Открытый журнал евразийских исследований, 2026, №1, сс. 101-109
doi: 10.65469/eijournal.2026.1.12
eijournal.ilimbilim.kg

ИНФОРМАТИКА / COMPUTER SCIENCE
УДК 004.056:004.738.5:336.71

Защита персональных и платёжных данных на серверах веб-приложений

Абдумиталип уулу Кубатбек
к.ф.-м.н., доцент, Ошский государственный университет, Кыргызстан, kuba@oshsu.kg,
ORCID: 0009-0000-5208-0741

Омаралиев Абдималик Чырмашович
к.п.н., доцент, Ошский государственный университет, Кыргызстан, aomaraliev@oshsu.kg,
ORCID: 0009-0000-9214-7488

Арынова Кумушай Арыновна
магистрант, Ошский государственный университет, Кыргызстан, loik91166@gmail.com,
ORCID: 0009-0000-1018-6986

Замирбек кызы Ыкыбал
магистрант, Ошский государственный университет, Кыргызстан, ykybalzamirbek@gmail.com,
ORCID: 0009-0008-8542-801X

Аннотация
Серверная инфраструктура веб-приложений банков и платёжных сервисов обрабатывает персональные профили клиентов, журналы операций и платёжные реквизиты, поэтому ошибки конфигурации серверов, баз данных и межсервисного взаимодействия приводят к наиболее тяжёлым инцидентам нарушения конфиденциальности, целостности и доступности данных. Построена модель серверной обработки персональных и платёжных данных, выделены ключевые потоки информации и зоны доверия. Для шести типовых угроз рассчитаны оценки риска в диапазоне от 12 до 20 баллов. Сформирована таблица мер защиты с количественными показателями влияния на снижение риска, задержку обработки запросов и трудоёмкость внедрения. Полученные результаты могут использоваться при проектировании и модернизации серверной инфраструктуры банковских веб-приложений, выборе приоритетных мер защиты и обосновании поэтапного внедрения средств обеспечения информационной безопасности.

Ключевые слова: персональные данные, платёжные данные, веб-приложения, серверная инфраструктура, информационная безопасность, банковские системы, контроль доступа, журналирование, токенизация

Для цитирования: Абдумиталип уулу К., Омаралиев А.Ч., Арынова К.А., Замирбек кызы Ы. (2026). Защита персональных и платёжных данных на серверах веб-приложений. *Открытый журнал евразийских исследований*, №1, сс. 101-109. doi: 10.65469/eijournal.2026.1.12

Введение

Развитие онлайн-банкинга, платёжных сервисов и дистанционного обслуживания привело к тому, что критически важные данные всё чаще концентрируются именно на стороне сервера. В серверной инфраструктуре веб-приложений хранятся персональные сведения клиентов, платёжные токены, журналы транзакций, ключевой материал и служебные данные, обеспечивающие выполнение финансовых операций. В отличие от клиентской части, компрометация серверного уровня затрагивает сразу большие массивы данных и обычно приводит не только к прямому финансовому ущербу, но и к регуляторным, репутационным и операционным потерям [1; 2; 3].

В публикациях чаще разбирают либо общую безопасность веб-приложений, либо банковские ИС в целом; сочетание «архитектура веб-приложения — серверная обработка — платёжная инфраструктура» освещено недостаточно [4; 5; 6]. На практике меры нередко задаются перечнем без измеримых критериев: неочевидно, какие контроли дают наибольшее снижение риска и как они сказываются на задержках и трудозатратах.

Целью работы является разработка модели защиты персональных и платёжных данных на серверах веб-приложений и сравнительная оценка конфигураций серверной защиты для систем финансового профиля. Для достижения этой цели решаются следующие задачи: описывается архитектура серверной обработки данных; систематизируются основные угрозы; формируется набор применимых мер защиты; выполняется количественная сравнительная оценка конфигураций серверной защиты; формулируются практические рекомендации по поэтапному внедрению контрмер.

