



УДК 339.54

КОНЦЕПЦИЯ РАЗРАБОТКИ ЦИФРОВОЙ ПЛАТФОРМЫ ОСНАЩЕНИЯ ТАМОЖЕННЫХ ОРГАНОВ ТЕХНИЧЕСКИМИ СРЕДСТВАМИ ТАМОЖЕННОГО КОНТРОЛЯ НА БАЗЕ ПЛАНШЕТНЫХ ТЕХНОЛОГИЙ

П. Н. Афонин, А. Ю. Лебедева

Санкт-Петербургский им. В.Б. Бобкова филиал Российской таможенной академии

В статье предлагается способ повышения эффективности осуществления таможенного контроля с применением технических средств путем внедрения в таможенные органы унифицированной цифровой платформы; анализируются ее преимущества и предлагаются способы минимизации рисков, связанных с ее применением.

Ключевые слова: унифицированная цифровая платформа, фактический таможенный контроль, цифровизация, технические средства таможенного контроля, оптимизация.

Для цитирования:

Афонин П. Н., Лебедева А. Ю. Концепция разработки цифровой платформы оснащения таможенных органов техническими средствами таможенного контроля на базе планшетных технологий // Системный анализ и логистика: журнал.: выпуск №2(24), ISSN 2007-5687. – СПб.: ГУАП., 2020 – с. 51-61. РИНЦ.

THE CONCEPT OF THE DEVELOPMENT OF A DIGITAL PLATFORM FOR EQUIPMENT OF CUSTOMS AUTHORITIES WITH TECHNICAL MEANS OF CUSTOMS CONTROL ON THE BASIS OF TABLET TECHNOLOGIES

P. N. Afonin, A. Yu. Lebedeva

Russian Customs Academy St.-Petersburg branch named after Vladimir Bobkov

The article proposes a way to improve the efficiency of customs control using technical means by introducing a unified digital platform into the customs authorities; its advantages are analyzed and ways to minimize the risks associated with its use are proposed.

Keywords: unified digital platform, actual customs control, digitalization, technical means of customs control, optimization.

For citation:

Afonin P. N., Lebedeva A. Yu. The concept of the development of a digital platform for equipment of customs authorities with technical means of customs control on the basis of tablet technologies // System analysis and logistics.: №2(24), ISSN 2007-5687. – Russia, Saint-Petersburg.: SUAI., 2020 – p. 51-61.

Введение

В рамках цифровизации федеральных органов исполнительной власти качественные изменения претерпевает Федеральная таможенная служба России (далее – ФТС России) [1, 2], необходимость повышения эффективности деятельности которой объясняется ее значимостью в формировании государственного бюджета. Подтверждением этому выступают находящиеся в открытом доступе на официальном портале бюджетной системы России «Электронный бюджет» статистические данные о том, что совокупность доходов, поступивших от ФТС России, составила 47,6% от всех доходов (6 742 млрд руб. из 14 172 млрд руб.) [3]. При этом, ключевым элементом системы таможенных органов, обеспечивающим получение информации о реальных характеристиках перемещаемых товаров, являются подразделения фактического таможенного контроля, оснащенные парком технических средства таможенного контроля (далее – ТСТК) [4]. Однако, по причине постоянной модернизации технического обеспечения, направленной на непрерывное привлечение достижений научно-технического прогресса для эффективной борьбы с новыми схемами нарушения таможенного законодательства, программная и аппаратная составляющая ТСТК приобретает



определенную разрозненность и неунифицированность. Многообразие системных программных средств и мобильных технологий, обеспечивающих работу аппаратной части ТСТК, приводит к увеличению необходимых для обеспечения таможенного контроля материальных и человеческих ресурсов, затрат на эксплуатацию, становится потенциальной причиной уязвимости информационно-технического обеспечения таможенного контроля в целом.

Актуальной проблеме унификации и оптимизации структуры и состава ТСТК уже были посвящены работы авторов и таких ученых, как В.Г. Анисимов, Е.Г. Анисимов, Т.Н. Сауренко, позволивших сформировать системное понимание сложившейся ситуации и определить математический аппарат решения проблемы на глобальном уровне [5, 6]. Направлением настоящей работы является развитие научно-методических принципов оптимизации имеющегося в таможенных органах парка ТСТК на основе предлагаемой концепции унифицированной цифровой платформы [7] (далее – УнЦиП), развертывание которой возможно на доступных по ряду выбранных характеристик планшетных компьютерах с возможностью загрузки и обновления их прикладного программного обеспечения из единого информационного ресурса по аналогии с ресурсом Google «Play Маркет», обязанность формирования и обслуживания которого представляется целесообразным возложить на Центральное информационно-техническое таможенное управление – интегратор процессов по техническому обслуживанию информационно-техническому обеспечению ФТС России.

