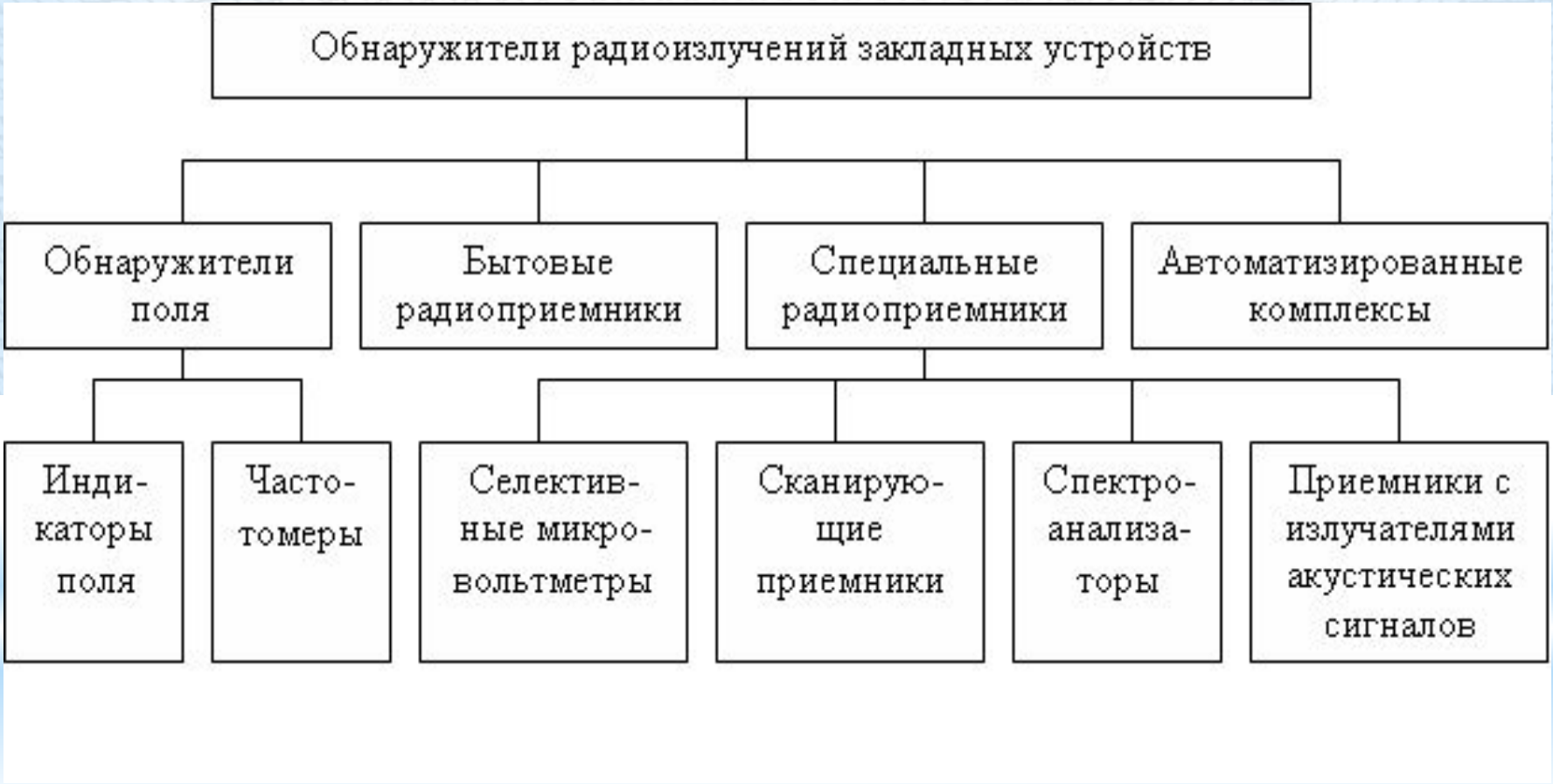
* - по данным исследования Аналитического центра Infowatch