Материалы и методы исследования

В качестве теоретической базы использованы нормативные документы и научные источники: Федеральный закон «О персональных данных», ГОСТ Р 57580.1-2017, PCI DSS v4.0, NIST SP 800-53, ГОСТ Р ИСО/МЭК 27001-2021, а также работы по защите информации в банковских системах и тестированию безопасности веб-приложений [1; 2; 3; 4; 5; 6; 7; 10; 11].

Модель исследования основана на типовом серверном стенде, включающем обратный прокси в демилитаризованной зоне, сервер приложений, сервер баз данных, подсистему журналирования, сервис управления ключами и платёжный шлюз. Для сравнения были рассмотрены три конфигурации защиты:

1. Базовая: TLS на внешнем контуре, парольная аутентификация пользователей, стандартное журналирование операций.

2. Усиленная: дополнительно шифрование данных при хранении, сегментация зон обработки, MFA для администраторов, централизованное управление ключами и разграничение привилегий сервисных учётных записей.

3. Комплексная: дополнительно токенизация платёжных реквизитов, централизованный SIEM-мониторинг, неизменяемые журналы, изолированные резервные копии и регулярные тесты восстановления.

Оценка угроз выполнялась по двум шкалам: вероятность реализации P и ущерб I, каждая по пятибалльной шкале. Итоговая оценка риска определялась как $R = P \times I$. Для сопоставления конфигураций использован интегральный показатель защищённости S, рассчитываемый по формуле: $S = 0{,}35K_{conf} + 0{,}25K_{int} + 0{,}20K_{avail} + 0{,}20K_{comp}$, где K_{conf}, K_{int}, K_{avail} и K_{comp} представляют частные оценки конфиденциальности, целостности, доступности и регуляторного соответствия по шкале от 1 до 5. Такой подход позволяет не только описывать меры защиты качественно, но и сопоставлять их по измеримым критериям.

Архитектура серверной обработки данных

Типовая архитектура веб-приложения, обрабатывающего персональные и платёжные данные, включает три базовых логических уровня: внешний контур взаимодействия с клиентами, прикладной уровень и уровень хранения данных. На внешнем контуре располагаются клиентские интерфейсы, балансировщик нагрузки, WAF и обратный прокси; на прикладном уровне выполняются аутентификация, бизнес-логика и интеграция с внешними сервисами; на уровне хранения функционируют СУБД, журнальные хранилища и сервисы резервного копирования. Для финансовых систем критически важно разделение этих уровней на зоны доверия с жёстко регламентированными каналами связи [2; 3; 4].

Серверная архитектура должна обеспечивать разделение потоков персональных и платёжных данных. Персональные данные передаются от клиентского интерфейса к серверу приложений и далее к профильной БД, тогда как платёжные реквизиты должны либо обрабатываться в выделенном сегменте, либо как можно раньше преобразовываться в токены. Дополнительные меры защиты включают обязательное шифрование межсервисного трафика, хранение ключей в отдельном защищённом контуре и вывод журналов в централизованную подсистему мониторинга.

