УДК 004.056.5

БАРАННИК В.В., д.т.н., профессор,
ВЛАСОВ А.В., научный сотрудник научного центра Воздушных Сил,
СИДЧЕНКО С.А., к.т.н., старший научный сотрудник (Харьковский университет Воздушных Сил им. Ивана Кожедуба),
БЕКИРОВ А.Э., соискатель (Харьковский национальный университет радиоэлектроники)

Обоснование значимых угроз безопасности видеоинформационного ресурса систем видеоконференцсвязи профильных систем управления

В статье рассмотрены особенности формирования уязвимостей и угроз безопасности видеоинформационные ресурса в процессе функционирования видеоконференцсвязи для профильных систем управления. Для анализа обеспечения данного информационного ресурса предлагается применять характеристики безопасности модели CIA (конфиденциальность, целостность, доступность). Для оценки и формирования подходов обеспечения информационной безопасности видеоинформационного ресурса видеоконференцсвязи требуется выполнить анализ возможных нарушений видеоинформации с обязательной идентификацией источников угроз безопасности, факторов, способствующих их проявлению и уязвимостей. Рассмотрены уязвимости безопасности, которые формируются при функционировании видеоконференцсвязи и обусловливают угрозы безопасности видеоданных, а именно угрозы доступности и целостности. Для определения актуальных уязвимостей и угроз безопасности видеоинформационные ресурса проведена оценка характеристик видеоинформационные ресурса видеоконференцсвязи. На основании данной оценки выделены значимые (актуальные) угрозы нарушения доступности и целостности видеоинформационные ресурса в процессе функционирования видеоконференцсвязи.

Ключевые слова: *видеоконференцсвязь, видеоинформационный ресурс, уязвимость, угроза безопасности, модель угроз, пространственное разрешение, видеокадр, время доступа.*

Вступление

В профильных системах управления специального назначения (Вооруженные Силы, МВД и т.д.) одной из составляющих современного процесса организации управления и обеспечения объективного контроля является применение видеоконференцсвязи (ВКС) [1, 2]. При этом, как показано в работах [3, 4], видеоинформационный (ВИ) ресурс ВКС в данных системах управления приобретает значение государственного информационного ресурса. В связи, с чем обеспечение безопасности ВИ ресурса ВКС решается в составе единого комплекса мероприятий по обеспечению информационной безопасности. Здесь необходимо учитывать специфику организации видеоконференцсвязи и условия обеспечения безопасности видеоданных в системах управления специального назначения. В этой области недостаточно проработаны и исследованы вопросы оценки уязвимостей и угроз безопасности видеоинформационного ресурса ВКС. Поэтому повышение безопасности ВИ ресурса при организации видеоконференцсвязи в профильных системах управления специального назначения является ***актуальной научно – прикладной задачей.***

В процессе решения данной задачи необходимо:

- оценить множество факторов негативного воздействия на информационную безопасность видеоинформации;
- выявить возможные уязвимости и угрозы безопасности;
- оценить воздействие факторов, приводящих к нарушению безопасности видеоинформации непосредственно при реализации видеоконференцсвязи;
- определить значимые факторы и угрозы, которые влияют на безопасность ВИ ресурса.

В тоже время, на данный момент, в недостаточной степени проведена оценка безопасности ВИ ресурса ВКС. В связи с этим требуется разработать модель угроз безопасности данного информационного ресурса и выполнить анализ значимых (актуальных) угроз. Вопросы разработки модели угроз безопасности рассмотрены в работе [5], в которой представлена обобщенная модель угроз безопасности ВИ ресурса ВКС.

Данная модель угроз безопасности позволяет учесть целевое назначение видеоинформации, влияние объектов и субъектов доступа на ВИ ресурс, источники возникновения угроз. В тоже время особенностью обеспечения безопасности ВИ ресурса видеоконференцсвязи является то, что в зависимости от условий и режимов функционирования ВКС варьируются уязвимости безопасности ВИ ресурса. Вследствие чего происходят изменение не только самих угроз безопасности видеоданных видеоконференцсвязи, но и их значимости (актуальности).

Поэтому актуальным является обоснование значимых уязвимостей и угроз безопасности видеоинформационного ресурса. Отсюда, ***целью исследований*** статьи является определение значимых (актуальных) угроз безопасности видеоинформационного ресурса видеоконференцсвязи в профильных системах государственного управления.