УГАТУ
ФИРТ кафедра ВТиЗИ

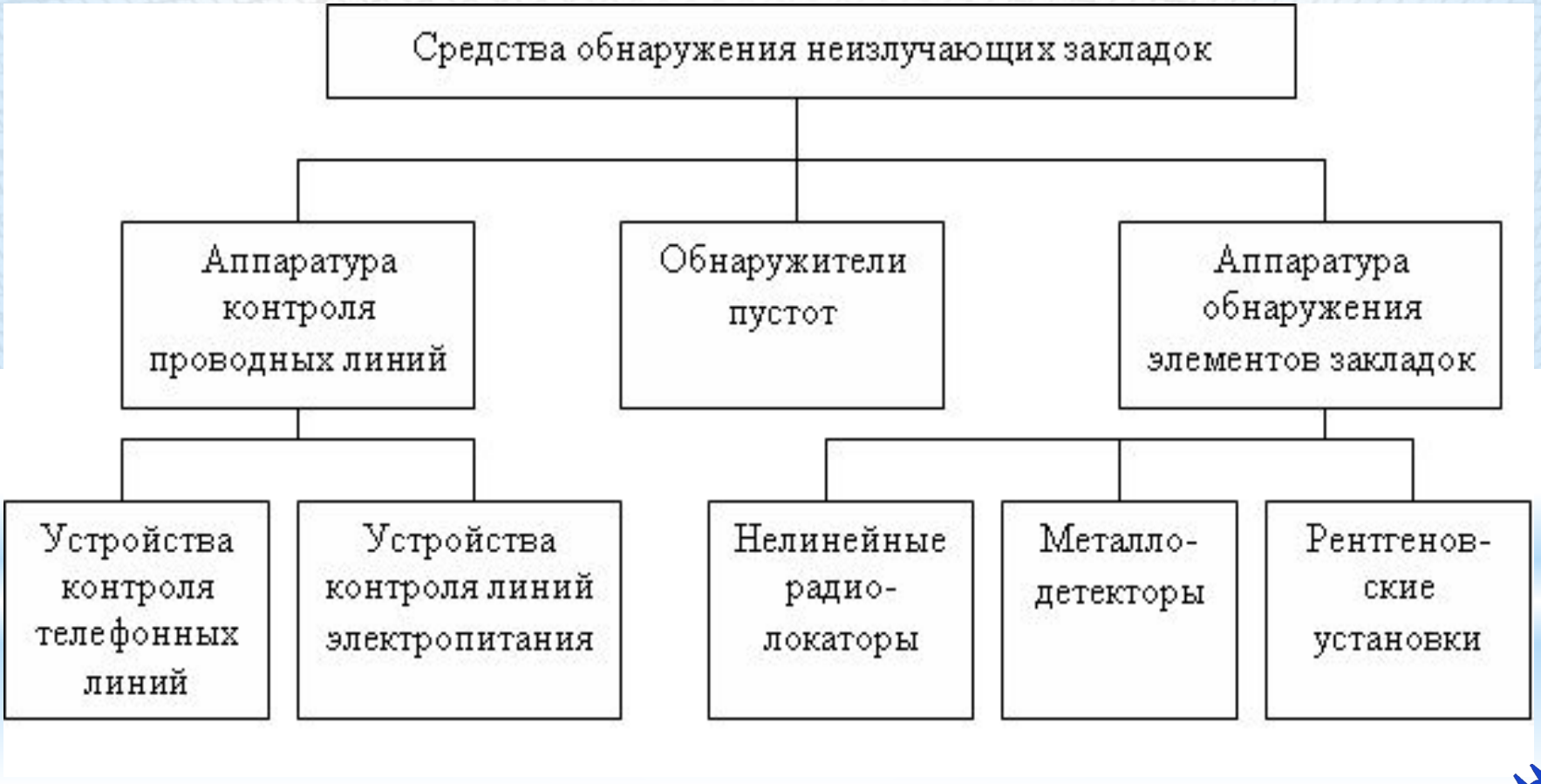
Основные группы технических средств перехвата информации

