Для цитирования: *А.М. Каднова. Экспериментальная оценка операционных характеристик систем защиты информации. Вестник Дагестанского государственного технического университета. Технические науки. 2021; 48 (1): 90-99. DOI:10.21822/2073-6185-2021-48-1-90-99*
For citation: *A.M. Kadnova. Experimental evaluation of the operational characteristics of information protection systems. Herald of Daghestan State Technical University. Technical Sciences. 2021; 48 (1): 90-99. (In Russ.) DOI:10.21822/2073-6185-2021-48-1-90-99*

ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ
COMPUTER SCIENCE, COMPUTER ENGINEERING AND MANAGEMENT

УДК 621.3
DOI: 10.21822/2073-6185-2021-48-1-90-99

ЭКСПЕРИМЕНТАЛЬНАЯ ОЦЕНКА ОПЕРАЦИОННЫХ ХАРАКТЕРИСТИК СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

А.М. Каднова
Воронежский институт МВД России,
394065, г. Воронеж, пр-т Патриотов, 53, Россия

Резюме. Цель. *Статья посвящена решению практической проблемы оценки операционного показателя характеристики качества функционирования системы защиты информации (СЗИ) «Удобство использования».* ***Метод.*** *Оценка операционных характеристик программных систем может выполняться теоретически и экспериментально. Так как теоретическая оценка операционных характеристик имеет ряд недостатков и ограничений целесообразна экспериментальная оценка. При этом в качестве основного показателя характеристики качества функционирования СЗИ «Удобство использования» целесообразно использовать показатель «Сложность» типовой операции выполняемой администратором безопасности, выражающий среднее время ее выполнения. Экспериментальная оценка операционных характеристик СЗИ осуществлялась с использованием методов отслеживания движения взгляда и мыши.* ***Результат.*** *В статье приведена оценка показателя «Сложность» всех типовых операций, выполняемых администратором безопасности при эксплуатации СЗИ «Страж NT 3.0» в соответствии с программной документацией.* ***Вывод****. Полученные значения показателя «Сложность» могут быть использованы при формировании плана работ по эксплуатации, сопровождению и обслуживанию автоматизированных систем (АС) в защищенном исполнении, в частности, установленной на ней СЗИ, при проведении оценки своевременности выполнения перечисленных работ, а также при обосновании структуры подразделений, ответственных за защиту информации, и их численности.*

Ключевые слова: *автоматизированная система, система защиты информации, защита информации, операционный показатель, администратор безопасности, пользовательский интерфейс*

EXPERIMENTAL EVALUATION OF THE OPERATIONAL CHARACTERISTICS OF INFORMATION PROTECTION SYSTEMS

A.M. Kadnova
Voronezh Institute of the Ministry of Internal Affairs of Russia,
53 Patriotov Ave., Voronezh 394065, Russia

Abstract. Objective. *The article is devoted to solving the practical problem of evaluating the operational indicator of the quality characteristics of the information security system usability.* ***Methods****. Evaluation of the operational characteristics of software systems can be performed theoretically and by measurement. Since the theoretical assessment of operational characteristics has some disadvantages and limitations, an experimental assessment is advisable. Simultaneously, it is advisable to*

use the "Complexity" indicator of a typical operation performed by a security administrator, which expresses the average time of its execution as the primary indicator of the quality of the functioning of the information security system usability. Measurement evaluation of the operational characteristics of the information security system was carried out using the eye and mouse movement tracking methods. ***Results.*** *The article provides an assessment of the "Complexity" indicator of all typical operations performed by the security administrator during the Sentinel NT 3.0 ISS operation following the program documentation.* ***Conclusion****. The obtained values of the "Complexity" indicator can be used in the formation of a work plan for the operation and maintenance of protected automated systems, in particular, with the installed information security system, when evaluating the timeliness of the performance of the listed works, as well as when justifying the structure of the units responsible for information protection and their quantity.*

Keywords*: automated system, information security system, information security, operational indicator, security administrator, user interface*

Введение. Расширение сфер применения информационных технологий привело к широкому распространению СЗИ в АС различного типа. СЗИ используются в связи с реализацией требований по обеспечению безопасности информации, обрабатываемой АС. СЗИ, как правило, представляет собой самостоятельную программную систему, устанавливаемую в состав защищаемой АС на этапе технической реализации [1]. Наличие СЗИ не только решает проблему обеспечения безопасности обрабатываемой информации, но и вызывает негативные последствия. Одним из таких последствий является неизбежное взаимодействие пользователей АС с СЗИ, которое приводит к снижению характеристики качества функционирования СЗИ «Удобство использования».

На основе анализа программной документации СЗИ и нормативно-правовых актов, посвященных требованиям по защите информации, можно выделить следующие категории персонала АС [2-4]:

1. Обычные пользователи;
2. Администратор безопасности.

