*ISSN 2500-316X (Online)*

*https://doi.org/10.32362/2500-316X-2020-8-6-34-46*



*УДК 004.7*

# Разработка технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок времени реакций пользователей

**Ш.Г. Магомедов[1,@], П.В. Колясников[1,2], Е.В. Никульчев[1,2]**

*[1]МИРЭА – Российский технологический университет, Москва 119454, Россия*
*[2]Российская академия образования, Дата-центр, Москва 119121, Россия*
*[@]Автор для переписки, e-mail: magomedov_sh@mirea.ru*

Статья посвящена разработке технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок персональных характеристик поведения пользователей. В распределенных цифровых платформах и порталах, использующих персональные данные, осуществляется сбор и обработка данных большого объема с помощью специализированных приложений, использующих компьютерные сети. Согласно законодательству Российской Федерации хранение данных происходит на внутрикорпоративных серверах и центрах обработки данных. Задачам разграничения и контроля доступа в современных информационных системах уделяется особое внимание. Широкая доступность и массовость сервисов должна сопровождаться более тщательным контролем и верификацией пользователя. Обеспечение контроля доступа к таким системам не может быть осуществлено только за счет технологий и средств информационной безопасности, повысить эффективность можно за счет программно-аппаратных архитектурных решений. В работе предлагается расширить развивающуюся в настоящее время SIEM-технологию (Security information and event management), объединяющую концепцию управления событиями безо-

пасности и управление информационной безопасностью, блоками анализа поведения пользователей. В качестве характеристики, которая может быть оценена без перегрузок каналов связи и независима от используемого типа устройств, предложено использовать время психомоторной реакции, измеряемое при выполнении действий с интерфейсом. Разработано технологическое решение, которое может быть реализовано в широком спектре цифровых платформ – банковских, медицинских, образовательных и др. Приведены результаты экспериментов с использованием цифровой платформы массовых психологических исследований. Для анализа использовались данные массового опроса при ответе (в форме выбора из имеющихся вариантов) на анкетные вопросы об уровне образования. Анализ данных о времени реакции показал возможность нормирования и одинаковые показатели конкретных пользователей при ответах на разные вопросы.

***Ключевые слова:*** контроль доступа, цифровые платформы, обработка больших объемов данных, управление событиями безопасности, информационная безопасность, вычислительные комплексы, анализ поведения пользователей.

***Для цитирования:*** Магомедов Ш.Г., Колясников П.В., Никульчев Е.В. Разработка технологии контроля доступа к цифровым порталам и платформам на основе встроенных в интерфейс оценок времени реакций пользователей. *Российский технологический журнал.* 2020;8(6):34-46. https://doi.org/10.32362/2500-316X-2020-8-6-36-46

# Development of technology for controlling access to digital portals and platforms based on estimates of user reaction time built into the interface

**Shamil G. Magomedov[1,@], Pavel V. Kolyasnikov[1,2], Evgeny V. Nikulchev[1,2]**

*[1]MIREA – Russian Technological University, Moscow 119454, Russia*
*[2]Russian Academy of Education, Data Center, Moscow 119121, Russia*
*[@]Corresponding author e-mail: magomedov_sh@mirea.ru*

The paper addresses the development of technology for controlling access to digital portals and platforms based on assessments of personal characteristics of user behavior built into the interface. In distributed digital platforms and portals using personal data, big data is collected and processed using specialized applications using computer networks. In accordance with the law, the data is stored on internal corporate servers and data centers. Special attention is paid to the tasks of differentiation and control of access in modern information systems. Wide availability and mass scale of services should be accompanied by more careful control and user verification. Access control to such systems cannot be ensured only through technologies and information security tools; efficiency can be increased through software and hardware architectural solutions. The paper proposes to expand the currently developing SIEM technology (Security information and event management), which combines the concept of security event management and information security management, with blocks of user behavior analysis. As a characteristic that can be measured without overloading communication channels and is independent of the type of device used, the psychomotor reaction time is proposed, measured as the performance of actions with the interface. A technological solution has been developed for implementation in a wide range of digital platforms: banking, medical, educational, etc. The results of experimental research using a digital platform of mass psychological research are presented. For the research, data from a

mass survey were used when answering (in the form of a choice from the available options) to questions about the level of education. Analysis of the reaction time data showed the possibility of standardization and the same indicators of specific users when answering different questions.

***Keywords:*** access control, digital platforms, big data processing, security event management, information security, computing systems, user behavior analysis.

***For citation:*** Magomedov Sh.G., Kolyasnikov P.V., Nikulchev E.V. Development of technology for controlling access to digital portals and platforms based on estimates of user reaction time built into the interface. *Rossiiskii tekhnologicheskii zhurnal = Russian Technological Journal.* 2020;8(6):34-46 (in Russ.). https://doi.org/10.32362/2500316X-2020-8-6-34-46

## Введение

Цифровизация внесла во все сферы общественной жизни широкое распространение платформ, порталов, вычислительных сервисов, что определило развитие новых технологий сбора, хранения, обработки и передачи данных, и соответственно, специализированных архитектур вычислительных комплексов и служб передачи данных по компьютерным сетям, механизмов взаимодействия клиентов с элементами вычислительного комплекса с использованием различных телекоммуникационных технологий, технологий защиты компьютерных сетей и приложений.

В распределенных цифровых платформах и порталах (ЦП), использующих персональные данные, осуществляется сбор и обработка большого объема данных с помощью специализированных приложений с использованием компьютерных сетей и, согласно законодательству, хранение данных происходит на серверах на территории РФ [1]. К ЦП относятся такие системы, как платформы государственных услуг, муниципальные и региональные платформы, банковские порталы, медицинские системы, платформы психологических исследований, образовательные системы дистанционного обучения и др. Задачам разграничения и контроля доступа в современных информационных системах уделяется особое внимание. Широкая доступность и массовость сервисов должна сопровождаться более тщательным контролем и верификацией пользователей. Обеспечение контроля доступа к таким системам не может быть осуществлено только за счет технологий и средств информационной безопасности, повысить эффективность можно за счет программно-аппаратных архитектурных решений.

