МОДЕЛЬ ОЦЕНКИ ВЛИЯНИЯ СИСТЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА КАЧЕСТВО ПРЕДОСТАВЛЯЕМЫХ УСЛУГ КОРПОРАТИВНОЙ СЕТИ СВЯЗИ

М.М. Добрышин, *к.т.н., Академия ФСО России, dobrithin@ya.ru;*
В.А. Фролов, *Академия ФСО России, r414@bk.ru.*

УДК 004.942

Аннотация. Современный этап развития средств обеспечения информационной безопасности свидетельствует о том, что помимо положительного влияния на защищаемую корпоративную сеть связи указанные средства способны существенно затруднять, а в некоторых случаях и блокировать предоставления абонентам сети требуемых услуг связи. Для разрешения указанного противоречия сформулирована модель, позволяющая выявить зависимости между отдельными свойствами услуг связи, сети связи и качества средств обработки информации, с одной стороны, и применяемых средств обеспечения информационной безопасности – с другой стороны. Применение модели позволит определить способность корпоративной сети связи предоставлять требуемые услуги связи при использовании заданного набора средств обеспечения информационной безопасности.

Ключевые слова: качество связи и услуг связи; корпоративная сеть связи; система обеспечения информационной безопасности; моделирование.

A MODEL FOR ASSESSING THE IMPACT OF AN INFORMATION SECURITY SYSTEM ON THE QUALITY OF SERVICES PROVIDED BY A CORPORATE COMMUNICATION NETWORK

M.M. Dobryshin, *Candidate of Technical Science, Academy of the FSO of Russia;*
V.A. Frolov, *Academy of the FSO of Russia.*

Annotation. The current stage of development of information security tools indicates that in addition to a positive impact on the protected corporate communications network, these tools can significantly complicate, and in some cases block the provision of required communication services to network subscribers. To resolve this contradiction, a model has been formulated that allows us to identify the dependencies between individual properties of communication services, communication networks and the quality of information processing tools on the one hand and the means used to ensure information security on the other hand. The application of the model will determine the ability of a corporate communication network to provide the required communication services when using a given set of information security tools.

Keywords: quality of communication and communication services; corporate communication network; information security system; modeling.

Введение

Изучение процесса обеспечения информационной безопасности (ИБ) требует комплексного рассмотрения всех протекающих подпроцессов в защищаемой системе. Результаты практической деятельности свидетельствуют о том, что определенный набор применяемых средств обеспечения информационной безопасности (в настоящее время существует – 17 видов)[1] не только защищает от

[1] Министерство цифрового развития, связи и массовых коммуникаций Российской Федерации. Приказ от 22 сентября 2020 г. № 486 «Об утверждении классификатора программ для электронных вычислительных машин и баз данных».

различных воздействий, но и затрудняет процесс предоставления абонентам сети требуемых услуг связи и ухудшает качество этих услуг [1-3].

