Оценка качества защищенной видеоконференции в условиях компьютерных атак

Assessment of the Quality of a Protected Video Conference Under the Conditions of Computer Attacks

УДК 004.942
Получено: 12.11.2021 Одобрено: 01.12.2021 Опубликовано: 25.12.2021

Белов А.С.
Канд. военных наук, Академия ФСО России, сотрудник.
e-mail: andrej2442016@yandex.ru

Belov A.S.
Candidate of Military Sciences, Academy of the FSO of Russia, employee.
e-mail: andrej2442016@yandex.ru

Добрышин М.М.
Канд. техн. наук, Академия ФСО России, сотрудник
e-mail: dobrithin@yandex.ru

Dobryshyn M.M.
Candidate of Technical Sciences, Academy of the FSO of Russia, employee.
e-mail: dobrithin@yandex.ru

Горбуля Д.С.
Академия ФСО России, сотрудник
e-mail: gorbulia_d@mail.ru

Gorbulya D.S.
Academy of the FSO of Russia, employee
e-mail: gorbulia_d@mail.ru

Новиков В.Г.
Д-р техн. наук, Конструкторское бюро машиностроения

Novikov V.G.
Doctor of Technical Sciences, Mechanical Engineering Design Bureau

Аннотация
В статье представлен подход к оценке качества защищенной видеоконференции с использованием результатов анализа параметров, характеризующих информационный поток. Подход основан на применении машинного обучения распознавания образов для выявления артефактов в видеоизображении, сопоставлении полученных результатов со значениями параметров, характеризующих качество информационного потока и формировании нейросети. Сформированная нейросеть совместно с известными аппаратно-программными решениями позволяет прогнозировать качество видеоконференции и своевременно применять имеющиеся механизмы информационной безопасности.
Ключевые слова: видеоконференция, качество, компьютерные атаки.

Abstract
The article presents an approach to assessing the quality of a secure video conference using the results of the analysis of parameters characterizing the information flow. The approach is based on the application of image recognition machine learning to identify artifacts in the video image, comparing the results obtained with the values of parameters characterizing the quality of the information flow and the formation of a neural network. The formed neural network, together with well-known hardware and software solutions, allows you to predict the quality of video conferencing and timely apply existing information security mechanisms.
Keywords: video conference, quality, computer attacks.

Ухудшение эпидемиологической обстановки в стране и мире, а также расширение возможностей телекоммуникационных услуг способствовали активному использованию видеоконференции при принятии решений. В то же время количество инцидентов информационной безопасности, а также ущерб от них за 2020 г. значительно увеличились [1−6].

Для обеспечения информационной безопасности применяются различные виды защищенных протоколов сетевых соединений и средств криптографической защиты информации, что позволяет обеспечить требуемую конфиденциальность и целостность информации [7−11].

Однако тенденция увеличения компьютерных атак (DDoS, MiTM), направленных на разрыв соединений и его блокирование с целью получения «выкупа», свидетельствует о том, что существующие механизмы активной защиты от компьютерных атак все еще недостаточно продуктивны, в результате системы обеспечения информационной безопасности часто недостаточно эффективно минимизируют ущерб от компьютерных атак [12−21].

Активные мероприятия обеспечения информационной безопасности и противодействия выявленной компьютерной атаке проводятся после ухудшения качества или разрыва сеанса связи [22−24]. Разрыв сеанса видеоконференции или значительное его ухудшение вызвано увеличением количества ошибок и задержки информационного потока.

Для анализа качества нешифрованного видеопотока разработаны и активно применяются различные методы оценки и восстановления изображения [25−28]. Однако при использовании средств криптографической защиты указанные методы недостаточно эффективны по причине применения статистических оценок, что не позволяет своевременно активировать и применять механизмы активной защиты от компьютерных атак [29].

Для устранения указанного противоречия и повышения обоснованности и своевременности применения механизмов активной защиты от компьютерных атак, сеансов видеоконференции, предлагается с использованием методов машинного обучения и нейронных сетей оценивать на качественном уровне предоставляемую услугу видеоконференции на основе параметров, характеризующих информационный поток.