Цифровые платформы и порталы, обрабатывающие большие данные, имеют ряд общих особенностей: как правило, веб-интерфейс или приложение с доступом по сети; большое количество пользователей; сложную инфраструктуру вычислительного комплекса; разграничение прав доступа к данным; различные типы интерфейсов в зависимости от прав доступа; большие объемы обрабатываемых данных; наличие конфиденциальных, а часто и частных (банковские, медицинские) данных; веб-интерфейсы, формирующие запросы к базам данных.

Верификация пользователей не обеспечивает требуемый контроль доступа к данным. Например, в образовательных системах передача пароля позволяет одному учащемуся удаленно сдать тесты за нескольких человек; в системах здравоохранения, в случае, когда компьютер оставлен включенным, другой сотрудник может получить доступ к медицинским данным. Стоит отметить, что в банковских системах разрабатываются

антифрод-системы, контролирующие транзакции для выявления мошенников. Важной особенностью такого нарушения доступа к большим данным является отсутствие аномалий на уровне трафика. Получение индивидуальных характеристик пользователей, особенностей работы однотипной группы пользователей с системой позволит также повысить эффективность хранения данных за счет структурирования наиболее вероятных запросов данных, а также сформировать клиент-ориентированный интерфейс на основе предпочтений пользователей. Указанные особенности новых технологий создают сложности в разграничении доступа.

В настоящее время развивается концепция [2] SIEM (Security information and event management). Она объединяет две концепции: управление событиями безопасности (Security Event Management, SEM), основанную на мониторинге и корреляции событий безопасности в реальном времени; управление информационной безопасностью (Security Information Management, SIM), предназначенную для хранения, обработки и анализа данных. Системы SIEM создаются для выявления кибератак, уязвимостей, оценки рисков безопасности через программно-аппаратные комплексы, предоставляющие информацию из различных источников данных. SIEM-система разворачивается над защищаемой информационной системой [3] и представляет собой интегрированные устройства либо многокомпонентные комплексы. Существуют коммерческие решения SIEM-систем: QRadar IBM, Arc Sight HP, Symantec Security Services, FortiSIEM и др.[4]. Однако разработка альтернативных моделей, которые предоставляют дополнительную информацию на основе тех же источников данных, а также формирование новых источников данных на этапе разработки комплексов с критически важным разграничением доступа является важной и актуальной задачей современных исследований.

Настоящая статья посвящена разработке технологии повышения эффективности контроля доступа на основе встроенных в интерфейс вычислительных комплексов оценок времени реакций пользователей как индивидуальных индикаторов психологических и психофизических реакций.

## 1. Разработка технологии

Разработке архитектур SIEM-систем, обнаружения источников угроз и механизмов их выявления посвящено значительное количество современных исследований [5]: в распределенных системах [6], для блокировки вредоносного трафика с устройств IoT [7], по интеллектуальной обработке данных из нескольких источников [8, 9], по использованию методов классификации событий [10] и др.

Существует направление исследований, связанное с анализом поведения пользователей (User behavior analytics, UBA) [11], направленное на обеспечение процесса безопасности – обнаружение внутренних угроз, целевых атак и финансового мошенничества. Решения UBA изучают шаблоны человеческого поведения, после чего применяют алгоритмы обнаружения аномалий этих шаблонов. Например, в [12] рассмотрена ситуация, когда злоумышленник в сети компании может использовать украденные учетные данные для скрытого сбора конфиденциальных данных. Такое поведение трудно обнаружить, если оно не вызывает предупреждение о нарушении доступа или утечке данных.

Альтернативой многоуровневой технологии является использование встраиваемых динамических моделей в интернет-приложения [13]. Авторами разработаны структуры,

включающие ситуационные модели и интерпретатор. Модель содержит заданные конечные наборы состояний, переходов и правил, определяющих переходы. Интерпретатор отслеживает и сохраняет текущие состояния модели, проверяя условия переходов. Известен подход [14], включающий получение характеристик действий пользователя (логин пользователя, движение мыши, среднее время между нажатием клавиши мыши и началом движения курсора, скорость набора текста и др.). Подобные исследования интересны, но носят ограниченный характер – для многопользовательских систем получение, передача, хранение и обработка данных вычислительно очень затратны. Кроме того, использование манипулятора мыши для анализа реакций сложно реализуемо – задержки сильно зависят от производителя и от поверхности, на которой в данный момент работает пользователь. Кроме того, веб-интерфейсы подразумевают использование их на разных устройствах, в том числе с сенсорными экранами.

Однако использовать психомоторные реакции представляется целесообразным. Современные психологические исследования выявили достоверность данных по исследованию реакций, полученных с использованием веб-интерфейсов с данными, полученными в лабораторных условиях. Например, в [15] сравнивались результаты сложных лингвокогнитивных тестов, что в некотором смысле соответствует выполнению действий с интерфейсами ЦП.

Таким образом, предлагается разработать технологию построения архитектуры многоуровневой защиты, использующую в качестве дополнительного идентификатора пользователя время реакций при работе с элементами интерфейса. При этом сбор данных будет осуществляться встроенными программными средствами, а элементы интерфейса передаваться в систему.

На рис. 1 представлена ситуация, когда «Пользователь 1» ввел все необходимые данные для доступа, однако он может быть заменен другим пользователем, как с рабочего места «Пользователя 1», так и из другого места. Если в системе отсутствуют блоки, связанные с поведением пользователя и его местонахождением, «Пользователь 2» может осуществлять доступ к данным.

