УДК 004.056.5
DOI: 10.26102/2310-6018/2021.35.4.038

Анализ защищенности веб-приложения для доступа к системе хранения критически важных данных

А.М. Вульфин

Уфимский государственный авиационный технический университет, Уфа, Российская Федерация

Резюме: В работе рассматривается проблема обеспечения защищенного доступа с помощью веб-приложения к существующей базе данных, содержащей критически важную информацию о параметрах жизненного цикла сложных технических изделий. На основе анализа документа международной организации Web Application Security Consortium (WASC) «The WASC Threat Classification v2.0» выделены возможные атаки на веб-приложение, выступающее в качестве однонаправленной прослойки доступа к базе данных, эксплуатирующие потенциальные уязвимости (недостатки аутентификации, недостатки авторизации, атаки на стороне клиента, выполнение вредоносного кода на стороне сервера), разработан комплекс контрмер применительно к архитектуре веб-приложения. Разработана схема, описывающая контрмеры применительно к Model-View-Controller архитектуре web-приложения. Представлена диаграмма первого уровня декомпозиции функциональной модели работы веб-приложения. Для обеспечения безопасности на уровне сети модернизирована базовая архитектура сети предприятия с демилитаризованной зоной и соответствующей конфигурацией межсетевых экранов. Для оценки защищенности использованы внутренние метрики защищенности программного обеспечения, а также использована методика анализа рисков кибербезопасности на основе нечетких серых когнитивных карт, позволившая количественно оценить снижение относительно риска нарушения целостности накапливаемых данных в 3,5 раза. Рассмотрены четыре сценария воздействия злоумышленника: без использования дополнительных контрмер, применение архитектурной организации веб-приложения прослойки, учитывающего основные паттерны обеспечения кибербезопасности, применение Web-application Firewall (WAF), применение архитектурной организации приложения и WAF.

Ключевые слова: защищенный доступ, базовая архитектура, архитектурный паттерн Model-View-Controller, вектор атак, Web-application Firewall, нечеткая когнитивная карта, оценка рисков.

Благодарности: Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 20-08-00668.

Для цитирования: Вульфин А.М. Анализ защищенности веб-приложения для доступа к системе хранения критически важных данных. *Моделирование, оптимизация и информационные технологии.* 2021;9(4). Доступно по: https://moitvivt.ru/ru/journal/pdf?id=1112 DOI: 10.26102/2310-6018/2021.35.4.038

Security analysis of a web application for accessing the critical data storage system

A.M. Vulfin

Ufa State Aviation Technical University, Ufa, Russian Federation

Abstract: The paper deals with the issue of providing secure access using a web application to an existing database containing critical information about the parameters of complex technical products

life cycle. Based on the analysis of the document of the international organization Web Application Security Consortium (WASC) "The WASC Threat Classification v2.0", possible attacks on a web application, acting as a unidirectional layer of access to the database, exploiting potential vulnerabilities (authentication flaws, authorization flaws, client-side attacks, execution of malicious code on the server-side) have been highlighted and a set of countermeasures has been devised in relation to the architecture of a web application. A pattern has been developed that describes countermeasures concerning the Model-View-Controller architecture of a web application. The diagram of the first level of the web application functional model decomposition is presented. To ensure security at the network level, the basic architecture of the enterprise network with a demilitarized zone and the corresponding configuration of firewalls has been modernized. To assess the security, the internal metrics of software security were utilized, and the cybersecurity risk analysis method by means of fuzzy gray cognitive maps was applied which made it possible to quantitatively assess the reduction with regard to the risk of the accumulated data integrity violation by 3.5 times. Four scenarios of the attacker's impact are considered: without the use of additional countermeasures, the use of the web application layer architectural organization, which takes into account the main patterns of cybersecurity, the use of the Web-application Firewall (WAF), the use of the application architectural organization, and WAF.

Keywords: secure access, basic architecture, Model-View-Controller architectural pattern, attack vector, Web-application Firewall, fuzzy cognitive map, risk assessment.

Acknowledgments: The study was funded by RFBR as a part of the research project No. 20-08-00668.

For citation: Vulfin A.M. Security analysis of a web application for accessing the critical data storage system. *Modeling, Optimization and Information Technology*. 2021;9(4). Available from: https://moitvivt.ru/ru/journal/pdf?id=1112 DOI: 10.26102/2310-6018/2021.35.4.038 (In Russ).

Введение

На этапе эксплуатации авиационной техники актуальной является задача сбора информации о фактическом состоянии эксплуатируемых сложных технических изделий (СТИ) и передачи телеметрической информации (ТМИ) на предприятие-изготовитель (ПИ). На основе такого информационного сопровождения предприятие может разработать дополнительные рекомендации, направленные на повышение эксплуатационных характеристик СТИ. Собирается и хранится информация о месте эксплуатации изделий и агрегатов, результатах контрольных проверок аппаратуры, отказах и т. д.

В одном из сценариев передачи ТМИ собирается на наземных станциях обслуживания и вносится в базу данных предприятия изготовителя через веб-приложение, являющееся дополнительной изолирующей прослойкой между внешними сетями и автоматизированной информационной системой (АИС) ПИ, поскольку доступ из внешней сети даже по защищенным каналам является одним из самых уязвимых элементов системы. Архитектура подобного решения представлена в работах [1-3]. Повышение защищенности веб-приложений от воздействия внешнего злоумышленника актуально не только при обработке ТМИ, но и является одной из ключевых проблем минимизации финансовых и репутационных рисков предприятий.

Все большее значение приобретают аспекты информационной и кибербезопасности, связанные со средой выполнения и организационным уровнем приложения, т. к. акцент в задачах обеспечения кибербезопасности по мере роста сложности программно-технических комплексов смещается в сторону обеспечения защищенности именно программного обеспечения.

Анализируя документы консорциума безопасности веб-приложений (Web Application Security Consortium – WASC) [4], а также сообщества открытого проекта

безопасности веб-приложений (Open Web Application Security Project – OWASP) [5, 6], необходимо отметить, что большинство атак возможно осуществить, опираясь на логику работы веб-приложения и среды выполнения. Об этом же говорит и OWASP TOP 10 [6-8], определяющий наиболее критичные угрозы для веб-приложения со стороны внешнего и внутреннего злоумышленника. По данным Positive Technologies в 2020 г. угроза утечки данных выявлена в 68 % веб-приложений. В 2019 году для 16 % веб-приложений удалось получить наивысший уровень привилегий, а в 8 % систем контроль над сервером веб-приложения позволял проводить атаки на корпоративную информационную сеть организации. 82 % уязвимостей содержались в коде приложения.