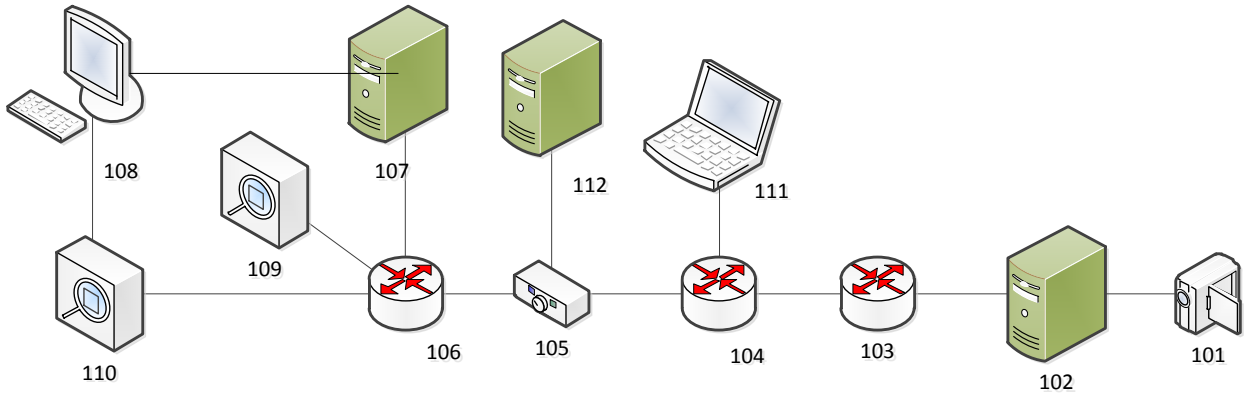
Разработанный подход заключается в следующем.

На первоначальном этапе предлагается декомпозиция изучаемого процесса на части с последующей оценкой полученных результатов.

Затем формируется испытательный стенд (рис. 1), осуществляется передача эталонного видеосообщения (101-102-103-104-105-106-107-108) и обучение нейросети по оценке качества передаваемого видеоизображения (108-110).

Собираются статистические данные о качестве информационного потока (109). Вносятся изменения (с использованием закона распределения случайной величины) в битовый поток передаваемого эталонного видеопотока (101-102-103-104-111-105-106-107-108) и происходит обучение нейросети по выявлению количества, формы и площади возникающих артефактов при нормальных условиях эксплуатации (рис. 2). Осуществляется сбор статистических данных о качестве информационного потока (109).

С помощью программы VCDemo имитируется случайная битовая ошибка (111) в передаваемом информационном потоке (распределение Гаусса) (рис. 3).



101 - источник видеосигнала
102 - сервер видеоконференцсвязи
103 - средство криптографической защиты
104 - маршрутизатор
105 - коммутатор
106 - средство криптографической защиты
107 - сервер видеоконференцсвязи
108 - приемник видеосигнала
109 - система оценки качества цифрового потока
110 - программное средство оценки качества видеоизображения
111 - источник битовых ошибок в сети связи
112 - источник компьютерной атаки