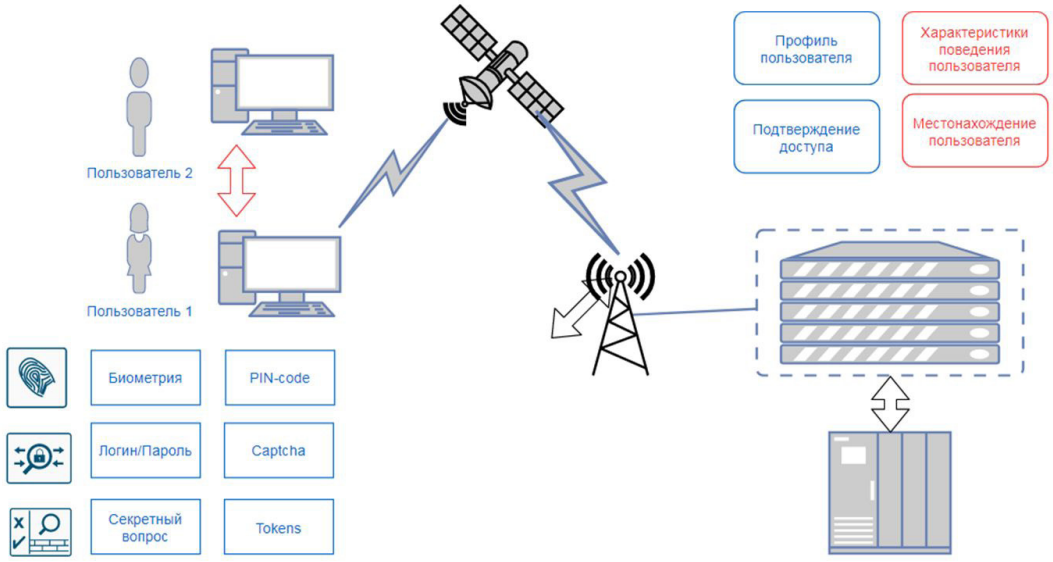


**Рис. 1.** Пример системы с контролем доступа.

Для ЦП предлагается встроить в системы контроля доступа и верификации вспомогательные индикаторы использования элементов интерфейса – время реакции (ВР) при выполнении определенных, заранее зафиксированных действий. Это позволит использовать только персональные реакции, исключив ситуации смены пользователя в одном сеансе работы. Также возможно определение пользователя при использовании чужих паролей для входа в систему. Возможные ситуации с изменением реакций под текущим психоэмоциональным состоянием требуют проведения дополнительных подтверждений личности пользователя. Так, в случаях, например, болезни или снижения концентрации пользователя допуск пользователя в системы с критическим доступом может быть проверен специальными службами.

В общем виде разрабатываемую технологию можно представить в следующем виде:

1. Технология реализуется вычислительным комплексом (ВК). ВК может предоставлять клиенту одну или несколько услуг, таких как, например, услуги мониторинга событий, финансовые, банковские, правительственные, образовательные услуги, услуги передачи данных в реальном времени, игровые услуги, услуги поиска и т.п.

2. ВК включает компьютерные сети, системы управления передачей данных, то есть среду, используемую для обеспечения каналов связи между компьютерами, системами обработки данных и другими устройствами. Сеть может включать в себя соединения в виде проводных линий связи, каналов беспроводной связи и оптоволоконные кабели.

3. ВК могут отправлять инциденты безопасности на облачную платформу для дальнейшего анализа приложением машинного обучения на основе идентифицированных характеристик инцидентов безопасности, обнаруженных во время локального анализа с помощью модуля безопасности и диспетчера событий. Идентифицированные характеристики могут включать, например, информацию о том, что наблюдаемые параметры имеют оценку риска безопасности выше порогового значения.

4. В ВК создается постоянное хранилище информации о безопасности и менеджер событий, которые могут быть аппаратным компонентом или комбинацией аппаратных и программных компонентов. Менеджер информации и событий безопасности управляет процессом выбора только определенных инцидентов безопасности для локального и удаленного анализа.

5. Интервал оценки психомоторных реакций пользователя представляет собой заранее определенный интервал времени, на основе которого формируются инциденты безопасности.

Архитектура ВК, реализующего технологии контроля доступа с использованием персональных психомоторных реакций, имеет 4 уровня:

– уровень аппаратного и программного обеспечения;
– уровень виртуализации;
– уровень управления;
– уровень рабочих нагрузок.

Уровень аппаратного и программного обеспечения может включать мэйнфреймы, серверы, блейд-серверы, устройства хранения, программное обеспечение серверов и сетевых приложений, программное обеспечение базы данных, прикладное программное обеспечение.

Уровень виртуализации обеспечивает уровень абстракции: виртуальные серверы, виртуальная память, виртуальные сети, виртуальные приложения, операционные системы и виртуальные клиенты.

Уровень управления определяет контроль доступа к сервисам ВК по компьютерным сетям, обеспечивает доступ к ВК для пользователей и системных администраторов. Управление уровнями обслуживания обеспечивает распределение ресурсов ВК и управление таким образом, чтобы удовлетворялись заданные уровни доступа.

Уровень рабочих нагрузок предоставляет функциональные возможности, для которых используется ВК. В интерфейс клиентских приложений необходимо встроить сбор характеристик поведения. Так, для систем, подразумевающих передачу состояния Representational State Transfer (REST), необходимо собирать данные о запросах пользователей к Application programming interface (API), ведя учет времени, параметров и идентификатора пользователя, а для систем с графическим пользовательским интерфейсом Graphical user interface (GUI) – собирать данные о действиях в отношении интерфейса, ведя учет времени осуществления действий и идентификаторы пользователя.

Таким образом, элементы интерфейса вместе со встроенными реакциями передаются в ВК и анализируются на уровне доступа (рис. 2).