Таким образом, цель работы – анализ защищенности доступа к автоматизированной информационной системе, обрабатывающей критически важную информацию об эксплуатируемом сложном техническом изделии, с помощью веб-приложения, реализующего на архитектурном уровне основные механизмы обеспечения кибербезопасности.

Анализ архитектурных особенностей веб-приложений для защищенного доступа к системе хранения данных

Общая схема взаимодействия АИС и веб-приложения, выступающего в качестве однонаправленного механизма (прослойки), представлена на Рисунке 1.

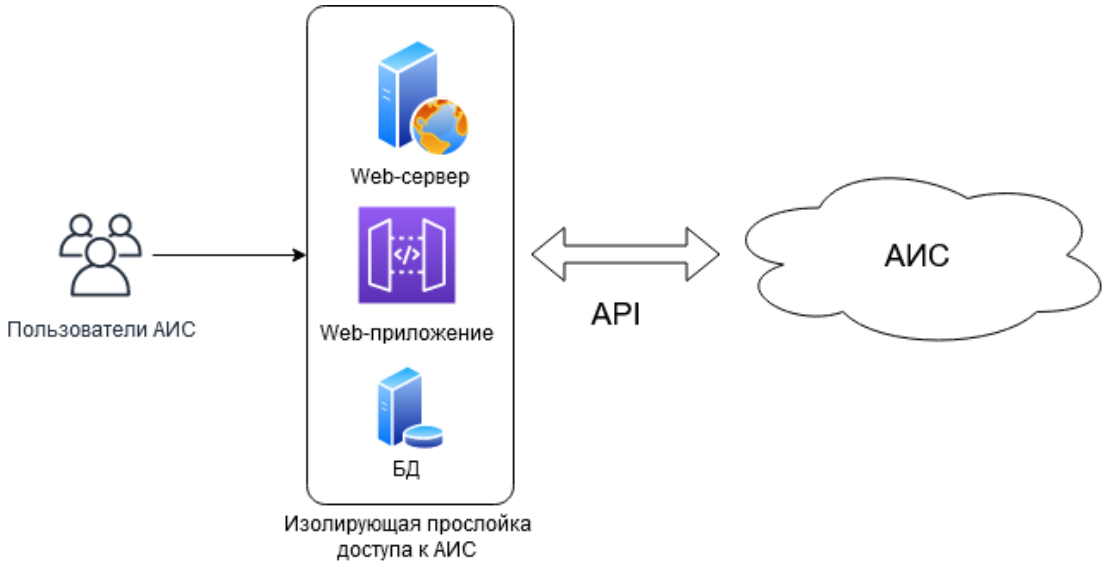


Рисунок 1 – Схема взаимодействия АИС, веб-приложения и внешних пользователей
Figure 1 – Scheme of interaction between AIS, web application and external users

Веб-приложение, обеспечивающее защищенный доступ к АИС, является промежуточным звеном между АИС и клиентом и взаимодействует с клиентом через Интернет, а с АИС – через локальную сеть предприятия. Веб-приложение обращается к АИС посредством API, посылая секретный токен приложения для аутентификации. Соединение между веб-приложением и АИС является защищенным. Обращаясь на сервер веб-приложения, клиент полагает, что он работает с АИС, однако доступ для прямого обращения к серверу АИС он не имеет.

Базовая архитектура сети предприятия (Рисунок 2) определяет безопасность веб-приложения на уровне сети и соответствует следующим требованиям [9]:

1. Сеть сотрудников и кластер серверов АИС изолированы при помощи межсетевого экрана с построением демилитаризованной зоны (DMZ).
2. Сервер доступа к АИС имеет следующие соединения с:
   - сетью Интернет;
   - сервером БД доступа к АИС по локальной сети;
   - АИС по локальной сети.
3. Сервер АИС имеет соединение с серверами БД и сервером доступа к АИС.
4. Все остальные соединения запрещены на уровне межсетевых экранов.

Краткая характеристика элементов базовой архитектуры сети (Рисунок 2) приведена в Таблице 1.

Таблица 1 – Элементы базовой архитектуры сети доступа к АИС
Table 1 – Elements of the basic architecture of the AIS access network

Элемент	Функционал
1	Межсетевой экран на периметре сети
2	Сервер приложений для обеспечения работы изолирующего web-приложения доступа к АИС
3	Web-сервер для работы с удаленными клиентами АИС; совместно с 2 образуют Front-сервер с которым взаимодействует посредствам обратного подключения Back сервер внутренней сети
4	База данных сервера приложений
5	Web Application Firewall (WAF, межсетевой экран для веб-приложений) в режиме работы Monitor (режим сетевого мониторинга через SPAN порт базового коммутатора)
6	Сервер АИС, осуществляющий взаимодействие с (2) для внесения данных в основную БД предприятия (7) по схеме обратного подключения
7	Основная БД хранения данных телеметрии о состоянии СТИ
8	Сервер приложений для обеспечения работы внутренних сервисов сети предприятия

Общее количество уязвимостей веб-приложений и их вариаций не позволяет в полной мере полагаться только лишь на системы предотвращения вторжений, компоненты которой интегрированы в пограничный межсетевой экран. Для эффективной защиты web-приложений необходим комплексный анализ их кодовой базы, структуры, включая: URL-параметры, cookie-файлы, формы ввода данных и так далее. Для информационных систем, требующих усиленной защиты, применяются системы Web-application Firewall (WAF), которые позволяют блокировать как известные типы атак, так и атаки, против которых еще не разработаны контрмеры (Zero-Day Attacks). WAF системы являются узкоспециализированными решениями с высоким потенциалом развития.

Для определения векторов атак на веб-приложение, выступающее в качестве однонаправленной прослойки доступа, будем опираться на документ международной организации Web Application Security Consortium (WASC) «The WASC Threat Classification v2.0» [10]. Атаки и соответствующе подобранные контрмеры на уровне архитектурной организации приложения приведены в Таблице 2.