Анализ данных о реальном использовании ТСТК с целью проведения проверочных мероприятий в результате срабатывания системы управления рисками (таблица 1) свидетельствует о незначительной интенсивности применения отдельных видов ТСТК при достаточно сходном по ресурсоемкости и типу их аппаратно-программных платформ. Иными словами, у таможенных органов имеется редко используемое оборудование с практически одинаковой компьютерной базой. В связи с этим, помимо вопроса пересмотра количества единиц техники на оснащении таможенных органов, актуальным является пересмотр парадигмы оснащения таможенных органов со смещением акцентов на реализацию парадигмы унифицированной цифровой платформы на базе планшетных технологий как инструмента оптимизации комплектного состава ТСТК [7]. Аналогичный подход уже успешно зарекомендовал себя в других силовых ведомствах России, например, в МВД, где в настоящее время функционирует цифровая платформа на базе ОС «Astra Linux Special Edition» – разработке НПО «Русские базовые информационные технологии».

Таблица 1 – Эксплуатация сложных ТСТК за IV квартал 2019 года

№	ТСТК	Кол-во ТСТК на оснащении	Количество применений	Количество не используемых ТСТК	
				шт.	%
1.	ПРФА «МетЭксперт»	278	594	132	47
2.	СПИДК «Контроль»	137	51	94	69
3.	ПРА «ХимЭксперт»	148	159	85	57
4.	Регула 7505-М	213	6114	143	67

Анализ размещенных на сайте zakupki.gov.ru технических заданий на обеспечение таможенными органами ряда ТСТК позволил сделать вывод, что критерии выбора портативных компьютеров и программного обеспечения являются сходными, однако единых, нормативно установленных требований к компьютерной части ТСТК нет. Для каждого вида ТСТК формулируются отдельные перечни критериев при размещении технического задания в рамках государственных закупок, что, в конечном итоге, приводит к ряду проблем, выявленных, в том числе по результатам проводившихся авторами экспертных опросов:

1. отсутствию унифицированного подхода к обеспечению информационной безопасности;
2. невозможности автоматического обновления программных продуктов, что противоречит концепции модернизации сферы обеспечения таможенных услуг путем цифровизации;



3. необходимости принудительного обновление баз данных эталонных объектов по запросу пользователя. Расширение перечня веществ, входящих в состав товаров, перемещаемых через таможенную границу, предполагает постоянное обновление баз таможенных органов, однако в настоящее время функция их автоматического обновления не предусмотрена, а единый ресурс и система администрирования для обновления – отсутствует;
4. приросту массогабаритных характеристик ТСТК за счет обязательного включения в конструкцию ноутбука со встроенным прикладным программным обеспечением, в то время как характеристики планшетных компьютеров в ряде случаев могут даже превышать характеристики ноутбуков;
5. росту числа неисправностей, обусловленных эпизодичностью использования ТСТК отдельных видов.

Решение указанных проблем лежит в плоскости внедрения концепции УнЦиП на базе планшетных технологий, параметры которых (см. табл. 2) определены в рамках комплекса проведенных авторами исследований по разработке событийно-ориентированной модели таможенного контроля при использовании унифицированной цифровой платформы ТСТК, а также математической модели информационной безопасности унифицированной цифровой платформы ТСТК на базе планшетных технологий.