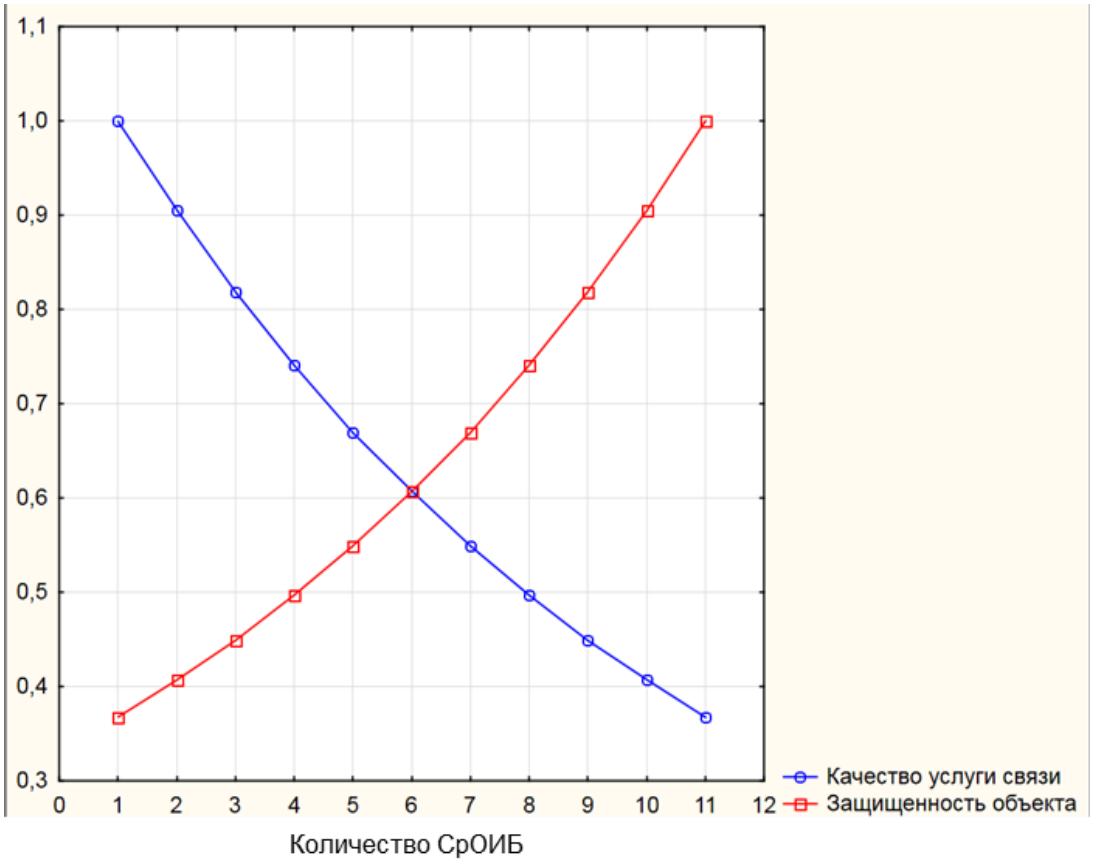
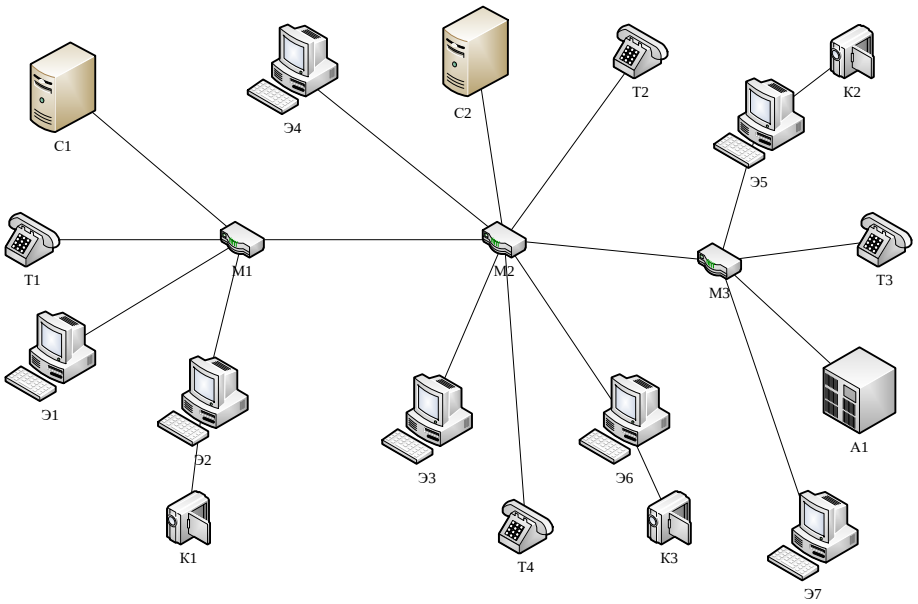


Рисунок 1

Таким образом, возникает задача о нахождении набора средств обеспечения ИБ (СрОИБ), объединенного в систему обеспечения информационной безопасности (СОИБ), который, с одной стороны, позволит предоставить требуемое количество услуг связи с заданным качеством, а с другой стороны обеспечит требуемую защищенность элемента сети (рис. 1) и уровень информационной безопасности корпоративной сети связи (КСС) [4-6].