Рис. 1. Схема испытательного стенда

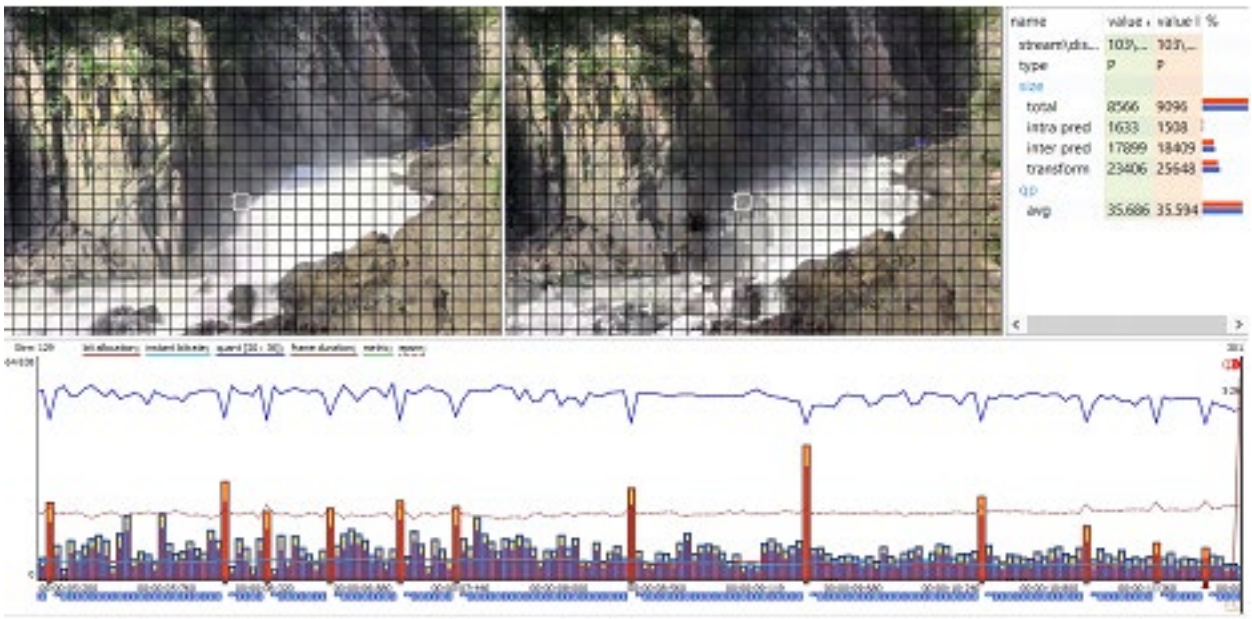


Рис. 2. Результаты обучения нейросети оценке качества видеоизображения при нормальных условиях эксплуатации

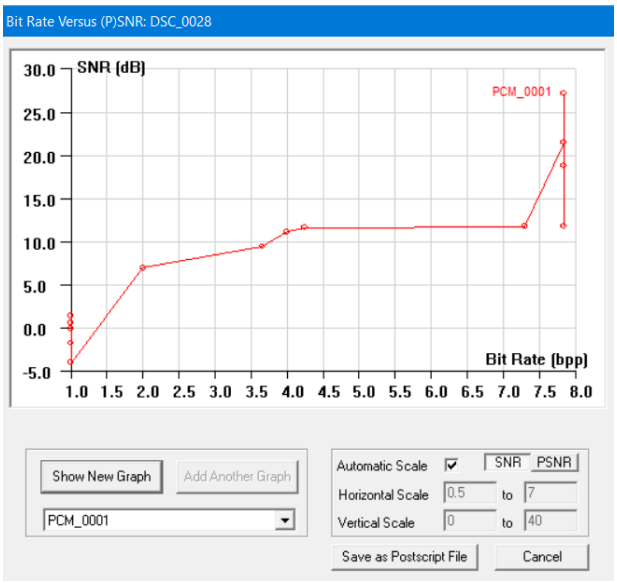


Рис. 3. Интерфейс программы VCDemo, применяемый для имитации битовых ошибок

По заданному закону вносятся изменения в битовый поток передаваемого эталонного видеопотока (101-102-103-104-111-105-112-106-107-108). Происходит обучение нейросети по выявлению количества, формы и площади возникающих артефактов (рис. 4), а также сбор статистических данных о качестве информационного потока (109).