Обычный пользователь при взаимодействии с СЗИ использует ее функции в прозрачном для себя режиме.

Важнейшая роль при взаимодействии с СЗИ отведена администратору безопасности, отвечающему за установку, настройку и управление функционированием системы защиты [3]. Администратор безопасности является центральной частью подсистемы защиты, существенно влияющей на уровень защиты АС. Учитывая эргатическую составляющую администрирования в процессе функционирования СЗИ, можно обеспечить соответствие настроек СЗИ требованиям политики безопасности и устранить ошибки в работе всех категорий пользователей, а также оценить дальнейшую работу системы защиты с высокой точностью.

Исследование эргатических процессов подразумевает выбор показателей, которые характеризовали бы возможности и способности человека в процессе администрирования СЗИ. Конструирование показателя, который характеризовал бы качество администрирования СЗИ, является сложной научной задачей. Данный показатель должен учитывать не только способности индивидуума, но и статистические данные о поступающих заявках на выполнение стандартных функций администратором безопасности.

Анализ руководящих документов, а также опыт эксплуатации СЗИ, позволяют выделить следующие категории операций, выполняемых в процессе администрирования [3,5-7]:

1. Установка и настройка системы защиты (создание идентификатора администратора безопасности, задание правил аутентификации пользователей, установка меток конфиденциальности, параметров целостности, принципа контроля доступа, назначение грифа и т.д.);

2. Непрерывный контроль за функционированием АС в защищенном исполнении (контроль адекватности и правильности настроек системы защиты, контроль за соблюдением требований по защите информации обычными пользователями, анализ отчетов о работе системы

защиты по журналу регистрации и т.п.);

3. Адекватное реагирование на возникающие в процессе обеспечения безопасности информации инциденты и внештатные ситуации в соответствии с установленной политикой и «Обязанностями администратора безопасности».

Каждая типовая технологическая операция, выполняемая администратором безопасности, характеризуется следующими показателями:

1. Состав – показатель, определяющий порядок действий администратора при взаимодействии с интерфейсом СЗИ в процессе выполнения типовой технологической операции;

2. Время выполнения – комплексный (операционный) показатель, формируемый на основе показателей элементарных действий администратора безопасности и позволяющий провести оценку среднего времени выполнения типовой операции, а также построить временной профиль операции;

3. Частота – показатель, определяющий, какое количество раз администратор безопасности выполнит типовую технологическую операцию. Высокий показатель частоты выполнения типовой технологической операции определяет ее важность.

В данной статье не рассматривается показатель частоты выполнения операций администратором безопасности, так как его оценка уже проводилась в ряде исследований [8,11].

При решении вопросов, связанных с внедрением и эксплуатацией системы защиты в составе АС в защищенном исполнении наиболее важным является определение операционных показателей СЗИ как основы подразделения по защите информации, в том числе документальной базы, регламентирующей планы мероприятий и внутренних проверок по обеспечению безопасности информации [9, 10].

Постановка задачи. Целью исследования является разработка методики экспериментальной оценки операционных характеристик СЗИ и представление результатов их оценки.

Методы исследования. Проведем анализ методов оценки операционного показателя, выражающего среднее время выполнения операции администратором безопасности, назовем его «Сложность».

Теоретический анализ комплексного показателя времени выполнения операции пользователем можно выполнить путем использования законов Хика и Фиттса [12,13].

Закон Хика используется для количественной оценки времени необходимого пользователю на принятие решения, связанного с выбором одного варианта из нескольких (чем больше вариантов, тем больше времени необходимо на выбор). Латентный период интеллектуальной деятельности пользователя при совершении над объектом любого действия из множества возможных вариантов начинается с момента выбора пользователем этого объекта или действия.

В соответствии с законом Хика, при выборе из *n* вариантов, время на выбор необходимого пропорционально логарифму по основанию 2 от количества вариантов плюс 1. При этом должно выполняться условие равной вероятности всех вариантов.

Закон Хика описывается математическим выражением оценки времени принятия решения следующего вида [12]:

$$T = a + b\log_2(n+1)$$

где

T – общее время реакции;

a и b – константы, которые зависят от задачи и условий и могут быть определены эмпирически;

n – число равновероятных альтернативных вариантов.

Закон Фиттса гласит, что время, необходимое для достижения элемента, прямо пропорционально дистанции до элемента и обратно пропорционально размеру элемента [12]:

$$T = a + b\log_2(D/W+1)$$

где T – среднее время, затрачиваемое на совершение действия;

a – константа, зависящая от выбора устройства ввода и определяемая эмпирически с по-

мощью регрессионного анализа, интерпретируется как задержка;

b – константа, зависящая от выбора устройства ввода и определяемая эмпирически с помощью регрессионного анализа, описывает ускорение;

W – ширина элемента, измеренная вдоль оси движения устройства ввода;

D – дистанция от точки старта до центра элемента, с учетом того, что конечная точка движения должна находиться в пределах $\pm\frac{W}{2}$ от центра элемента.