Основная часть

В соответствие с моделью угроз безопасности ВИ ресурса ВКС [5], все угрозы безопасности классифицированы на три основные группы в зависимости от источника возникновения: угрозы, обусловленные действиями субъекта доступа (*антропогенные* угрозы); угрозы, обусловленные техническими средствами (*техногенные* угрозы); угрозы, обусловленные стихийными источниками (*стихийные* угрозы) (рис. 1). Данные угрозы сформированы априорно и в первую очередь для статики процесса организации видеоконференцсвязи. При этом возникновение дестабилизирующих факторов и оценка их влияния на формирование уязвимостей, угроз безопасности ВИ ресурса непосредственно в динамике ВКС (обработка и передача видеоданных) проработана не в полной мере. В связи, с чем выполним оценку значимости (актуальности) уязвимостей и порождаемых ними угроз безопасности видеоинформации при организации ВКС в системе управления Вооруженных Сил (системе управления авиацией и противоздушной обороной).

На рис. 1 представлена классификация угроз безопасности ВИ ресурсу ВКС [5].

Уязвимости безопасности видеоинформации и как следствие угрозы информационной безопасности, возникают вследствие:

- умышленного нарушения безопасности;
- субъективных дестабилизирующих факторов;
- дестабилизирующих факторов, проявляющихся при функционировании видеоконференцсвязи.

К угрозам умышленного нарушения безопасности ВИ ресурса ВКС (рис. 1) отнесем: кражи (технических средств, носителей информации, видеоинформации, средств доступа), уничтожение (технических средств, комплексов ВКС и их ПО, носителей информации, серверов хранилищ ВИ, средств передачи и обработки видеоинформации, паролей, ключей, помещений и персонала). Данные угрозы безопасности рассматриваются как преднамеренные действия нарушителей безопасности по проникновению и внедрению в систему управления (ее составные элементы), и блокируются за счет выполнения организационно-штатных мероприятий и инструктажа персонала.

К угрозам безопасности видеоинформации, обусловленные субъективными дестабилизирующими факторами (рис. 1) отнесем: перехват видеоинформации (от технических средств, от ПО комплексов ВКС, от ПО серверов хранилищ ВИ и др.), модификацию (видеоинформации при передаче и обработке, при хранении на серверах), модификацию (ПО комплексов ВКС и серверов хранилищ ВИ, паролей, ключей, правил доступа), ошибки (ПО комплексов ВКС и серверов хранилищ ВИ, прикладного ПО, передачи, кодирования/ декодирования ВИ). Данные типы угроз блокируются за счет внедрения гостированных технологий защиты информации (технической защиты, криптографической защиты и др.).

Рассмотренные 2 подкласса угроз информационной безопасности ВИ ресурсу ВКС учитываются на этапе проектирования (разработки) комплексной системы обеспечения безопасности информации в профильных системах управления. При этом существуют угрозы нарушения безопасности видеоинформационного ресурса видеоконференцсвязи (рис. 1), которые возникают в процессе функционирования ВКС вследствие дестабилизирующих факторов, а именно – нарушения работы системы ВКС и нарушения условий функционирования. Данный сегмент угроз безопасности ВИ ресурса ВКС недостаточно изучен и исследован.

В тоже время анализ применения видеоконференцсвязи в профильных системах управления [1] показывает, что в целом информационный ресурс ВКС очень чувствителен к потерям пакетов, временным задержкам, а также к ошибкам, возникающим в процессе обработки и передачи видеоинформации. Существующие уязвимости при организации видеоконференцсвязи обуславливают предпосылки к возникновению угроз безопасности ВИ ресурса ВКС, в первую очередь категорий безопасности - доступности и целостности [2, 5].