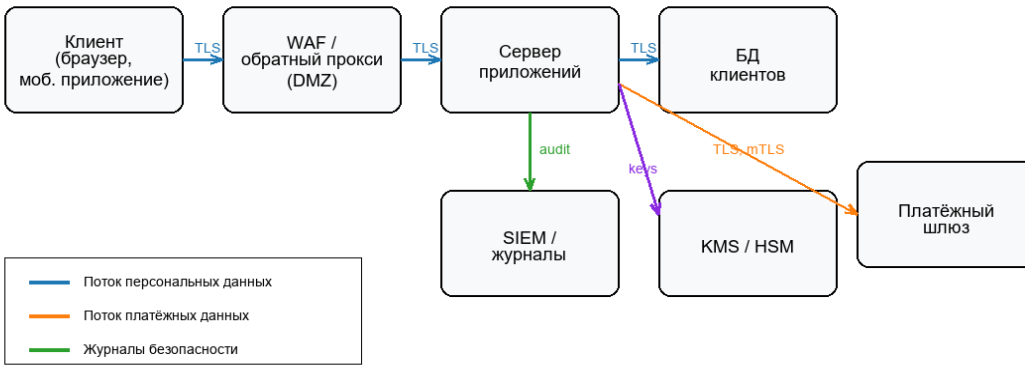

Рисунок 1. Архитектура серверной обработки персональных и платёжных данных

Количественная оценка угроз серверной части

Анализ серверной инфраструктуры показал, что наибольший риск для финансовых веб-приложений представляют угрозы, сочетающие высокую вероятность эксплуатации и тяжёлые последствия для транзакционной среды. Наиболее критичными оказались несанкционированный доступ к базам данных и DDoS-воздействие на внешний сервис, тогда как манипуляции с журналами и межсервисным трафиком имеют несколько меньшую вероятность, но сохраняют высокий ущерб из-за регуляторных последствий и сложности расследования инцидентов.

Таблица 1. Оценка основных угроз серверной части веб-приложения

Угроза	P, балл	I, балл	R = P x I	Наиболее уязвимый компонент	Приоритетная мера защиты
Несанкционированный доступ к БД с профилями клиентов и историей операций	4	5	20	Сервер БД	Шифрование при хранении, выделенные сервисные учётные записи, MFA для администраторов
DDoS-воздействие на	4	4	1	Веб-сервер,	WAF, фильтрация трафика,

внешний веб-контур			6	балансировщик	балансировка нагрузки, резервирование каналов
Перехват межсервисного трафика между приложением и БД	3	5	15	Каналы приложений и БД	TLS 1.3, mTLS, контроль сертификатов, отказ от небезопасных протоколов
Подмена транзакционных записей	3	5	15	Сервер приложений, журналы операций	Разделение прав, контроль целостности записей, неизменяемые журналы
Шифровальщик в контуре резервного хранения	3	5	15	Сервер резервного копирования	Изолированные бэкапы, контроль записи, регулярные тесты восстановления
Сокрытие следов атаки через модификацию логов	3	4	12	Подсистема журналирования	Централизованное логирование, WORM-хранилище, контроль целостности

Представленные значения показывают, что для финансовых веб-приложений недостаточно ограничиваться только защитой внешнего периметра. Даже при наличии TLS на пользовательском контуре уязвимыми остаются внутренние соединения, административные интерфейсы и контуры хранения резервных копий. Следовательно, архитектура защиты должна строиться по принципу "от данных", а не по принципу "от границы сети".

Оценка мер защиты и особенности банковских систем

Банковские и платёжные системы предъявляют повышенные требования к неотказуемости операций, прослеживаемости действий пользователей и сотрудников, а также к защите чувствительных реквизитов в ходе межсистемного обмена [2; 3; 11]. Поэтому серверные меры защиты необходимо рассматривать не изолированно, а как набор взаимосвязанных контролей, обеспечивающих снижение конкретных групп рисков. С точки зрения архитектуры прохождения платёжной транзакции критичными являются три участка: передача данных от клиента к внешнему контуру, обработка реквизитов в приложении и обмен с платёжным шлюзом. На каждом из этих участков должны применяться собственные меры защиты: TLS и WAF на внешнем входе, разграничение прав и токенизация в сервере приложений, mTLS и проверка доверенной среды при взаимодействии со шлюзом.

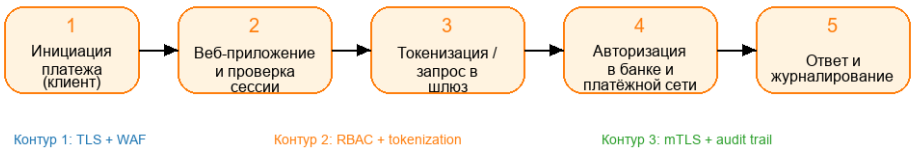

Рисунок 2. Потоки платёжных данных между веб-приложением, платёжным шлюзом и банковской инфраструктурой

Для количественного сопоставления серверных мер защиты в Таблице 2 приведены экспертные оценки их влияния на снижение совокупного риска и эксплуатационные характеристики модельного стенда. Проценты отражают ожидаемое уменьшение совокупного риска относительно базовой конфигурации при изолированном внедрении соответствующей меры.

