Аналогичные данные получены при тепловлажностной обработке образцов, а также при введении добавки волластонита. При этом добавка диопсида более эффективна вследствие большей его твердости.

Введение таких добавок оказывает существенное влияние также на поровую структуру цементного камня. При этом, по данным ртутной порометрии, значительно уменьшается средний диаметр пор, возрастает их характеристическая длина и уменьшается извилистость. По-видимому, вводимые добавки являются подложками, на которых происходит образование и рост игольчатых кристаллогидратов.

Во всех случаях четко проявляется оптимальное количество добавки. Если ее дисперсность близка к дисперсности цемента, то оптимальное количество добавки составляет 7–8 %. При увеличении дисперсности добавки ее оптимальная концентрация уменьшается. При введении оптимального количества диопсида прочность бетона значительно возрастает.

Введение дисперсных минеральных добавок (диопсида, волластонита) оказывает влияние на формирование структуры цементного камня. Об ее упрочнении свидетельствует смещение эндоэффектов на термограмме цементного камня в область более высоких температур.

Таким образом, минеральные микронаполнители, вводимые в состав композиционных цементных материалов, способствуют упрочнению структуры таких материалов и продуктов гидратационного твердения портландцемента. Это приводит к изменению поровой структуры композиционных материалов и повышению их важнейших свойств: механической прочности, морозостойкости. Критериями, определяющими активность микронаполнителя, являются: высокая химическая стойкость в воде, в агрессивных средах; высокая механическая прочность. Эффективность действия веществ, составляющих микронаполнитель, определяется близостью их удельной энтальпии образования, удельной энтропии к аналогичным характеристикам вяжущих веществ. К числу эффективных микронаполнителей композиционных материалов относятся диопсид, волластонит. При введении в состав композиционных цементных материалов минеральных наполнителей наблюдаются четко выраженные максимальные значения прочности, соответствующие оптимальному количеству добавок. При увеличении дисперсности микронаполнителя оптимальное количество его уменьшается.

**Список литературы**

1. Горчаков Г.И. Строительные материалы / Г.И. Горчаков, Ю.М. Боженов. – М.: Стройиздат, 1986. – 688 с.

2. Добавки в бетон. Справочное пособие: Пер. с англ. / Под ред. В.С. Рамачадрана. – М.: Стройиздат, 1988. – 575 с.

3. Хозин В.Г. Эффективность применения золы-уноса Гусиоозерской ГРЭС в составе цементов низкой водопотребности / В.Г. Хозин, О.В. Хохряков, А.В. Битцер, Л.А. Урханова // Строительные материалы, 2011, № 7. – С. 76–77.

4. Лесовик В.В. Повышение эффективности вяжущих за счет использования нова // Строительные материалы, 2011, № 12. – С. 60–62.

5. Uchikawa Hiroshi. Similarities and discrepancies of hardened cement paste, mortar and concrete from the standpoints of composition and structure / Uchirawa Hiroshi // J. Res, Onoda Cem. Co. – 1988 – 40, № 119. – С. 87-121.

## МОДЕЛЬ ОПТИМАЛЬНОЙ ЗАЩИТЫ НЕПРЕРЫВНОЙ ИНФОРМАЦИИ

Котенко В.В., Румянцев К.Е., Поляков А.И., Ежов А.И.

*Южный федеральный университет, Таганрог, e-mail: virtsecurity@mail.ru*

Виртуализация процесса защиты непрерывной информации заключается в установлении условий виртуализации, оптимизирующих этот процесс, и определении решений, соответствующих данным условиям. Отличительной особенностью процесса защиты непрерывной информации является высокая избыточность непрерывных сообщений, которую, как правило, не удается в полной мере устранить в формируемых криптограммах.

В процессе синтеза модели оптимальной защиты непрерывной информации с позиций виртуализации относительно условий теоретической недешифруемости устанавливались основные условия теоретической недешифруемости и определялись теоретические основы защиты непрерывной информации (скремблирования) для установленных условий. Основу определения условий обеспечения абсолютной недешифруемости при защите непрерывной информации составляло определение теорем скремблирования.

Теорема 1. Теорема цифрового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений S, дискретным ансамблем криптограмм E и дискретным ансамблем ключей K. Пусть дискретный ансамбль $\hat{U}$ является ансамблем виртуальных сообщений, полученным в результате виртуализации непрерывного ансамбля S. Тогда, если среднее количество взаимной информации равно

$$I[\hat{U}K;E]=0, \qquad (1)$$

то всегда существует цифровое скремблирование $\hat{O}_{CD}$, обеспечивающее теоретическую недешифруемость.

