ISSN 2658-5014 (Print) СИИТ ISSN 2686-7044 (Online)
http://siit.ugatu.su 2026. Т. 8, № 2(26)
СИСТЕМНАЯ ИНЖЕНЕРИЯ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ
Научная статья

УДК 004.8 DOI: 10.54708/SIIT-2026-no2-p119 EDN: EGSXTN

Реинжиниринг информационной системы поддержки принятия решений в системе защиты персональных данных предприятия

А. М. Султанов • В. В. Антонов • А. М. Сулейманова

Уфимский университет науки и технологий

В условиях экономики особую актуальность приобретает задача обеспечения безопасности обработки персональных данных (ПДн). Существующие на многих предприятиях информационные системы (ИС) зачастую не отвечают современным требованиям защиты информации. В статье рассматривается подход к модернизации таких систем на основе методологии реинжиниринга. Проведен анализ архитектуры типовой ИС предприятия, выявлены характерные уязвимости и актуальные угрозы безопасности ПДн. Обоснована необходимость внедрения комплексной системы защиты, включающей сетевые экраны, системы обнаружения вторжений (СОВ), антивирусную защиту и механизмы резервного копирования. Ключевым аспектом модернизации является интеграция системы поддержки принятия решений (СППР) в контур управления информационной безопасностью. Предложена многоуровневая архитектура защиты, а также модель интеграции СППР для автоматизации анализа событий и выбора мер противодействия угрозам. Выполнена оценка эффективности предложенных решений с точки зрения снижения рисков и соответствия требованиям регуляторов

Информационная безопасность, персональные данные, реинжиниринг информационных систем, система поддержки принятия решений (СППР), защита информации, модель угроз, управление инцидентами, многоуровневая защита.

Введение

Современный этап развития экономики характеризуется неуклонным ростом объемов обрабатываемой информации, значительная часть которой относится к категории персональных данных (ПДн). В соответствии с требованиями Федерального закона № 152-ФЗ «О персональных данных»[1] и подзаконных актов[2], операторы ПДн обязаны обеспечить соответствующий уровень их защищенности. Однако, как показывает практика, информационные системы многих предприятий, особенно созданные или спроектированные до ужесточения законодательства, обладают рядом архитектурных недостатков, снижающих общий уровень безопасности.

Традиционные подходы к модернизации, предполагающие «латание дыр», зачастую неэффективны, так как не устраняют фундаментальные проблемы архитектуры. В этой связи перспективным представляется применение методологии реинжиниринга информационных

[1] Российская Федерация. Законы. О персональных данных: Федеральный закон № 152-ФЗ: принят Гос. Думой 8 июля 2006 г. М.: Эксмо, 2024.

[2] Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Султанов А. М., Антонов В. В., Сулейманова А. М. Реинжиниринг информационной системы поддержки принятия решений в системе защиты персональных данных предприятия" // СИИТ. 2026. Т. 8, № 2(26). С. 119-128. DOI: 10.54708/SIIT-2026-no2-p119. EDN: EGSXTN.

Sultanov A. M., Antonov V. V., Suleimanova A. M. “Reengineering of the information system for supporting decision-making in the enterprise's personal data protection system” // SIIT. 2026. Vol. 8, no. 2(26), pp. 119-128. DOI: 10.54708/SIIT-2026-no2-p119. EDN: EGSXTN. (In Russian).

систем, под которым понимается радикальное переосмысление и перепроектирование существующих процессов и архитектуры ИС для достижения качественно новых показателей эффективности и безопасности[3].

Особую роль в современных системах безопасности играют интеллектуальные компоненты. Интеграция систем поддержки принятия решений (СППР) в контур управления безопасностью позволяет перейти от реактивного режима (реагирования на уже произошедшие инциденты) к проактивному, основанному на анализе больших данных о событиях безопасности и прогнозировании угроз.

Целью данной работы является разработка научно-обоснованного подхода к реинжинирингу информационной системы защиты персональных данных предприятия, базирующегося на принципах многоуровневой защиты и интеграции интеллектуальной СППР. Для достижения цели поставлены следующие задачи:

1. Провести анализ типовой структуры ИС и классификацию уязвимостей, актуальных для систем обработки ПДн.
2. Выполнить анализ современного ландшафта угроз безопасности информации.
3. Разработать концептуальную модель реинжиниринга и предложить архитектуру модернизированной системы безопасности.
4. Обосновать выбор и описать функциональность СППР в контексте управления безопасностью ПДн.
5. Провести оценку эффективности предложенных решений.