Таблица 2. Сравнительная оценка основных серверных мер защиты

Мера защиты	Снижение совокупного риска, %	Рост средней задержки обработки, %	Трудоёмкость внедрения, чел.-нед.	Влияние на выполнение регуляторных требований
TLS 1.3 на внешнем контуре и mTLS между сервисами	18	4	02.мар	Высокое
Шифрование данных при хранении + KMS/HSM	22	6	04.июн	Высокое
RBAC для сервисов и MFA для администраторов	20	2	03.апр	Высокое
Централизованное журналирование и SIEM-мониторинг	15	5	04.май	Среднее / высокое
Токенизация платёжных реквизитов	24	7	06.авг	Высокое
Изолированные резервные копии и тесты восстановления	17	1	03.апр	Высокое

Из Таблицы 2 видно, что наиболее заметное снижение риска обеспечивают токенизация платёжных реквизитов, шифрование при хранении и жёсткое разграничение доступа. При этом по соотношению "эффект / стоимость внедрения" высокую практическую ценность имеют RBAC + MFA и корректно настроенные защищённые каналы связи. Это подтверждает целесообразность поэтапного внедрения средств защиты: в первую очередь следует закрывать контроли с высокой регуляторной значимостью и умеренной стоимостью реализации, а затем переходить к более сложным механизмам.

Сравнение конфигураций серверной защиты

Сводная оценка трёх конфигураций показала, что базовая защита позволяет решить только минимальный набор задач и не обеспечивает достаточного покрытия рисков, характерных для банковского веб-приложения. Усиленная конфигурация заметно уменьшает остаточный риск за счёт сегментации, шифрования хранения и усиления административного доступа. Комплексная конфигурация обеспечивает наилучший результат благодаря сочетанию криптографических, архитектурных и организационных мер.

Таблица 3. Сравнительная оценка конфигураций серверной защиты

Конфигурация	Количество реализованных мер	Покрытие регуляторных требований, %	Остаточный риск, балл	Рост средней задержки, %	Трудоёмкость внедрения, чел.-нед.	Интегральный показатель защищённости, балл
Базовая	3	54	15	4	04.май	2,6
Усиленная	6	79	9	9	09.ноя	4,2
Комплексная	8	93	5	14	16-18	5

Значения Таблицы 3 показывают, что переход от базовой к усиленной конфигурации почти в 1,6 раза уменьшает остаточный риск и существенно повышает уровень соответствия

нормативным требованиям. Комплексная конфигурация обеспечивает максимальный интегральный показатель защищённости, однако требует более серьёзных организационных ресурсов и зрелых процессов сопровождения. Для большинства организаций банковского профиля рациональной стратегией является переход к комплексной модели через промежуточный усиленный этап.

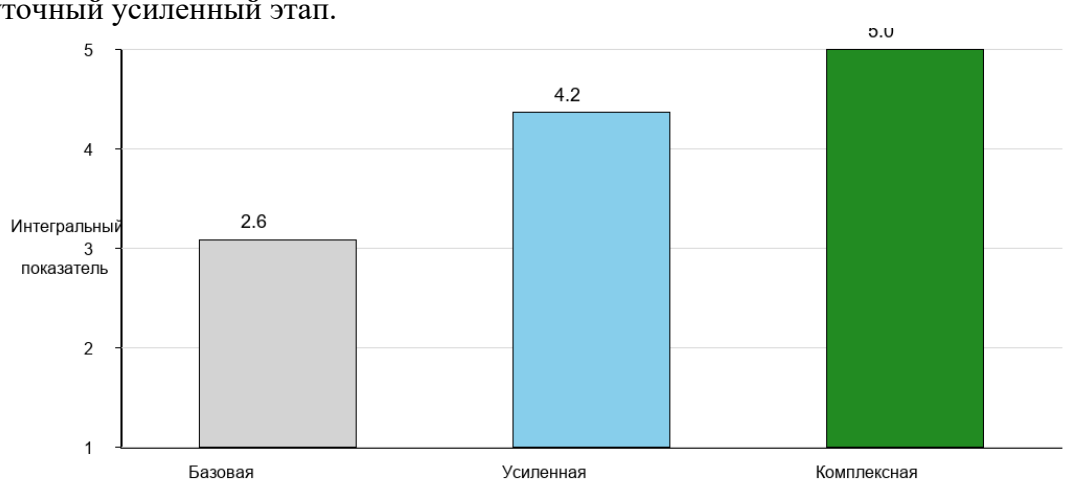

Рисунок 3. Сравнительная диаграмма интегрального показателя защищённости конфигураций серверной защиты