Теорема 2. Теорема виртуализации цифрового скремблирования. Пусть скремблирование определяется непрерывным ансамблем сообщений S, дискретным ансамблем криптограмм E и дискретным ансамблем ключей K. Пусть дискретный ансамбль $\hat{U}$ является ансамблем виртуальных сообщений, полученным в результате виртуализации непрерывного ансамбля S. Пусть

элементы выборочного пространства ансамбля $\hat{U}$ формируются в результате цифрового компандирования сообщений выборочного пространства ансамбля S. Тогда, если при цифровом скремблировании, заданном дискретными ансамблями ключей K и криптограмм E, средняя взаимная информация $I[\hat{U}K;E]=0$, то всегда и только всегда будет справедливо равенство $I[SK;E]=0$.

Теоремы 1–2 определяют обобщенную модель виртуализации защиты непрерывной информации с позиций условий теоретической недешифруемости. Особенностью полученной модели является предусматриваемая виртуализация алгоритма формирования ключей, осуществляемая путем обеспечения адаптивно регулируемой неопределенности состояний источника ключа. Ансамбль $\hat{U}$ является результатом виртуализации ансамбля S непрерывного источника информации. Таким образом, эффективность обобщенной модели процесса защиты непрерывной информации, с позиций условий теоретической недешифруемости, зависит от установленных условий виртуализации непрерывного источника информации.

Основу виртуализации непрерывных источников при цифровом скремблировании составляет цифровое компандирование, предусматривающее компрессию при скремблировании и экспандирование при дескремблировании. С этих позиций к основным условиям виртуализации непрерывных источников при цифровом скремблировании относятся: 1) минимизация информационных потерь; 2) обеспечение минимальной избыточности.

Полученная модель составляет фундаментальную основу стратегии оптимизации процесса защиты непрерывной информации, открывающей принципиально новую область возможностей разработки методов скремблирования, обеспечивающих абсолютную недешифруемость.

**Список литературы**

1. Котенко В.В. Теоретические основы виртуализации представления объектов, явлений и процессов // Информационное противодействие угрозам терроризма: Науч.-практ. журн., 2011, № 17. С. 32-48.

2. Котенко В.В. Теоретические основы виртуализации информационных потоков // Информационное противодействие угрозам терроризма: Науч.–практ. журн., 2011, № 17. С. 69-80.

3. Котенко В.В. Виртуализация защиты дискретной информации относительно условий непродуктивности анализа ключа. // Информационное противодействие угрозам терроризма.: Науч.–практ. журн., 2011, № 17. С. 96-104.

4. Котенко В.В. Новый подход к оценке информационного образа объекта исследования с позиций теории виртуального познания // Информационное противодействие угрозам терроризма: Науч.-практ.журн., 2005, № 4. С. 34-41.

## МОДЕЛЬ ЗАЩИТЫ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ НА ОСНОВЕ ИНФОРМАЦИОННОЙ ВИРТУАЛИЗАЦИИ ВИДЕОИДЕНТИФИКАТОРОВ

Котенко В.В., Румянцев К.Е., Котенко С.В., Поляков А.И., Аверьянов П.С., Иванков И.М.

*Южный федеральный университет, Таганрог, e-mail: virtsecurity@mail.ru*

Внушительные достижения в области защиты объектов информатизации на основе анализа видеоидентификаторов, наблюдаемые в последнее время, к сожалению не обеспечивают в полной мере решение целого ряда проблем надежного обнаружения несанкционированного доступа. Основу этих проблем составляют ограничения областей эффективности различного вида обнаружителей несанкционированного доступа (НСД). В следствии этого складывается ситуация, когда решение задачи повышения эффективности защиты объектов информатизации может быть достигнуто только путем многоуровневого комплексного применения значительного числа обнаружителей НСД различных видов. То есть повышение надежности обнаружения НСД достигается путем увеличения числа различных видов обнаружителей НСД и увеличения количества уровней их комплексного применения. В итоге это приводит к значительным финансовым затратам на фоне снижения функциональной устойчивости системы защиты объектов информатизации в целом. Возможность решения этой проблемы открывает подход, основанный на информационной виртуализации идентификаторов [1]. Реализация на основе этого подхода модели защиты объектов информатизации на основе информационной виртуализации видеоидентификаторов включает следующие этапы.

Первый этап состоит в инъективном отображении ансамбля измеренных значений параметра видеоидентификатора в ансамбль соответствующих значений количества информации.

Второй этап состоит в инъективном отображении ансамбля количества информации, соответствующего измеренным значениям параметра, в ансамбль оценок количества информации. Реализация этапа состоит в решении задачи определения оценки исходного процесса по наблюдению, обеспечивающей минимально допустимую величину информационных потерь:

$$J_k^*(i) = e^{-\alpha T} J_k^*{}_{(i-1)} + K_i^{(k)} \left[ J_{\Psi k}(i) - e^{-\alpha T} J_k^*{}_{(i-1)} - h_0 \right] + h_0,$$

$$J_k^*(t) = J_k^*(i) e^{-\alpha(t-t_i)},$$