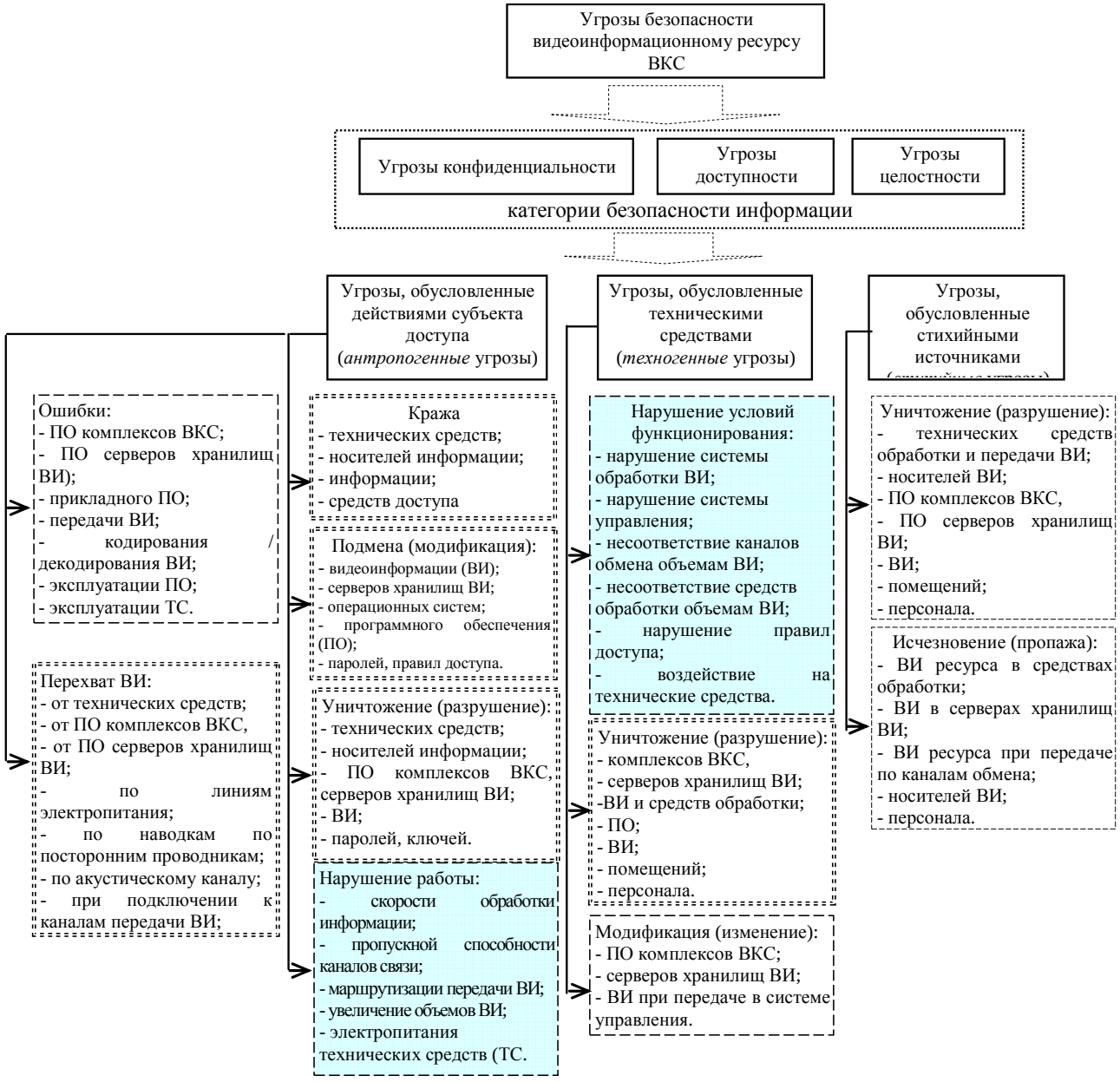

Рис. 1. Угрозы безопасности ВИ ресурсу ВКС в профильной системе управления

Угроза доступности ВИ ресурса возникает в результате действий, которыми блокируется или нарушается принятая политика доступа к информации. Реализация угрозы доступности приводит к блокированию видеоинформации или к ее задержкам, возможно достаточно длительным для цикла управления, при которых утрачивается целевая значимость (ценность) ВИ ресурса ВКС.

Угроза нарушения целостности видеоинформационного ресурса это любое изменение (нарушение, повреждение, искажение) видеоинформации в процессе функционирования ВКС в системе управления на этапах ее обработки, передачи и хранения.

Для определения значимых уязвимостей и актуальных угроз доступности и целостности ВИ ресурсу в процессе функционирования ВКС выполним оценку характеристик видеоинформационного ресурса. Данная оценка необходима для определения соответствия характеристик ВИ ресурса (объема видеоданных, средней скорости видеопотока, времени передачи несжатого видео-потока, битовой скорости

сжатого видеопотока и др.) современным требованиям обработки и доставки видеоинформации в профильных системах управления.

Оценка средней скорости потока несжатой видеоинформации в зависимости от требуемого качества

В общем случае структура видеопотока в комплексах ВКС в профильной системе управления зависит от:

- пространственного разрешения $N \cdot M$ кадра, определяемого как произведение разрешения по горизонтали (количество столбцов, N) и разрешения по вертикали (количество строк, M);
- разрешения d по яркости или глубины пикселя (количество бит на один элемент изображения);
- частота f_t кадров.

