

(рис. 5). Наличие в САПР SilidWoks встроенного САМ модуля обеспечивает возможность разработки g-кода для изготовления разработанных узлов при помощи станков с числовым программным

обеспечением. Таким образом, разработка современных электронных приборов при помощи САПР позволяет сократить сроки не только проектирования изделий, но и подготовки производства.

УДК 621.383.92

## ПОТЕРИ ИНФОРМАЦИИ ПРИ ЕЕ ИЗМЕРЕНИИ В АСИНХРОННОМ КВАНТОВО-КРИПТОГРАФИЧЕСКОМ КАНАЛЕ СВЯЗИ

Тимофеев А.М., Колядич А.С., Корбут М.В.

*Белорусский государственный университет информатики и радиоэлектроники  
Минск, Республика Беларусь*

**Введение.** При разработке современных систем связи одной из наиболее важных задач является обеспечение конфиденциальности передаваемой информации [1]. Решение этой задачи возможно посредством систем квантово-криптографической связи, перспективность использования которых обусловлена возможностью достижения абсолютной конфиденциальности передаваемых данных [1]. При реализации таких систем связи особенно важно, чтобы приемо-передающее оборудование легитимных пользователей имело наименьшее количество ошибок (потерь информации) [2]. В противном случае решить задачи защиты передаваемой информации зачастую не представляется возможным. Отметим, что в системах квантово-криптографической связи информация передается предельно слабыми оптическими импульсами со средним числом фотонов не более десяти, что требует использования высокочувствительных приемных модулей – счетчиков фотонов [1, 2]. Известные методики [2, 3] позволяют оценить потери информации. Однако методики, описанные в [3], не применимы для систем квантово-криптографической связи, т.к. не учитывают такой важный параметр приемного модуля, как мертвое время [1, 2]. В течение этого времени счетчик фотонов не чувствителен к падающему на него оптическому излучению, что приводит к ошибкам при измерении оптического излучения на выходе канала связи. Методика [2] учитывает наличие мертвого времени счетчика фотонов только в случае регистрации одноименных двоичных символов. Однако данные, передаваемые по каналам связи, как правило, представляют собой последовательности, содержащие как символы «0», так и символы «1». В этой связи **целью данной работы** являлось определить влияние мертвого времени счетчика фотонов на потери передаваемой информации в квантово-криптографическом канале связи, в котором данные представляют собой последовательности двоичных символов «0» и «1». **Объект исследования** – асинхронный квантово-криптографический канал связи [2], который не требует наличия линий связи для передачи и приема синхронимпульсов. **Предмет**

**исследования** – установление влияния продлевающегося мертвого времени типа на энтропию потерь. Данным типом мертвого времени характеризуются счетчики фотонов на базе лавинных фотоприемников, включенные по схеме пассивного гашения лавины [1].

**Выражение для оценки потерь информации.** Потери информации определяются энтропией, рассчитать которую для рассматриваемого канала связи можно, воспользовавшись математической моделью [2]:

$$H(B/A) = -P_s(0)[P(0/0) \log_2 P(0/0) + P(1/0) \log_2 P(1/0) + P(-/0) \times \log_2 P(-/0)] - P_s(1)[P(0/1) \log_2 P(0/1) + (1/1) \log_2 P(1/1) + P(-/1) \log_2 P(-/1)], \quad (1)$$

где  $P_s(0)$  и  $P_s(1)$  – вероятности появления символов «0» и «1» соответственно на входе канала связи;  $P(0/0)$  и  $P(0/1)$  – вероятности регистрации на выходе канала связи символа «0» при наличии на его входе символов «0» и «1» соответственно;  $P(1/0)$  и  $P(1/1)$  – вероятности регистрации на выходе канала связи символа «1» при наличии на его входе символов «0» и «1» соответственно;  $P(-/0)$  и  $P(-/1)$  – вероятности отсутствия символов на выходе канала связи, в то время как на его входе был сформирован символ «0» и символ «1» соответственно.

