Однако практически всем им присущ один существенный недостаток: они детектируют сигнал вторжения лишь после проникновения злоумышленника на территорию объекта. Главным фактором, определяющим эффективность любой охранной системы, является минимизация интервала времени обнаружения факта проникновения.

Волоконные датчики, построенные из диэлектрических элементов, можно применять не только на оградах или стенах, но также и на взрывоопасных объектах или под водой.

При оценке стоимости волоконно-оптических систем по сравнению с системами с использованием медных линий в системах замкнутого телевидения и охраны периметра при прочих равных условиях следует учитывать не только стоимость передатчиков, приемников и кабелей, но и стоимость других составляющих каналов связи (ретрансляторов, источников питания и т.д.).

Расчеты показывают, что в диапазоне длин соединительных линий от 100 м до 1 км стоимость каналов связи с использованием медных кабелей фактически вдвое (1,85-1,95) ниже стоимости каналов с использованием волоконно-оптических линий. При увеличении длин линий до 1,5 км стоимость этих каналов фактически уравнивается, правда, без гарантии сохранения качества сигнала в случае применения медных линий даже в отсутствие внешних помех, в то время как применение оптоволоконной линии обеспечивает качественный сигнал, независимый от внешних воздействий.

Таким образом, периметральные оптоволоконные системы оправданы для закрытия периметра от нескольких до десятков километров. Применение таких систем для периметров небольшой протяженности, к примеру, частных домовладений, неоправданно дорого.

Если раньше к ограничениям применения оптоволоконных систем можно было отнести сложность процедуры сращивания и ремонта кабелей в полевых условиях, для которых требовалось применение микроскопа и дорогостоящего устройства для сварки волокон, то теперь активному внедрению этих технологий в нашей стране способствует наличие на мировом и отечественном рынках широкого спектра ВОК, электронной аппаратуры и инструментов для разделки/монтажа ВОК в полевых условиях, не требующих высокой квалификации монтажников.

При использовании данной охранной системы возникает возможность надежной охраны режимных объектов таких как: пункты управления, аэропорты, ядерные реакторы, склады.

Можно сделать вывод, что использование данного устройства позволит повысить уровень боевой готовности Вооруженных Сил Республики Беларусь которая, напрямую зависит от состояния вооружения и военной техники, а также материально-технического обеспечения.

Список использованных источников:

1. Урядов, В.Н. Электронный учебно-методический комплекс по дисциплине “Волоконно-оптические системы передачи” / В.Н. Урядов - Минск: БГУИР, 2008. - 228 с.

2. Фриман, Р. Волоконно-оптические системы связи / Р. Фриман ; пер. с англ.; под ред. Н. Н. Слепова - М.: Техносфера, 2007. – 512 с.

РАССМОТРЕНИЕ ПОСТРОЕНИЯ МОДЕЛИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Султанбаев А.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Макатерчик А.В.

Защита информации – комплекс мероприятий, направленных на обеспечение важнейших аспектов информационной безопасности. Система защиты информации – совокупность ресурсов персонала структурных подразделений по защите информации, используемых способов и средств информации, а также объектов защиты, организованная и функционирующая по правилам и нормам, установленными нормативно-правовыми актами в области защиты информации.

Комплексная система защиты информации должна отвечать следующим требованиям:

1) Оперативно реагировать на изменение факторов, определяющих методы и средства защиты;

2) Иметь удобную и достаточно надёжную ключевую систему, обеспечивающую безопасность при работе с информацией;

3) Иметь элементы идентификации пользователей;

4) Надёжность контроля передаваемой и хранимой экономической информации;

5) Обеспечения учета и расследования случаев нарушения безопасности;

6) Использование комплекса программно-технических средств и организационных мер по защите комплексной системы.

Существуют две системы оценки текущей ситуации в области информационной безопасности на предприятии:

- «Исследование снизу вверх». Этот метод достаточно прост, требует намного меньших капитальных вложений, но и обладает меньшими возможностями. Служба информационной безопасности, основываясь на данных о всех известных видах атак, пытается применить их на практике с целью проверки, возможна ли такая атака со стороны реального злоумышленника

- «Исследование сверху вниз» представляет собой детальный анализ всей существующей схемы хранения и обработки информации. Первым этапом этого метода является определение, какие информационные объекты и потоки необходимо защищать. Далее следует изучение текущего состояния системы информационной безопасности с целью определения, что из классических методик защиты информации уже реализовано, в каком объеме и на каком уровне. На третьем этапе производится классификация всех информационных объектов на классы в соответствии с ее конфиденциальностью, требованиями к доступности и целостности.