Разрешение видеокадров определяет объем видео-потока V_ℓ (бит)

$$V_\ell = M \cdot N \cdot d \,. \qquad (1)$$

Профильные системы управления являются системами управления реального времени с тактом обновления информации $t = 1$ сек. Соответственно на приемной стороне за время $t = 1$ сек необходимо получить видео-поток с исходным объемом, равным V_ℓ (бит).

Таким образом, реальный (требуемый) объем видео-потока V_ℓ, формируемый за такт обновления t, определяет среднюю скорость потока несжатой видеоинформации (бит/с):

$$V_t = f_t \cdot V_\ell \,. \qquad (2)$$

На основании значений требуемых разрешений видеокадров, характеристик телекоммуникационных технологий при организации ВКС в профильных системах управления [1] выполнена оценка объемов ВИ ресурса ВКС в зависимости от требований субъекта доступа (требуемого пространственного разрешения видеоизображений и частоты кадров). Результаты оценки значений средней скорости потока несжатой видеоинформации V_t в зависимости от требуемого качества видеоданных (пространственного разрешения и частоты кадров) в профильной системе управления, приведены в таблице 1.

Таблица 1

Оценка значений средней скорости потока несжатой видеоинформации V_t при ВКС в зависимости от требований субъекта доступа (пространственного разрешения и частоты кадров)

Уровни качества изображений	Формат CIF	Нормальный (SD)	Повышенный (ED)	Высокий (HD)	Продвинутый (Full HD)	Advantage HD
Количество строк	320 – 352	640 – 720	720	1280	1280 – 1920	1920 – 2048
Разрешение по вертикали, пикселей	240 – 288	480 – 576	480 – 576	720	720 – 1080	1080
Частота кадров/сек	12 – 15; 24 – 30	24 – 30	50	50	24 – 30; 50	48; 60
Средняя скорость потока несжатой видеоинформации (Мбит/сек)	33 – 66	252	500	1105	1500; 2500	2548; 3180

Из полученных результатов (табл. 1) можно сделать следующие выводы:

а) значения средней скорости V_t несжатого видеопотока за 1 сек в зависимости от требований субъекта доступа к качеству видеоинформации (существующих стандартов изображений для ВКС) находится в пределах от 33 Мбит/с до 3180 Мбит/с;

б) для наиболее востребованного стандарта качества повышенной четкости ED с прогрессивной разверткой и форматом изображения 720×576×50 при использовании комплексов ВКС на стратегическом и оперативном уровнях управления, для решения некоторых задач на тактическом уровне средняя скорость доступа несжатого видеопотока за 1 сек достигает значения 500 Мбит/с;

в) наименьшая скорость несжатого видео-потока обеспечивается для кадров формата CIF, используемых в комплексах ВКС на базе мобильной радиосвязи с размером кадров 352×288;

г) наибольшие требования к скорости доступа несжатого видео-потока предъявляются для форматов HD и Full HD (пространственное разрешение на уровне 1280×720 и 1920×1080), именно для частоты кадров - 30 кадров/с.

скрость несжатого видеопотока будет достигать значений $V_t = 1{,}5$ Гбит/с, для частоты 60 кадров/с - $V_t = 2{,}5$ Гбит/с.

Таким образом, для функционирования ВКС в профильных системах управления с выполнением требований по доступности и целостности ВИ ресурса необходимо обеспечить:

- соответствие характеристик каналов обмена видеоинформацией по пропускной способности, требуемым значениям скорости потока видеоинформации;
- уменьшение объемов видеоданных за счет технологий компрессии с обеспечением их целостности.

Оценка времени передачи несжатого видео-потока в зависимости от пространственного разрешения

Выполним оценку времени $t_{\text{п}}$ передачи несжатого видео-потока (в объеме одного видеокадра) в зависимости от его пространственного разрешения. Из формул (1) и (2) видно, что доступ к ресурсу в объеме одного видеокадра должен осуществляться за время:

$$t_{\text{п1}} = 1/f_t. \qquad (3)$$

Следовательно, представляется возможным оценить требуемые значения по времени доступа одного видеокадра для граничных частот обновления видеоинформации в комплексах ВКС.

В соответствие с выражением (3) время доступа без задержек для одного видеокадра $t_{\text{п1}}$ не должно превышать:

- для частоты $f_t = 15$ кадров/сек. соответственно $t_{\text{п1}} \le$ 0,06 сек.;
- для частоты $f_t = 50$ кадров/сек. соответственно $t_{\text{п1}} \le$ 0,02 сек.