* Радиопередатчики с микрофоном
* Электронные "уши"
* Устройства перехвата телефонных сообщений
* Устройства приема, записи, управления
* Видеосистемы записи и наблюдения
* Системы определения местоположения контролируемого объекта
* Системы контроля компьютеров и

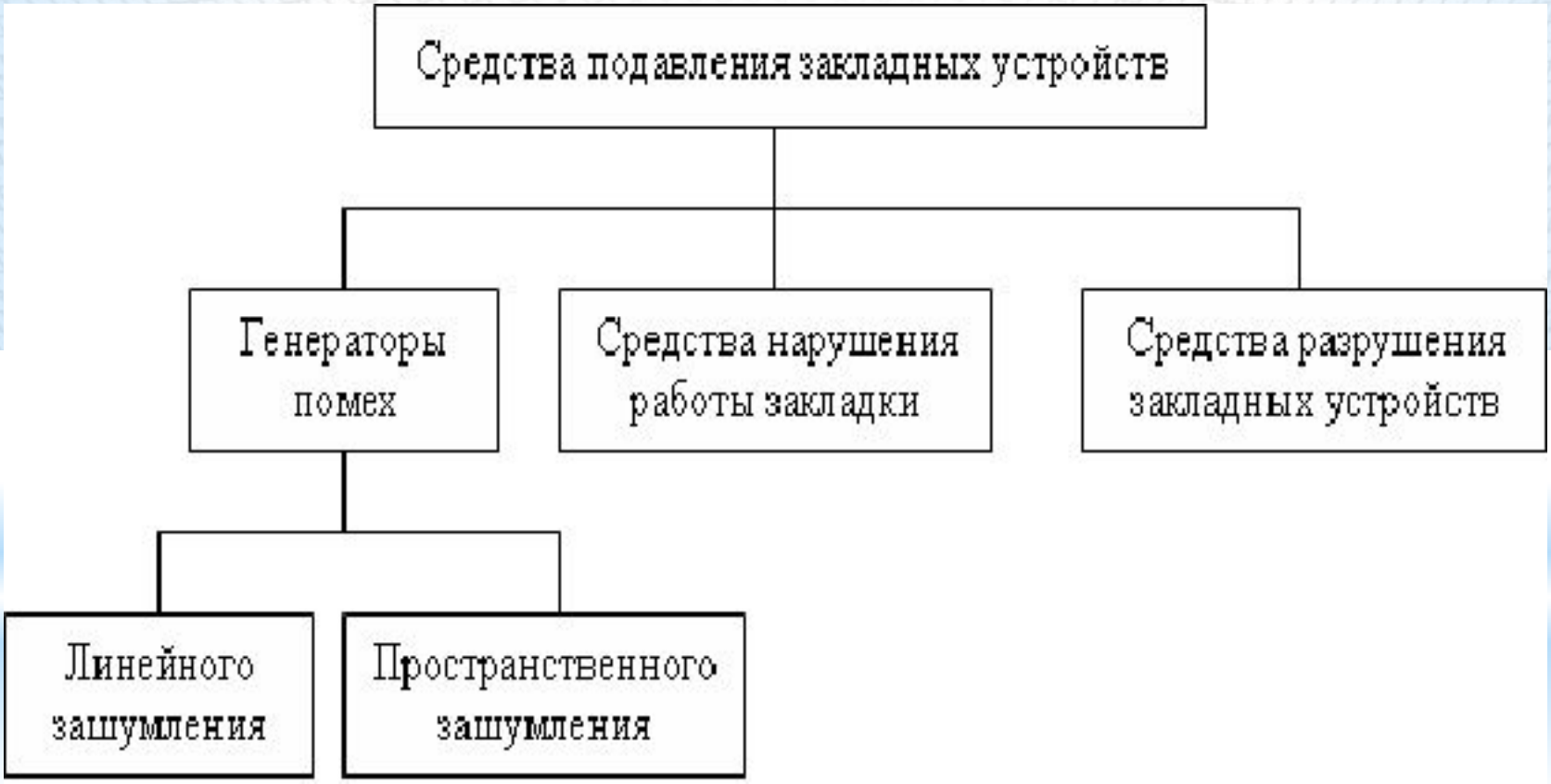
Классификация обнаружителей радиоизлучений закладных устройств