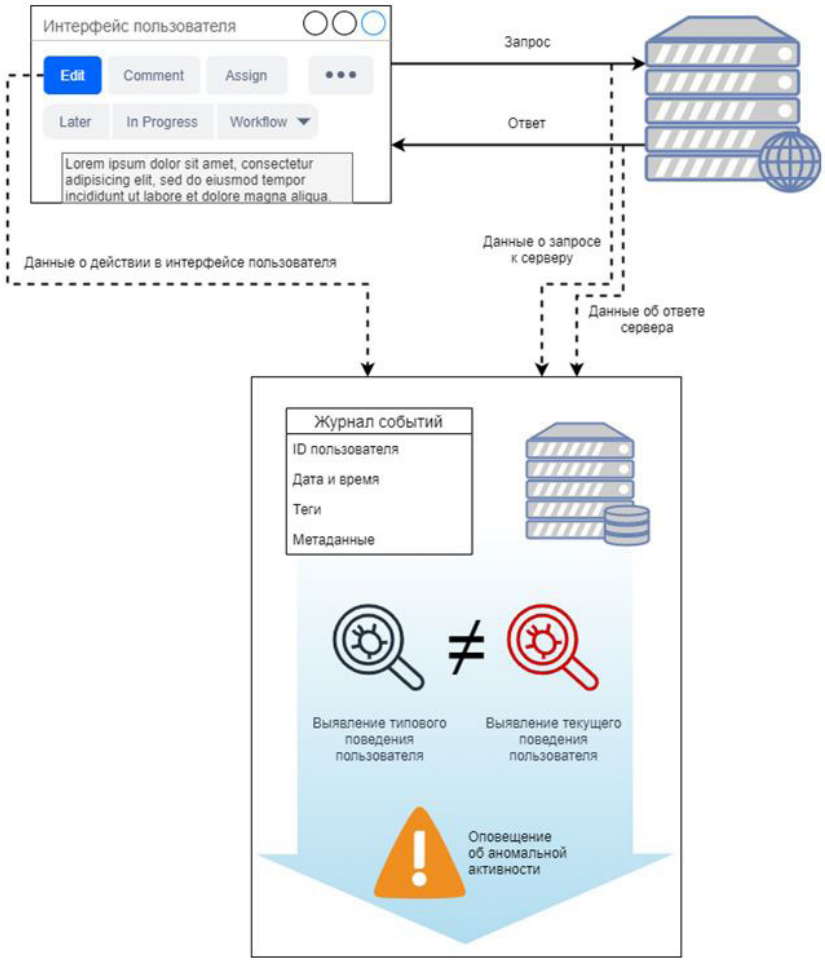


**Рис. 2.** Уровень анализа действий пользователя в архитектуре ВК.

Концептуальная схема взаимодействия уровня управления и серверной части приведена на рис. 3.

В процессе работы пользователя с интерфейсом системы необходимо проверять условия переходов на основе ранее совершенных наборов действий, записанных в журнал событий.

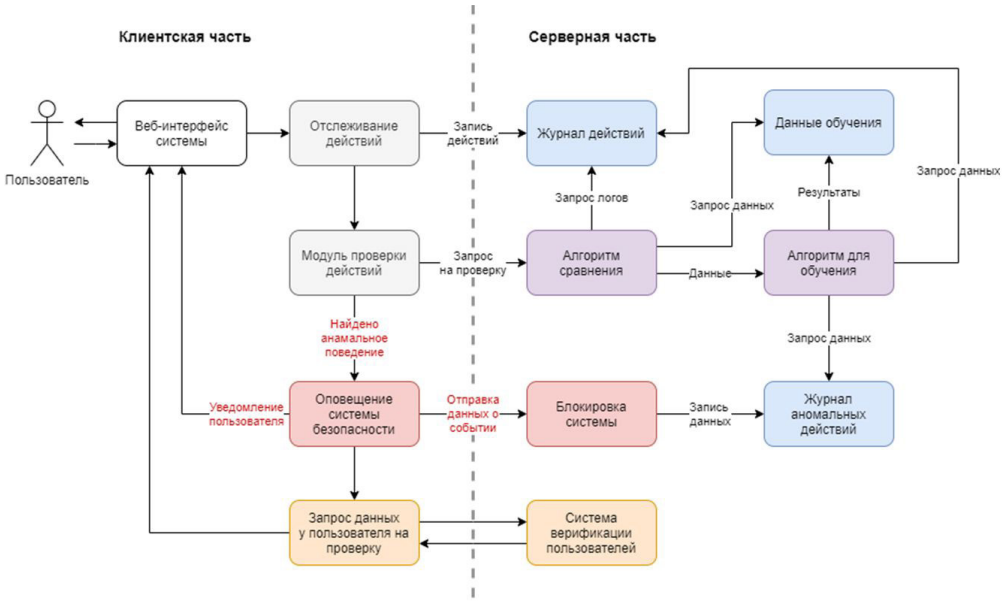


**Рис. 3.** Технология взаимодействия уровня управления с клиентскими интерфейсами.

## 2. Экспериментальные исследования

Исследования проводились с помощью цифровой платформы DigitalPsyTools [16]. Система является одновременно цифровой платформой с веб-интерфейсом и инструментом психодиагностики, используемым для популяционных исследований в системе образования. В элементы ее интерфейса встроены платформонезависимые функции оценки когнитивных реакций. Идентифицируемость распределения, определяемого действием пользователя, базируется на моделях, аналогичных [17].

Между приложением внешнего стимула и соответствующей двигательной реакцией на стимул существует определенный период времени, называемый временем реакции. Оценка этого времени – один из важных методов изучения скорости когнитивной обработки информации человеком и скоординированной реакции периферических движений.

На время реакции влияют многие факторы, такие как пол, возраст, физическое состояние, утомляемость, состояние здоровья и т.п. Увеличенное время реакции означает снижение производительности. Время показа является временем от начала показа страницы, на которой можно сделать действие, до времени на момент, когда пользователь осуществил какое-либо действие в интерфейсе. Иными словами, ВР – это время от появления стимула до нажатия кнопки (на основании психологических терминов).