В общем же случае время доступа к видеоданным зависит от: объема видеопотока V_ℓ (требований к качеству видеоданных); средней скорости несжатого видеопотока V_t; пропускной способности S_c каналов обмена видеоинформации при организации ВКС [1, 6]. Выполним оценку реализуемых значений времени доступа одного видеокадра для комплексов ВКС в системе управления ВС.

Оценка реализуемых значений времени доступа одного видеокадра $t_{\text{п1}}$ выполнена в зависимости от средней скорости несжатого видеопотока V_t, характеристик каналов обмена видеоинформацией S_c и используемых в комплексах ВКС разрешений видеокадров - CIF, ED, HD, FullHD. Результаты оценка времени доступа одного видеокадра $t_{\text{п1}}$ представлены на рис. 2.

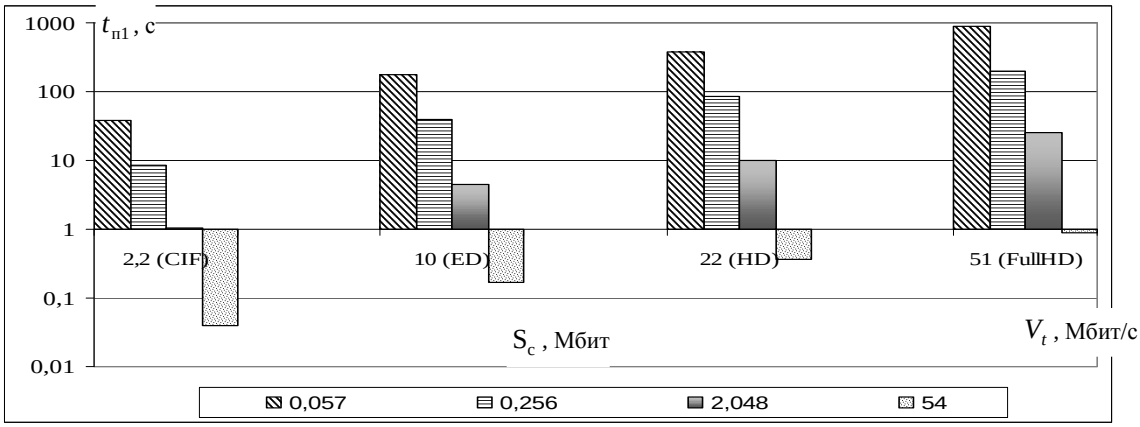

Рис. 2. Оценка времени передачи $t_{\text{п1}}$ одного кадра в зависимости от пропускной способности S_c и средней скорости видеопотока V_t

Анализ результатов оценки времени доступа одного видеокадра $t_{\text{п1}}$ (рис. 2) позволяет констатировать, что время доступа при организации ВКС в соответствие с (3) обеспечивается только для видеокадров с низким пространственным разрешением (CIF, ED). Время доступа видеокадров несжатого видео-потока с высоким пространственным разрешением (HD, FullHD) достигает сотен секунд и как следствие доступ к ВИ ресурсу будет осуществлен с задержками.

Таким образом, в процессе функционирования ВКС даже с использованием высокоскоростных каналов ($S_c \ge 2$ Мбит) время доступа одного видеокадра $t_{\text{п1}}$ (для несжатого видеопотока) превышает требуемое значение времени доступа одного видеокадра в несколько десятков раз (для систем управления реального времени и разрешений видеокадров HD, FullHD). Данный дисбаланс при организации ВКС обусловленный несоответствием характеристик

каналов обмена (пропускной способности S_c) в профильных системах управления требуемым значениям по скорости передачи V_t несжатых видеопотоков создает угрозу доступности и целостности ВИ ресурсу ВКС.

В настоящее время наименее затратным и основным подходом к решению данного временного дисбаланса, является уменьшение объемов видеоинформации с использованием технологий сжатия видеоизображений. Выполним оценку значений скорости видеопотока при использовании технологии компрессии.

Оценка битовой скорости сжатого видеопотока в зависимости от качества реконструируемых видеокадров

В настоящее время при организации ВКС для компрессии видеоизображений используются JPEG ориентированные технологии сжатия. При организации ВКС в системе управления ВС одной из основных задач является обеспечение целостности ВИ ресурса, особенно при использовании технологий сжатия. Поэтому оценку битовой скорости сжатого видеопотока будем проводить с контролем целостности ВИ ресурса (в зависимости от качества реконструируемых видеокадров).