Классификация средств обнаружения неизлучающих закладок



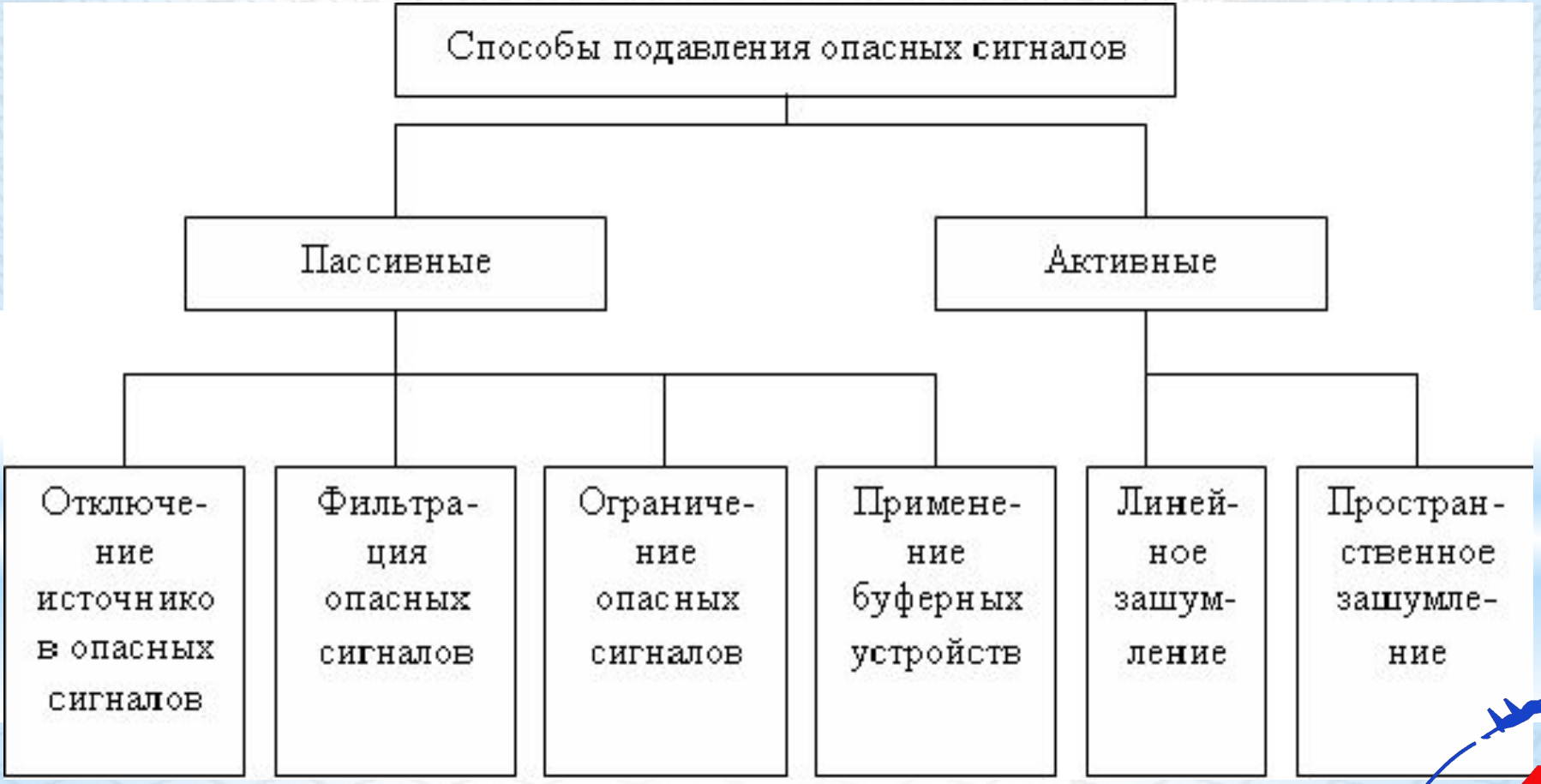
Классификация средств подавления закладных устройств