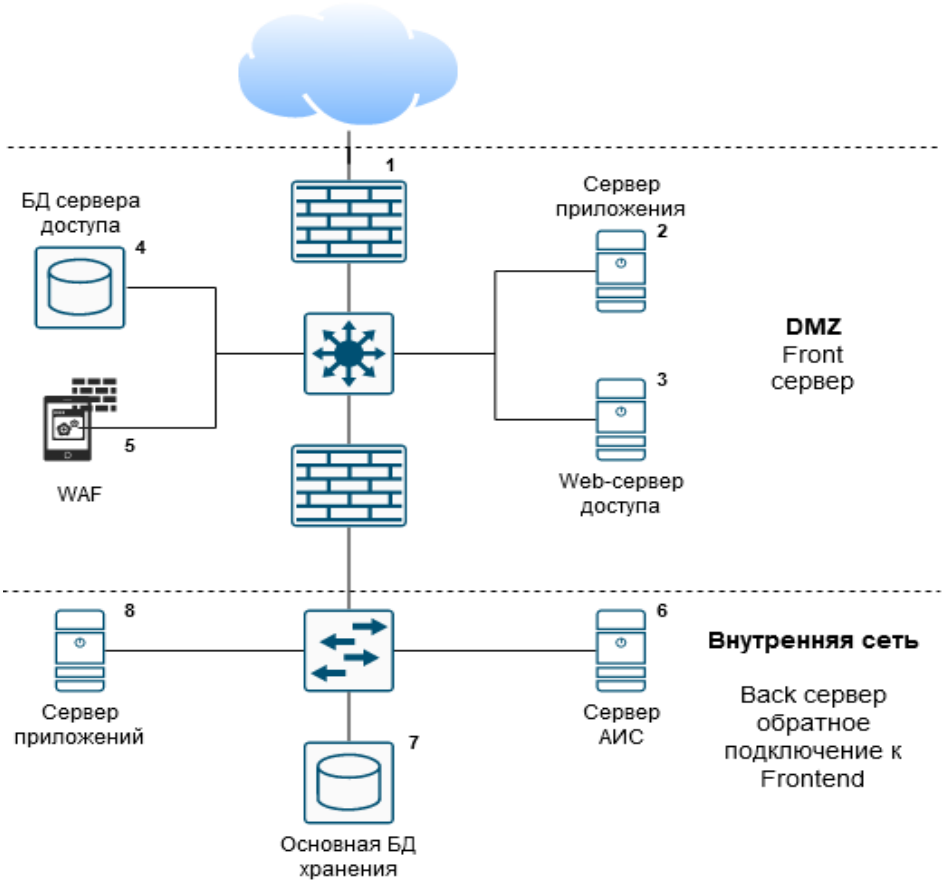


Рисунок 2 – Базовая архитектура сети доступа к АИС
Figure 2 – Basic architecture of the AIS access network

Таблица 2 – Сопоставление атак и контрмер на уровне архитектурной организации web-приложения доступа
Table 2 – Comparison of attacks and countermeasures at the level of the architectural organization of the access web application

Класс атак	Атака	Контрмеры	Уровень реализации	Метрика
Недостатки аутентифи-кации	Подбор пароля	Отображение минимума информации об ошибке при неправильно введенном логине или пароле	Уровень представления	Контроль доступа
		Введение CAPTCHA после нескольких неудачных попыток входа подряд у одного пользователя	Уровень контроллера сессии и модели пользователя	
		Проверка сложности пароля пользователя с	Уровень контроллера	Контроль доступа

		целью предотвращения использования простых паролей.	пользователя и представления	
	Атака через уязвимость в недостаточной аутентифи-кации	Использовать аутентификацию на уровне протокола TLS, что потребует от злоумышленника доступ к компьютеру с сертификатом.	Уровень логики веб–сервера	Контроль доступа
		Предоставление доступа к ресурсам административной части после аутентификации через логин и пароль.	Уровень маршрутизаци и приложения	
	Атака через уязвимость в небезопасном восстановлени и паролей	При восстановлении пароля требовать старый пароль.	Уровень контроллера пользователя и представления	Контроль доступа
		Реализовать функционал восстановления пароля в автоматизированно м режиме с проверкой запроса восстановления пароля администратором.	Все урони веб–приложения.	
Недостатки авторизации	Атака через уязвимость в недостаточной авторизации	На уровне сервера БД реализовать Таблицы: ролей, пользовательских действий, истории действий	Уровень модели данных.	Протоколировани е доступа
		При каждом запросе к АИС осуществлять проверку прав доступа к АИС.	Уровень контроллера и модели данных.	
	Атака по отсутствию таймаута сессии	Установить срок действия сессии.	Уровень контроллера сессии.	Контроль доступа
	Фиксация сессии	После успешного входа создавать новый идентификатор сессии.	Уровень контроллера сессии.	Контроль доступа

		При закрытии вкладки браузера закрывать сессию	Уровень представления.	
		При смене IP адреса закрывать сессию	Уровень контроллера сессии.	
Атаки на стороне клиента	Подделка межсайтовых запросов	Для запросов, которые каким–либо образом изменяют данные в БД, передавать вместе с запросом токен, находящийся на HTML странице, с которой совершается запрос.	Уровень контроллера сессии, уровень представления.	Контроль доступа
	XSS инъекции	Фильтрация пользовательского ввода, в том числе с применением библиотек, распознающих вредоносный код в различных кодировках.	Уровень контроллера приложения.	Предотвращение повреждения данных
		Экранирование специальных символов в приложении, которые могли попасть в него через отправку пользователями данных.	Уровень контроллера приложения, уровень представления.	
Выполнение вредоносного кода на стороне сервера	Выполнение команд ОС	Использование методов, которые передают параметры командной строки безопасно	Уровень служебных подпрограмм.	Предотвращение повреждения данных
	SQL инъекции	Безопасная передача параметров в массиве при любом исполнении SQL	Уровень модели и драйвера баз данных.	Предотвращение повреждения данных
	Внедрение серверных расширений	Запрет на использование функций выполнения пользовательского кода на сервере приложений	Все урони веб-приложения	Предотвращение повреждения данных

Разработка архитектуры защищенного веб-приложения

Диаграмма функциональной модели работы веб-приложения прослойки в нотации IDEF0 изображена на Рисунке 3.