Предположим, что в канале связи организована высокоскоростная передача данных, тогда  $P_s(0) = P_s(1) = 0,5$  [2]. Переходные вероятности, входящие в (1), равны [4]:

$$P(0/0) = \sum_{N=N_1}^{N_2} \left\{ \frac{[(n_t + n_{s0})(\Delta t - \tau_d)]^N}{N!} \times \exp[-(n_t + n_{s0})(\Delta t - \tau_d)] \right\}, \quad (2)$$

$$P(0/1) = \sum_{N=N_1}^{N_2} \left\{ \frac{[(n_t + n_{s1})(\Delta t - \tau_d)]^N}{N!} \times \exp[-(n_t + n_{s1})(\Delta t - \tau_d)] \right\}, \quad (3)$$

$$P(1/0) = 1 - P(0/0) - P(-/0), \quad (4)$$

$$P(1/1) = 1 - P(0/1) - P(-/1), \quad (5)$$

$$P(-/0) = \sum_{N=0}^{N_1-1} \left\{ \frac{[(n_t + n_{s0})(\Delta t - \tau_d)]^N}{N!} \times \exp[-(n_t + n_{s0})(\Delta t - \tau_d)] \right\}, \quad (6)$$

$$P(-/1) = \sum_{N=0}^{N_1-1} \left\{ \frac{[(n_t + n_{s1})(\Delta t - \tau_d)]^N}{N!} \times \exp[-(n_t + n_{s1})(\Delta t - \tau_d)] \right\}, \quad (7)$$

где  $n_t$  – средняя скорость счета темновых импульсов на выходе счетчика фотонов;  $n_{s0}$  и  $n_{s1}$  – средние скорости счета сигнальных импульсов на выходе счетчика фотонов при передаче символов «0» и «1» соответственно;  $\tau_d$  – средняя длительность мертвого времени продлевающегося типа;  $\Delta t$  – среднее время однофотонной передачи данных;  $N_1$  и  $N_2$  – нижний и верхний пороговые уровни регистрации соответственно.

Таким образом, рассчитать энтропию потерь информации для рассматриваемого канала связи можно путем подстановки в (1) соответствующих выражений (2) ÷ (7) при заданных пороговых уровнях регистрации  $N_1$  и  $N_2$ , скоростях счета импульсов  $n_t$ ,  $n_{s0}$  и  $n_{s1}$  и длительностях  $\Delta t$  и  $\tau_d$ .

#### Результаты исследования и их обсуждение.

На рис. 1 представлены зависимости энтропии потерь от средней длительности мертвого времени продлевающегося типа для различных средних скоростей счета сигнальных импульсов при передаче символов «0»  $n_{s0}$  и символов «1»  $n_{s1}$ .

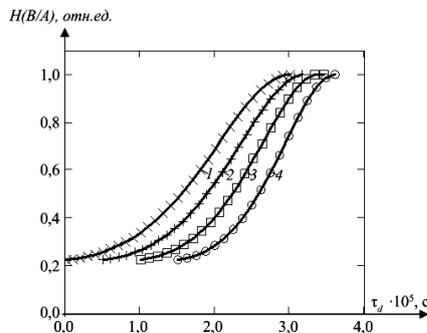


Рисунок 1 – Зависимость энтропии потерь от средней длительности мертвого времени:

$N_1 = 1, N_2 = 7, n_t = 10^3 \text{ с}^{-1}, \Delta t = 50 \text{ мкс}$ ; средние скорости счета сигнальных импульсов:  
 1 –  $\times n_{s0} = 66,6 \times 10^3 \text{ с}^{-1}$ ,  
 $n_{s1} = 35,0 \times 10^4 \text{ с}^{-1}$ ; 2 –  $+ n_{s0} = 74,1 \times 10^3 \text{ с}^{-1}$ ,  
 $n_{s1} = 38,9 \times 10^4 \text{ с}^{-1}$ ; 3 –  $\circ n_{s0} = 83,5 \times 10^3 \text{ с}^{-1}$ ,  
 $n_{s1} = 43,7 \times 10^4 \text{ с}^{-1}$ ; 4 –  $\square n_{s0} = 95,6 \times 10^3 \text{ с}^{-1}$ ,  
 $n_{s1} = 50,0 \times 10^4 \text{ с}^{-1}$

Расчет проводился для одинаковых значений  $N_1 = 1, N_2 = 7, n_t = 10^3 \text{ с}^{-1}$  и  $\Delta t = 50 \text{ мкс}$  по методикам [5, 6]. Отметим, что при других значениях  $N_1$  и  $N_2$ , и отношениях  $n_t/n_{s0}$  и  $n_t/n_{s1}$  проявление эффекта мертвого времени продлевающегося типа

для рассматриваемого канала связи аналогично представленному на рис. 1. Диапазон значений  $\tau_d$  определялся по методикам [2, 7] с учетом того, что вероятность ошибочной регистрации символов («0» и «1») должна быть менее 0,5. Все графики нормированы на максимальное значение  $H(B/A)$ .