Противодействие перехвату речевой информации

* Информационное скрытие
* Энергетическое скрытие
* Обнаружение, локализация и изъятие закладных устройств

Способы подавления опасных электрических сигналов



Наименование Угроз Безопасности Информации

1. Угроза автоматического распространения вредоносного кода в грид-системе (система, которая координирует распределенные ресурсы посредством стандартных, открытых, универсальных протоколов и интерфейсов)
2. Угроза агрегирования данных, передаваемых в грид-системе
3. Угроза анализа криптографических алгоритмов и их реализации
4. Угроза аппаратного сброса пароля BIOS
5. Угроза внедрения вредоносного кода в BIOS
6. Угроза внедрения кода или данных
7. Угроза воздействия на программы с высокими привилегиями
8. Угроза восстановления аутентификационной информации
9. Угроза восстановления предыдущей уязвимой версии BIOS

10. Угроза выхода процесса за пределы виртуальной машины
11. Угроза деавторизации санкционированного клиента беспроводной сети
12. Угроза деструктивного изменения конфигурации/среды окружения программ
13. Угроза деструктивного использования декларированного функционала BIOS
14. Угроза длительного удержания вычислительных ресурсов пользователями
15. Угроза доступа к защищаемым файлам с использованием обходного пути
16. Угроза доступа к локальным файлам сервера при помощи URL
17. Угроза доступа/перехвата/изменения HTTP cookies
18. Угроза загрузки нештатной операционной системы

19. Угроза заражения DNS-кеша
20. Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг
21. Угроза злоупотребления доверием потребителей облачных услуг
22. Угроза избыточного выделения оперативной памяти
23. Угроза изменения компонентов системы
24. Угроза изменения режимов работы аппаратных элементов компьютера
25. Угроза изменения системных и глобальных переменных
26. Угроза искажения XML-схемы
27. Угроза искажения вводимой и выводимой на периферийные устройства информации
28. Угроза использования альтернативных путей доступа к ресурсам

29. Угроза использования вычислительных ресурсов суперкомпьютера «паразитными» процессами
30. Угроза использования информации идентификации/аутентификации, заданной по умолчанию
31. Угроза использования механизмов авторизации для повышения привилегий
32. Угроза использования поддельных цифровых подписей BIOS
33. Угроза использования слабостей кодирования входных данных
34. Угроза использования слабостей протоколов сетевого/локального обмена данными
35. Угроза использования слабых криптографических алгоритмов BIOS
36. Угроза исследования механизмов работы программы
37. Угроза исследования приложения через отчёты об ошибках

38. Угроза исчерпания вычислительных ресурсов хранилища больших данных
39. Угроза исчерпания запаса ключей, необходимых для обновления BIOS
40. Угроза конфликта юрисдикций различных стран
41. Угроза межсайтового скриптинга
42. Угроза межсайтовой подделки запроса
43. Угроза нарушения доступности облачного сервера
44. Угроза нарушения изоляции пользовательских данных внутри виртуальной машины
45. Угроза нарушения изоляции среды исполнения BIOS
46. Угроза нарушения процедуры аутентификации субъектов виртуального информационного взаимодействия
47. Угроза нарушения работоспособности грид-системы при нетипичной сетевой нагрузке

48. Угроза нарушения технологии обработки информации путём несанкционированного внесения изменений в образы виртуальных машин
49. Угроза нарушения целостности данных кеша
50. Угроза неверного определения формата входных данных, поступающих в хранилище больших данных
51. Угроза невозможности восстановления сессии работы на ПЭВМ при выводе из промежуточных состояний питания
52. Угроза невозможности миграции образов виртуальных машин из-за несовместимости аппаратного и программного обеспечения
53. Угроза невозможности управления правами пользователей BIOS
54. Угроза недобросовестного исполнения обязательств поставщиками облачных услуг
55. Угроза незащищённого администрирования облачных услуг