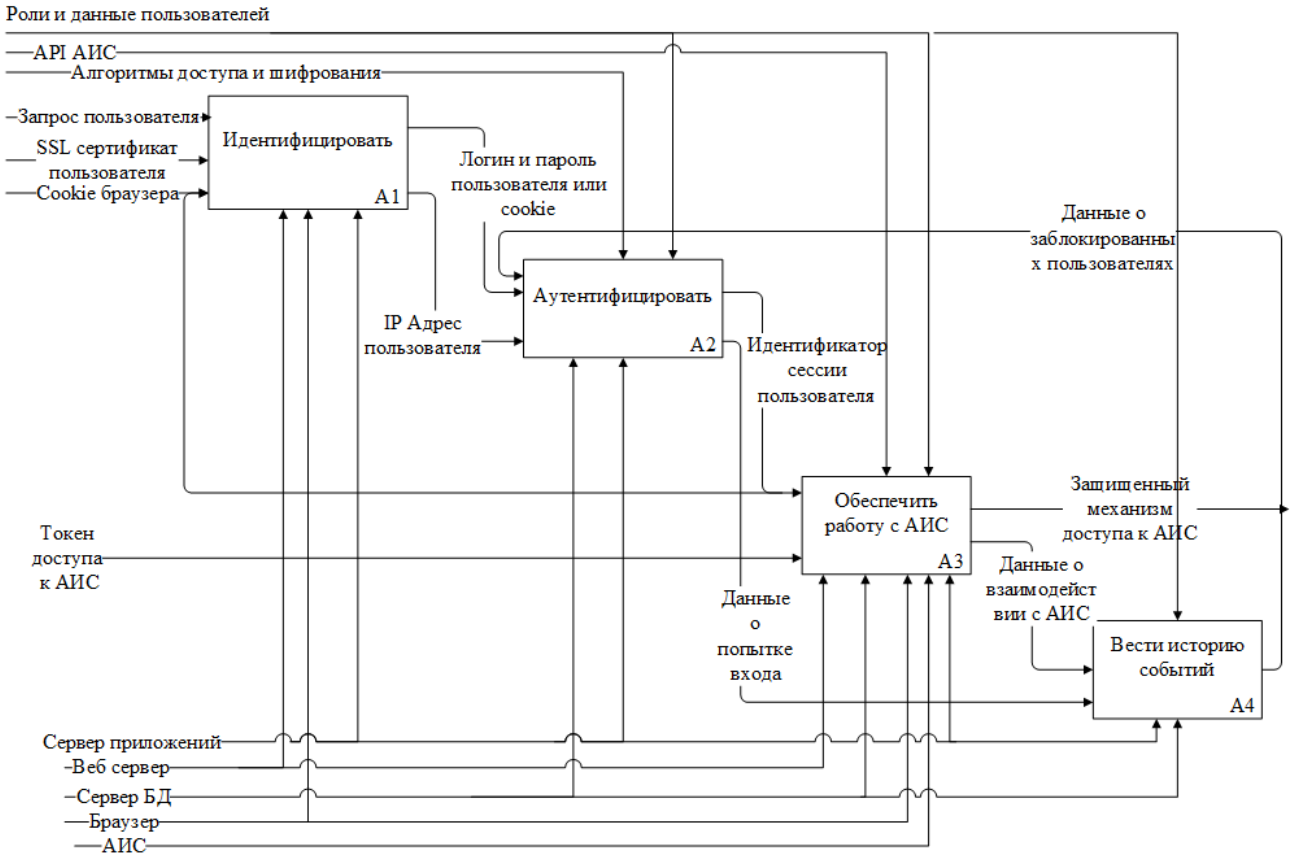


Рисунок 3 – IDEF0 диаграмма работы веб-приложения
Figure 3 – IDEF0 diagram of the web application

Входные данные для веб-приложения:

1. Запрос пользователя предполагает данные о методе запроса, IP адресе пользователя, используемом браузере других HTTP заголовков.
2. SSL сертификат пользователя – сертификат, заранее выданный предприятием (открытый ключ которого известен поддомену проверки сертификатов предприятия или домену веб-приложения) и установленный в браузере пользователя.
3. Cookie пользователя – данные о идентификаторе сессии, IP адресе, текущем входе и т. д.
4. Токен доступа к АИС – ключ, посредством которого веб-приложение осуществляет доступ к АИС. Токен доступа к АИС представляет собой случайную 24-символьную строку.

Взаимодействие сервера и клиента на уровне TLS протокола выполнено согласно RFC 5246 (The Transport Layer Security Protocol Version 1.2). Отметим, что использование двусторонней аутентификации еще до открытия первой HTML страницы многократно усложняет вероятность любой атаки на веб-приложение, поскольку в этом случае у

злоумышленника нет возможности каким-либо образом взаимодействовать с веб-приложением без сертификата.

Веб-приложение применяет архитектурный паттерн Model-View-Controller (MVC, «Модель-Представление-Контроллер»), декомпозирующий приложения на слой обработки данных приложения, слой пользовательского интерфейса и слой логики управления: модель, представление и контроллер. Модель предоставляет данные, изменяя свое состояние, а также отвечает за алгоритмы обработки данных. Слой представления обеспечивает отображение данных. Контроллер реализует взаимодействие пользователя и системы, контролирует и управляет потоком данных. Еще один компонент приложения – маршрутизатор необходим для отождествления адреса запроса и контроллера.

Поскольку специфика работы приложения при запросе аутентификации и при запросах на работу с АИС отличаются, разработаны схемы, отображающие реализацию контрмер: при аутентификации пользователя (Рисунок 4) и при работе пользователя с системой (Рисунок 5).

Рисунок 4 – Контрмеры при аутентификации пользователя
Figure 4 – Countermeasures for user authentication