Основным показателем оценки целостности ВИ ресурса является показатель пикового отношения сигнала/шум (ПОСШ) - PSNR, который определяет величину расхождения исходного F(i,j) и восстановленного G(i,j) видеоизображений при использовании технологий компрессии [6].

Под пиковым отношением сигнала/шум PSNR будем понимать величину

$$\mathrm{PSNR} = 10\log_{10}\left(\frac{\mathrm{MAX}_\mathrm{I}^2}{\mathrm{MSE}}\right) = 20\log_{10}\left(\frac{\mathrm{MAX}_\mathrm{I}}{\sqrt{\mathrm{MSE}}}\right), \quad (4)$$

где MAX_I - это максимальное значение, принимаемое пикселем (i,j) видеоизображения;

MSE - среднеквадратичное отклонение, которое для двух сравниваемых видеоизображений F(i,j) и G(i,j) одинакового размера m×n определяется для всех пикселей с координатами (i,j)

$$\mathrm{MSE} = \frac{1}{\mathrm{m\,n}} \sum_{\mathrm{i}=0}^{\mathrm{m}-1} \sum_{\mathrm{j}=0}^{\mathrm{n}-1} \left|\mathrm{F(i,j)} - \mathrm{G(i,j)}\right|^2. \quad (5)$$

Оценку значений битовой скорости сжатого видеопотока выполним по формуле

$$V_1 = t_{n1}\, f_t\, S_c \quad , \quad (6)$$

где $t_{\text{п}1}$ - значение времени доступа одного видеокадра в видеопотоке в зависимости от пространственного разрешения видеоизображения;

f_t - значение кадровой частоты видеопотока;

S_c - значение пропускной способности каналов обмена информацией при ВКС.

Для условий предыдущих оценок реализуемых значений скорости несжатого видеопотока (табл.1) и времени передачи одного видеокадра (рис.2) выполнен анализ зависимости битовой скорости для JPEG ориентированных технологий сжатия с оценкой сохранения целостности видеоизображений ПОСШ (рис.3).

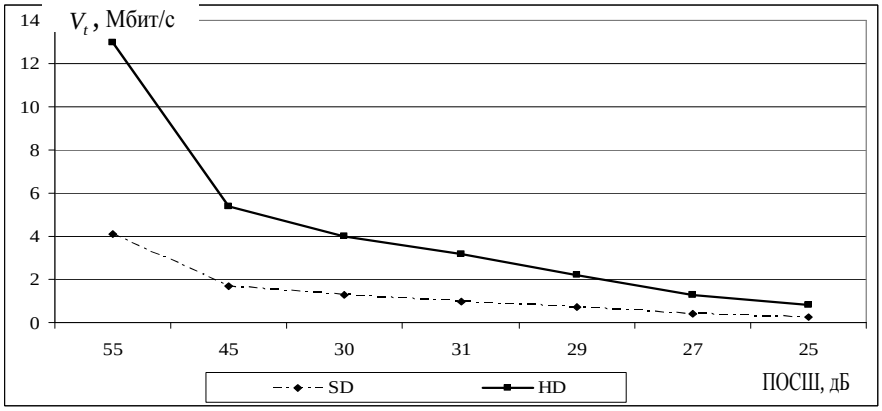

Рис. 3. Графики зависимости значений битовой скорости сжатого видеопотока от ПОСШ для разных пространственных разрешений видеокадров

Оценка проводилась для видеокадров форматов комплексов ВКС - SD и HD качества. На рис. 3

представлен результат анализа зависимости битовой скорости для JPEG ориентированных технологий сжатия от пикового отношения сигнал / шум (ПОСШ).

На выходе кодера образовывается сжатый видео-поток с битовой скоростью V_1 с требуемым временем доступа равным $t_{\text{пд}} \le 0{,}06$ сек. для $f_t = 15$ кадров/сек. и $t_{\text{пд}} \le 0{,}02$ сек для $f_t = 50$ кадров/сек. соответственно.