Таблица 2 – Матрица оптимальных параметров унифицированной цифровой платформы

№	Показатель	Критерий	Оптимальное значение
1.	Операционная система	Источник разработки	Российское производство
		Объем	≤ 8 Гб
		Стоимость 1 лицензии	5-6 тыс. руб.
		Обновление в фоновом режиме	Да
2.	Программное обеспечение	Ресурс	Единый
		Объем	1-1,5 Гб
		Необходимость повышения квалификации для работы	Нет
3.	Базы данных	Автоматическое обновление	Да
4.	Информационная безопасность	Совместимость антивирусных программ	Да
		Поддержка электронной цифровой подписи	Да
5.	Технические характеристики прикладного ПК	Вес	≤ 600 г
		Диагональ/разрешение экрана	10.1” / 1920x1080
		Количество USB-портов	≥ 2
		Объем памяти	≥ 16 Гб

В основу построения субъектно-ориентированной модели таможенного контроля с использованием унифицированной цифровой платформы была положена система оценки рисков НАЗОР, предназначенная для выявления угроз при внедрении и эксплуатации сложных технологий путем выявления «слабых мест» в функционировании системы (ГОСТ Р 51901.11-2005 Менеджмент риска. Исследование опасности и работоспособности. Прикладное руководство). Поскольку сложные ТСТК, которые предлагается оснастить планшетными компьютерами для функционирования цифровой платформы, применяются преимущественно на постах фактического контроля для осуществления таможенного контроля товарных партий и транспортных средств, перемещаемых через таможенную границу в качестве эталонного средства для исследования



событийно-ориентированной траектории была выбрана «Регула 7505-М», предназначенная для идентификации VIN-номеров автотранспортных средств, комплектация которой подразумевает наличие портативного компьютера с предустановленным программным обеспечением «НУКА», функционирующим на базе операционной системы MS Windows. В рамках парадигмы УнЦиП предполагается, что ноутбук будет заменен на планшетный компьютер на базе операционной системы Linux российских разработчиков с установленным программным обеспечением.

Исследование алгоритма осуществления операций при использовании «Регулы 7505-М» позволило определить потенциальные «слабые места», характеризующиеся возможностью появления рискованных ситуаций:

1. R_1 – риск некорректной работы операционной системы вследствие ошибочных действий должностных лиц таможенных органов. Несмотря на преимущества операционной системы Linux (надежность в рамках обеспечения информационной безопасности, небольшой объем занимаемой памяти и дистрибутивов, невысокая стоимость официальной лицензии и т.д.), некорректные действия пользователя могут привести к нарушению целостности программного кода, выходу из строя операционной системы.
2. R_2 – риск технической неисправности планшета, обусловленной возможно слабым контролем за техническим состоянием ТСТК отдельными должностными лицами таможенных органов.
3. R_3 – риск ошибочных действий должностных лиц таможенных органов в процессе работы в прикладной программе «Регулы 7505-М». В настоящее время должностные лица отмечают сложность интерфейса программного обеспечения, обеспечивающего работу с ТСТК как один из существенных недостатков в процессе проведения таможенного контроля, что, по их мнению, может привести к совершаемым ими ошибкам при проведении таможенного контроля.
4. R_4 – риск ошибки анализа идентифицированного VIN-номера транспортного средства с использованием не обновлённого программного обеспечения сопровождающего «Регулу 7505-М».

В соответствии с методикой HAZOP предложена рабочая матрица, в которой отражаются риски отклонения в процессе проведения таможенного контроля. Информация, полученная в результате анализа на основе алгоритма функционирования «Регулы 7505-М» представлена в табл. 3.

Аналитическая составляющая HAZOP основана на внедрении «управляющих слов», позволяющих сформулировать ответы на проблемные вопросы, выявленные при идентификации отклонений (см. табл. 4). В качестве рекомендаций для уменьшения последствий или полной ликвидации выявленного ряда проблем предлагается:

1. Ограничить доступ пользователей к программному коду системы, что позволит избежать несанкционированного вмешательства в работу системного программного обеспечения
2. Использовать один планшет для работы с различными видами ТСТК – на каждом планшете должно быть установлено программное обеспечение, соответствующее каждому техническому средству.
3. Обеспечить возможность установки и обновления прикладного программного обеспечения и соответствующих баз данных из единого унифицированного ресурса.