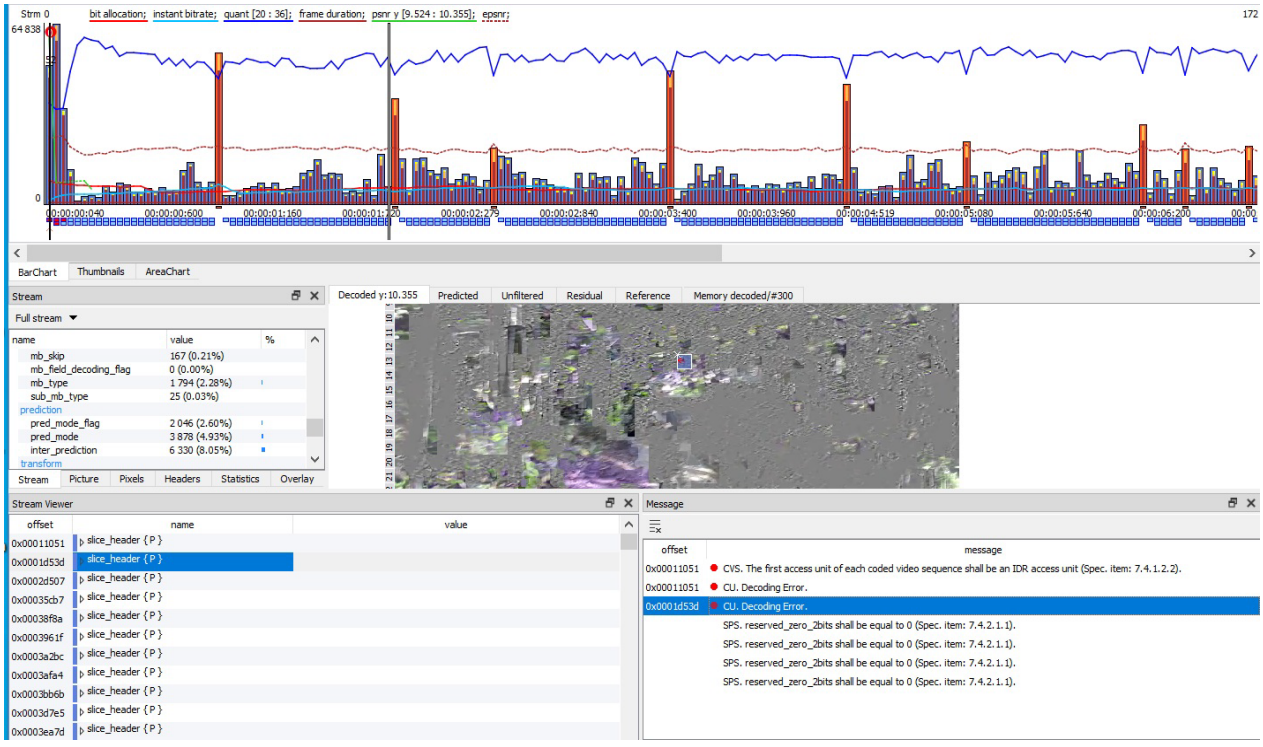


Рис. 4. Результаты обучения нейросети по оценке качества видеоизображения в условиях компьютерной атаки

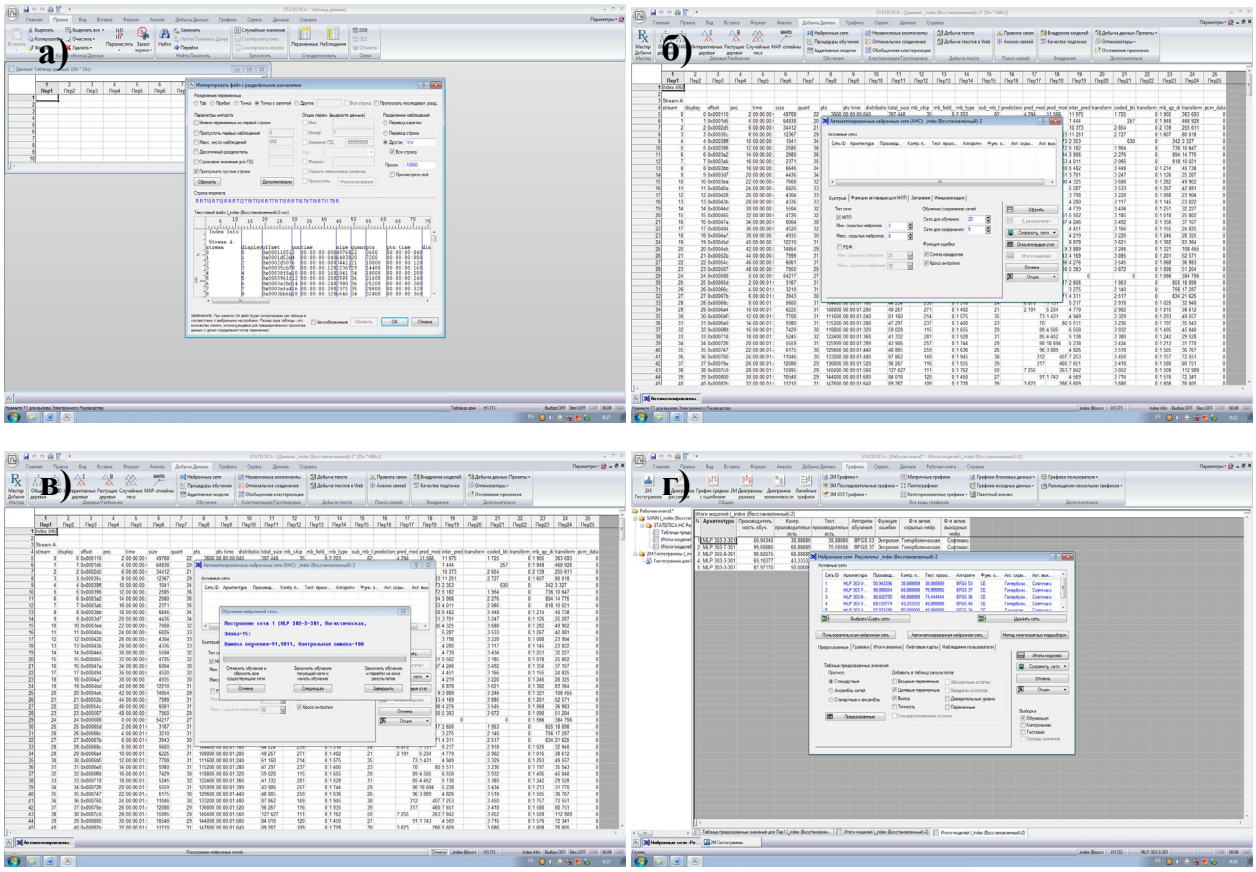
Далее сопоставляются исходные точки отсчета собранных временных рядов относительно друг друга и формируются критерии принятия решения о качестве изображения (значение битовой ошибки – количество артефактов):