56. Угроза некачественного переноса инфраструктуры в облако
57. Угроза неконтролируемого копирования данных внутри хранилища больших данных
58. Угроза неконтролируемого роста числа виртуальных машин
59. Угроза неконтролируемого роста числа зарезервированных вычислительных ресурсов
60. Угроза неконтролируемого уничтожения информации хранилищем больших данных
61. Угроза некорректного задания структуры данных транзакции
62. Угроза некорректного использования прозрачного прокси-сервера за счёт плагинов браузера
63. Угроза некорректного использования функционала программного и аппаратного обеспечения

64. Угроза некорректной реализации политики лицензирования в облаке
65. Угроза неопределённости в распределении ответственности между ролями в облаке
66. Угроза неопределённости ответственности за обеспечение безопасности облака
67. Угроза неправомерного ознакомления с защищаемой информацией
68. Угроза неправомерного/некорректного использования интерфейса взаимодействия с приложением
69. Угроза неправомерных действий в каналах связи
70. Угроза непрерывной модернизации облачной инфраструктуры
71. Угроза несанкционированного восстановления удалённой защищаемой информации

72. Угроза несанкционированного выключения или обхода механизма защиты от записи в BIOS
73. Угроза несанкционированного доступа к активному и (или) пассивному виртуальному и (или) физическому сетевому оборудованию из физической и (или) виртуальной сети
74. Угроза несанкционированного доступа к аутентификационной информации
75. Угроза несанкционированного доступа к виртуальным каналам передачи
76. Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети
77. Угроза несанкционированного доступа к данным за пределами зарезервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение

78. Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети
79. Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин
80. Угроза несанкционированного доступа к защищаемым виртуальным устройствам из виртуальной и (или) физической сети
81. Угроза несанкционированного доступа к локальному компьютеру через клиента грид-системы
82. Угроза несанкционированного доступа к сегментам вычислительного поля
83. Угроза несанкционированного доступа к системе по беспроводным каналам

84. Угроза несанкционированного доступа к системе хранения данных из виртуальной и (или) физической сети
85. Угроза несанкционированного доступа к хранимой в виртуальном пространстве защищаемой информации
86. Угроза несанкционированного изменения аутентификационной информации
87. Угроза несанкционированного использования привилегированных функций BIOS
88. Угроза несанкционированного копирования защищаемой информации
89. Угроза несанкционированного редактирования реестра
90. Угроза несанкционированного создания учётной записи пользователя
91. Угроза несанкционированного удаления защищаемой информации

92. Угроза несанкционированного удалённого внеполосного доступа к аппаратным средствам
93. Угроза несанкционированного управления буфером
94. Угроза несанкционированного управления синхронизацией и состоянием
95. Угроза несанкционированного управления указателями
96. Угроза несогласованности политик безопасности элементов облачной инфраструктуры
97. Угроза несогласованности правил доступа к большим данным
98. Угроза обнаружения открытых портов и идентификации привязанных к нему сетевых служб
99. Угроза обнаружения хостов
100. Угроза обхода некорректно настроенных механизмов аутентификации

101. Угроза общедоступности облачной инфраструктуры
102. Угроза опосредованного управления группой программ через совместно используемые данные
103. Угроза определения типов объектов защиты
104. Угроза определения топологии вычислительной сети
105. Угроза отказа в загрузке входных данных неизвестного формата хранилищем больших данных
106. Угроза отказа в обслуживании системой хранения данных суперкомпьютера
107. Угроза отключения контрольных датчиков
108. Угроза ошибки обновления гипервизора
109. Угроза перебора всех настроек и параметров приложения
110. Угроза перегрузки грид-системы вычислительными заданиями

111. Угроза передачи данных по скрытым каналам
112. Угроза передачи запрещённых команд на оборудование с числовым программным управлением
113. Угроза перезагрузки аппаратных и программно-аппаратных средств вычислительной техники
114. Угроза переполнения целочисленных переменных
115. Угроза перехвата вводимой и выводимой на периферийные устройства информации
116. Угроза перехвата данных, передаваемых по вычислительной сети
117. Угроза перехвата привилегированного потока
118. Угроза перехвата привилегированного процесса
119. Угроза перехвата управления гипервизором
120. Угроза перехвата управления средой виртуализации
121. Угроза повреждения системного реестра
122. Угроза повышения привилегий