Материальной основой обеспечения требуемого качества предоставляемых услуг связи является инфраструктура КСС (вариант локальной сети показан на рис. 2), которая характеризуется группой свойств, описывающих качество сети (рис. 3)[2,3] [7, 8] и свойств элементов, из которых состоит сеть. Элементами могут выступать узлы сети и серверы информационных ресурсов, объединяющие средства обработки информации (СОИ) (совокупность автономных устройств сбора, накопления, передачи, обработки и представления информации)[4], и программное обеспечение (ПО), установленное на указанных СОИ.

[2] ГОСТ Р 53111-2008. Устойчивость функционирования сети связи общего пользования. Требования и методы проверки.
[3] ГОСТ Р 53801-2010. Связь федеральная. Термины и определения.
[4] ГОСТ Р ИСО/МЭК 25023-2021. Системная и программная инженерия. Требования и оценка качества систем и программной продукции (*SQuaRE*). Измерения качества системы и программной продукции.



К1– Камера видеоконференцсвязи
К2– Камера видеоконференцсвязи
К3– Камера видеоконференцсвязи
М1– Маршрутизатор
М2– Маршрутизатор
М3– Маршрутизатор
Т1– Телефон
Т2– Телефон
Т3– Телефон
С1– Сервер видеоконференцсвязи
С2– Сервер быстрых сообщений
А1– Автоматическая телефонная станция
Э1– Персональный компьютер
Э2– Персональный компьютер
Э3– Персональный компьютер
Э4– Персональный компьютер
Э5– Персональный компьютер
Э6– Персональный компьютер
Э7– Персональный компьютер

Рисунок 2

Рисунок 3

Анализ подходов оценки качества СОИ и ПО[5] [8, 9] возможно проводить как самостоятельно существующих объектов отдельно СОИ, так и отдельно ПО, однако результаты носят в значительной степени абстрагированный анализ и не позволяют получить адекватную оценку. В актуальных регламентирующих документах порядок оценки качества аппаратно-программных средств, предлагается производить комплексно [10], группа свойств, характеризующих качество СОИ при использовании указана на рис. 4.

Рисунок 4

Основываясь на предположении, что в начальных условиях функционирования сеть способна обеспечить предоставление заданного количества услуг связи с требуемым качеством, следует вывод, о том, что существуют воздействия, выводящие систему (КСС) из равновесного состояния и снижающие качество [11].

Опираясь на теорию устойчивости Ляпунова и различные направления теории управления, и теорию рисков, воздействия целесообразно разделить на внешние и внутренние воздействия.

Под внешними воздействиями понимаются все действия из внешней среды, способные повлиять на цель функционирования КСС – предоставление абонентам заданного количества услуг связи с требуемым качеством.

Под внутренними воздействиями понимаются влияние элементов на цель функционирования КСС.

Воздействия могут нести отрицательное (негативное) влияние – ухудшение качества предоставляемой услуги связи, и положительное влияние – расширение количества предоставляемых услуг связи, повышение качества и минимизация внешнего деструктивного воздействия.

Внешними воздействиями на КСС, способными ухудшить качество предоставляемых услуг связи выступают действия, направленные на поиск новых уязвимостей ПО или выявление новых условий, при которых возможно реализовать известные уязвимости, различные компьютерные атаки (КА) и действия абонентов и/или инженерно-технического персонала, направленные на предоставление новых услуг связи или формирования новых элементов сети.

[5] ГОСТ Р ИСО/МЭК 25010-2015. Информационные технологии. Системная и программная инженерия. Требования и оценка качества систем и программного обеспечения (*SQuaRE*). Модели качества систем и программных продуктов.