Из представленных результатов видно, что с увеличением средней длительности мертвого времени продлевающегося типа энтропия потерь увеличивается во всех исследуемых диапазонах значений  $\tau_d$ . Причем при прочих равных параметрах с ростом скоростей счета  $n_{s0}$  и  $n_{s1}$  энтропия потерь уменьшается. Так, например, при  $\tau_d = 18 \text{ мкс}$  энтропия потерь равна 0,54 отн. ед. для  $n_{s0} = 66,6 \times 10^3 \text{ с}^{-1}$  и  $n_{s1} = 35,0 \times 10^4 \text{ с}^{-1}$ ; 0,42 отн. ед. для  $n_{s0} = 74,1 \times 10^3 \text{ с}^{-1}$  и  $n_{s1} = 38,9 \times 10^4 \text{ с}^{-1}$ ; 0,31 отн. ед. для  $n_{s0} = 83,5 \times 10^3 \text{ с}^{-1}$  и  $n_{s1} = 43,7 \times 10^4 \text{ с}^{-1}$ ; 0,23 отн. ед. для  $n_{s0} = 95,6 \times 10^3 \text{ с}^{-1}$  и  $n_{s1} = 50,0 \times 10^4 \text{ с}^{-1}$ . Такое влияние  $\tau_d$  и скоростей счета  $n_{s0}$  и  $n_{s1}$  на  $H(B/A)$  объясняется следующим. При увеличении  $\tau_d$  вероятности ошибочной регистрации символов «0» и «1» растут, увеличивая  $H(B/A)$  [2, 4]. Вместе с тем, при прочих равных параметрах с ростом скоростей счета  $n_{s0}$  и  $n_{s1}$  в исследуемых диапазонах  $\tau_d$  вероятности ошибочной регистрации символов «0» и «1» уменьшаются, что снижает  $H(B/A)$ . Указанные особенности изменения вероятностей ошибочной регистрации символов «0» и «1» с ростом  $n_{s0}, n_{s1}$  и  $\tau_d$  обусловлены смещением статистических распределений смеси числа темновых и сигнальных импульсов при передаче символов «0» и «1», что достаточно подробно исследовано в работах [2, 4].

**Заключение.** Таким образом, в данной работе получено выражение для оценки энтропии потерь информации при ее измерении в асинхронном квантово-криптографическом канале связи. Выполненные исследования показали, что с ростом средней длительности мертвого времени продлевающегося типа энтропия потерь увеличивается. Причем при прочих равных параметрах с ростом средних скоростей счета сигнальных импульсов при передаче символов «0» и символов «1» энтропия потерь уменьшается.

#### Литература

1. Килин, С.Я. Квантовая криптография: идеи и практика / С.Я. Килин; под ред. С.Я. Килин, Д.Б. Хорошко, А.П. Низовцев. – Мн.: Бел. наука, 2007. – 391 с.
2. Тимофеев, А.М. Оценка влияния продлевающегося мертвого времени счетчика фотонов на вероятность ошибочной регистрации данных квантово-криптографических каналов связи / А.М. Тимофеев // Вестник связи. – 2018. – № 1(147). – С. 56–62.
3. Дмитриев, С.А. Волоконно-оптическая техника: современное состояние и перспективы / С.А. Дмитриев, Н.Н. Слепов. – 2-е изд., перераб. и доп. – М.: ООО «Волоконно-оптическая техника», 2005. – 576 с.

4. Тимофеев, А.М. Энтропия потерь однофотонного асинхронного волоконно-оптического канала связи с приемником на основе счетчика фотонов с продлевающимся мертвым временем / А.М. Тимофеев // Актуальные проблемы науки XXI века, 2018. – вып. 7. – С. 5–10.

5. Тимофеев, А.М. Методика повышения достоверности принятых данных счетчика фотонов на основе анализа скорости счета импульсов при передаче двоичных символов «0» / А.М. Тимофеев // Приборы и методы измерений. – 2019. – т. 10. – № 1. – С. 80–89.