123. Угроза подбора пароля BIOS
124. Угроза подделки записей журнала регистрации событий
125. Угроза подключения к беспроводной сети в обход процедуры аутентификации
126. Угроза подмены беспроводного клиента или точки доступа
127. Угроза подмены действия пользователя путём обмана
128. Угроза подмены доверенного пользователя
129. Угроза подмены резервной копии программного обеспечения BIOS
130. Угроза подмены содержимого сетевых ресурсов
131. Угроза подмены субъекта сетевого доступа
132. Угроза получения предварительной информации об объекте защиты

133. Угроза получения сведений о владельце беспроводного устройства
134. Угроза потери доверия к поставщику облачных услуг
135. Угроза потери и утечки данных, обрабатываемых в облаке
136. Угроза потери информации вследствие несогласованности работы узлов хранилища больших данных
137. Угроза потери управления облачными ресурсами
138. Угроза потери управления собственной инфраструктурой при переносе её в облако
139. Угроза преодоления физической защиты
140. Угроза приведения системы в состояние «отказ в обслуживании»
141. Угроза привязки к поставщику облачных услуг

142. Угроза приостановки оказания облачных услуг вследствие технических сбоев
143. Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
144. Угроза программного сброса пароля BIOS
145. Угроза пропуска проверки целостности программного обеспечения
146. Угроза прямого обращения к памяти вычислительного поля суперкомпьютера
147. Угроза распространения несанкционированно повышенных прав на всю грид-систему
148. Угроза сбоя автоматического управления системой разграничения доступа хранилища больших данных
149. Угроза сбоя обработки специальным образом изменённых файлов

150. Угроза сбоя процесса обновления BIOS
151. Угроза сканирования веб-сервисов, разработанных на основе языка описания WSDL
152. Угроза удаления аутентификационной информации
153. Угроза усиления воздействия на вычислительные ресурсы пользователей при помощи сторонних серверов
154. Угроза установки уязвимых версий обновления программного обеспечения BIOS
155. Угроза утраты вычислительных ресурсов
156. Угроза утраты носителей информации
157. Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации
158. Угроза форматирования носителей информации
159. Угроза «форсированного веб-браузинга»

160. Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации
161. Угроза чрезмерного использования вычислительных ресурсов суперкомпьютера в ходе интенсивного обмена межпроцессорными сообщениями
162. Угроза эксплуатации цифровой подписи программного кода
163. Угроза перехвата исключения/сигнала из привилегированного блока функций
164. Угроза распространения состояния «отказ в обслуживании» в облачной инфраструктуре
165. Угроза включения в проект не достоверно испытанных компонентов
166. Угроза внедрения системной избыточности
167. Угроза заражения компьютера при посещении неблагонадёжных сайтов

168. Угроза «кражи» учётной записи доступа к сетевым сервисам
169. Угроза наличия механизмов разработчика
170. Угроза неправомерного шифрования информации
171. Угроза скрытного включения вычислительного устройства в состав бот-сети
172. Угроза распространения «почтовых червей»
173. Угроза «спама» веб-сервера
174. Угроза «фарминга»
175. Угроза «фишинга»
176. Угроза нарушения технологического/производственного процесса из-за временны́х задержек, вносимых средством защиты
177. Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью

178. Угроза несанкционированного использования системных и сетевых утилит
179. Угроза несанкционированной модификации защищаемой информации
180. Угроза отказа подсистемы обеспечения температурного режима
181. Угроза перехвата одноразовых паролей в режиме реального времени
182. Угроза физического устаревания аппаратных компонентов
183. Угроза перехвата управления автоматизированной системой управления технологическими процессами
184. Угроза агрегирования данных, обрабатываемых с помощью мобильного устройства
185. Угроза несанкционированного изменения параметров настройки средств защиты информации

