Алексеев Алексей Александрович,
генеральный директор
ООО «НПП «Анна»

Защита информации от утечки по техническим каналам на базе оборудования НПО «Анна»

Научно-производственное объединение «Анна» основано в 1991 году и, как следует из названия, более 20 лет занимается разработкой и производством различной аппаратуры.

Основные направления деятельности НПО «Анна»:

- защита информации от утечки по техническим каналам;
- гарантированное уничтожение информации, хранящейся на магнитных носителях.

С точки зрения проблемы защиты информации, устройства уничтожения информации могут быть полезны только в случае выхода из строя жестких дисков компьютера, если на них хранится секретная информация или информация ограниченного доступа. Вышедший из строя диск необходимо либо отремонтировать, либо выбросить — в любом из этих случаев возникает угроза утечки информации, поэтому лучше ее гарантированно уничтожить заранее.

А вот аппаратуру защиты информации от утечки по техническим каналам необходимо устанавливать при защите не только секретной информации, но и персональных данных 1 и 2 классов.

Итак, что такое технические каналы? Их всего три основные группы:

1 группа — акустический и виброакустический каналы. Все прекрасно знают, что разговор можно подслушать, и, если подслушивать через приоткрытую дверь, форточку или окно, канал утечки называется акустическим, а если с помощью стакана через стенку или с помощью докторского или электронного стетоскопа — то виброакустическим.

2 группа — электроакустические каналы. Это тоже утечка речи, но за счет преобразования звука в электрический сигнал, например в динамиках системы оповещения, телефонов и т.д.

Сразу замечу, что защита от утечки информации по этим каналам в соответствии с требованиями руководящих документов необходима при защите секретной информации, а для персональных данных нужна только в случаях, когда используется т.н. голосовой ввод информации или ее воспроизведение с помощью аппаратуры звукоусиления. В остальных случаях документы не требуют такой защиты.

А вот **3 группа** каналов утечки (ПЭМИН) требует более серьезного отношения, поскольку защиту персональных данных от утечки за счет ПЭМИН руководящие документы требуют выполнять в полном объеме.

Таким образом нам необходимо блокировать следующие технические каналы утечки информации:

- акустические и виброакустические;
- за счет акустоэлектрических преобразований;
- за счет побочных электромагнитных излучений и наводок.

Как это сделать? С помощью организационно-технических мероприятий, которые включают в себя:

- проведение специсследований;
- оборудование помещений и объектов информатизации аппаратурой защиты информации;
- проверку эффективности принятых мер защиты информации.

Мы как производители предлагаем для решения задач защиты информации следующую аппаратуру:

1. Средства виброакустической и акустической защиты: серия «Соната-АВ» модель 3Б. В настоящее время осуществляется поставка этой модели МВД, планируется установка во всех регионах страны.
2. Защита от утечки за счет акустоэлектрических преобразований. Это новая разработка нашего предприятия. Устройства «Соната-ВК» обеспечивают физический разрыв слаботочных линий. Конструктивно устройство выполнено в трех модификациях:

Модель ВК1 предназначена для защиты абонентских телефонных аппаратов. Особенность модели состоит в том, что при появлении вызывного сигнала в линии устройство умеет оповещать об этом звуковым сигналом.

Модель ВК2 предназначена для защиты речевой информации от утечки через линии системы оповещения и системы охранной сигнализации.

Модель ВК3 — для защиты от утечки по линиям Ethernet.

Особенность устройств «Соната-ВК» — возможность интеграции в систему виброакустической защиты «Соната-АВ» модель 3Б.

3. Защита от утечки за счет ПЭМИН: серия «Соната-Рхх» и клавиатура в защищенном исполнении «Фарватер-КВ1», которая не позволяет совершить перехват вводимой с нее информации по побочным электромагнитным излучениям. В технических решениях, использованных в нашей клавиатуре, реализован запатентованный новый способ защиты информации, который предотвращает даже теоретическую возможность перехвата вводимой информации.