Время реакции пользователя для конкретного действия можно разделить на:

– минимальное ВР (минимальная латентность ответа),
– максимальное ВР (максимальная латентность ответа),
– усредненное ВР (усредненная латентность ответа).

Для анализа использованы реакции 1980 студентов при ответе на 4 вопроса:

1. Основа обучения (выбор из трех вариантов: бюджетная/контрактная/целевая).
2. Вы поступили на ту специальность, которую хотели? (Да/Нет).
3. Укажите профиль Вашего образования (выбор из четырех вариантов: технический/гуманитарный/естественнонаучный/нет профиля).
4. Программа обучения (выбор из четырех вариантов: бакалавриат/магистратура/специалитет/аспирантура).

Анкета организована в виде веб-интерфейса. После получения архива с опросом он распаковывается и загружается в браузер на устройстве клиента. В каждом элементе опроса фиксируется ответ и время реакции в миллисекундах (с момента загрузки до выбора ответа и нажатия кнопки «далее»), т.е. время, за которое пользователь прочитал вопрос, выбрал нужный вариант и нажал кнопку «далее». Опрос был большой и включал когнитивные тесты, и пользователь был заинтересован перейти на следующую страницу. Данные передавались в платформу после окончания всего опроса, либо после закрытия пользователем веб-страницы. Это гарантировало невмешательство сетей в оценку времени реакции.

Также были собраны сведения об используемых при проведении опроса операционных системах и браузерах. Эти сведения представлены на рис. 4 и 5.

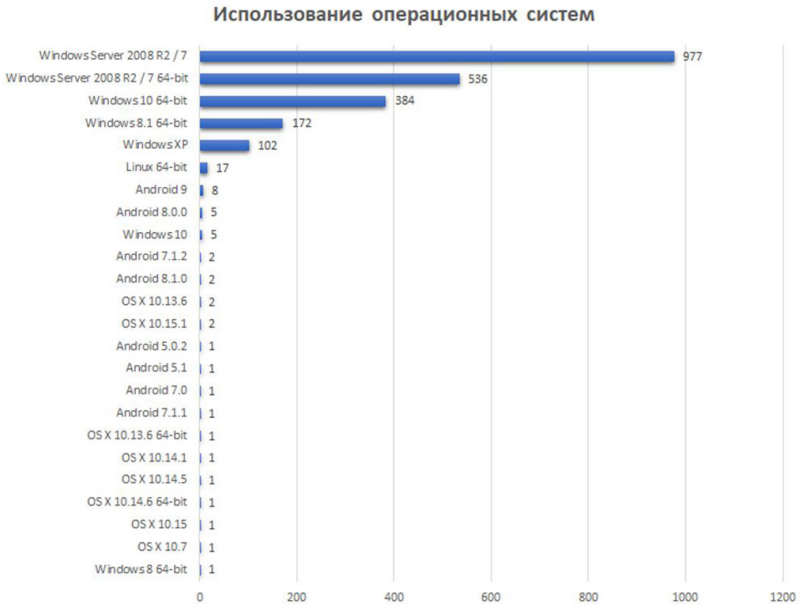


**Рис. 4.** Операционные системы, используемые пользователями в опросе.

Гипотеза анализа данных о времени реакции состояла в возможности определения зависимости в реакциях пользователей в работе с элементами интерфейса при ответе на заданный вопрос, а также возможности определения индивидуальных психомоторных реакций при работе с интерфейсом. Анализ данных показал состоятельность гипотезы.

На рис. 6 представлены полученные гистограммы для каждого вопроса и индивидуальные реакции трех произвольно выбранных пользователей. Из представленных результатов видно, что замедленная реакция (рис. 6а) характерна для ответа на все вопросы, средние и быстрые реакции (рис. 6б,в) сохраняются при изменении вопроса и количества вариантов ответов, то есть этот подход позволяет выявить, был ли в процессе ответа на анкетные вопросы заменен пользователь.