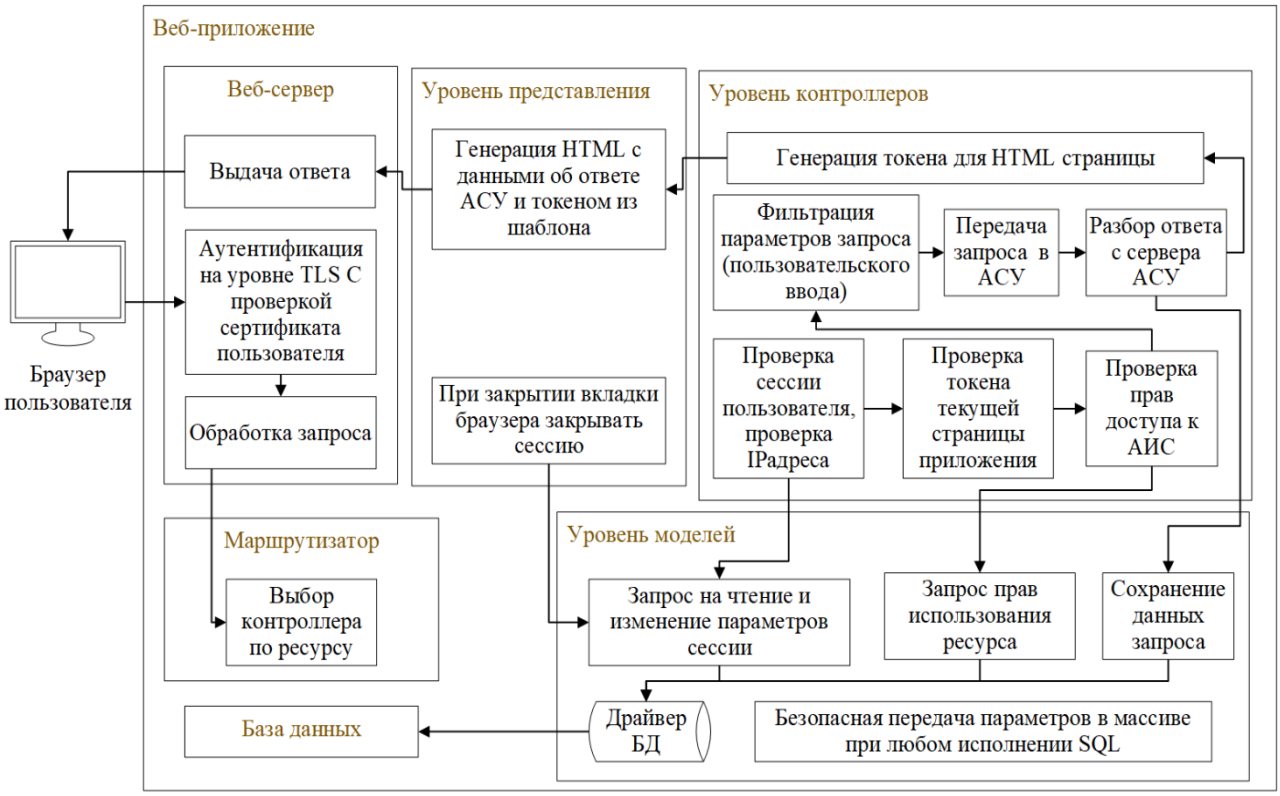


Рисунок 5 – Контрмеры при работе пользователя с системой
Figure 5 – Countermeasures when the user works with the system

Оценка защищенности доступа к АИС с помощью веб-приложения

Оценка защищенности доступа к АИС на основе разработанного веб-приложения была произведена согласно классификатору атак «The WASC Threat Classification v2.0» и методике международного стандарта ISO/IEC 14598–1–6:1998–2001 «Оценивание программного продукта». Оценка защищенности с использованием внутренних метрик безопасности разрабатываемого ПО основывается на вычислении корректно нейтрализованных атак к общему числу атак на программное обеспечение. После выявления векторов возможных атак и их анализа сформулированы контрмеры противодействия для каждого из векторов на разных уровнях архитектурной организации веб-приложения (Таблица 2).

Для количественной оценки защищенности веб-приложения воспользуемся также методикой анализа рисков информационной безопасности и кибербезопасности на основе нечетких серых когнитивных карт, подробно изложенной в [11].

Серая нечеткая когнитивная карта (СНКК) – это ориентированный граф, заданный с помощью кортежа множеств [11]

$$\text{СНКК}=\langle C,F,W\rangle,$$

где C – множество концептов, в качестве которых выступают значимые факторы (вершины графа), F – множество связей между концептами (направленные дуги) и W – множество весов связей СНКК, которые могут быть как положительными, так и отрицательными для «усиления» и «ослабления» влияния концепта соответственно.

Применения алгебры «серых» чисел при задании множества W позволяет использовать нечеткую лингвистическую шкалу с учетом степени уверенности эксперта в текущей оценке (Таблица 3). Состояние концептов X также будет определяться как «серое» число (1) в произвольный дискретный момент времени $t \in N \cup \{0\}$:

$$X_i(t+1) = f\left(X_i(t) + \sum_{\substack{j=1 \\ (j \neq i)}}^{n} W_{ji} X_j(t) \right), \quad (1)$$

где $X_i(t)$ и $X_i(t+1)$ – значения переменной состояния концепта в моменты времени t и t+1, n – число концептов в СНКК, $f(\,)$ – нелинейная функция (гиперболический тангенс).

Таблица 3 – Нечеткая лингвистическая шкала для оценки связи между концептами
Table 3 – Fuzzy linguistic scale for assessing the relationship between concepts

Лингвистическое значение	Диапазон	Обозначение терма
Не влияет	0	Z
Очень слабая	(0; 0,15]	VL
Слабая	(0,15; 0,35]	L
Средняя	(0,35; 0,6]	M
Сильная	(0,6; 0,85]	H
Очень сильная	(0,85; 1]	VH

Оценка локальных относительных рисков нарушения кибербезопасности доступа к АИС через веб-приложение выполнена для наиболее вероятных векторов атак (Таблица 2). Соответствующая СНКК представлена на Рисунке 6.

В Таблице 4 основным угрозам C_2 – C_5 соответствуют сценарии воздействия внешнего злоумышленника в ходе эксплуатации одной или нескольких уязвимостей системы. Каждый из концептов группы C_2 – C_5 представляет собой укрупненную группу концептов, детализирующих действия злоумышленника при реализации класса атак и эксплуатации соответствующих уязвимостей. Оценка весовых коэффициентов взаимовлияния концептов НКК выполнена экспертами на основе международных баз данных угроз и уязвимостей (БДУ ФСТЭК, NVD), метрик CVSS и отчетов аудиторов ИБ. Механизм обобщения группы концептов подробно описан в [12-13].

Рассмотрим четыре сценария воздействия злоумышленника:

– без использования дополнительных контрмер;
– применение архитектурной организации веб-приложения прослойки, учитывающей основные паттерны обеспечения кибербезопасности;
– применение Web-application Firewall;
– применение архитектурной организации приложения и WAF.