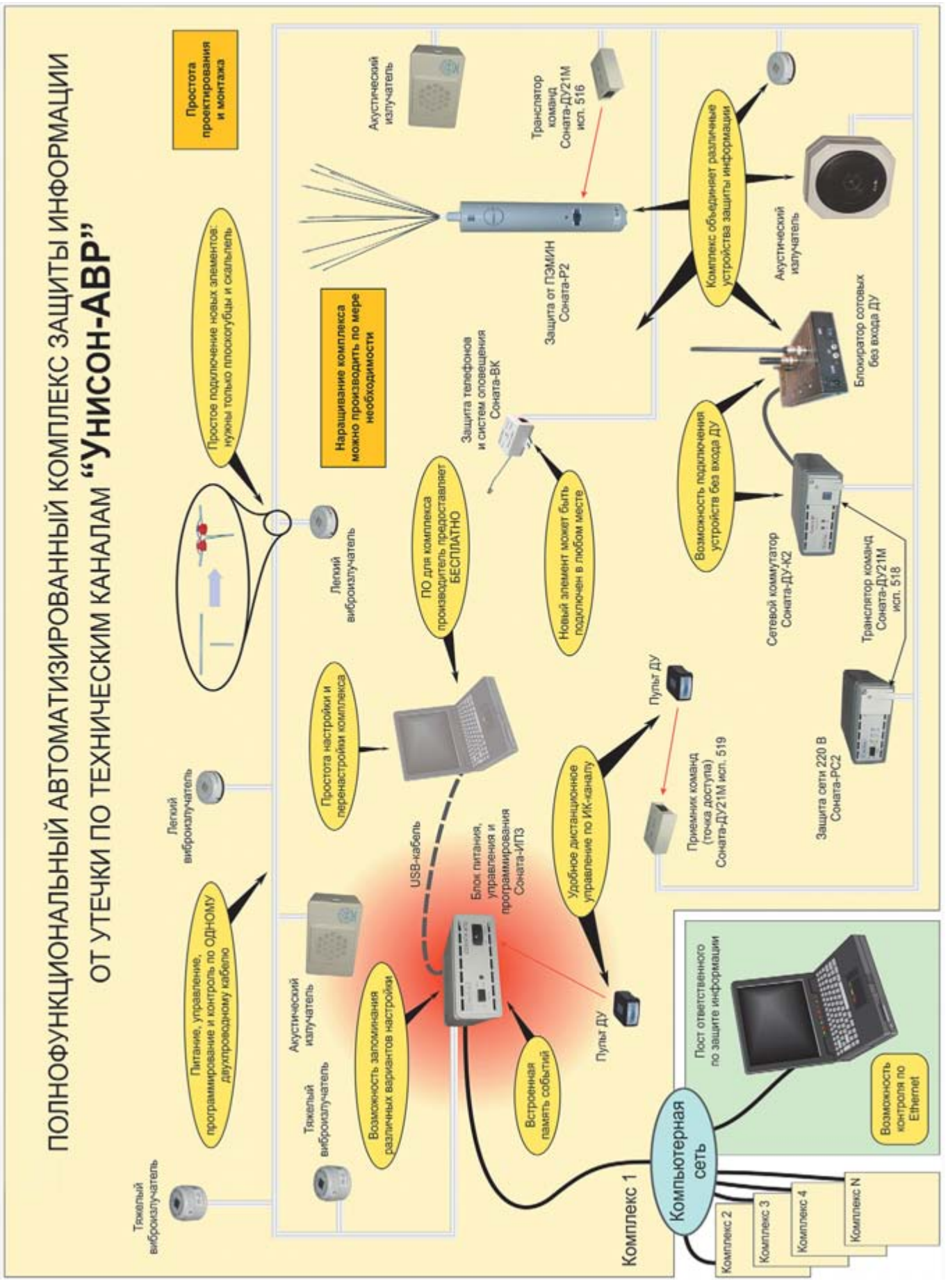
Производство клавиатуры, также как и генераторов, сертифицировано ФСТЭК России для применения на объектах вычислительной техники, в том числе обрабатывающих секретную информацию.

Как эту аппаратуру использовать наиболее эффективно?

Дело в том, что защита информации в современных условиях практически невозможна без комплексного подхода. Прежде всего это обусловлено многообразием объектов защиты, различными условиями эксплуатации как средств обработки, так и средств защиты информации, а также меняющимися во времени требованиями к конкретным объектам и возможностями организаций и предприятий по обеспечению режимных подразделений средствами защиты информации.