– видеоизображение без искажений и артефактов;
– появление единичных артефактов;

– появление большого количества артефактов;
– «рассыпание» видеоизображения (рис. 4).

Проводится поиск корреляционных связей между параметрами, характеризующих качество видеоданных и информационного потока [30, 31].

После накопления необходимого объема данных об изменении качества видеоизображения и качестве канала связи с помощью программы STATISTICA 10 (Ver. 10.0.1011.0) формируется группа нейросетей для обработки и анализа собранных статистических данных о битовой ошибке и количестве артефактов в видеоизображении. В качестве входной переменной выступает битовая ошибка в информационном потоке, а в качестве зависящей переменной выступает количество артефактов в видеоизображении. Результаты обучения нейросети показаны на рис. 5.



а) визуальное представление обработки статистических данных эксперимента;
б) визуальное представление выбора параметров для обучения нейросети;
в) визуальное представление обучения нейросети;
г) результаты обучения нейросети.

Рис. 5. Результаты формирования нейросети по предсказанию количества артефактов

Созданная нейросеть способна на основании обработки фактического значения битовой ошибки оцениваемого информационного потока предсказать количество возникающих артефактов в сеансе видеосвязи.

Разработанный авторами программный модуль обработки событий информационной безопасности дополняется исполняющим файлом, обеспечивающим работу выбранной наилучшей нейросети. Далее подключаются средства измерения, и производится анализ параметров качества информационного потока и признаков, характеризующих ведение компьютерной атаки. При выявлении признаков начала компьютерной атаки или снижении параметров информационного потока прогнозируют качество предоставляемой услуги видеосвязи [32−35].

Для быстрого понимания возможного состояния видеоизображения оператором, вывод результатов прогнозирования проводится на качественном уровне (исходя из указанных критериев) в цветовой гамме:

- зеленый – видеоизображение без искажений и артефактов;
- желтый – возможно появление единичных артефактов;
- оранжевый – возможно появление большого количества артефактов;
- красный – возможно «рассыпание» видеоизображения.

Время прогнозирования качества видеоизображения должно превышать суммарное время, необходимое для прогнозирования состояния, оценки результатов прогноза, принятия решения и применения мероприятий, направленных на недопущение разрыва сеанса связи (переключение на резервные информационные потоки, использование протоколов, имеющих большую стойкость при меньшем качестве изображения).

Созданная нейросеть применима только для того узла связи, для которого производились измерения параметров информационного потока, и происходило обучение и для тех же технических характеристик (видеокодеки, протоколы сетевого соединения, средствах криптографической защиты информации).

Подход к оценке качества защищенной видеоконференции позволяет за счет методов машинного обучения повысить обоснованность и своевременность применения механизмов активной защиты при выявлении фактов компьютерных атак. Разработанный подход возможно применять в составе систем обеспечения информационной безопасности [29, 35, 36] как инструмент поддержки принятия решений должностных лиц, отвечающих за обеспечение информационной безопасности элементов компьютерной сети, интегрированной в мировое информационное пространство.