Действия абонентов и технического персонала по целенаправленному или непреднамеренному воздействию на сеть также относятся к внешним воздействиям. Причем в отличие от действий злоумышленника, действия абонентов и технического персонала носят разнонаправленный характер. Так, применение нового оборудования или ПО потенциально повышает качество предоставляемых УС, а с другой стороны, новое программное обеспечение обладает новым набором уязвимостей, что изменяет поверхность защиты и выводит КСС из состояния «защищено» в состояние «не защищено».

К источникам внутренних воздействий на КСС относятся элементы, которые входят в состав сети, т.е. СОИ, ПО, СОИБ, объединяющая СрОИБ.

В качестве отрицательных (дестабилизирующих) воздействий, оказываемых СОИ, и ПО на КСС рассматриваются эксплуатационные отказы и сбои [12].

В качестве положительных воздействий, оказываемых СОИ, и ПО на КСС выступают обновления и изменение настроек, устраняющие известные уязвимости или блокирующие реализацию известных техник реализации КА.

СОИБ также вносит разнонаправленные воздействия – с одной стороны, СОИБ минимизирует или предотвращает ущерб от различных видов КА, с другой стороны – СОИБ затрудняет процесс предоставления УС.

Модель оценки влияния системы обеспечения информационной безопасности на качество предоставляемых услуг связи корпоративной сети связи

Влияние СОИБ на качество функционирования КСС (рис. 5), описывающих эксплуатационные характеристики применяемых СОИ с установленным набором ПО, информационных технологий сетевого взаимодействия и затрудняющих (ухудшающих) качество предоставления УС возможно описать следующими выражениями:

$$\begin{cases} q_i^{\text{СОИБ}}(t) = f\left(p_{ij}^{g}(t), \langle n_g \rangle\right) \\ Q^{\text{СОИБ}}(t) = f\left(p_{ij}^{g}(t), q_i^{\text{СОИБ}}(t), S, \langle n_g \rangle\right), \\ Q_m^{\text{СОИБ}}(t) = Q^{\text{СОИБ}}(t) \otimes q_i^{\text{СОИБ}}(t) \end{cases} \quad (1)$$

где: $p_{ij}^{g}(t)$ – значения j-го параметра, отражающего функциональные характеристики i-го защищаемого СОИ, входящего в состав элемента КСС в условиях применения g-о средства СрОИБ $\left(\langle n_g \rangle\right)$, входящего с состав СОИБ.

Исходными данными для модели являются значения параметров эксплуатационных характеристик СОИ, информационных технологий, топология и структура сети, схемы, описывающие взаимодействия элементов для организации и предоставления услуг связи.

Промежуточными результатами блочной модели влияния СОИБ на качество предоставления УС являются: отклонение фактических значений (измеренных значений в условиях применения СОИБ) параметров, характеризующих эксплуатационные характеристики СОИ от допустимых (требуемых) соответствующих значений; отклонение фактических значений (измеренных значений в условиях применения СОИБ) параметров,

характеризующих эксплуатационные характеристики применяемых ИТ сетевого взаимодействия от допустимых (требуемых) соответствующих значений.

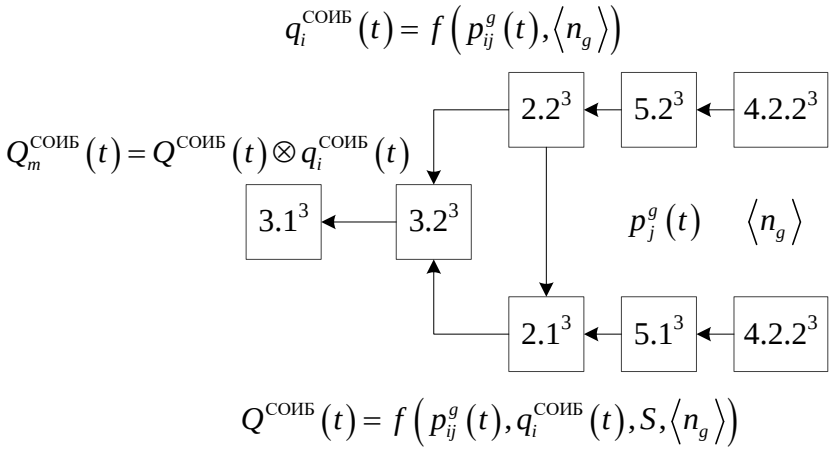


Рисунок 5

Выходными результатами являются изменение значений параметров, описывающих следующие свойства:

для средств обработки информации:

– результативность $\left(X_{in}^R(t)\right)$ – доля задач *i*-го СОИ, которые выполняются правильно в условиях *n*-й конфигурации СОИБ (применения заданного набора СрОИБ и режимов их работы):

$$X_{in}^R(t) = \frac{A_{in}^R(t)}{B_i^R}, \tag{2}$$

где: $A_{in}^R(t)$ – количество выполненных уникальных задач при *n*-й конфигурации СОИБ *i*-м СОИ, B_i^R – общее количество выполненных уникальных задач *i*-м СОИ;

– эффективность / производительность – эффективность затраченного времени на успешное выполнение задачи $\left(X_{in}^O\right)$ *i*-м СОИ в условиях *n*-й конфигурации СОИБ:

$$X_{in}^O = \frac{A_{in}^O}{T_i^O}, \tag{3}$$

где: A_{in}^O – количество выполненных уникальных задач *i*-м СОИ при *n*-й конфигурации СОИБ, T_i^O – время на выполнение заданного количества задач *i*-м СОИ;

– покрытие контекста – доля предполагаемых контекстов использования $\left(X_{in}^K(t)\right)$, в которых *i*-е СОИ может использоваться в условиях *n*-й конфигурации СОИБ:

$$X_{in}^{K}(t)=\frac{A_{in}^{K}(t)}{B_{i}^{K}}, \tag{4}$$

где: $A_{in}^{K}(t)$ – количество контекстов с приемлемым удобством использования и риском *j*-м СОИ при *n*-й конфигурации СОИБ, B_i^K – общее количество требуемых различных контекстов использования *j*-го СОИ.

Значения $A_{in}^{R}(t)$, $A_{in}^{O}(t)$, $A_{in}^{K}(t)$ – определяются экспериментально для каждого СОИ, функционирующего в условиях *n*-й конфигурации СОИБ.

Значения B_i^R, B_i^O, B_i^K – определяются на основе требований абонента предъявляемых к количеству предоставляемых услуг связи *i*-м СОИ.

для сети связи:

– целостность сети – вероятность связности (связность, $\left(S^{j}(t)\right)$) элементов сети при предоставлении *j*-й услуги связи в условиях *n*-й конфигурации СОИБ:

$$S^{j}(t)=\prod_{a=1}^{b}s_{an}^{j}(t), \tag{5}$$

$$s_{an}^{j}(t)=\prod_{i=1}^{m}X_{in}^{R}(t), \tag{6}$$

где: $s_{an}^{j}(t)$ – вероятность связности элементов сети при предоставлении *j*-й услуги связи *a*-у абоненту в условиях *n*-й конфигурации СОИБ, *m*-набор СОИ, используемых для предоставления *j*-й услуги связи.

Пример для схемы КСС, показанной на рис. 2:

$$\begin{aligned}
&s_{1n}^{\text{вкс}}(t)=X_{\text{К1}\,n}^{\text{вкс}}(t)\,X_{\text{Э2}\,n}^{\text{вкс}}(t)\,X_{\text{М2}\,n}^{\text{вкс}}(t)\,X_{\text{С1}\,n}^{\text{вкс}}(t),\\
&s_{2n}^{\text{вкс}}(t)=X_{\text{К2}\,n}^{\text{вкс}}(t)\,X_{\text{Э5}\,n}^{\text{вкс}}(t)\,X_{\text{М3}\,n}^{\text{вкс}}(t)\,X_{\text{М2}\,n}^{\text{вкс}}(t)\,X_{\text{М1}\,n}^{\text{вкс}}(t)\,X_{\text{С1}\,n}^{\text{вкс}}(t),\\
&s_{3n}^{\text{вкс}}(t)=X_{\text{К3}\,n}^{\text{вкс}}(t)\,X_{\text{Э6}\,n}^{\text{вкс}}(t)\,X_{\text{М2}\,n}^{\text{вкс}}(t)\,X_{\text{М1}\,n}^{\text{вкс}}(t)\,X_{\text{С1}\,n}^{\text{вкс}}(t),\\
&S^{j}(t)=s_{1n}^{\text{вкс}}(t)\,s_{2n}^{\text{вкс}}(t)\,s_{3n}^{\text{вкс}}(t),
\end{aligned}$$