Таким образом, общее время выполнения операции пользователем можно подсчитать путем комплексного применения законов Хика и Фиттса.

Действия, описываемые законами, как правило, следуют одно за другим (осуществление выбора из множества возможных и попадание в нужный элемент), а, значит, общее время выполнения операции есть сумма значений двух формул. Данные законы, сформулированные как общие принципы взаимодействия человека и машины, оказались не только чрезвычайно важными для развития первых интерфейсов, но и остаются актуальными по сегодняшний день, обретают новые интерпретации и сферы применения.

Недостатком применения данных аналитических методов является ориентировочный и усредненный характер вычислений. Несмотря на то, что оба закона демонстрируют достаточно высокую степень соответствия практическим данным, закон Хика применим только к простым и быстрым решениям в соответствующем контексте, а закон Фиттса в определенных обстоятельствах неверно воспроизводит время, затрачиваемое на движения некоторыми категориями пользователей [14-16].

Оценка операционных показателей СЗИ может быть проведена экспериментально. Одной из распространённых методик, позволяющих оценить временные показатели пользовательских интерфейсов, является технология Eye-tracking (айтрекинг). Это совершенная технология, которая основана на фиксации движения взгляда пользователя с помощью специального оборудования (стационарного, мобильного или портативного) [17].

Вышеописанная методика может быть реализована путем использования специального устройства Tobii Eye Tracker 4C. Данное устройство позволяет отследить направление взгляда пользователя и зарегистрировать движение головы пользователя, в частности, оценить время фиксации взгляда пользователя на элементах интерфейса СЗИ. Данное устройство носит характер дополнения традиционных устройств управления, таких как мышь, клавиатура, сенсорная панель и т.д.

В основе Tobii Eye Tracker 4C лежит метод регистрации контраста между зрачком и радужной оболочкой, возникающего при инфракрасной подсветке глаз. Основным результатом, получаемым в ходе использования данного устройства, являются тепловая карта, которая может быть проанализирована по окончании выполнения операции.

Анализ тепловой карты позволяет сделать вывод о рациональности и эффективности размещения элементов интерфейса, о том какие элементы подвержены большему вниманию пользователя, а какие – меньше (чем дольше пользователь смотрит на определенный элемент или область, тем более теплым цветом они окрашиваются).

Айтрекинговые исследования являются проверенными и актуальными научными методами с мощной методологической базой и направлены на качественный анализ операционных характеристик СЗИ.

Чтобы получить количественные оценки операционных характеристик СЗИ целесообразно применить метод Mouse-tracking. Mouse-tracking (отслеживание курсора) – технология, основанная на использовании специального программного обеспечения и позволяющая отследить и зафиксировать движение и клики мыши пользователя [18].

Вышеописанная методика может быть реализована путем использования специального инструмента IOGraph V1.0.1. Данное приложение позволяет построить карту передвижения мыши по интерфейсу и кликов пользователя по элементам интерфейса СЗИ [19].

Обсуждение результатов. Для проведения экспериментальной оценки операционных

характеристик СЗИ выбрана одна из наиболее часто используемых систем защиты информации «Страж NT 3.0».

Полный перечень типовых операций выполняемых администратором можно составить на основе анализа программной документации [3] и открытых литературных источников [8-10].

Средства администрирования СЗИ «Страж NT 3.0» предназначены для [6]:

1. Управления носителями информации (добавления и удаления зарегистрированных носителей информации, редактирования свойств для групп носителей, экспорта настроек, редактирования свойств носителей);
2. Управления пользователями (создания пользователей, просмотра паролей и идентификаторов, смены пароля пользователей, просмотра и редактирования свойств пользователей, формирования персональных идентификаторов, чтения и очистки идентификаторов);
3. Работы с файлами (редактирования разрешений, изменения владельца, редактирования параметров аудита, назначения грифа, установки режима запуска, редактирования параметров аудита, установки целостности, выполнения проверки целостности);
4. Контроля устройств (редактирования свойств группы устройств, экспорта настроек);
5. Работы с принтерами (редактирования разрешений или смены владельцев, назначения грифа);
6. Работы с журналами событий (работы с группами событий, работы с фильтрами событий, открытия и сохранения журнала событий);
7. Тестирования защиты;
8. Блокировки компьютера;
9. Разблокировки компьютера.

На примере типовой операции «Создание пользователя» с использованием программы «Менеджер пользователей» СЗИ «Страж NT 3.0» рассмотрим подробно состав типовой технологической операции администратора безопасности и экспериментальную оценку его операционного показателя «Сложность».