Литература

1. *Тебекин А.В.* Квалиметрическая оценка уровня цифровизации экономики в Российской Федерации // Журнал технических исследований. − 2018. − Т. 4. − № 3. − С. 1-13.
2. *Анисимов Е.Г., Анисимов В.Г., Солохов И.В.* Проблемы научно-методического обеспечения межведомственного информационного взаимодействия // Военная мысль. − 2017. − № 12. − С. 45-51.
3. *Зегжда П.Д.* Модель формирования программы развития системы обеспечения информационной безопасности организации // Проблемы информационной безопасности. Компьютерные системы. − 2021. − № 2 (46). − С. 109-117.
4. *Сауренко Т.Н.* Прогнозирование инцидентов информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2019. − № 3. − С. 24-28.
5. *Ямпольский С.М.* Научно-методические основы информационно-аналитического обеспечения деятельности органов государственного и военного управления в ходе межведомственного информационного взаимодействия. − Москва: Военная академия Генерального штаба Вооруженных Сил Российской Федерации, Военный институт (управления национальной обороной). 2019. 146 с.
6. *Saurenko T.N.* Methodology control function realization within the electronic government concept framework / *T.N. Saurenko* [*и др.*] // International Journal of Scientific and Technology Research. 2020. Т. 9. № 2. С. 6259-6262.
7. *Anisimov V.G.* A risk-oriented approach to the control arrangement of security protection subsystems of information systems // Automatic Control and Computer Sciences, 2016, 50(8). С. 717-721.
8. *Белов А.С., Добрышин М.М., Шугуров Д.Е.* Алгоритм адаптивного управления удаленной аутентификацией в корпоративных сетях связи // Журнал технических исследований. − 2021. − Т. 7. − № 3. − С. 38-46.
9. *Anisimov V.G.* The problem of innovative development of information security systems in the transport sector // Automatic Control and Computer Sciences. − 2018. − Т. 52. − № 8. − С. 1105-1110.

10. *Зегжда П.Д.* Модель оптимального комплексирования мероприятий обеспечения информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2020. − № 2. − С. 9-15.
11. *Гринюк О.Н., Сысоев К.А., Шевченко Е.В.* Исследование методов защиты информации в облачных сервисах // Журнал технических исследований. − 2019. − Т. 5. − № 1. − С. 12-14.
12. *Добрышин М.М., Шугуров Д.Е.* Иерархическая многоуровневая модель таргетированных компьютерных атак в отношении корпоративных компьютерных сетей // Проблемы информационной безопасности. Компьютерные системы. − 2020. – № 4. – С. 35-46.
13. *Белов А.С., Добрышин М.М., Борзова Н.Ю.* Формирование модели угроз информационной безопасности на среднесрочный период // Приборы и системы. Управление, контроль, диагностика. – 2021. – № 7. – С. 41−48.
14. *Анисимов В.Г.* Обобщенный показатель эффективности взаимодействия федеральных органов исполнительной власти при решении задач обеспечения национальной безопасности государства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. − 2017. − № 5-6 (107-108). − С. 101-106.
15. *Анисимов Е.Г.* Показатели эффективности межведомственного информационного взаимодействия при управлении обороной государства // Вопросы оборонной техники. Серия 16: Технические средства противодействия терроризму. − 2016. − № 7-8 (97-98). − С. 12-16.
16. *Гречишников Е.В., Белов А.С., Скубьев А.В., Трахинин Е.Л.* Формализованная модель оценивания живучести распределенной сети связи в условиях деструктивных воздействий // Проблемы информационной безопасности. Компьютерные системы. − 2020. − №2. − С. 53-57.
17. *Анисимов В.Г., Селиванов А.А., Анисимов Е.Г.* Методика оценки эффективности защиты информации в системе межведомственного информационного взаимодействия при управлении обороной государства // Информация и космос. − 2016. − № 4. − С. 76-80.
18. *Anisimov, V.G.* Indices of the effectiveness of information protection in an information interaction system for controlling complex distributed organizational objects / *V.G Anisimov*, *E.G. Anisimov* Automatic Control and Computer Sciences, 2017, 51(8), pp. 824–828. https://doi.org/10.3103/S0146411617080053.
19. *Зегжда П.Д.* Подход к оцениванию эффективности защиты информации в управляющих системах // Проблемы информационной безопасности. Компьютерные системы. − 2020. − № 1 (41). − С. 9-16.
20. *Анисимов В.Г.* Показатели эффективности защиты информации в системе информационного взаимодействия при управлении сложными распределенными организационными объектами // Проблемы информационной безопасности. Компьютерные системы. − 2016. − № 4. − С. 140-145.
21. *Зегжда П.Д.* Эффективность функционирования компьютерной сети в условиях вредоносных информационных воздействий // Проблемы информационной безопасности. Компьютерные системы. − 2021. − № 1 (45). − С. 96-101.
22. *Добрышин М.М., Локтионов А.Д., Спирин А.А.* Предложения по раннему обнаружению деструктивных воздействий Botnet на компьютерные сети связи // Научный журнал : Телекоммуникации. – 2020. – № 12. – С. 25-29.
23. *Добрышин М.М.* Моделирование процессов деструктивных воздействий на компьютерную сеть связи с применением компьютерной атаки типа "человек посередине"// Научный журнал : Телекоммуникации. – 2019. – № 11. – С. 32-36.
24. *Anisimov V.G.* Models of forecasting destructive influence risks for information processes in management systems // Информационно-управляющие системы. 2019. № 5 (102). С. 18-23.
25. Aguiar A. C., Hoene C., Klaue J., Karl H., Wolisz A., and Miesmer H. Channel-aware schedulers for voip and MPEG-4 based on channel prediction. to be published at MoMuC, 2003.
26. Sanneck H., Mohr W., Le L., Hoene C., and Wolisz A. Quality of service support for voice over ip over wireless. Wireless IP and Building the Mobile Internet, December 2002.