где: $s_{1n}^{\text{вкс}}(t)$, $s_{2n}^{\text{вкс}}(t)$, $s_{3n}^{\text{вкс}}(t)$ – вероятность связности элементов сети, участвующих в предоставлении видеоконференцсвязи для абонентов №1, №2, №3 при *n*-й конфигурации СОИБ; $X_{\text{К1}\,n}^{\text{вкс}}(t)$, $X_{\text{Э2}\,n}^{\text{вкс}}(t)$, $X_{\text{М2}\,n}^{\text{вкс}}(t)$, $X_{\text{С1}\,n}^{\text{вкс}}(t)$ – вероятность выполнения требуемой функции: камерой видеоконференцсвязи № 1 (К1, рис. 2), персонального компьютера № 2 (Э2, рис. 2), маршрутизатора № 2 (М2, рис. 2), сервера видеоконференцсвязи (С1, рис. 2) соответственно;

– доступность сети – вероятность того, что пользователь услуги после запроса (направленного в сеть) получает сигнал ответа в условиях *n*-й конфигурации СОИБ $\left(P_n^{\text{отв}\,j}(t)\right)$:

$$P_n^{\text{отв}\,j}=\prod_{i}X_{in}^{O}. \tag{7}$$

– устойчивость (живучесть) функционирования сети – вероятность предоставления хотя бы одной услуги $\left(Q(t)\right)$ из всего перечня предоставляемых услуг связи $\left(J=1,2,...,j\right)$:

$$Q^J(t)=K_n^{\text{г}}(t)P_{jn}(t), \tag{8}$$

$$Q(t)=\prod_j Q^J(t), \tag{9}$$

где: $K_n^{\text{г}}(t)$ – коэффициент готовности фрагмента сети, используемого для предоставления услуг связи, $P_{jn}(t)$ – вероятность предоставления *j*-й услуги связи в условиях *n*-й конфигурации СОИБ (определяется экспериментально).

для качества услуг связи:

– удобство – количество операций, выполненных абонентом для получения требуемой услуги связи $\left(Y_{an}^j\right)$ в условиях *n*-й конфигурации СОИБ:

$$\begin{aligned} &Y_{an}^j=\left(n_n^{\text{доступ }j},T_n^{\text{доступ }j}\right),\\ &n_n^{\text{доступ }j}>N^{\text{доп доступ}},\\ &T_n^{\text{доступ }j}>T^{\text{доп доступ}}, \end{aligned} \tag{10}$$

где: $n_n^{\text{доступ }j}$ – количество операций, которые должен выполнить *a*-й абонент, для доступа к *j*-й услуге связи, $N^{\text{доп доступ}}$ – допустимое количество операций, которые должен выполнить *a*-й абонент, $T_n^{\text{доступ }j}$ – время, затрачиваемое *a*-м абонентом на доступ к *j*-й услуге связи, $T_n^{\text{доступ}}$ – желаемое (ожидаемое) время, затрачиваемое *a*-м абонентом на доступ к *j*-й услуге связи.

$n_n^{\text{доступ }j}$, $T_n^{\text{доступ }j}$ – определяются экспериментально, $N^{\text{доп доступ}}$, $T_n^{\text{доступ}}$ – определяется на основе опросов абонентов.