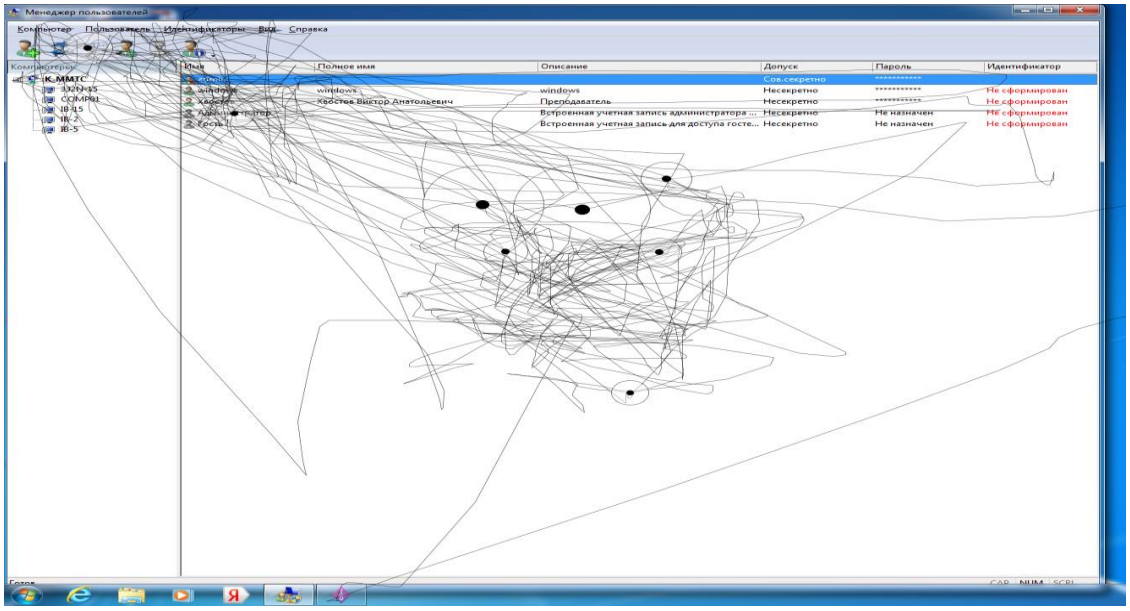

Рис. 1. Интерфейс программы «Менеджера пользователей» СЗИ «Страж NT 3.0» при выполнении типовой операции «Создание пользователя», запись движения курсора и его фиксации на элементах интерфейса, записанная с использованием IOGraph V1.0.1

Fig. 1. Interface of the «User Manager» program of the SZI «Guardian NT 3.0» when performing a typical operation «Create a user», recording the cursor movement and fixing it on the interface elements, recorded using IOGraph V1.0.1

Для создания пользователя в СЗИ «Страж NT 3.0» необходимо запустить программу «Менеджер пользователей», выбрать пункт меню «Компьютер», затем – «Новый пользова-

тель». На экране появится диалоговое окно «Новый пользователь», в котором необходимо ввести полное имя, имя пользователя, описание, пароль и допуск. Далее необходимо нажать кнопку «Создать» [3].

Траектория перемещения курсора и время фиксации его на элементе интерфейса «Менеджера пользователей» СЗИ «Страж NT 3.0», записанная с использованием IOGraph V1.0.1, представлена на рис. 1.

Тепловая карта фиксации взгляда администратора безопасности на элементах интерфейса программы «Менеджер пользователей» СЗИ «Страж NT 3.0», записанная с использованием Tobii Eye Tracker 4C, представлена на рис. 2.