Анализ зависимости битовой скорости видеопотока от ПОСШ для разных пространственных разрешений видеоизображений (рис. 3) свидетельствует о том, что:

- наиболее высокие степени сжатия достигаются для методов с потерей качества, т.е. для более низких значений ПОСШ. С другой стороны психофизиологические особенности лица принимающих решений допускают наличие ограниченных потерь качества изображений. Нижний предел искажений соответствует уровню ПОСШ равного 30 дБ;

- за счет использования систем сжатия видеоданных обеспечивается передача изображений нормального SD качества и изображений формата CIF по высокоскоростным каналам связи ($S_c \ge 10$ Мбит/с) на небольшие расстояния. Однако такая возможность достигается только при наличии потерь качества реконструируемых изображений на уровне пикового отношения сигнал/шум равного 30дБ. В случае необходимости обеспечить ПОСШ на уровне 50 дБ битовую скорость необходимо дополнительно снизить в 2 раза;

- для изображений формата HD с высоким пространственным разрешением кадра значение битовой скорости сжатого видео-потока с ПОСШ на уровне 30 дБ необходимо уменьшить минимум в 2 раза, чтобы обеспечить его передачу в реальном времени по телекоммуникационной сети с пропускной способностью $S_c \ge 100$ Мбит/с.

Анализ результатов полученных оценок позволяют сформировать следующие выводы:

- в зависимости от реализованных скоростей передачи данных по существующим каналам обмена и требуемых объемов видеоинформации (разрешений видеоизображений) время полной доставки видеоданных может варьироваться в пределах от 0,3 сек. до 8 часов;

- существующие технологии при организации ВКС в профильных системах управления обеспечивают доступность ВИ ресурса ВКС в реальном времени для несжатых видео-потоков только с низким пространственным разрешением (соответствует качеству формата SD);

- для обеспечения доступности и целостности видеоинформационного ресурса при реализации управления в режиме реального времени минимальное время передачи видеоданных должно быть не ниже нескольких секунд (для видеоизображений с количеством элементов более 2 Mpix);

- существующие технологии обработки и передачи видеоинформации при организации ВКС в профильных системах управления не обеспечивают гарантированную доступность и целостность ВИ ресурса при управлении в реальном времени для высоких значений пространственных разрешений видеокадров (HD, Full HD, Advantage HD);

- временные задержки при передаче ВИ ресурса для высоких значений пространственных разрешений видеокадров превышают допустимые временные задержки в десятки раз.

Таким образом, анализ функционирования ВКС в профильных системах управления [1, 2, 5] показывает, что в процессе функционирования видео-конференцсвязи формируются уязвимости и, как следствие, угрозы безопасности ВИ ресурсу ВКС, вследствие противоречий между требованиями субъектов доступа к характеристикам (качеству) видеоинформации и существующими технологиями обработки в комплексах ВКС и передачи видеоинформации в системе управления.

Выводы

1. Выполненный анализ оценок характеристик ВИ ресурса и анализ их соответствия технологиям обработки и доставки видеоинформации в профильных системах управления показывает, что требования субъектов доступа по динамическому изменению (в сторону увеличению) качества видеоданных при осуществлении ВКС будет приводить к существенному возрастанию объемов видеоданных и как следствие к возникновению дестабилизирующих факторов, приводящих у нарушению безопасности ВИ ресурса ВКС, а именно категорий доступности и целостности.

2. В системе управления ВС (системе управления авиацией и противоздушной обороной) не блокируются комплексной системой защиты информации угрозы безопасности видеоинформации, обусловленные уязвимостями, которые возникают вследствие :

- неоднородности существующих структур инфокоммуникационных систем на разных уровнях системы управления (тактический, оперативный, стратегический);

- недостатков технологий обработки и передачи видеоинформации;

- ограниченных характеристик производи-тельности технологий передачи и обработки видеоинформации в комплексах ВКС;

- несоответствия существующих характеристик каналов обмена по пропускной способности возрастающим объемам видеоданных.

- динамически изменяющихся в процессе управления требований к качеству видеоинформации (разрешающая способность, частота кадров и др.).

- неравномерности интенсивности обмена ВИ на разных уровнях системы управления (тактический, оперативный, стратегический);

- несоответствия (противоречия) между требованиям к минимизации времени передачи ВИ по каналам обмена с требованиями по увеличению качества ВИ.

3. Значимыми (актуальными) угрозами нарушения доступности и целостности ВИ ресурса ВКС являются:

- превышение времени передачи видеокадров над реализуемым значением пропускной способности каналов обмена видеоинформацией при организации ВКС;

- превышение интенсивности видеопотока над уровнем, который необходимый для обеспечения допустимой степени потерь пакетов;

- превышение интенсивности видеопотока над реализуемым значением пропускной способности каналов обмена информацией при организации ВКС;

- нарушение семантической целостности ВИ ресурса ВКС вследствие увеличения степени компрессии (увеличения искажений в процессе сжатия) для уменьшения объема видеопотока.