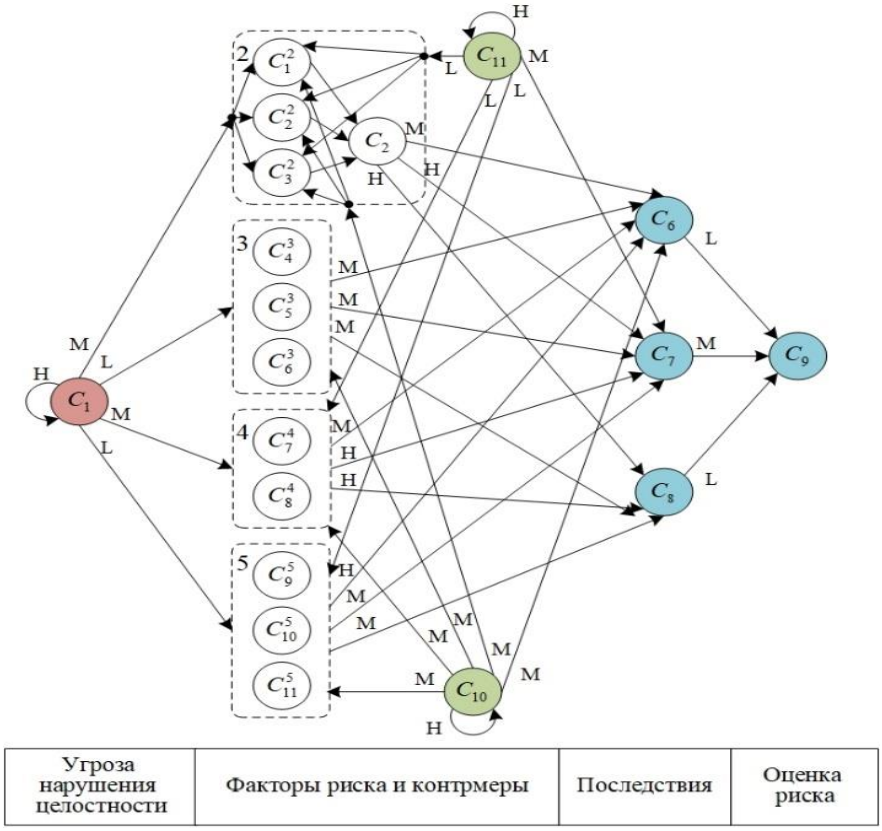
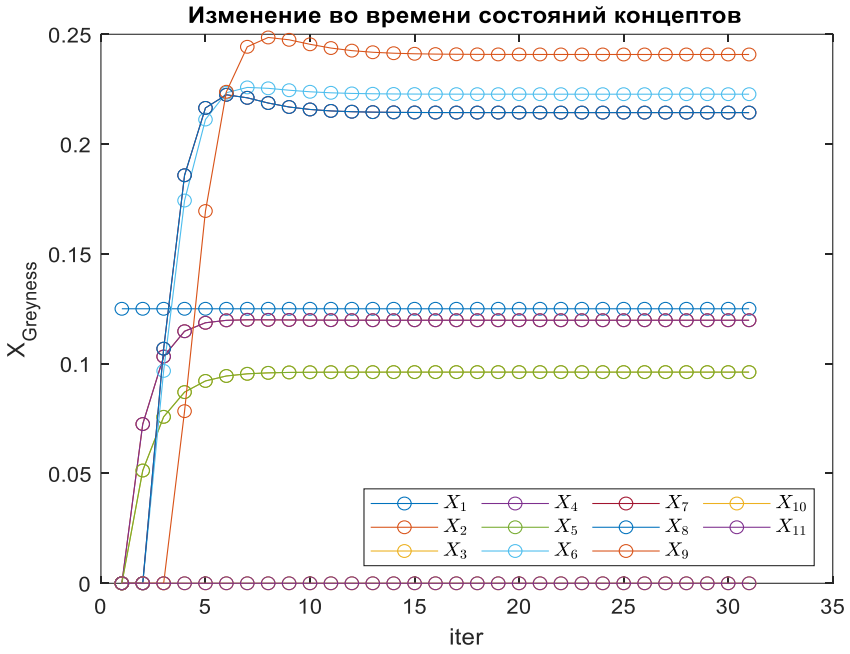


Рисунок 6 – Нечеткая когнитивная карта оценки локальных относительных рисков нарушения кибербезопасности системы доступа к АИС через веб-приложение
Figure 6 – Fuzzy cognitive map for assessing local relative risks of cybersecurity violation of the AIS access system via a web application

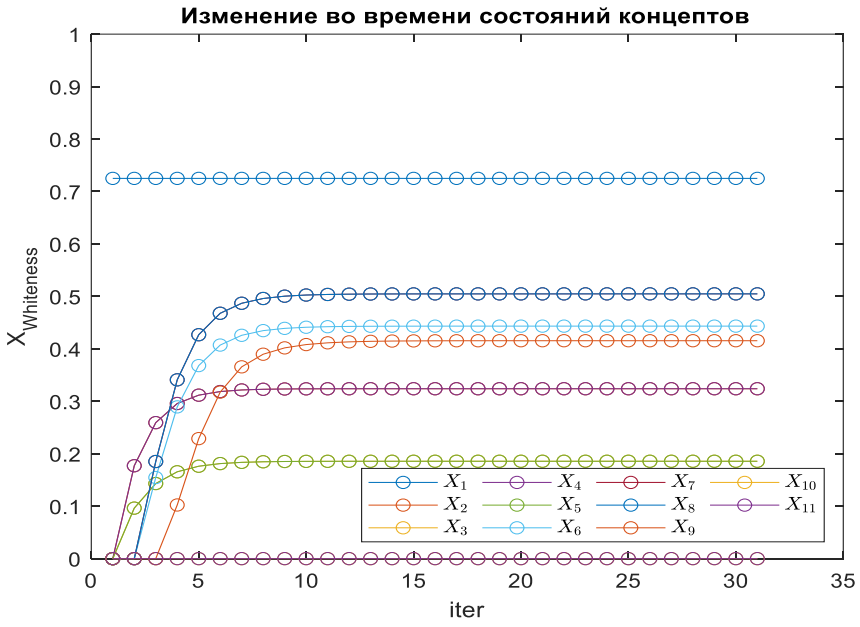
Таблица 4 – Описание концептов нечеткой серой когнитивной карты
Table 4 – Description of fuzzy gray cognitive map concepts

Концепт	Наименование	Тип концепта
$ВЗ_1$	Внешний злоумышленник	Концепт-драйвер
C_2	Недостатки аутентификации	Реализация угрозы нарушения целостности накапливаемых в АИС данных при эксплуатации соответствующих уязвимостей системы доступа
C_3	Недостатки авторизации	
C_4	Атаки на стороне клиента	
C_5	Выполнение вредоносного кода на стороне сервера	
C_6	Сервер БД (хост 4, рис. 2)	Целевые ресурсы системы
C_7	Web-сервер (узел 3, рис. 2)	
C_8	Сервер приложений (узел 2, рис. 2)	
C_9	Нарушение целостности накапливаемых данных	Последствия
C_{10}	Архитектурный дизайн web-приложения	Концепт-драйверы – дополнительные средства защиты
C_{11}	Применение WAF	

Ниже на Рисунках 7 и 8 показан процесс изменения состояния концептов СНКК в случае воздействия злоумышленника без использования и с использованием контрмер.