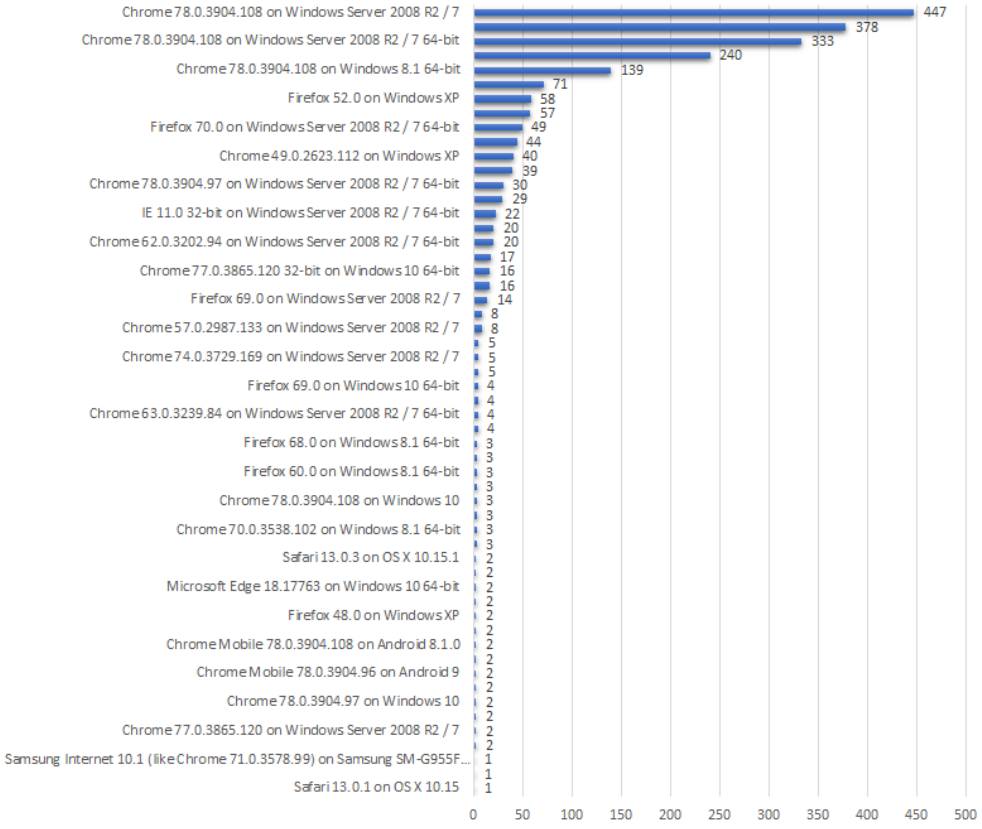


**Рис. 5.** Типы и версии браузеров, используемых в опросе.

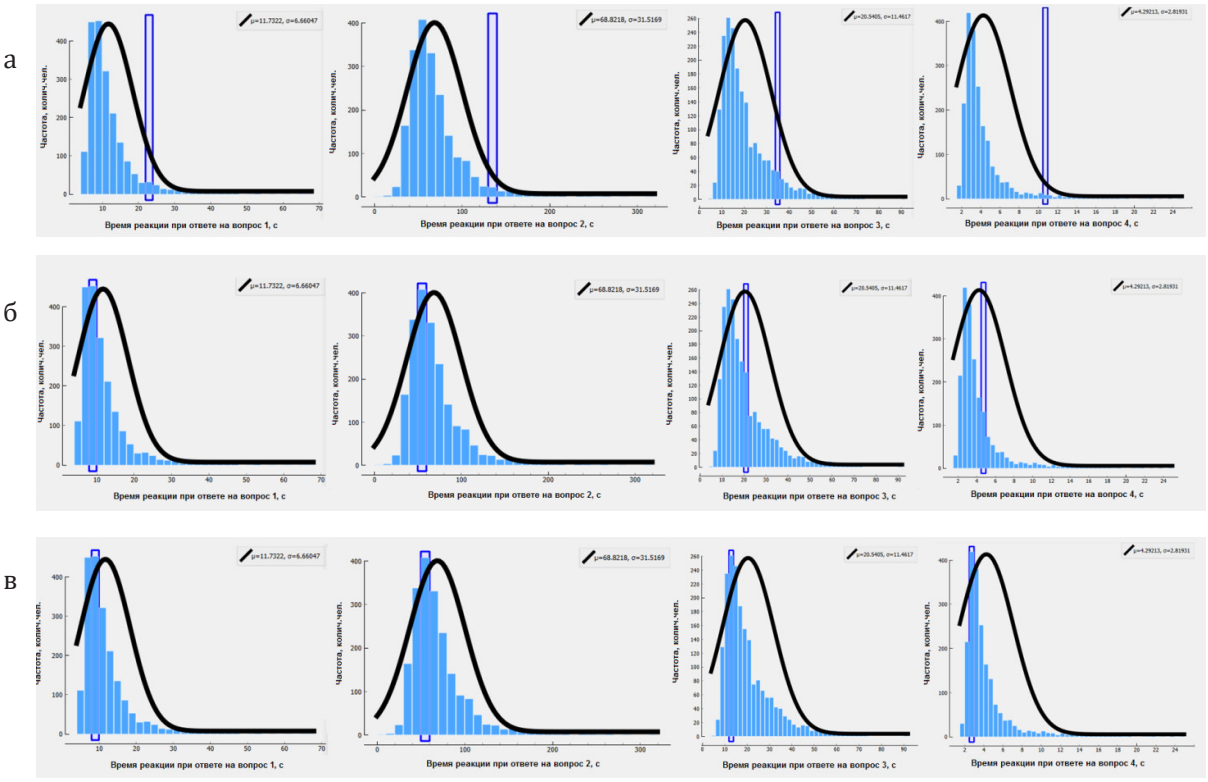


**Рис. 6.** Примеры реакций случайно выбранных пользователей при ответах на 4 вопроса в веб-опросе:
а – замедленная реакция; б – средняя реакция; в – быстрая реакция.

На основании предварительных результатов анализа можно сделать вывод, что данные реакции могут быть использованы в разработанной технологии контроля доступа к ЦП, в том числе с использованием веб-интерфейсов. Данные могут использоваться для валидации и дополнительной верификации пользователей, участвующих в опросах и использующих интерфейсы.

## Заключение

В работе предлагается расширить SIEM-технологии анализом психомоторных реакций пользователей. В качестве характеристики, которая может быть измерена без перегрузок каналов связи и быть независимой от используемого типа устройств, предложено время реакции, измеряемое при выполнении действий с интерфейсом. Разработано технологическое решение, которое может быть реализовано в широком спектре цифровых платформ – банковских, медицинских, образовательных и др. Приведены результаты экспериментальных исследований с использованием цифровой платформы массовых психологических исследований. Для исследований использовались данные массового опроса при ответе (в форме выбора из имеющихся вариантов) на анкетные вопросы об уровне образования. Анализ данных о времени реакции показал возможность нормирования и одинаковые показатели конкретных пользователей при ответах на разные вопросы.

В качестве развития разработанного подхода представляется актуальным использование инструментов искусственного интеллекта для выявления скрытых зависимостей в данных, полученных с логирования пользователей и выявления наиболее вероятных действий пользователей.

*Работа выполнена при финансовой поддержке РФФИ (грант 17-29-02198).*

## Литература:

1. Никульчев Е.В., Ильин Д.Ю., Колясников П.В., Исматуллина В.И., Захаров И.М., Малых С.Б. Разработка открытой цифровой платформы масштабных психологических исследований. *Вестник РФФИ.* 2019;4(104):99-113.
https://doi.org/10.22204/2410-4639-2019-104-04-105-119

2. Khan A., Khan R., Nisar F. Novice threat model using SIEM system for threat assessment. In: 2017 International Conference on Communication Technologies (ComTech). IEEE. 2017. P. 72-77.
https://doi.org/10.1109/COMTECH.2017.8065753

3. El Arass M., Souissi N. Smart SIEM: From big data logs and events to smart data alerts. *Int. J. Innov. Technol. Explor.* Eng. 2019;8(8):3186-3191.

4. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things. *Automatic control and computer sciences.* 2016;50(8):673-681.
https://doi.org/10.3103/S0146411616080125

5. Khan T., Alam M., Akhunzada A., Hur A., Asif M., Khan M.K. Towards augmented proactive cyberthreat intelligence. *J. Parallel Distrib. Comput.* 2019;124:47-59.
https://doi.org/10.1016/j.jpdc.2018.10.006

6. Kufel L. Security event monitoring in a distributed systems environment. *IEEE Secur. Priv.* 2013;11(1):36-43.
https://doi.org/10.1109/MSP.2012.61

7. Al-Duwairi B., Al-Kahla W., AlRefai M.A., Abdelqader Y., Rawash A., Fahmawi R. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. *Int. J. Electr. Comput. Eng.* 2020;10(2):2182-2191.
http://doi.org/10.11591/ijece.v10i2.pp2182-2191

8. Lee J., Kim J., Kim I., Han K. Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access.* 2019;7:165607-16562.
https://doi.org/10.1109/ACCESS.2019.2953095

9. Moukafih N., Orhanou G., El Hajji S. Neural Network-Based Voting System with High Capacity and Low Computation for Intrusion Detection in SIEM/IDS Systems. *Security and Communication Networks.* 2020; Article ID 3512737.
https://doi.org/10.1155/2020/3512737

10. Sancho J.C., Caro A., Ávila M., Bravo A. New approach for threat classification and security risk estimations based on security event management. *Future Generation Computer Systems.* 2020;113:488-505.
https://doi.org/10.1016/j.future.2020.07.015

11. Csaba K., Péter H.B. Analysis of Cyberattack Patterns by User Behavior Analytics. *AARMS – Academic and Applied Research in Military Science* 2018;17(3):101-114.

12. Xi X., Zhang T., Ye W., Wen Z., Zhang S., Du D., Gao Q. An Ensemble Approach for Detecting Anomalous User Behaviors. *Int. J. Softw. Eng. Knowl. Eng.* 2018;28(11n12):1637-1656.
https://doi.org/10.1142/S0218194018400211

13. Миронов В.В., Гусаренко А.С., Юсупова Н.И. Применение веб-сервисов на основе ситуационно-ориентированной базы данных для мониторинга просмотра учебного видеоконтента. *Моделирование, оптимизация и информационные технологии.* 2019;7(3(26): 27.
https://doi.org/10.26102/2310-6018/2019.26.3.031

14. Монахова М.М., Шерунтаев Д.А., Марков И.С., Мазуро Д.В. Модель поведения пользователя корпоративной сети передачи данных. В: Сб. трудов Девятой всероссийской научно-практической конференции по имитационному моделированию и его применению в науке и промышленности. Екатеринбург; 2019. С. 603-608.

15. Kim J., Gabriel U., Gygax P. Testing the effectiveness of the Internet-based instrument PsyToolkit: A comparison between web-based (PsyToolkit) and lab-based (E-Prime 3.0) measurements of response choice and response time in a complex psycholinguistic task. *PloS ONE.* 2019;14(9):e0221802.
https://doi.org/10.1371/journal.pone.0221802

16. Nikulchev E., Ilin D., Silaeva A., Kolyasnikov P., Belov V., Runtov A., Pushkin P., Laptev N., Alexeenko A., Magomedov S., Kosenkov A., Zakharov I., Ismatullina V., Malykh S. Digital Psychological Platform for Mass Web-Surveys. *Data.* 2020;5(4):95.
https://doi.org/10.3390/data5040095

17. Борисов А.В., Босов А.В., Иванов А.В., Чавтараев Р.Б. Имитационное моделирование пользовательской активности для оценивания вероятностно-временных характеристик программного обеспечения. *Системы и средства информатики.* 2018;28(2):20-33.
https://doi.org/10.14357/08696527180202

## References:

1. Nikulchev E.V., Ilyin D.Yu., Kolyasnikov P.V., Ismatullina V.I., Zakharov I.M., Malykh S.B. Development of the open digital platform for conducting the large-scale psychological research. *RFBR Journal.* 2019;(104):99-113 (in Russ.).
https://doi.org/10.22204/2410-4639-2019-104-04-105-119

2. Khan A., Khan R., Nisar F. Novice threat model using SIEM system for threat assessment. In: 2017 International Conference on Communication Technologies (ComTech). IEEE. 2017. P. 72-77.
https://doi.org/10.1109/COMTECH.2017.8065753

3. El Arass M., Souissi N. Smart SIEM: From big data logs and events to smart data alerts. *Int. J. Innov. Technol. Explor. Eng.* 2019;8(8):3186-3191.

4. Lavrova D.S. An approach to developing the SIEM system for the Internet of Things. *Automatic control and computer sciences.* 2016;50(8):673-681.
https://doi.org/10.3103/S0146411616080125

5. Khan T., Alam M., Akhunzada A., Hur A., Asif M., Khan M.K. Towards augmented proactive cyberthreat intelligence. *J. Parallel Distrib. Comput.* 2019;124:47-59.
https://doi.org/10.1016/j.jpdc.2018.10.006

6. Kufel L. Security event monitoring in a distributed systems environment. *IEEE Secur. Priv.* 2013;11(1):36-43.
https://doi.org/10.1109/MSP.2012.61

7. Al-Duwairi B., Al-Kahla W., AlRefai M.A., Abdelqader Y., Rawash A., Fahmawi R. SIEM-based detection and mitigation of IoT-botnet DDoS attacks. *Int. J. Electr. Comput. Eng.* 2020;10(2):2182-2191.
http://doi.org/10.11591/ijece.v10i2.pp2182-2191