Таблица 3 – Матрица рисков внедрения УЦП ТО в процессе применения ТСТК

№	Управляющее слово	Рисковая ситуация	Предпосылки	Последствия	Пути решения
1.	НЕТ	Некорректная работа	Сложность программного кода ОС	Невозможность запустить ТСТК и провести	Разграничение доступа пользователей



		дистрибутивов ОС Linux	Отсутствие навыков работы ДЛТО в системе	таможенный контроль	Повышение квалификации ДЛТО
2.	НЕТ	Техническая неисправность планшета	Повреждение элементов платы внутри планшета	Невозможность запустить ТСТК для проведения таможенного контроля	Регулярная техническая проверка планшетов
			Завершение срока действия аккумулятора		Оснащение постов большим количеством планшетов на базе УЦП ТО
			Повреждения шлейфа экрана		
			Подключение несовместимых девайсов к планшету		
			Недостаточный уровень заряда аккумулятора		
3.	ТАК ЖЕ, КАК	Ошибочные действия ДЛТО	Отсутствие навыков работы ДЛТО в системе	Недостовверная идентификация	Повышение квалификации ДЛТО
4.	ДРУГОЙ, ЧЕМ	Ошибочная идентификация VIN-номера автотранспортного средства	Недостаточное разрешение экрана планшетного компьютера	Возможность невыявления факта нарушения законов	Выбор наиболее оптимального планшета в соответствии с моделью оценивания
				Снижение эффективности таможенного контроля в целом	

Таблица 4 – Расшифровка управляющих слов методологии HAZOP в рамках оценки УЦП ТО

№	Управляющее слово	Описание
1.	НЕТ	Функция (целевое назначение) не осуществляется; параметр не реализуется
2.	ТАК ЖЕ, КАК	Выполняется некорректная операции (шаг)
3.	ДРУГОЙ, ЧЕМ	Результат не соответствует первоначальной цели

Эффективное применение парадигмы УнЦиП основывается на использовании современных ИТ-технологий в рамках обеспечения необходимых для проведения таможенного контроля функций технических средств с помощью специального программного обеспечения. В качестве общих задач таких программных продуктов можно выделить следующее:

1. сбор, обработка и хранение данных, полученных в результате таможенного контроля с применением ряда сложных ТСТК, оснащенных планшетными компьютерами;
2. моментальный анализ данных, подразумевающий сверку полученной информации с эталонными образцами из библиотек;



3. создание отчетов в стандартизированном виде с целью оптимизации временных ресурсов таможенных органов;
4. формирование новых библиотек эталонных образцов;
5. возможность контролировать пользовательскую активность (каждый случай использования сложного ТСТК) для минимизации риск неправомерных действий должностных лиц, связанных с фактическим таможенным контролем товаров и транспортных средств международной перевозки.

В целях обеспечения функционирования УнЦиП предлагается также внедрить:

1. беспроводную технологию управления аппаратной частью ТСТК (системой датчиков и преобразователей), в настоящее время управление компонентами ППИДК «Контроль» осуществляется только посредством интерфейсов USB, что на практике приводит к повышенному износу соответствующих портов USB;
2. облачное хранение данных, предусмотренное концепцией цифровизации. Управления такими хранилищами целесообразно возложить на подразделения ЦИТТУ в связи с тем, что подобные задачи уже указаны в Положении о данном управлении [8].

Применение облачных хранилищ данных также предполагает:

- существенное расширение БД за счет увеличения объема памяти, что может привести к минимизации риска отсутствия эталонного образца для каждого факта использования ТСТК;
- контроль пользовательской активности посредством протокола передачи данных Cloud Gateway, с целью минимизации рисков неправомерных действий должностных лиц, связанных с фактическим таможенным контролем.

Процесс управления техническими средствами и анализ данных, полученных в результате контрольных мероприятий представлен на рисунке 2.