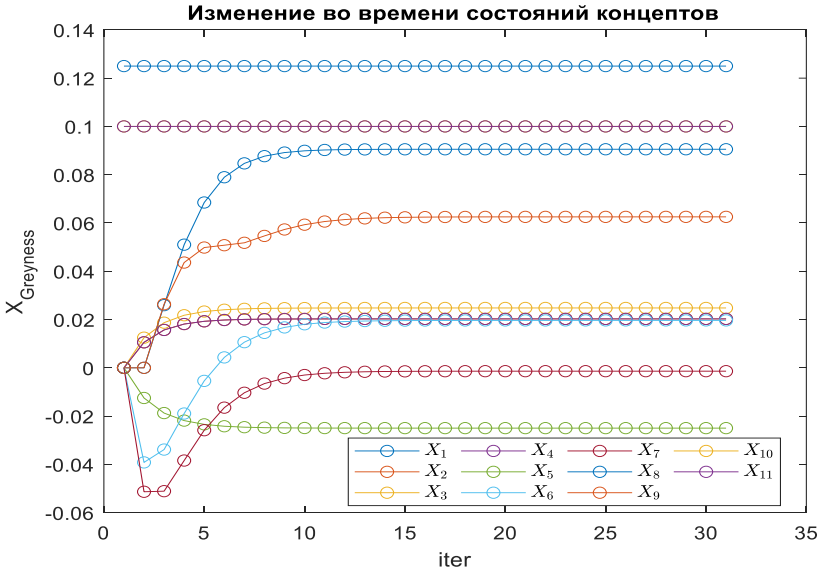
а)



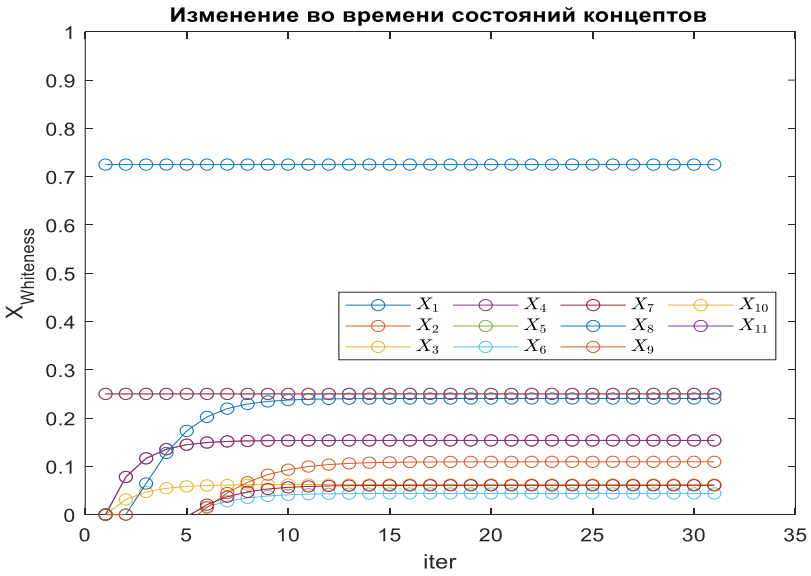
б)

Рисунок 7 – Изменение во времени состояния концептов: (а) «серости» ($X_{Greyness}$) – разброса оценки, б) «отбеленное» ($X_{Whitness}$) – центральное значение интервальной оценки при воздействии злоумышленника без применения дополнительных контрмер

Figure 7 – Change in the state of concepts over time: (a) “grayness” (XGreyness) – the spread of the estimate, b) “whitness” (XWhitness) – the central value of the interval estimate when exposed to an intruder without applying additional countermeasures



а)



б)

Рисунок 8 – Изменение во времени состояния концептов: (а) «серости» ($X_{Greyness}$) – разброса оценки, б) «отбеленное» ($X_{Whitness}$) – центральное значение интервальной оценки при воздействии злоумышленника и применении дополнительных контрмер

Figure 8 – Change in the state of the concepts over time: (a) “grayness” (XGreyness) – the spread of the estimate, b) “whitness” (XWhitness) – the central value of the interval estimate under the influence of an intruder and the use of additional countermeasures

Показатели относительного риска для целевого концепта C_9, характеризующего нарушение целостности накапливаемых данных ТМИ, отражены в Таблице 5 (в виде интервальных оценок) и на Рисунке 9 (в виде центрального значения и разброса оценки).

Таблица 5 – Результаты анализа рисков на основе СНКК
Table 5 – Results of the risk analysis based on the FGCM

Целевой концепт	Без применения дополнительных контрмер	Применение архитектурной организации web-приложения	Применение WAF	Применение и архитектурной организации, и WAF
Нарушение целостности накапливаемых данных	[0,1747; 0,6563]	[0,1157; 0,4729]	[0,1304; 0,5668]	[0,0468; 0,1719]

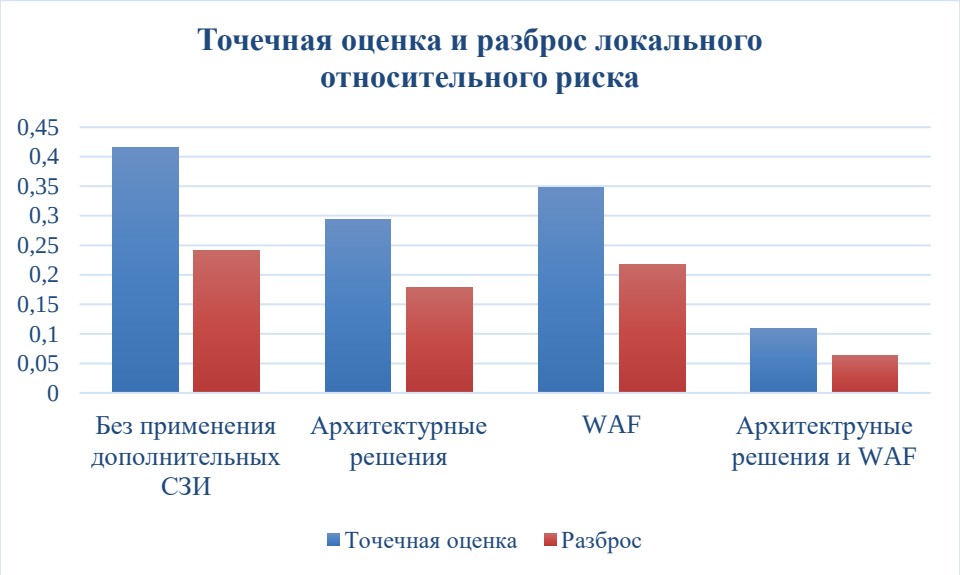


Рисунок 9 – Точечная оценка и разброс локального относительного риска для целевого концепта, определяющего вероятность нарушения целостности накапливаемых данных
Figure 9 – Point estimate and spread of local relative risk for the target concept, which determines the likelihood of violation of the integrity of the accumulated data

Поскольку для всех потенциальных векторов атак на программное обеспечение выработаны контрмеры на архитектурном уровне и дополнительно применены средства организации мониторинга запросов к веб-приложению с помощью WAF, доступ к АИС на основе разработанного веб-приложения можно считать достаточно защищенным. Оценка локального относительно риска нарушения целостности накапливаемых данных улучшилась в 3,5 раза и снизилась до относительной величины $0{,}109 \pm 0{,}063$.