Литература

1. Власов А.В. Анализ особенностей применения видеоконференцсвязи в интересах профильных органов государственного управления / А.В. Власов, В.В. Баранник // Сучасна спеціальна техніка. – 2014. – Вип. 1. – С. 22 – 32.
2. Власов А.В. Кодирование информационных ресурсов систем видеоконференцсвязи для повышения их безопасности. / А.В. Власов, В.В. Лукин // Радиоэлектроника и информатика. – 2013. – № 2. – С. 65 – 73.
3. Богуш В.М. Інформаційна безпека держави /В.М. Богуш, О.К. Юдин. – К.: МК–Прес, 2005. – 432 с.
4. Юдін О.К. Концептуальний аналіз уразливості державних інформаційних ресурсів / О.К. Юдін, С.С. Бучик // Наукоємні технології. – 2013. - № 3 (19). – С. 299 – 304.
5. Власов А.В. Модель загроз безпеки відеоінформаційного ресурсу систем відеоконференцзв'язку. / А.В. Власов, В.В. Бараннік // Наукоємні технології. – 2014. - № 1 (19). – С. 299 – 304.
6. Ватолин В.И. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / В.И. Ватолин, А. Ратушняк, М. Смирнов, В. Юкин. М.: ДИАЛОГ - МИФИ, 2002. - 384 с

V.V. Barannik, d - r of techn. sciences, prof.; A.V. Vlasov, S.A. Sidchenko, cand. of techn. science, Bekirov A.E. **THE FOUNDATION OF SIGNIFICANT SAFETY HAZARDS TO VIDEO INFORMATIONAL RESOURCE OF VIDEO TELECONFERENCING SYSTEMS OF CORE CONTROL SYSTEMS.**

The peculiarities of the formation of vulnerabilities and safety hazards to video-informational resource in the course of video-conferencing functioning for core control systems has been considered in the article. CIA model safety characteristics (privacy, integrity, accessibility) have been offered to apply to analyze the coverage of the given information resource. The analysis of possible violations of video information with obligatory identification of safety hazards, factors, contributing to their display and vulnerabilities is required to be performed for the estimation and formation of the approaches to provide information safety of video informational resource of video-conferencing. Safety vulnerabilities being formed while video-conferencing is functioning and causing safety hazards to video data, namely hazards to accessibility and integrity, have been considered. The estimation of characteristics of video-conferencing video-informational resource has been conducted to determine urgent vulnerabilities and safety hazards to video-informational resource. Actual hazards to the breach of accessibility and integrity of video-informational resource in the course of video-conferencing functioning have been detected on the basis of the given estimation.

Key words: video-conferencing, video-information resource, vulnerability, safety hazard, threat model, spatial resolution, still frame, access time.

Бараннік В.В., Власов А.В., Сідченко С.О., Бекиров А.Є. **ОБГРУНТУВАННЯ ВАГОМИХ ЗАГРОЗ БЕЗПЕКИ ВІДЕОІНФОРМАЦІЙНОГО РЕСУРСУ СИСТЕМ ВІДЕОКОНФЕРЕНЦЗВ'ЯЗКУ ПРОФІЛЬНИХ СИСТЕМ УПРАВЛІННЯ.**

У статті розглянуто особливості формування вразливостей і загроз безпеки відеоінформаційного ресурсу в процесі функціонування відеоконференцзв'язку для профільних систем управління. Для аналізу забезпечення даного інформаційного ресурсу пропонується застосовувати характеристики безпеки моделі CIA (конфіденційність, цілісність, доступність). Для оцінки та формування підходів забезпечення інформаційної безпеки відеоінформаційного ресурсу відеоконференцзв'язку потрібно виконати аналіз можливих порушень відеоінформації з обов'язковою ідентифікацією джерел загроз безпеці, факторів, що

сприяють їх прояву і вразливостей. Розглянуто вразливості безпеки, які формуються при функціонуванні відеоконференцзв'язку і обумовлюють загрози безпеки відеоданих, а саме загрози доступності і цілісності. Для визначення актуальних вразливостей і загроз безпеки відеоінформаційному ресурсу проведено оцінку характеристик відеоінформаційного ресурсу відеоконференцзв'язку. На підставі даної оцінки виділені значущі (актуальні) загрози порушення доступності та цілісності відеоінформаційного ресурсу в процесі функціонування відеоконференцзв'язку.

Ключові слова: відеоконференцзв'язок, відеоінформаційний ресурс, вразливість, загроза безпеці, модель загроз, просторова роздільність, відеокадр, час доступу.

Рецензент д.т.н., профессор Хаханов В.И. (ХНУРЭ)

Поступила 26.03.2014г.