Заключение

В работе предложена модель защиты персональных и платёжных данных на серверах веб-приложений для банковского и платёжного контекста. Архитектура серверной обработки увязана с количественной оценкой угроз и сравнением конфигураций по измеримым критериям; эффективность контролей отражена в риск-ориентированных и эксплуатационных показателях, а не только в описательной форме.

Установлено, что наибольший вклад в снижение совокупного риска дают шифрование при хранении, токенизация платёжных реквизитов, разграничение привилегий и защищённое журналирование. Базовая конфигурация пригодна лишь для минимально допустимого уровня защиты, тогда как устойчивость к критичным для финансового сектора сценариям достигается при переходе к усиленной и комплексной конфигурациям.

Практическая ценность работы заключается в возможности использовать предложенные таблицы и модель оценки при проектировании серверной архитектуры, выборе приоритетов внедрения и подготовке обоснований для модернизации средств защиты данных. Перспективой дальнейших исследований является верификация предложенных оценок на экспериментальном стенде с реальными нагрузочными и инцидентными сценариями.

Список литературы

1. Федеральный закон от 27.07.2006 № 152-ФЗ "О персональных данных" // Собрание законодательства Российской Федерации. 2006. № 31 (ч. 1). Ст. 3451.
2. ГОСТ Р 57580.1-2017. Защита информации финансовых организаций. Общие положения. М.: Стандартинформ, 2018.
3. Payment Card Industry Data Security Standard (PCI DSS). Requirements and Security Assessment Procedures. Version 4.0. PCI SSC, 2022.

4. NIST Special Publication 800-53 Rev. 5. Security and Privacy Controls for Information Systems and Organizations. Gaithersburg: NIST, 2020.
5. OWASP Foundation. OWASP Top 10: The Ten Most Critical Web Application Security Risks. 2021.
6. Внуков А. А. Защита информации в банковских системах: учеб. пособие. М.: Юрайт, 2018. 235 с.
7. Воронцова С. Ю. Обеспечение информационной безопасности в банковской сфере: монография. М.: КноРус, 2015. 198 с.
8. Аркабаев Н. К. Разработка web серверных приложений на базе .NET Core в примере интернет-магазина // Вестник Ошского государственного университета. 2024. № 1. С. 142-154. https://doi.org/10.52754/16948610_2024_1_13
9. Кыштообаева Ч. Роль компьютерных технологий в повышении качества образования учащихся // Вестник Ошского государственного университета. 2023. № 3. С. 51-58. https://doi.org/10.52754/16948610_2023_3_6
10. Омаралиев А., Карабаев С., Омаралиева Г., Данг В. Методология тестирования безопасности веб-приложений на Django с акцентом на выявление уязвимостей бизнес-логики // Вестник Ошского государственного университета. 2025. № 4. С. 199-211. https://doi.org/10.52754/16948610_2025_4_14
11. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. М.: Стандартинформ, 2021.