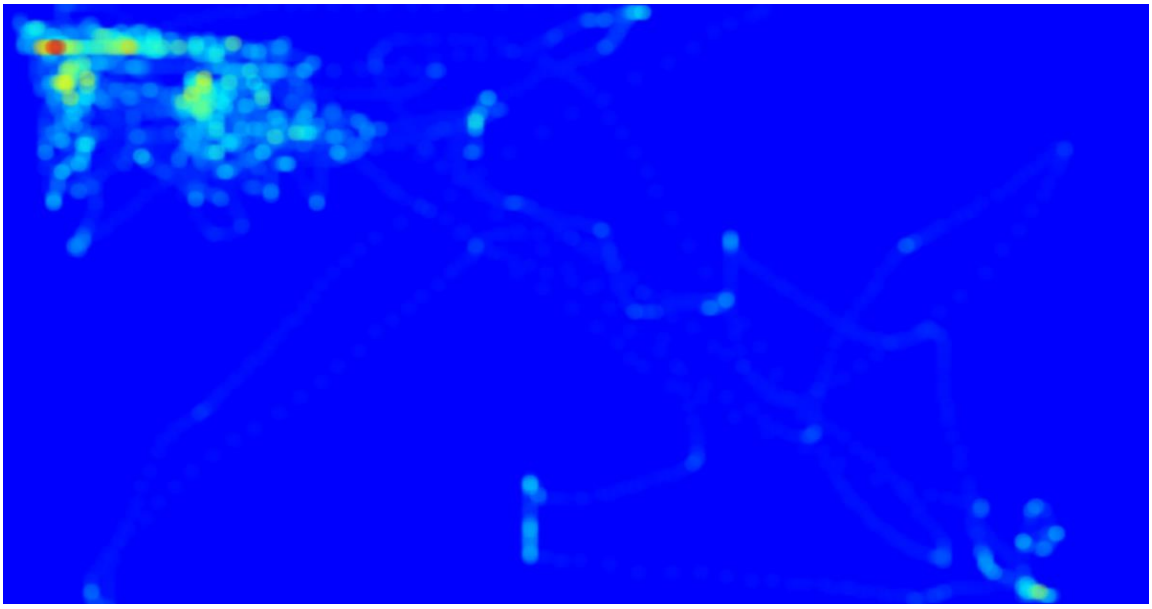

Рис. 2. Тепловая карта фиксации взгляда администратора безопасности на элементах интерфейса программы «Менеджер пользователей» СЗИ «Страж NT 3.0» при выполнении типовой операции «Создание пользователя», записанная с использованием Tobii eye tracker 4C
Fig. 2. Heat map of fixing the security administrator's gaze on the interface elements of the «User Manager» program of the «Guardian NT 3.0» information security facility when performing a typical operation «Create a user», recorded using Tobii eye tracker 4C

Анализ записи перемещения курсора показал, что среднее время выполнения операции по созданию пользователя в СЗИ «Страж NT 3.0» составляет порядка 60 с.

При этом в ходе реализации типовой операции администратором безопасности зафиксированы 6 остановок курсора на элементах диалогового окна длительностью по 5 с и две остановки по 15 с. Таким образом, показатель «Сложность» операции «Создание пользователя» СЗИ «Страж NT 3.0» оставляет величину порядка 60 с.

Тепловая карта фиксации внимания администратора безопасности системы показывает, что при создании пользователя основное внимание было направлено на элементы «Компьютеры» и «Имя пользователя» интерфейса программы «Менеджер пользователей».

Экспериментальная оценка осуществлялась в ходе выполнения лабораторных работ по изучению механизмов защиты, реализованных в СЗИ «Страж NT 3.0». Лабораторные работы выполняли студенты 5 курса при изучении дисциплины «Информационная безопасность организации». Количество студентов – 83.

В результате экспериментальной оценки операционных характеристик СЗИ «Страж NT 3.0» были получены значения, представленные в табл. 1.

Таблица 1. Результаты экспериментальной оценки операционных характеристик СЗИ «Страж NT 3.0»
Table 1. Results of an experimental assessment of the operational characteristics of the SZI «Guard NT 3.0»

№ п.п.	Наименование типовой операции выполняемой администратором Name of a typical operation performed by the administrator	Значение показателя «Сложность» The value of the «Difficulty» indicator
1.	Добавление зарегистрированных носителей информации Adding registered media	60 с
2.	Редактирование свойств для групп носителей Editing Properties for Media Groups	75 с
3.	Редактирование свойств носителей Editing media properties	104 с
4.	Экспорт настроек Export settings	55 с
5.	Создание пользователей Create users	60 с
6.	Просмотр пароля и списка идентификаторов пользователя View password and list of user IDs	35 с
7.	Просмотр и редактирование свойств пользователя Viewing and Editing User Properties	60 с
8.	Смена пароля пользователя Change user password	65 с
9.	Формирование персональных идентификаторов Formation of personal identifiers	55 с
10.	Чтение и очистка идентификаторов Reading and clearing identifiers	45 с
11.	Редактирование разрешений Editing Permissions	120 с
12.	Редактирование параметров системного аудита Editing system audit parameters	40 с
13.	Изменение владельца Change of ownership	35 с
14.	Назначение грифа Neck purpose	35 с
15.	Редактирование параметров дополнительного аудита Editing Additional Auditing Options	50 с
16.	Установка режима запуска и допуска Setting the trigger mode and tolerance	45 с
17.	Установка параметров целостности Setting integrity parameters	45 с
18.	Редактирование разрешений Editing Permissions	120 с
19.	Назначение грифа Neck purpose	75 с
20.	Редактирование свойств для групп устройств Editing properties for device groups	110 с
21.	Экспорт настроек Export settings	50 с
22.	Открытие и сохранение журнала событий Opening and saving the event log	35 с
23.	Работа с фильтром событий Working with an event filter	300 с
24.	Задание группы событий Setting a group of events	290 с
25.	Тестирование системы защиты Testing the protection system	50 с
26.	Блокировка компьютера Locking your computer	30 с
27.	Разблокировка компьютера Unlocking your computer	30 с
28.	Повторная идентификация пользователя Re-identifying a user	100 с

Вывод. Применение специального программно-аппаратного обеспечения, реализующего технологии Eye-tracking и Mouse-tracking, позволяет экспериментально оценить показатель качества функционирования СЗИ «Удобство использования» – «Сложность», который характеризует среднее время выполнения типовых операций администратором безопасности.