Заключение

Атаки на веб-приложения на периметре информационных систем организуются злоумышленниками с целью получения первичного доступа и закрепления в инфраструктуре предприятия. Основными средствами защиты веб-приложений является проектирование архитектуры приложения с учетом основных паттернов обеспечения безопасности и применение решений класса Web Application Firewall.

В ходе анализа выявлены векторы возможных атак на веб-приложение, которые определили основные функциональные требования к технологиям реализации и к архитектуре. Разработана схема, описывающая контрмеры применительно к Model-

View-Controller архитектуре web-приложения. Для обеспечения безопасности на уровне сети была модернизирована базовая архитектура сети предприятия с демилитаризованной зоной и соответствующей конфигурацией межсетевых экранов.

Для оценки защищенности использованы внутренние метрики защищенности программного обеспечения. Поскольку для выявленных атак на программное обеспечение для каждой метрики контрмеры на архитектурном уровне внедрены в полном объеме, доступ к АИС на основе разработанного веб-приложения можно считать защищенным. Для оценки защищенности также применена методика анализа рисков информационной безопасности и кибербезопасности на основе нечетких серых когнитивных карт, позволившая количественно оценить снижение оценки локального относительного риска нарушения целостности накапливаемых данных в 3,5 раза.

СПИСОК ИСТОЧНИКОВ

1. Frid A.I. et al. Architecture of the Security Access System for Information on the State of the Automatic Control Systems of Aircraft. *Acta Polytechnica Hungarica.* 2020;17(8):151–164.
2. Frid A.I. et al. The architecture of the web application for protected access to the informational system of processing critically important information. *Proceedings of 19th International Workshop «Computer Science and Information Technologies» (CSIT'2017), Baden-Baden, Germany*. 2017;16–22.
3. Гузаиров М.Б. и др. Защищенный доступ к базе данных о состоянии систем автоматического управления (САУ) авиационными ГТД через веб-приложение. *Информация и безопасность*. 2017;20(3):410–413.
4. Web Application Security Consortium. Доступно по: http://www.webappsec.org/ (дата обращения: 20.10.2021).
5. Huang H.C. et al. Web application security: Threats, countermeasures, and pitfalls. *Computer*. 2017;50(6):81–85.
6. OWASP Top Ten Project. Доступно по: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (дата обращения: 20.10.2021).
7. Wichers D. OWASP TOP-10 2013. *OWASP Foundation, February*. 2013.
8. Wiradarma A.A.B.A., Sasmita G.M.A. IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*. 2019;11(12):17–29.
9. Recommendations of the National Institute of Standards and Technology. *NIST*. 2014:128.
10. The WASC Threat Classification v2.0. Доступно по: http://projects.webappsec.org/w/page/13246978/Threat%20Classification (дата обращения: 20.10.2021).
11. Васильев В.И., Вульфин А.М., Гузаиров М.Б., Кириллова А.Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт. *Информационные технологии*. 2018;24(10):657–664.
12. Васильев В.И. и др. Оценка рисков кибербезопасности АСУ ТП промышленных объектов на основе вложенных нечетких когнитивных карт. *Информационные технологии.* 2020;26(4):213–221.
13. Васильев В.И., Вульфин А.М., Черняховская Л.Р. Анализ рисков инновационных проектов с использованием технологии многослойных нечетких когнитивных карт. *Программная инженерия*. 2020;11(3):142–151.

REFERENCES

1. Frid A.I. et al. Architecture of the Security Access System for Information on the State of the Automatic Control Systems of Aircraft. *Acta Polytechnica Hungarica*. 2020;17(8):151–164.
2. Frid A.I. et al. The architecture of the web application for protected access to the informational system of processing critically important information. *Proceedings of 19th International Workshop «Computer Science and Information Technologies» (CSIT'2017)*, Baden-Baden, Germany. 2017:16–22.
3. Guzairov M.B. et al. Protected access to the database on the state of automatic control systems (ACS) of aviation gas turbine engines via a web application. *Informacija i bezopasnost'*. 2017;20(3):410–413. (In Russ.)
4. *Web Application Security Consortium*. Available from: http://www.webappsec.org/ (accessed 20.10.2021).
5. Huang H.C. et al. Web application security: Threats, countermeasures, and pitfalls, *Computer*. 2017;50(6):81–85.
6. OWASP Top Ten Project. Available from: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project (accessed on 20.10.2021).
7. Wichers D. OWASP TOP-10 2013. *OWASP Foundation.* February 2013.
8. Wiradarma A.A.B.A., Sasmita G.M.A. IT Risk Management Based on ISO 31000 and OWASP Framework using OSINT at the Information Gathering Stage (Case Study: X Company). *International Journal of Computer Network and Information Security*. 2019;11(12):17–29.
9. *Recommendations of the National Institute of Standards and Technology*. NIST. 2014:128.
10. *The WASC Threat Classification v2.0.* Available from: http://projects.webappsec.org/w/page/13246978/Threat%20Classification (дата обращения 20.10.2021).
11. Vasilyev V.I., Vulfin A.M., Guzairov M.B., Kirillova A.D. Interval estimation of information risks with use of fuzzy grey cognitive maps. *Informacionnye tehnologii = Information technologies*. 2018;24(10):657–664. (In Russ.)
12. Vasilyev V.I. et al. Cybersecurity risk assessment of industrial objects' ACS of TP on the basis of nested fuzzy cognitive maps technology. *Informacionnye tehnologii = Information technologies*. 2020;26(4):213–221. (In Russ.)
13. Vasilyev V.I., Vulfin A.M., Chernyakhovskaya L.R. Risk analysis of innovative projects with use of multilayer fuzzy cognitive maps. *Programmnaja inzhenerij = Software Engineering.* 2020;11(3):142–151. (In Russ.)

ИНФОРМАЦИЯ ОБ АВТОРАХ / INFORMATION ABOUT THE AUTHORS

Вульфин Алексей Михайлович, кандидат технических наук, доцент Уфимского государственного авиационного технического университета, Уфа, Российская Федерация.
e-mail: vulfin.alexey@gmail.com
ORCID: 0000-0001-5857-2413

Alexey Mikhailovich Vulfin, Candidate of Technical Sciences, Associate Professor, Ufa State Aviation Technical University, Ufa, Russian Federation.

Статья поступила в редакцию 14.12.2021; одобрена после рецензирования 23.12.2021; принята к публикации 26.12.2021.

The article was submitted 14.12.2021; approved after reviewing 23.12.2021; accepted for publication 26.12.2021.