186. Угроза внедрения вредоносного кода через рекламу, сервисы и контент
187. Угроза несанкционированного воздействия на средство защиты информации
188. Угроза подмены программного обеспечения
189. Угроза маскирования действий вредоносного кода
190. Угроза внедрения вредоносного кода за счет посещения зараженных сайтов в сети Интернет
191. Угроза внедрения вредоносного кода в дистрибутив программного обеспечения
192. Угроза использования уязвимых версий программного обеспечения
193. Угроза утечки информации за счет применения вредоносным программным обеспечением алгоритмов шифрования трафика
194. Угроза несанкционированного использования привилегированных функций мобильного устройства

195. Угроза удаленного запуска вредоносного кода в обход механизмов защиты операционной системы
196. Угроза контроля вредоносной программой списка приложений, запущенных на мобильном устройстве
197. Угроза хищения аутентификационной информации из временных файлов cookie
198. Угроза скрытной регистрации вредоносной программой учетных записей администраторов
199. Угроза перехвата управления мобильного устройства при использовании виртуальных голосовых ассистентов
200. Угроза хищения информации с мобильного устройства при использовании виртуальных голосовых ассистентов
201. Угроза утечки пользовательских данных при использовании функций автоматического заполнения аутентификационной информации в браузере
202. Угроза несанкционированной установки приложений на мобильные устройства

203. Угроза утечки информации с неподключенных к сети Интернет компьютеров
204. Угроза несанкционированного изменения вредоносной программой значений параметров программируемых логических контроллеров
205. Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы СЗИ
206. Угроза отказа в работе оборудования из-за изменения геолокационной информации о нем
207. Угроза несанкционированного доступа к параметрам настройки оборудования за счет использования «мастер-кодов» (инженерных паролей)
208. Угроза нецелевого использования вычислительных ресурсов средства вычислительной техники
209. Угроза несанкционированного доступа к защищаемой памяти ядра процессора

210. Угроза нарушения работы информационной системы, вызванного обновлением используемого в ней программного обеспечения
211. Угроза использования непроверенных пользовательских данных при формировании конфигурационного файла, используемого программным обеспечением администрирования информационных систем
212. Угроза перехвата управления информационной системой
213. Угроза обхода многофакторной аутентификации

СЗИ от утечки по ТКУИ

Комплекс для проведения акустических и виброакустических измерений СПРУТ-7А

Система «Барон»

Соната

"Копейка" вибрационный излучатель на стекло

"Молот" вибрационный излучатель на стену

Вибропреобразователь на оконное стекло КВП-7

Вибропреобразователь на стену КВП-2

Акустический преобразователь на дверной проём

Система «Шорох-2М»

"Серп" вибрационный излучатель на раму окна

СЗИ от утечки по ТКУИ

Акустический сейф "Ладья"

Нелинейный локатор

«МОРФЕЙ-МК» предназначен для блокирования возможности организации связи между базовыми станциями (дальность подавления до 50 метров)

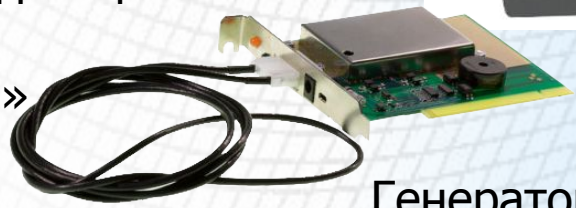
Эндоскоп, зеркала

СЗИ от утечки по ТКУИ

Сетевые генераторы шума СОПЕРНИК

Стационарные шумогенераторы ГНОМ-3М

Селективный обнаружитель цифровых радиопередающих устройств «Скорпион»



Генератор шума ГШ-К-1000

Компьютеризированный металлодетектор «КОРНЕТ»

Селективный обнаружитель оружия в ручной клади «РУБЕЖ»

Портативная рентгенотелевизионная установка «НОРКА»

СЗИ от утечки

Кейс «ТЕНЬ» для транспортировки ноутбуков с возможностью автоматического уничтожения информации при попытке НСД

Защиты от НСД «SecretNet»

Устройство для быстрого уничтожения информации на HDD «СТЕК-Н»

USB-ключи и пр.

КРИПТО ПРО

MAXPATROL

Электронный замок для защиты от НСД «Соболь»

Презентация доступна по ссылке