6. Тимофеев, А.М. Достоверность принятой информации при ее регистрации в однофотонном канале связи при помощи счетчика фотонов / А.М. Тимофеев // Информатика. – 2019. – Т. 16. – № 2. – С. 90–98.

7. Тимофеев, А.М. Влияние времени однофотонной передачи информации на вероятность ошибочной регистрации данных асинхронных квантово-криптографических каналов связи / А.М. Тимофеев // Вестник ТГТУ. – 2019. – т. 25. – № 1. – С. 36–46.

УДК 625.7.08

## ГЕОРАДАРНОАКУСТИЧЕСКИЙ МЕТОД ОПРЕДЕЛЕНИЯ ВЛАЖНОСТИ ПОДПОВЕРХНОСТНЫХ ГРУНТОВ АВТОМОБИЛЬНЫХ ДОРОГ

Кучинский П.В., Романов А.Ф., Ходасевич А.И., Чернобай И.А.

Научно-исследовательское учреждение «Институт прикладных физических проблем имени А.Н. Севченко» Белорусского государственного университета  
Минск, Республика Беларусь

Одной из основных и важных составляющих обеспечения безопасности жизнедеятельности является надежность и качество автомобильных дорог. В целом надежность и качество дорог в сильной мере зависят от прочности и устойчивости подповерхностных грунтов, минимум влагосодержания которых является определяющим фактором прочности. На сегодняшний день не существует быстрых и доступных методов глубинного контроля влажности грунтов. Настоящая работа посвящена разработке нового георадарноакустического метода определения влажности подповерхностных грунтов автомобильных дорог.

Реализация метода основывается на комбинированном применении георадарного и акустического способов измерений, причем применяемая комбинация сочетает в себе положительные достоинства георадарного и акустического способов, что позволяет получить новый качественный результат по определению влажности подповерхностных слоев автомобильной дороги. Функционирование предлагаемого георадарноакустического способа заключается в одновременном излучении в подповерхностные грунты акустических импульсов и излучении коротких зондирующих радиоимпульсных сигналов с последующим приемом и детектированием сигналов, отраженных внутренними границами подповерхностных грунтов. Метод позволяет измерять толщину каждого слоя и времена распространения акустических импульсов в каждом подповерхностном слое. На основании измерений вычисляется скорость распространения акустической волны в каждом слое грунта. По результатам полученных вычислений определяется влагосодержание каждого слоя и оценивается его устойчивость и прочность.

Измерения скорости распространения акустических колебаний реализуется по временам распространения  $T_{P1}, T_{P2}, \dots, T_{Pn}$  акустических

волн, определяемым по моментам выделения фазоамплитудных флуктуаций отраженных радиолокационных сигналов от каждой границы между слоями, вибрирующей в соответствии со сдвигом фаз, вызванным распространением акустических волн от излучателя через контролируемые подповерхностные слои грунта. На основании полученных результатов для времен распространения вычисляются скорости распространения акустических волн в первом, втором, третьем ... и  $n$  – ом слоях:

$$v_1 = \frac{l_1}{T_{P1}}; v_n = \frac{l_n}{T_{Pn} - T_{Pn-1}}, \quad (1)$$

где  $l_1; l_2; \dots; l_n$  – толщины каждого слоя, измеряемые посредством отраженных радиолокационных сигналов по следующим формулам:

$$l_1 = \frac{c_0 t_1}{2\sqrt{\xi_1}}; \dots; l_n = \frac{c_0(t_n - t_{n-1})}{2\sqrt{\xi_n}}, \quad (2)$$

где:  $c_0$  – скорость распространения электромагнитной волны в вакууме;  $t_1, t_2, \dots, t_n$  – отметки времени, измеряемые радиолокационным сигналом от момента времени излучения радиолокационного импульса до момента его приема при отражении от каждой границы между слоями;  $\xi_1, \xi_2, \dots, \xi_n$  – величины диэлектрической проницаемости слоев.

Алгоритмом, описывающим функциональную зависимость диэлектрической проницаемости от влажности, является известная по литературным источникам достаточно сложная эмпирическая зависимость диэлектрической проницаемости грунтов от влажности [1,2]:

$$\xi = 3,03 + 9,3W_{об} + 146W_{об}^2 - 76,6W_{об}^3, \quad (3)$$