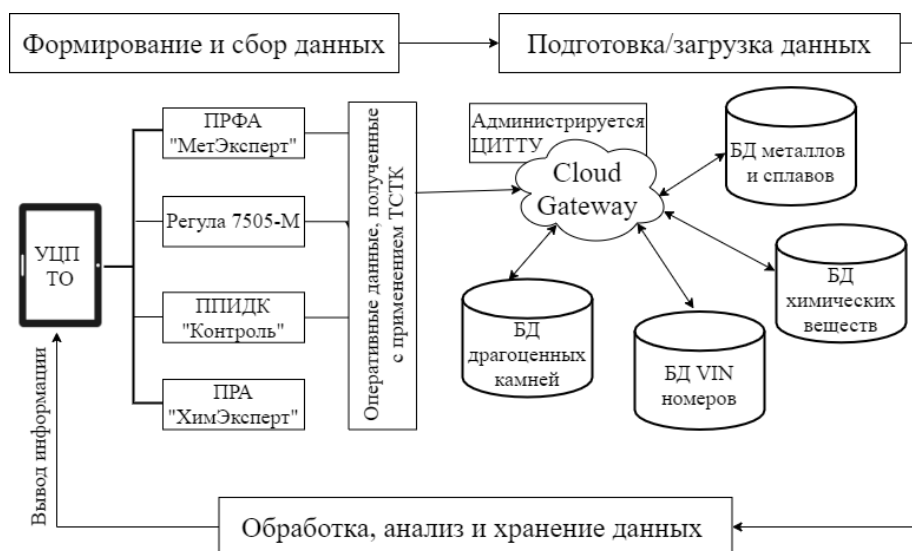


Рис. 2. Концепция реализации задачи анализа данных, полученных в ходе применения ТСТК

Для корректного функционирования унифицированной цифровой платформы таможенных органов обязательным условием является внедрение оптимальной системы защиты информации, обусловившей необходимость построения математической модели информационной безопасности в условиях внедрения парадигмы УнЦиП.

Поскольку оценка эффективности системы обеспечения информационной безопасности от несанкционированного доступа основывается на критерии защищенности, в качестве основных его параметров введены следующие показатели:



1. $C_{инф}$ – ценность защищаемой информации.
2. $P_{взл}$ – вероятность утечки информации в результате несанкционированного доступа.
3. $Ц_{СИ}$ – стоимость обеспечения функционирования системы обеспечения информационной безопасности от кибератак.
4. $П_{СИ}$ – производительность системы защиты унифицированной цифровой платформы.

Защищенность системы в условиях внедрения парадигмы УнЦиП предлагается рассчитывать следующим образом:

$$Z = f(C_{инф}, P_{взл}, Ц_{СИ}, П_{СИ}).$$

Оптимизационная задача заключается в достижении максимального значения критерия в математическом выражении при минимальных затратах на обеспечение функционирования системы защиты информационной безопасности [9]. Для оценки уровня защищенности предлагается ввод дополнительного параметра – риска – с целью последующей мультипликативной сверки основных параметров оценки критерия защищенности:

$$R(p) = C_{инф} * p_{взл},$$

где $p_{взл}$ – вероятность утечки данных в результате несанкционированного доступа.

Также риск предлагается рассчитывать как потери данных за единицу времени:

$$R(\lambda) = C_{инф} * \lambda_{взл},$$

где $\lambda_{взл}$ – интенсивность успешных попыток несанкционированного доступа к таможенной информации через унифицированную цифровую платформу.

$$P_{взл} = \frac{\lambda_{взл}}{\Lambda},$$

где Λ – общая интенсивность потока попыток кражи информации путем несанкционированного доступа через унифицированную цифровую платформу.

В рамках оценки эффективности системы обеспечения информационной безопасности предлагается рассматривать коэффициент защищенности – критерий, обозначающий относительное значение уменьшения риска в защищенной информационной системе в сравнении с системой, не обладающей защитой от кибератак.

Коэффициент защищенности рассчитывается следующим образом:

$$D\% = \left(\frac{R_{защ}}{R_{незащ}} \right) \cdot 100\%,$$

где $R_{защ}$ – риск кражи информации в защищенной системе в рамках платформы; $R_{незащ}$ – риск кражи информации в незащищенной системе.



В связи с этим, задачу оптимизации можно визуализировать следующим образом:

$$\begin{cases} D(C_{инф}, p \dots) \rightarrow \max; \\ C_{СЗИ} \rightarrow \min; \\ П_{СЗИ} \rightarrow \max. \end{cases}$$

Далее необходимо ввести ограничения с целью приведения системы к виду однокритериальной:

$$\begin{cases} D(C_{инф}, p_{взл}) \rightarrow \max; \\ C_{СЗИ} \leq C_{зад}; \\ П_{СЗИ} \geq П_{зад}. \end{cases}$$

где $C_{зад}$ – заданные ограничения на стоимость внедрения и эксплуатации системы обеспечения информационной безопасности унифицированной цифровой платформы таможенных органов; $П_{зад}$ – заданные ограничения на производительность системы.