Евразия изилдөөлөрү ачык журналы, 2026, №1, бб. 101-109
doi: 10.65469/eijournal.2026.1.12
eijournal.ilimbilim.kg

ИНФОРМАТИКА / COMPUTER SCIENCE
УДК 004.056:004.738.5:336.71

Веб-тиркемелердин серверлеринде жеке маалыматтарды жана төлөм маалыматтарын коргоо

Абдумиталип уулу Кубатбек
ф.-м.и.к., доцент, Ош мамлекеттик университети, Кыргызстан, kuba@oshsu.kg, ORCID: 0009-0000-5208-0741

Омаралиев Абдималик Чырмашович
п.и.к., доцент, Ош мамлекеттик университети, Кыргызстан, aomaraliev@oshsu.kg,
ORCID: 0009-0000-9214-7488

Арынова Күмүшай Арыновна
магистрант, Ош мамлекеттик университети, Кыргызстан, loik91166@gmail.com,
ORCID: 0009-0000-1018-6986

Замирбек кызы Ыкыбал
магистрант, Ош мамлекеттик университети, Кыргызстан, ykybalzamirbek@gmail.com,
ORCID: 0009-0008-8542-801X

Аннотация
Банктардын жана төлөм сервистеринин веб-тиркемелеринин сервердик инфраструктурасы кардарлардын жеке профилдерин, операциялар журналдарын жана төлөм реквизиттерин иштетет. Ошондуктан серверлердин, маалымат базаларынын жана кызматтар аралык өз ара аракеттенүүнүн туура эмес конфигурацияланышы маалыматтардын купуялуулугун, бүтүндүгүн жана жеткиликтүүлүгүн бузууга алып келген эң оор инциденттерди жаратышы мүмкүн. Жеке жана төлөм маалыматтарын серверде иштетүүнүн модели түзүлүп, негизги маалымат агымдары жана ишеним зоналары аныкталды. Алты типтүү коркунуч үчүн 12ден 20 баллга чейинки тобокелдик баалары эсептелди. Коргонуу чараларынын таблицасы түзүлүп, алардын тобокелдикти азайтууга тийгизген таасири, сурамдарды иштетүү кечигүүсү жана ишке киргизүүнүн эмгек сыйымдуулугу сандык көрсөткүчтөр менен берилди. Алынган жыйынтыктар банктардын веб-тиркемелеринин сервердик инфраструктурасын долбоорлоодо жана модернизациялоодо, коргонуу чараларын тандоодо жана маалыматтык коопсуздук каражаттарын этап-этабы менен киргизүүнү негиздөөдө колдонулушу мүмкүн.

Ачкыч сөздөр: жеке маалыматтар, төлөм маалыматтары, веб-тиркемелер, сервердик инфраструктура, маалыматтык коопсуздук, банктык системалар, жеткиликтүүлүктү көзөмөлдөө, журналдаштыруу, токенизация

Open Journal of Eurasian Issues, 2026, no. 1, pp. 101-109
doi: 10.65469/eijournal.2026.1.12
eijournal.ilimbilim.kg

ИНФОРМАТИКА / COMPUTER SCIENCE
УДК 004.056:004.738.5:336.71

Protection of Personal and Payment Data on Web Application Servers

Abdumitalip uulu Kubatbek
Candidate of Physico-Mathematical Sciences, Associate Professor, Osh State University, Kyrgyzstan, kuba@oshsu.kg, *ORCID: 0009-0000-5208-0741*

Omaraliev Abdimalik Chyrmashovich
Candidate of Pedagogical Sciences, Associate Professor, Osh State University, Kyrgyzstan, aomaraliev@oshsu.kg, *ORCID: 0009-0000-9214-7488*

Arynova Kumushai Arynovna
Master's Students, Osh State University, Kyrgyzstan, loik91166@gmail.com, *ORCID: 0009-0000-1018-6986*

Zamirbek kyzy Ykybal
Master's Students, Osh State University, Kyrgyzstan, ykybalzamirbek@gmail.com, *ORCID: 0009-0008-8542-801X*

Abstract
Server-side infrastructure of banking and payment web applications processes customer profiles, transaction logs and payment credentials; therefore, misconfigurations of servers, databases and inter-service communication lead to severe confidentiality, integrity and availability incidents. A model of server-side processing of personal and payment data was developed, key data flows and trust zones were identified, and six typical threats were scored within the 12-20 risk range. The proposed model can be applied to the design and modernization of banking web infrastructures and to the prioritization of security controls under limited organizational resources.

Keywords: personal data, payment data, web applications, server infrastructure, information security, banking systems, access control, logging, tokenization