27. Wu D., Hou Y. T., Zhu W., Lee H.-J., Chiang T., Zhang Y.-Q., and Chao H. J. On end-to-end architecture for transporting mpeg-4 video over the internet. IEEE Transactions on Circuits and Systems for Video Technology, 10(6) pp. 923–941, September 2000.
28. *Hertrich D*. MPEG4 video transmission in wireless LANs – basic QoS support on the data link layer of 802.11b. Minor Thesis, 2002.
29. . *Зегжда П.Д.* Модели и метод поддержки принятия решений по обеспечению информационной безопасности информационно-управляющих систем // Проблемы информационной безопасности. Компьютерные системы. − 2018. − № 1. − С. 43-47.
30. *Видов М.И.* Использование перцепционной метрики и статистических моделей для оценки качества видеоизображений в условиях потери пакетов // Электротехнические и информационные комплексы и системы. − № 1. − Т. 9. − 2013. – С. 61–70.
31. *Шелухин О.И., Иванов Ю.А.* Оценка качества передачи потокового видео в телекоммуникационных сетях с помощью программно-аппаратных средств // Электротехнические и информационные комплексы и системы. − №4. − Т. 5. − 2009. – С. 48-56.
32. *Добрышин М.М., Берлизев А.В., Берлизева Е.С., Верижникова О.Н*. Расчет корреляционных связей между значениями параметров технического состояния средств связи / Свидетельство о государственной регистрации программы для ЭВМ № 2018615232 от 03.05.2018 г. бюл. № 5.
33. *Зегжда П.Д.* Модель и метод оптимизации вычислительных процессов в вычислительных системах с параллельной архитектурой // Проблемы информационной безопасности. Компьютерные системы. − 2018. − № 4. − С. 78-85.
34. *Зегжда П.Д.* Методический подход к построению моделей прогнозирования показателей свойств систем информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. − 2019. − № 4. − С. 45-49.
35. *Добрышин М.М., Горшков А.А., Манзюк В.В.* Вариант построения адаптивной системы мониторинга информационно-технических воздействий // Известия Тульского государственного университета. Технические науки. − 2020. − № 9. – С. 14-21.
36. *Добрышин М.М., Закалкин П.В., Гречишников Е.В.* Адаптивная система мониторинга информационно-технических воздействий // Патент РФ на изобретение № 2728763 31.07.2020 Бюл. № 22. Заявка № 2019123565, от 26.07.2019. Патентообладатель: Академия ФСО России. G06F 21/50 (2013.01).