– действенность – доля успешно установленных соединений (сессий) $\left(n_n^j(t)\right)$, от общего количества попыток установления соединений $\left(N^{\text{соед}}\right)$:

$$D_n^j(t)=\frac{n_n^j(t)}{N^{\text{соед}}}, \tag{11}$$

для качества восприятия:

– удовлетворенность абонента провайдером – своевременность выполнения заявки на подключение клиента к сети связи (субъективное мнение абонентов, определяется опросами).

Заключение

Перечисленные взаимосвязи между отдельными свойствами услуг связи, сети связи и качества средств обработки информации, с одной стороны, и применяемых средств обеспечения информационной безопасности – с другой

стороны, позволят разрешить сформулированную задачу по предоставлению требуемого количества услуг связи с заданным качеством и требуемым уровнем информационной безопасности.

Применение модели позволит определить способность корпоративной сети связи предоставлять требуемые услуги связи при использовании заданного набора средств обеспечения информационной безопасности.

Направлением дальнейших исследований является изучение влияния заданного набора средств обеспечения информационной безопасности на частные показатели выявленных зависимостей.

Литература

1. Белов А.С., Добрышин М.М., Шугуров Д.Е. Научно-методический подход к оцениванию качества систем обеспечения информационной безопасности // Приборы и системы. Управление, контроль, диагностика, 2022. – № 11. – С. 34-40.
2. Давлятова М.А., Мокшонкова А.А. Защита информации как основное направление повышения качества услуг // В сборнике: Торговля и сервис от настоящего к будущему: инновации в сфере товаров и услуг. Сборник трудов по материалам молодежной конференции, 2017. – С. 287-289.
3. Лаврова Д.С. Подход к разработке SIEM-системы для Интернета вещей // Проблемы информационной безопасности. Компьютерные системы, 2016. – С. 50-60.
4. Курочкина А.А., Стародубцев Г.Ю., Коровина Е.К. Факторы, влияющие на оценку качества услуг связи // Перспективы науки, 2016. – № 12 (87). – С. 104-106.
5. Зегжды Д.П. Кибербезопасность цифровой индустрии. Теория и практика функциональной устойчивости к кибератакам / Под редакцией профессора РАН, доктора технических наук Д.П. Зегжды. – М.: Горячая линия - Телеком, 2020. – 560 с.
6. Добрышин М.М. Выбор структуры и механизмов адаптивного управления системы обеспечения информационной безопасности // Известия Тульского государственного университета. Технические науки, 2022. – № 2. – С. 214-222.
7. Давлятова М.А., Курочкина А.А., Стародубцева В.В. Оценка нормативных документов в области качества услуг, предоставляемых на базе инфотелекоммуникационной сети // Перспективы науки, 2016. – № 12 (87). – С. 107-110.
8. Давлятова М.А., Стародубцев Г.Ю., Хныкина Т.С. Эволюция развития теории и практики управления качества // Международный технико- экономический журнал, 2017. – № 2. – С. 82-85.
9. Добрышин М.М., Горбуля Д.С. Подходы оценки качества связи и предоставления услуг связи и задачи по их совершенствованию в рамках обеспечения информационной безопасности // Экономика и качество систем связи, 2023. – № 3 (29). – С. 60-71.
10. Давлятова М. А., Стародубцев Ю. И. Оценка и управление качеством функционирования высших учебных заведений в условиях глобализации // Планирование и обеспечение подготовки кадров для промышленно-экономического комплекса региона, 2017. – Т. 1. – С. 228-230.
11. Белов А.С., Добрышин М.М., Шугуров Д.Е. Функциональный подход к комплексной оценке уровня информационной безопасности элемента корпоративной сети связи // Приборы и системы. Управление, контроль, диагностика, 2023. – № 3. – С. 30-39.
12. Белов А.С., Добрышин М.М., Горшков А.Н., Шугуров Д.Е. Предложение по определению эксплуатационной надежности программного обеспечения сложных

технических систем // Известия Тульского государственного университета. Технические науки, 2022. – № 9. – С. 143-148.