Такой параметр как $П_{СЗИ}$ необходимо рассчитывать на основе теории массового обслуживания и теории расписаний. Помимо этого, представляется возможным определение ограничения производительности системы обеспечения информационной безопасности не через требуемую производительность, а посредством $dП_{СЗИ}$ – снижения производительности информационной системы цифровой платформы таможенных органов от устанавливаемой системы защиты данных. Так задача оптимизации примет вид:

$$\begin{cases} D(C, p \dots) \rightarrow \max; \\ C_{СЗИ} \rightarrow \min; \\ dП_{СЗИ} \rightarrow \min. \end{cases}$$

В результате приведения задачи к однокритериальной, она будет выглядеть следующим образом:

$$\begin{cases} D(C, p \dots) \rightarrow \max; \\ C_{СЗИ} \leq dП_{зад}; \\ dП_{СЗИ} \leq dП_{зад}. \end{cases}$$

Далее предлагается определение D через параметры вероятных угроз. С целью упрощения модели вводятся следующие элементы:

1. w – количество видов угроз кражи информации.
2. $C_i(i=\overline{1, w})$ – потери от угроз i -того вида.
3. $\lambda_i(i=\overline{1, w})$ – интенсивность взломов i -того вида.
4. $Q_i(i=\overline{1, w})$ – потенциальная возможность угроз i -того вида в совокупности попыток взлома при условии, что

$$Q_i = \frac{\lambda_i}{\Lambda}.$$

5. $p_i(i=\overline{1, w})$ – вероятность ожидания угроз i -того вида.



В соответствии с заданными значениями, коэффициент потерь от взлома будет рассчитываться следующим образом:

$$R(p) = \sum_l^w R_i(p) = \sum_l^w C_i * p_{взл\ i},$$

где $R_i(p)$ – коэффициент потерь от несанкционированного доступа к информации унифицированной цифровой платформы таможенных органов i -того вида.

Для системы, не обеспеченной защитой информации справедливым будет утверждение, что $p_{взл\ i} = Q_i$, а для защищенной системы – $p_{взл\ i} = Q_i * (1 - p_i)$. Коэффициент потерь от взлома за единицу времени примет следующий вид:

$$R(\lambda) = \sum_l^w R_i(\lambda) = \sum_l^w C_i * \lambda_{взл\ i},$$

где $R(\lambda)$ – коэффициент потерь от несанкционированного доступа i -того вида за заданную единицу времени.

Для незащищенной системы задается условие, что $\lambda_{взл\ i} = \lambda_i$, а для защищенной системы – $\lambda_{взл\ i} = \lambda_i * (1 - p_i)$.

Получается следующее выражение:

$$D = 1 - \frac{\sum_l^w C_i * Q_i * (1 - p_i)}{\sum_l^w C_i * Q_i} = 1 - \frac{\sum_l^w C_i * \lambda_i * (1 - p_i)}{\sum_l^w C_i * \lambda_i}.$$

В рамках построения математической модели системы обеспечения ИБ обязательным условием являются определенные исходные параметры, на которых основывается объективная оценка степени защищенности такой системы. Однако при осуществлении практических расчетов возникает проблема определения входных параметров для системы защиты – вероятностей и интенсивностей угроз. Существует множество методов задания таких параметров; в условиях представленной модели предлагается использовать оптимистически-пессимистический подход, а именно, способ равных интенсивностей, согласно которому $\forall \lambda_i = \alpha, \alpha = const$. Способ подразумевает выбор любой константы α .

В конечном виде способ равных интенсивностей для оценки степени защищенности информации унифицированной цифровой платформы таможенных органов примет следующий вид:

$$\begin{aligned} D &= 1 - \frac{\sum_l^w C_i * \lambda_i * (1 - p_i)}{\sum_l^w C_i * \lambda_i} = 1 - \frac{\sum_l^w C_i * \alpha * (1 - p_i)}{\sum_l^w C_i * \alpha} = \\ &= 1 - \frac{\alpha * \sum_l^w C_i * (1 - p_i)}{\alpha * \sum_l^w C_i} = 1 - \frac{\sum_l^w C_i * (1 - p_i)}{\sum_l^w C_i}. \end{aligned}$$

В данном случае защищенность будет зависеть только от степени потери информации в результате несанкционированного доступа к ней. Установление соответствия между стоимостью потерь и интенсивностью угроз возможно с использованием статистического анализа, однако в случае отсутствия реальных данных, в целях выполнения оценки возможно применить пессимистический подход, основанный на принятии утверждения, что в рамках несанкционированного доступа к информации УнЦиП наносится наибольший вред.

