

Парламентское собрание Союза Беларуси и России
Постоянный Комитет Союзного государства
Оперативно-аналитический центр
при Президенте Республики Беларусь
Государственное предприятие «НИИ ТЗИ»
Полоцкий государственный университет



КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)
К63

К63

Комплексная защита информации : материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей государственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных направлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Бен+2)

В настоящее время одной из проблем повышения квалификации является низкий уровень профессиональной подготовки руководящих работников структурных подразделений. Встречаются случаи, когда подразделениями повышения квалификации руководит человек не имеющего не только подготовки в области информационной безопасности, но и вообще компьютерного образования, к тому же и нет опыта преподавательской работы.

Одним из путей совершенствования процесса повышения квалификации – проведение аттестации лиц, занимающихся подготовкой (переподготовкой) кадров. Они должны иметь обязательную специализированную подготовку и иметь опыт преподавательской работы.

Штатные преподаватели системы переподготовки кадров и повышения квалификации в полной мере не могут дать навыков и опыта в силу тех же причин, что и преподаватели базового образования.

Приоритетное направление – подготовка кадров высшей научной квалификации, которые бы проводили исследования в области технической защиты информации.

ЕДИНСТВО НАУЧНОГО ЗНАНИЯ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ

В.К. ЖЕЛЕЗНЯК, Д.С. РЯБЕНКО

Полоцкий государственный университет

«Всякое исследование основано на научной интуиции, экспериментальном искусстве, верном ощущении возможности техники и, что весьма важно, – на хорошем знании теории; только при овладении внутренними взаимосвязями явлений представляется возможным обозреть всю совокупность различных проблем и найти путь решения той или иной возникшей проблемы».

Е. Скучик [1]

Решение комплексной защиты информации является приоритетной научной и практической задачей. Теоретические и экспериментальные исследования основаны на логических методах моделирования (математического и физического), абстрагирования и обобщения. Научные знания устанавливают определенность научных результатов в оценке защищенности объектов информатизации, информационных автоматизированных систем, входящих в объект информатизации, проверенных при экспериментальных исследованиях на практике. Высокоточные малоинерционные автоматизированные системы измерения, методы обработки и анализа семантической информации (речевая, видео, передача данных) с высокой степенью определенности, воспроизводимости, обоснованности при влияющих факторах среды распространения, маскирующими сигналами, целостным и системным представлением является айсбергом поучения новых знаний, характеризующиеся истинностью и полезностью.

Методология познания определяется формированием основанных на опыте и интуиции абстрактных представлений, проверяемых практикой. Основным является выделение наиболее существенных свойств и признаков явления или объекта, выделение новых наиболее существенных для теоретического и экспериментального исследования формированием модели. Практическая полезность выводов формирует критерий адекватности цели исследований.

Значительные успехи информатики, включающие ее научное направление – техническая защита информации, теорию помехоустойчивости и помехозащищенности определяют дальнейшее теоретическое исследование проблемных задач комплексной защиты информации.

Прорывное развитие электроники, средств вычислительной техники обусловили решающую роль в научно-техническом прогрессе, развитии науки и научного эксперимента. Это позволило обрабатывать большие массивы для значительного круга информационных проблемных задач, из которых поиск – обнаружение сигналов при одновременном воздействии маскирующих и искусственных помех при высокой информационной производительности оценки вероятностно-временных характеристик, маскирующих помех, формирующих из полезных сигналов, мультипликативных маскирующих помех, адаптивным к сигналам.