В ходе экспериментальной оценки типовых операций, выполняемых администратором безопасности СЗИ «Страж NT 3.0», определенных в «Руководстве администратора» [3], получены операционные характеристики всех типовых операций, выполняемых администратором этой системы.

Анализ значений показателя «Сложность» типовых операций, представленных в табли-

це, показал, что значения показателя определяются количеством элементов интерфейса программы. Наибольшей сложностью, закономерно, характеризуются операции редактирования разрешений для доступа к файловым ресурсам, редактирования разрешений на доступ к принтерам и устройствам, а также работа с фильтром событий и с группами событий.

Малыми значениями показателя «Сложность» характеризуются операции блокировки и разблокировки компьютера.

Полученные значения показателя «Сложность» могут быть использованы при формировании плана работ по эксплуатации, сопровождению и обслуживанию АС в защищенном исполнении, в частности, установленной на ней СЗИ, при проведении оценки своевременности выполнения перечисленных работ, а также при обосновании структуры подразделений, ответственных за защиту информации, и их численности.

Библиографический список:

1. Каднова А.М. Алгоритм создания автоматизированных систем в защищенном исполнении / А.М. Каднова, О.Ю. Макаров, С.А. Мишин, Е.А. Рогозин // Безопасность информационных технологий. 2019. Т. 26. № 4. С. 93–100.
2. Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды : приказ от 14 марта 2014 г. № 31 [Электронный ресурс]. – URL : https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31
3. Система защиты информации «Страж NT». Руководство администратора [Электронный ресурс]. – URL : http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf.
4. Система защиты информации «Страж NT». Руководство пользователя [Электронный ресурс]. – URL : http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf.
5. Довгуля М.М. Оповещение администратора информационной безопасности о нарушениях в работе корпоративной сети / М.М. Довгуля, Р.В. Мещеряков // Научная сессия ТУСУР. 2005 : сб. науч. тр. Томск, 2005. С. 96–97.
6. Яремчук С. Защитник сети / С. Яремчук // Системный администратор. 2003. № 11(12). С. 56–60.
7. Бормотов С.В. Системное администрирование на 100%: монография/С.В. Бормотов. Санкт-Петербург : Питер, 2006. 256 с.
8. Хвостов В.А. Методы и средства повышения защищенности автоматизированных систем : монография / В.А. Хвостов [и др.]. Воронеж: Воронежский институт МВД России, 2013. 108 с.
9. Каднова А.М. Способ оценки операционных характеристик систем защиты информации от несанкционированного доступа на основе / А.М. Каднова, О.И. Бокова, Е.А. Рогозин, Н.С. Хохлов, О.Ю. Макаров // Актуальные проблемы прикладной математики, информатики и механики : сб. науч. тр. Воронеж, 2020. С. 656–659.
10. Каднова А.М. К вопросу о решении научной задачи количественной оценки эргатотехнических характеристик систем защиты информации от несанкционированного доступа в автоматизированных системах ОВД / А.М. Каднова, Е.А. Рогозин // Общественная безопасность, законность и правопорядок в III тысячелетии. 2019. № 5–2. С. 307–310.
11. Скрыпников А.В. Нормирование требований к характеристикам программных систем защиты информации / А.В. Скрыпников, В.А. Хвостов, Е.В. Чернышова, В.В. Самцов, М.А. Абасов // Вестник Воронежского государственного университета инженерных технологий. 2018. Т. 80. № 4(78). С. 96–110.
12. Королев Д.А. Эргономика и юзабилити пользовательского интерфейса программного обеспечения : методическое пособие / Д.А. Королев. Москва: Московский государственный институт электроники и математики (технический университет), 2004. 214 с.
13. Попов А.А. Эргономика пользовательских интерфейсов в информационных системах : учебное пособие /А.А. Попова [и др.]. Москва: Российский экономический университет им. Г.В. Плеханова, 2012. 21 с.
14. Soukoreff R.W. Towards a standard for pointing device evaluation, perspectives on 27 years of Fitts' law research / R.W. Soukoreff I.S. MacKenzie // Int. J. of Human-Computer Stud. 2004. Vol. 61(6). pp. 751–789.
15. Gump A. Application of Fitts' law to individuals with cerebral palsy / A. Gump, M. LeGare, D.L. Hunt // Perceptual and motor skills. 2002. Vol. 94(1). pp. 884–895.
16. Amazeen E.L. The effects of attention and handedness on coordination dynamics in a bimanual Fitts' law task / E.L. Amazeen, S.D. Ringenbach, P.G. Amazeen // Exper. brain research. 2005. Vol. 164(4). P. 484–499.
17. Спирин И.А. Исследование и применение eye-tracking технологии на человеке / И.А. Спирин // Молодой ученый. 2016. №2. С. 227–230.