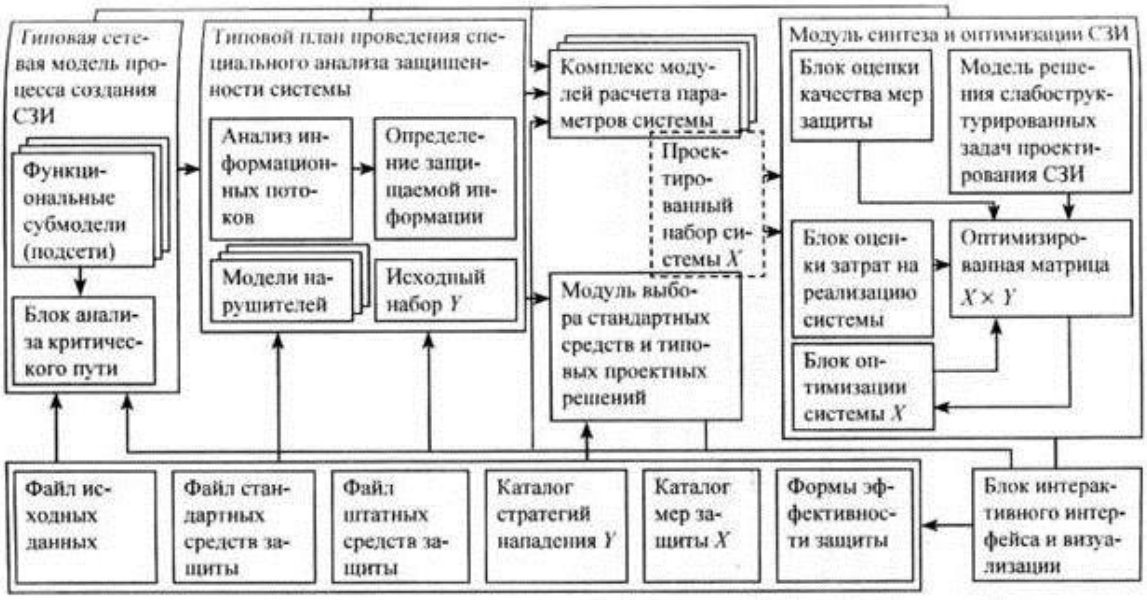

Рис 1. Модель системы проектирования защиты информации

Политика информационной безопасности необходима для обоснования введения защитных мер в компании и должна содержать:

Цели построения системы защиты информации информационной системы;

Перечень защищаемых сведений;

Определение ответственности субъектов информационных отношений за обеспечение защиты информации;

Определение прав и порядка доступа к защищаемой информации;

Порядок работы с электронной почтой и другими системами обмена и передачи сообщений;

Порядок применения средств технической и (или) криптографической защиты информации;

Организационные мероприятия по разграничению доступа к средствам технической защиты и обработки информации;

Порядок действий при возникновении угроз обеспечению целостности и конфиденциальности информационных ресурсов, в том числе чрезвычайных и непредотвратимых обстоятельств, и при ликвидации их последствий;

Инструкции для субъектов информационных отношений, регламентирующие порядок доступа к ресурсам информационной системы, установления подлинности субъектов, аудита безопасности, резервирования и уничтожения информации, контроля целостности защищаемых сведений, защиты от вредоносного программного обеспечения и вторжений.

Современные информационные системы защиты информации позволяют решить ряд стратегически важных задач, при выборе следует учитывать самый главный фактор – стратегию развития компании, которая и обслуживает конечный выбор системы. Качество реализации политики необходимо периодически анализировать и определять его эффективность.

Литература:
1. Организация комплексной системы защиты информации, И.В. Гришина;
2. «Нормативная база и стандарты в области информационной безопасности» (2017), Ю. Родичев;
3. «Основы информационной безопасности» (2016), С. Нестеров;
4. «Информационная безопасность: защита и нападение» 2-е изд. (2017), А. Бирюков.

ИПОЛЬЗОВАНИЕ КОМПЬЮТЕРНОЙ ПРОГРАММЫ ПРИ ИЗУЧЕНИИ ТРОПОСФЕРНЫХ СТАНЦИЙ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Трубкин В.О.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Романовский С.В.

Сокращение военного бюджета и проблемы обеспечения и поддержания боеготовности войск становится как никогда острыми. Одним из решений данной проблемы является удешевление боевой подготовки за счет использования компьютерных обучающих программ по обучению работе на тропосферных станциях. Использование данных программных продуктов является удобным и перспективным, поскольку позволяет проводить обучение работе на аппаратуре без использования самой аппаратуры, эффективным с экономической точки зрения, кроме того возможна самостоятельная подготовка, что позволяет эффективно использовать свободное время обучаемых.

В мирное время и в угрожаемый период основной вид деятельности Вооруженных сил в целом и их отдельных формирований – подготовка к ведению боевых действий. В условиях резкого сокращения военного бюджета проблема обеспечения и поддержания боеготовности войск становится как никогда острой. Одним из решений данной проблемы является удешевление боевой подготовки за счет использования компьютерных обучающих программ. К этому выводу приводят также и следующие факторы:

1) Уровень компьютерной грамотности обучаемых в сочетании с методическим опытом преподавательского состава позволяют разрабатывать обучающие программы современного уровня.

2) Подразделения связи Вооруженных сил все больше насыщаются современной компьютерной техникой, позволяющей использовать в процессе обучения современные информационные технологии.

3) С экономической точки зрения компьютерные обучающие технологии рентабельны. Затраты на создание обучающей системы определяются главным образом временем и средствами, потраченными на составление автоматизированных учебных программ, объединенных в автоматизированные учебные курсы. Использование их позволит существенно сократить стоимость эксплуатации вооружения и техники в учебных целях.

Разработанные обучающие программы целесообразно использовать и в войсках для совершенствования профессиональной подготовки радиомехаников. В обучающих программах моделируется не содержание предмета, а деятельность обучаемого. Именно это обстоятельство делает обучающие программы универсальным средством обучения. В одной и той же обучающей программе возможно изучение различных тем. В тоже время, компьютерное обучение не должен рассматриваться в качестве замены реальной