Свойство системы измерительной автоматизированной определяется свойствами и параметрами зондирующих измерительных сигналов, определяемых алгоритмом их формирования. Основными требованиями к таким информационным системам являются повышенная избирательность при их конечной длительности. Эти требования противоречивы. Сигналы с повышенной селективностью приема позволяют снижать уровни взаимных помех, повышают точность и разрешающую способность. В СИА используется финитный гармонический сигнал на временных интервалах T_i , $i=\overline{1,n}$ [2] либо финитный гармонический измерительный сигнал на частотном интервале $(-\Omega, \Omega)$, сложный финитный измерительный сигнал с большой базой на частотном интервале $(-\Omega, \Omega)$, обнаружение и обработка которых выполняется автокорреляционной и взаимокорреляционной обработкой, преобразованием Фурье и преобразованием Гильберта, синхронным накоплением.

Вероятность правильного решения о защищенности канала утечки информации реализуют селективным обнаружением – обработкой слабых финитных измерительных сигналов, выделяемых из маскирующих и искусственных помех на объектах информатизации, автоматизированных измерительных системах, разрешение классификационных числовых значений параметров для принятия решения о защищенности каналов утечки информации, оценку параметров аддитивных, мультипликативных источников измерительного сигнала и их маскирующих шумов, формирующие их физические информационные поля рассеивания, влияющих на вероятность принятия правильного решения: статистическая обработка измерительного сигнала оптимальным приемником либо сложного измерительного сигнала с большой базой в автоматизированном режиме, либо измерительный сигнал в виде двоичных посылок для оценки защищенности речевых сигналов, преобразованных в цифровую форму, для принятия правильного решения о степени защищенности объектов информатизации.

Превосходством в развитии защищенности речевой информации является ее оценка по единому критерию – разборчивость речи для ее аналоговой и преобразованной в цифровую форму, оцениваемой по вероятности ошибочного приема бита. Установление взаимосвязи численного значения, коэффициента разборчивости речи и численного значения вероятности ошибочного приема бита устанавливает нормативный показатель оценки защищенности речевой информации по критерию разборчивости речи. Предложен измерительный сигнал для оценки защищенности преобразованного в цифровую форму речевого сигнала, универсального для обработки в технических средствах передачи информации и каналах утечки информации.

Пригодность единого (универсального) критерия разборчивости речи обусловлена возможностью сравнения каналов утечки информации, образованных на различных физических принципах по рассеиванию информационных полей по их информа-

тивности. Этот фактор весьма важен при формировании рациональных требований при конструировании и оценке степени защищенности объектов информатизации, технических средств передачи информации, вспомогательных технических средств и систем, и их помехозащищенности.

Целесообразно расширена область применения по назначению системы измерительной автоматизированной для оценки каналов утечки информации аналоговой и преобразованной в цифровую форму речевой информации с дополнительным программным обеспечением.

Активная защита одновременно аналоговой и преобразованную в цифровую форму речевых сигналов является актуальной задачей [3].

Использование речевого сигнала для формирования маскирующего улучшает степень маскирования, снижает методическую и инструментальную неопределенность (погрешность) при одновременной возможности чувствительность, определяемой по минимальному значению отношения сигнал/шум при использовании сложного измерительного сигнала с большой базой, с более высокой точностью оценку защищенности при обработке более тонкой структуры такого измерительного сигнала, так как она играет существенную роль в помехоустойчивости, точности оценки временных, частотных, корреляционных и автокорреляционных характеристик.

Важными факторами, влияющими на параметры измерительного сигнала, являются характеристики среды распространения [4]. Степень защищенности речевого сигнала определяется степенью рассогласования ее параметров.

Пригодность единого (универсального) критерия разборчивость обусловлена возможностью сравнения каналов утечки информации. Образованные на различных физических принципах по их информативности. Этот фактор весьма важен при формировании рациональных требований при конструировании и исследовании технических средств передачи информации и вспомогательных технических средств и систем для оценки защищенности, и помехозащищенности [5].

Активная защита одновременно аналоговой и преобразованной в цифровую форму является очередной научной задачей. Использование исходного речеподобного сигнала снижает демаскирующие признаки такого сигнала, повышает защищенность маскируемых сигналов.