18. Каднова А.М. Методический подход к оценке вероятностного показателя своевременности выполнения типовых операций администратором системы защиты информации автоматизированной системы /А.М. Каднова // Вестник Дагестанского государственного технического университета. 2019. Т. 46. № 3. С. 87–96.
19. IOGraph [Электронный ресурс]. URL : https:// iographica.com.

References:

1. Kadnova A.M. Algoritm sozdaniya avtomatizirovannykh sistem v zashchishchennom ispolnenii / A.M. Kadnova, O.YU. Makarov, S.A. Mishin, Ye.A. Rogozin // Bezopasnost' informatsionnykh tekhnologiy. 2019. T. 26. № 4. S. 93–100. [Kadnova A.M. Algorithm for the creation of automated systems in a secure execution / A.M. Kadnova, O.Yu. Makarov, S.A. Mishin, E.A. Rogozin // Security of information technology. 2019. Vol. 26. No. 4. pp. 93–100.
2. Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"yektakh, potentsial'no opasnykh ob"yektakh, a takzhe ob"yektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i dlya okruzhayushchey prirodnoy sredy : prikaz ot 14 marta 2014 g. № 31 [Elektronnyy resurs]. URL : https://fstec.ru/index?id=868:prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 [On approval of requirements for information protection in automated control systems for production and technological processes at critical facilities, potentially hazardous facilities, as well as facilities that pose an increased danger to human life and health and the environment: order of March 14, 2014 No. 31 [Electronic resource]. URL: https://fstec.ru/index?id=868:prikaz–fstek–rossii–ot–14–marta–2014–g–n–31
3. Sistema zashchity informatsii «Strazh NT». Rukovodstvo administratora [Elektronnyy resurs]. – URL : http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf. [Information security system «Guard NT». Administrator Guide [Electronic resource]. URL: http: //www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf.
4. Sistema zashchity informatsii «Strazh NT». Rukovodstvo pol'zovatelya [Elektronnyy resurs]. – URL : http://www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf. [The information security system «Guard NT». User Guide [Electronic resource]. URL: http: //www.guardnt.ru/download/doc/admin_guide_nt_3_0.pdf.
5. Dovgulya M.M. Opoveshcheniye administratora informatsionnoy bezopasnosti o narusheniyakh v rabote korporativnoy seti / M.M. Dovgulya, R.V. Meshcheryakov // Nauchnaya sessiya TUSUR. 2005 : sb. nauch. tr. Tomsk, 2005. S. 96–97. [Dovgulya M.M. Alert of the information security administrator about violations in the work of the corporate network / M.M. Dovgul, R.V. Meshcheryakov // Scientific session TUSUR – 2005: Sat. Scientific tr. Tomsk, 2005. pp. 96–97.
6. Yaremchuk S. Zashchitnik seti / S. Yaremchuk // Sistemnyy administrator. 2003. № 11(12). S. 56–60. [Yaremchuk S. Defender of the network / S. Yaremchuk // System Administrator. 2003. No. 11 (12). pp. 56–60.
7. Bormotov S.V. Sistemnoye administrirovaniye na 100% : monografiya / S.V. Bormotov. Sankt-Peterburg : Piter, 2006. 256 s. [Bormotov S.V. 100% system administration: monograph / S.V. Bormotov. St. Petersburg: Peter, 2006. 256 p.
8. Khvostov V.A. Metody i sredstva povysheniya zashchishchennosti avtomatizirovannykh sistem : monografiya / V.A. Khvostov [i dr.]. Voronezh: Voronezhskiy institut MVD Rossii, 2013. 108 s. [Khvostov V.A. Methods and means of increasing the security of automated systems: monograph / V.A. Tails [et al.]. – Voronezh: Voronezh Institute of the Ministry of Internal Affairs of Russia, 2013. 108 p.
9. Kadnova A.M. Sposob otsenki operatsionnykh kharakteristik sistem zashchity informatsii ot nesanktsionirovannogo dostupa na osnove / A.M. Kadnova, O.I. Bokova, Ye.A. Rogozin, N.S. Khokhlov, O.YU. Makarov // Aktual'nyye problemy prikladnoy matematiki, informatiki i mekhaniki : sb. nauch. tr. Voronezh, 2020. S. 656–659. [Kadnova A.M. A method for assessing the operational characteristics of information security systems against unauthorized access based on / A.M. Kadnova, O.I. Bokova, E.A. Rogozin, N.S. Khokhlov, O.Yu. Makarov // Actual problems of applied mathematics, computer science and mechanics: collection of articles. Scientific tr. Voronezh, 2020. pp. 656–659.
10. Kadnova A.M. K voprosu o reshenii nauchnoy zadachi kolichestvennoy otsenki ergatotekhnicheskikh kharakteristik sistem zashchity informatsii ot nesanktsionirovannogo dostupa v avtomatizirovannykh sistemakh OVD / A.M. Kadnova, Ye.A. Rogozin // Obshchestvennaya bezopasnost', zakonnost' i pravoporyadok v III tysyacheletii. 2019. № 5–2. S. 307–310. [Kadnova A.M. On the issue of solving the scientific problem of quantifying the ergatotechnical characteristics of information protection systems against unauthorized access in automated ATS systems / A.M. Kadnova, E.A. Rogozin // Public safety, law and order in the III millennium. 2019. No. 5–2. pp. 307–310.
11. Skrypnikov A.V. Normirovaniye trebovaniy k kharakteristikam programmnykh sistem zashchity informatsii / A.V. Skrypnikov, V.A. Khvostov, Ye.V. Chernyshova, V.V. Samtsov, M.A. Abasov // Vestnik Voronezhskogo gosudarstvennogo universiteta inzhenernykh tekhnologiy. 2018. T. 80. № 4(78). S. 96–110. [Skrypnikov A.V. Rationing requirements for the characteristics of software information protection systems / A.V. Skrypnikov, V.A. Khvostov, E.V. Chernyshova, V.V. Samtsov, M.A. Abasov // Bulletin of the Voronezh State University of Engineering Technologies. 2018. Vol. 80. No. 4 (78). pp. 96–110.
12. Korolev D.A. Ergonomika i yuzabiliti pol'zovatel'skogo interfeysa programmnogo obespecheniya :