Комплексный подход должен позволять решать следующие задачи:

- создание простых и недорогих систем защиты информации с возможностью дальнейшего их расширения не только в количественном, но и в качественном смысле;
- минимизация расходов на проектирование и ин-


ПОЛНОФУНКЦИОНАЛЬНЫЙ АВТОМАТИЗИРОВАННЫЙ КОМПЛЕКС ЗАЩИТЫ ИНФОРМАЦИИ
ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ "УНИСОН-АВР"
Простота проектирования и монтажа
Простое подключение новых элементов: нужны только плоскогубцы и скальпель
Наращивание комплекса можно производить по мере необходимости
Акустический излучатель
Транслятор команд Соната-ДУ21М исп. 516
Защита от ПЭМИН Соната-Р2
Комплекс объединяет различные устройства защиты информации
Акустический излучатель
Блокиратор сотовых без входа ДУ
Защита телефонов и систем оповещения Соната-ВК
Легкий виброизлучатель
ПО для комплекса предоставляет БЕСПЛАТНО
Новый элемент может быть подключен в любом месте
Возможность подключения устройств без входа ДУ
Сетевой коммутатор Соната-ДУ-К2
Транслятор команд Соната-ДУ21М исп. 518
Защита сети 220 В Соната-РС2
Пульт ДУ
Приемник команд (точка доступа) Соната-ДУ21М исп. 519
Легкий виброизлучатель
Простота настройки и перенастройки комплекса
Питание, управление, программирование и контроль по ОДНОМУ двухпроводному кабелю
USB-кабель
Блок питания, управления и программирования Соната-ИП3
Удобное дистанционное управление по ИК-каналу
Пульт ДУ
Акустический излучатель
Тяжелый виброизлучатель
Возможность запоминания различных вариантов настройки
Встроенная память событий
Тяжелый виброизлучатель
Комплекс 1
Компьютерная сеть
Пост ответственного по защите информации
Возможность контроля по Ethernet
Комплекс 2
Комплекс 3
Комплекс 4
Комплекс N

сталляцию систем защиты информации;
- гибкое изменение и/или наращивание функциональных возможностей уже имеющихся систем защиты информации;
- комфортное оперативное управление;
- возможность включения в систему технических средств разных производителей и даже не имеющих входа дистанционного управления (**блокираторы мобильной связи, блокираторы диктофонов** и др.);
- мониторинг режима работы и исправности входящих в состав системы устройств;
- исключение возможности негативного взаимного влияния устройств защиты информации и других технических средств.

Именно с целью решения этих задач и был создан полнофункциональный автоматизированный комплекс технических средств защиты информации от утечки по техническим каналам **«УНИСОН — АВР»**.

Базовым элементом комплекса является устройство «Соната-ИП3» (блок питания, управления и программирования). **Для повышения универсальности комплекса разработан ряд устройств дистанционного управления:**

- «транслятор команд» **«Соната-ДУ21М» исп. 518**, который подключается к двухпроводному кабелю и обеспечивает связь между устройством «Соната-Рх» и блоком «Соната-ИП3» по ИК-каналу.
- «точка доступа» **«Соната-ДУ21М» исп. 519**, который также подключается к двухпроводному кабелю и принимает сигналы от ИК-пульта (включение выключение системы), может располагаться в любом месте защищаемого помещения.
- «транслятор команд» **«Соната-ДУ21М» исп. 516**, подключаемый к двухпроводному кабелю и обеспечивающий связь между устройствами «Соната-РСх», «Соната-ДУ-К2» и блоком «Соната-ИП3» по ИК-каналу.

Существует возможность удаленного контроля состояния системы по сети Ethernet с помощью компьютера. Причем с одного компьютера можно наблюдать за несколькими комплексами одновременно.

Достоинства и возможности комплекса «УНИСОН — АВР» представлены на рисунке на предыдущей странице.

Кроме того, комплекс позволяет осуществлять мониторинг режима работы и исправности входящих в состав системы устройств.

Мы надеемся, что разработанный нашим предприятием комплекс позволит решать задачи защиты информации легче и эффективнее.

В настоящее время наше предприятие имеет большой опыт работы с государственными заказчиками. Мы осуществили десятки поставок оборудования для различных государственных структур, в том числе:

- МВД РФ;
- МинОбороны РФ;
- ФСБ РФ;
- ФСО РФ;
- МинЮст РФ;
- Пенсионный фонд России;
- ФСИН России;
- Центр подготовки космонавтов;
- Предприятия атомной промышленности;
- Администрации многих областей, краёв и республик России;
- и многие другие.

Наша Фирма всегда открыта для сотрудничества. Наши специалисты готовы предоставить любую информацию по выпускаемой предприятием технике, проконсультировать по вопросам защиты государственной и служебной тайны, по защите персональных данных. Даже если мы не сможем оказать какие-либо услуги, консультанты коммерческого отдела порекомендуют наших проверенных партнеров в области защиты информации, которые помогут качественно решить возникшие у Вас проблемы.

Подробности — см. в приложении на CD