Снижение методической и инструментальной неопределенности (погрешности) при одновременной возможности повысить чувствительность в оценке отношения мощности сигнала к мощности шума возможно при принципиально новом формировании и использовании измерительного сигнала для оценки защищенности речевой информации; точности оценки защищенности обработкой тонкой структуры сигналов снижением нормативного порога отношения сигнал/шум, выбором формы сигнала, играющего существенную роль в помехоустойчивости, точности оценкой временных, частотных, корреляционных, автокорреляционных характеристик и их корректировок. Важными факторами, влияющими на параметры измерительного сигнала, являются характеристики среды распространения. Степень защищенности речевого сигнала определяется уровнем рассогласования его характеристик и параметров среды распространения. К таким характеристикам относятся ослабления сигнала при неравномерности АЧХ, реверберационных помехах замкнутого объема технических средств передачи информации, резонансными явлениями того же объема. Эти факторы устанавливают порог чувствительности обнаружения измерительного сигнала, ухудшая его параметры.

Актуально достоверное в режиме реального времени получение большого объема информации из излучений и наводок с ограниченной энергетикой для правильного и оперативного принятия решений. Это обусловлено случайными искажениями сигналов при прохождении через турбулентную среду с высоким уровнем помех [6].

Задача оптимального помехоустойчивого приема заключается в восстановлении полезной информации на основании оптимальных алгоритмов (оптимальных приемников), оптимальных систем. Оптимальная фильтрация реализует прием измерительного сигнала в шумах высокого уровня [6].

Список литературы

1. Скучик Е. Основы акустики. М.: Изд-во иностранной лит-ры, 1958. 618 с.
2. Железняк, В.К. Защита информации от утечки по техническим каналам: учебное пособие. СПб.: ГУАП, 2006. 188 с.
3. Рябенко Д.С., Железняк В.К. Оценка защищенности речевых сигналов в цифровой форме // Вестн. Воен. акад. 2014. № 2(43). С. 136–144.
4. Железняк В.К., Дворников С.В. Основы теории модулированных колебаний : учеб. пособие. СПб.: ГУАП, 2006. 160 с.
5. Железняк В.К., Рябенко Д.С., Лавров С.В. Системный подход: защита информации, помехозащищенность, помехоустойчивость // Вестн. Полоц. гос. ун-та. Сер. С. Фундаментальные науки. 2016. № 4. С. 2–7.
6. Тихонов В.И. Статистический анализ и синтез радиотехнических устройств и систем: уч. пособие для вузов. М.: Радио и связь, 1991. 608 с.

ПРОБЛЕМА ГАРМОНИЗАЦИИ ОБРАЗОВАТЕЛЬНЫХ И ПРОФЕССИОНАЛЬНЫХ СТАНДАРТОВ В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В.П. ЛОСЬ, Е.Д. ТЫШУК

ФГБОУ ВО «Московский технологический университет»

В докладе анализируется нынешняя ситуация с образовательными (ФГОС) [1-7] и профессиональными стандартами (ПС) [8-12], а именно:

I. Образовательные стандарты

1. 10.03.01 Информационная безопасность (уровень бакалавриата).
2. 10.04.01 Информационная безопасность (уровень магистратуры).
3. 10.05.01 Компьютерная безопасность (уровень специалитет).
4. 10.05.02 Информационная безопасность телекоммуникационных систем (уровень специалитет).
5. 10.05.03 Информационная безопасность автоматизированных систем (уровень специалитет).
6. 10.05.04 Информационно-аналитические системы безопасности (уровень специалитет).
7. 10.05.05 Безопасность информационных технологий в правоохранительной сфере (уровень специалитет).

II. Профессиональные

1. Специалист по безопасности компьютерных систем и сетей.
2. Специалист по защите информации в телекоммуникационных системах и сетях.
3. Специалист по защите информации в автоматизированных системах.
4. Специалист по автоматизации информационно-аналитической деятельности в сфере безопасности.
5. Специалист по технической защите информации.