metodicheskoye posobiye / D.A. Korolev. Moskva : Moskovskiy gosudarstvennyy institut elektroniki i matematiki (tekhnicheskiy universitet), 2004. 214 s. [Korolev D.A. Ergonomics and usability of the software user interface: methodological manual / D.A. Korolev. Moscow: Moscow State Institute of Electronics and Mathematics (Technical University), 2004. 214 p.

13. Popov A.A. Ergonomika pol'zovatel'skikh interfeysov v informatsionnykh sistemakh : uchebnoye posobiye /A.A. Popova [i dr.]. Moskva: Rossiyskiy ekonomicheskiy universitet im. G.V. Plekhanova, 2012. 21 s. [Popov A.A. Ergonomics of user interfaces in information systems: a training manual / A.A. Popova [et al.]. Moscow: Russian University of Economics G.V. Plekhanova, 2012. 21 p.
14. Soukoreff R.W. Towards a standard for pointing device evaluation, perspectives on 27 years of Fitts ’law research / R.W. Soukoreff I.S. MacKenzie // Int. J. of Human–Computer Stud. 2004. Vol. 61 (6). pp. 751–789.
15. Gump A. Application of Fitts' law to individuals with cerebral palsy / A. Gump, M. LeGare, D.L. Hunt // Perceptual and motor skills. 2002. Vol. 94 (1). pp. 884–895.
16. Amazeen E.L. The effects of attention and handedness on coordination dynamics in a bimanual Fitts' law task / E.L. Amazeen, S.D. Ringenbach, P.G. Amazeen // Exper. brain research. 2005. Vol. 164 (4). R. 484–499.
17. Spirin I.A. Issledovaniye i primeneniye eye-tracking tekhnologii na cheloveke / I.A. Spirin // Molodoy uchenyy. 2016. №2. S. 227–230 [Spirin I.A. Research and application of eye–tracking technology in humans / I.A. Spirin // Young scientist. 2016. No. 2. S. 227–230.
18. Kadnova A.M. Metodicheskiy podkhod k otsenke veroyatnostnogo pokazatelya svoyevremennosti vypolneniya tipovykh operatsiy administratorom sistemy zashchity informatsii avtomatizirovannoy sistemy /A.M. Kadnova // Vestnik Dagestanskogo gosudarstvennogo tekhnicheskogo universiteta. 2019. T. 46. № 3. S. 87–96. 19. IOGraph [Elektronnyy resurs]. URL : https:// iographica.com. [Kadnova A.M. Methodological approach to assessing the probability indicator of the timeliness of typical operations by the administrator of the information protection system of the automated system / A.M. Kadnova // Herald of the Daghestan State Technical University. 2019. Vol. 46. No. 3. pp. 87–96.
19. IOGraph [Electronic resource]. URL: https: // iographic.com.

Сведения об авторе:

Каднова Айжана Михайловна, старший преподаватель, аспирант, кафедра информационной безопасности, e-mail: aizhana_kadnova@mail.ru

Information about the author:

Aizhana M. Kadnova, Senior Lecturer, Postgraduate Student, Department of Information Security, e-mail: aizhana_kadnova@mail.ru

Конфликт интересов.
Автор заявляет об отсутствии конфликта интересов.
Поступила в редакцию 24.12.2020.
Принята в печать 01.02.2021.

Conflict of interest.
The author declare no conflict of interest.
Received 24.12.2020.
Accepted for publication 01.02.2021.