Таким образом, проведенное исследование позволило сформировать ключевые позиции научно-методического обеспечения парадигмы УнЦиП, позволяющей снизить затраты таможенных



органов на закупку и обслуживание разнотипных компьютерных подсистем, входящих в состав ТСТК, повысить эффективность использования имеющихся ресурсов, при поддержании уровня информационной безопасности на необходимом уровне, реализовать на практике требования по реализации программы импортозамещения в таможенных органах.

СПИСОК ЛИТЕРАТУРЫ

1. Стратегия развития таможенной службы Российской Федерации до 2020 года (утв. Распоряжением Правительства РФ от 28 декабря 2012 г. № 2575-р) // Официальный сайт ФТС РФ. – Режим доступа: <http://customs.ru> (дата обращения: 03.03.2020).
2. *Чикишев Н.С.*, Афонин П.Н. К вопросу о влиянии процесса экономических трансформаций на инновационное развитие таможенных органов Российской Федерации // Управление экономическими системами: электронный научный журнал. 2017. № 12 (106). С. 9.
3. Электронный бюджет // Единый портал бюджетной системы Российской Федерации. – Режим доступа: http://budget.gov.ru/epbs/faces/page_home?_adf.ctrl-state=zw88od3gb_4®ionId=40 (дата обращения: 03.03.2020).
4. *Афонин П.Н.*, Афонин Д.Н. Основы применения технических средств таможенного контроля: учебник / П.Н. Афонин, Д.Н. Афонин. СПб.: Российская таможенная академия, РИО Санкт-Петербургского имени В.Б. Бобкова филиала, 2018. – 302 с.
5. *Анисимов В.Г.* и др. Модель и метод оптимизации решений при управлении развитием технических средств таможенного контроля / В.Г. Анисимов, Е.Г. Анисимов, П.Н. Афонин, М.Р. Гапов, Т.Н. Сауренко // В сборнике: Таможенные чтения - 2017. Современная наука и образование на страже экономических интересов Российской Федерации сборник материалов Всероссийской научно-практической конференции с международным участием: В 3 т. 2017. – С. 11-21.
6. *Афонин П.Н.* Системный анализ и управление в таможенном деле : учебн. пособие. СПб.: ИЦ «Интермедия», 2012. 360 с.
7. *Афонин П.Н.*, Лебедева А.Ю. Внедрение унифицированной цифровой платформы оснащения ТСТК на базе планшетных технологий // Таможенные чтения-2019. Наука и образование в условиях становления инновационной экономики. СПб.: РИО Санкт-Петербургского филиала Российской таможенной академии, 2019. – Т. 1. – 296 с.
8. Положение о ЦИТТУ / Официальный сайт ФТС РФ. – Режим доступа: <http://customs.ru> (дата обращения: 04.03.2020).
9. *Щеглов А.Ю.* Защита компьютерной информации от несанкционированного доступа. СПб.: Наука и техника, 2004. – 384 с.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Афонин Петр Николаевич –

д.т.н., доцент, заведующий кафедрой технических средств таможенного контроля и криминалистики Санкт-Петербургский имени В.Б.Бобкова филиал Российской таможенной академии
192241, Россия, Санкт-Петербург, Софийская ул., д. 52, лит. А
E-mail: pnafonin@yandex.ru

Лебедева Анастасия Юрьевна –

студент 5 курса факультета таможенного дела
Санкт-Петербургский имени В.Б.Бобкова филиал Российской таможенной академии
192241, Россия, Санкт-Петербург, Софийская ул., д. 52, лит. А
E-mail: lebedewa.nastena2011@yandex.ru



INFORMATION ABOUT THE AUTHORS

Afonin Petr Nikolaevich –

Doctor of Technical Sciences, Associate Professor, Head of the Department of Technical Means of Customs Control and Criminalistics

Saint-Petersburg Branch named after V.B.Bobkov of Russian Customs Academy

52, Sofiyskaya str., St. Petersburg, 192241, Russia

E-mail: pnafonin@yandex.ru

Lebedeva Anastasia Yurievna –

5th year student of the Faculty of Customs

Saint-Petersburg Branch named after V.B.Bobkov of Russian Customs Academy

52, Sofiyskaya str., St. Petersburg, 192241, Russia

E-mail: lebedewa.nastena2011@yandex.ru