8. Lee J., Kim J., Kim I., Han K. Cyber threat detection based on artificial neural networks using event profiles. *IEEE Access.* 2019;7:165607-16562.
https://doi.org/10.1109/ACCESS.2019.2953095

9. Moukafih N., Orhanou G., El Hajji S. Neural Network-Based Voting System with High Capacity and Low Computation for Intrusion Detection in SIEM/IDS Systems. *Security and Communication Networks*. 2020; Article ID 3512737.
https://doi.org/10.1155/2020/3512737

10. Sancho J.C., Caro A., Ávila M., Bravo A. New approach for threat classification and security risk estimations based on security event management. *Future Generation Computer Systems.* 2020;113:488-505.
https://doi.org/10.1016/j.future.2020.07.015

11. Csaba K., Péter H.B. Analysis of Cyberattack Patterns by User Behavior Analytics. *AARMS – Academic and Applied Research in Military Science.* 2018;17(3):101-114.

12. Xi X., Zhang T., Ye W., Wen Z., Zhang S., Du D., Gao Q. An Ensemble Approach for Detecting Anomalous User Behaviors. *Int. J. Softw. Eng. Knowl. Eng.* 2018;28(11n12):1637-1656.
https://doi.org/10.1142/S0218194018400211

13. Mironov V.V., Gusarenko A.S., Yusupova N.I. Application of web services based on situation-oriented database for monitoring the viewing of the educational video content. *Modelirovanie, optimizatsiya i informatsionnye tekhnologii = Modeling, Optimization and Information Technology.* 2019;7(3(26):27 (in Russ.).
https://doi.org/10.26102/2310-6018/2019.26.3.031

14. Monakhova M.M., Sheruntaev D.A., Markov I.S., Mazurok D.V. Behavior model of the user for a corporate data transmission network. In: Proc. *The 9th All-Russian Scientific and Practical Conference on Simulation and Its Application in Science and Industry.* Ekaterinburg; 2019. P. 603-608 (in Russ.).

15. Kim J., Gabriel U., Gygax P. Testing the effectiveness of the Internet-based instrument PsyToolkit: A comparison between web-based (PsyToolkit) and lab-based (E-Prime 3.0) measurements of response choice and response time in a complex psycholinguistic task. *PloS ONE.* 2019;14(9):e0221802.
https://doi.org/10.1371/journal.pone.0221802

16. Nikulchev E., Ilin D., Silaeva A., Kolyasnikov P., Belov V., Runtov A., Pushkin P., Laptev N., Alexeenko A., Magomedov S., Kosenkov A., Zakharov I., Ismatullina V., Malykh S. Digital Psychological Platform for Mass Web-Surveys. *Data*. 2020;5(4):95.
https://doi.org/10.3390/data5040095

17. Borisov A.V., Bosov A.V., Ivanov A.V., Chavtaraev R.B. Monte Carlo based user activity simulation for software performance evaluation. *Sistemy i sredstva informatiki = Systems and Means of Informatics.* 2018;28(2):20-33 (in Russ.).
https://doi.org/10.14357/08696527180202

***Об авторах:***

***Магомедов Шамиль Гасангусейнович,*** кандидат технических наук, доцент, заведующий кафедрой «Интеллектуальные системы информационной безопасности» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). ResearcherID: M-5782-2016, Scopus Author ID 57204759220, https://orcid.org/0000-0001-8560-1937. https://www.researchgate.net/profile/Shamil_Magomedov

***Коляснико́в Павел Владимирович,*** главный аналитик Дата-центра, Российская академия образования (119121 Москва, ул. Погодинская, 8), ассистент кафедры «Интеллектуальные системы информационной безопасности» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). ResearcherID: O-1885-2018, Scopus Author ID 57204774687, https://orcid.org/0000-0003-3633-5913. https://www.researchgate.net/profile/Pavel_Kolyasnikov

***Никульчев Евгений Витальевич,*** доктор технических наук, профессор, профессор кафедры «Интеллектуальные системы информационной безопасности» Института комплексной безопасности и специального приборостроения ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78), главный аналитик Дата-центра, Российская академия образования (119121 Москва, ул. Погодинская, 8). ResearcherID: G-6557-2015, Scopus Author ID: 6504081534, http://orcid.org/0000-0003-1254-9132. https://www.researchgate.net/profile/Evgeny_Nikulchev

***About the authors:***

***Shamil G. Magomedov***, Cand. Sci. (Engineering), Associate Professor, Head of the Department of Intelligent Information Security Systems of the Institute of Integrated Security and Special Instrumentation MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia). ResearcherID: M-5782-2016, Scopus Author ID 57204759220, https://orcid.org/0000-0001-8560-1937. https://www.researchgate.net/profile/Shamil_Magomedov

***Pavel V. Kolyasnikov,*** Chief Analyst of the Data Center, Russian Academy of Education (8, Pogodinskaya ul., Moscow 119121, Russia), Assistant of the Department of Intelligent Information Security Systems, Institute of Integrated Security and Special Instrumentation MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia). ResearcherID: O-1885-2018, Scopus Author ID 57204774687, https://orcid.org/0000-0003-3633-5913. https://www.researchgate.net/profile/Pavel_Kolyasnikov

***Evgeny V. Nikulchev,*** Dr. Sci. (Engineering), Professor, Professor of the Department of Intelligent Information Security Systems of the Institute of Integrated Security and Special Instrumentation MIREA – Russian Technological University (78, Vernadskogo pr., Moscow 119454, Russia), Chief Analyst of the Data Center, Russian Academy education (8, Pogodinskaya ul., Moscow 119121, Russia). ResearcherID: G-6557-2015, Scopus Author ID: 6504081534, http://orcid.org/0000-0003-1254-9132. https://www.researchgate.net/profile/Evgeny_Nikulchev

*Поступила: 23.08.2020; получена после доработки: 30.09.2020; принята к опубликованию: 30.10.2020.*