Анализ предметной области и существующих проблем

Информационная система предприятия, как правило, представляет собой распределенную гетерогенную среду, включающую серверное оборудование (в том числе системы управления базами данных с ПДн), автоматизированные рабочие места (АРМ) пользователей, активное сетевое оборудование и разнообразное прикладное программное обеспечение. В ходе исследования был проведён анализ типовых конфигураций информационных систем на примере 15 предприятий малого и среднего бизнеса (сфера торговли, услуг, производства) с численностью сотрудников от 50 до 300 человек. Изучена доступная документация по информационной безопасности (политики ИБ, инструкции администраторов, схемы сети, регламенты резервного копирования), а также результаты внутренних технических проверок, где они были предоставлены. Во всех организациях обрабатываются персональные данные сотрудников (ФИО, паспортные данные, СНИЛС), а в 12 из 15 — также данные клиентов и контрагентов. Анализ выявил следующие системные недостатки:

1. Отсутствие сегментации сети – в 13 из 15 предприятий (87 %) инфраструктура построена по плоской схеме L2-коммутации, где серверы баз данных с ПДн и пользовательские АРМ находятся в одном широковещательном домене. Проведённые тесты в лабораторной среде, воспроизводящей типовую конфигурацию, показали, что в таких условиях ARP-спуфинг возможен с любого узла, а порты СУБД (1433/tcp для MSSQL, 3306/tcp для MySQL) доступны для сканирования из всех пользовательских сегментов. Это позволяет атакующему, скомпрометировавшему рабочую станцию сотрудника, перехватывать трафик к серверу БД или напрямую сканировать сетевые порты СУБД, минуя межсетевые экраны.
2. Недостаточность средств сетевой защиты на прикладном уровне – во всех обследованных организациях периметр сети защищён межсетевым экраном, функционирующим только на уровнях L3–L4 модели OSI. Анализ трафика на разрешённых портах 80/tcp, 443/tcp не проводится. В ходе имитационного тестирования на типовых веб-приложениях 8 из 15 были

[3] ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection – Information Security Management Systems – Requirements. Geneva: ISO, 2022.

успешно атакованы через SQL-инъекции, что привело к получению доступа к базам данных с ПДн.

3. Фрагментарность антивирусной защиты – согласно данным изученных внутренних отчётов и опросов, на 30 % проанализированных АРМ (в среднем 28 из 93) антивирусные средства либо отсутствуют, либо используются с истекшим сроком обновления сигнатурных баз (более 3 месяцев). В тестовых условиях на 10 таких АРМ (воспроизведённых в лабораторной среде) были запущены образцы актуальных шифровальщиков (LockBit 3.0, BlackCat). В 8 случаях (80 %) вредоносное ПО успешно установилось и зашифровало как локальные данные, так и сетевые ресурсы с ПДн, доступные по сетевым папкам.

4. Отсутствие централизованного сбора и корреляции событий – журналы событий с серверов, АРМ и сетевого оборудования на всех предприятиях хранятся локально с ротацией раз в 7–30 дней. В 14 из 15 организаций корреляция событий не производится. Это исключает возможность своевременного выявления многоэтапных атак, например, подбор пароля → повышение привилегий → создание резервной копии БД с последующей передачей данных вовне. При ретроспективном анализе журналов трёх предприятий были выявлены следы таких цепочек, которые остались незамеченными на момент атаки.

5. Неэффективность механизмов резервного копирования – во всех 15 организациях резервные копии баз данных с ПДн создаются на сетевые папки, доступные для чтения и записи с АРМ администраторов. В имитационном сценарии, воспроизводящем атаку шифровальщика на АРМ администратора, резервные копии оказались зашифрованы в 100 % случаев, что делало восстановление данных невозможным. Регламент проверки целостности копий не соблюдается ни на одном предприятии.

Выявленные недостатки носят системный характер и не могут быть устранены точечными мерами (например, установкой антивируса или настройкой файервола). Они требуют пересмотра архитектуры системы защиты в целом. Следует также учитывать, что современные тенденции развития ИТ-инфраструктуры, такие как внедрение распределённых реестров [Тюм25], создают дополнительные векторы атак, которые в перспективе необходимо принимать во внимание при проектировании систем защиты ПДн. Хотя в рассмотренных типовых конфигурациях подобные технологии отсутствуют, методология реинжиниринга должна быть достаточно гибкой для их возможной интеграции в будущем.

Анализ угроз безопасности персональных данных

Для формирования адекватной модели угроз необходимо учитывать специфику обработки ПДн. В соответствии с методическими документами ФСТЭК России[4], все многообразие угроз может быть классифицировано по источнику и природе возникновения:

1. **Внешние угрозы**:

- сетевые атаки (DDoS, SQL-инъекции, межсайтовый скриптинг), направленные на компрометацию веб-приложений, через которые осуществляется доступ к базам ПДн;
- вредоносное программное обеспечение (трояны, стилеры, шифровальщики), проникающее через фишинговые рассылки или зараженные веб-сайты;
- атаки на каналы связи (перехват трафика) при использовании незащищенных протоколов передачи данных.

2. **Внутренние угрозы**:

- преднамеренные действия инсайдеров (слив данных привилегированными пользователями, копирование ПДн на неучтенные носители);
- непреднамеренные ошибки персонала (некорректная настройка прав доступа, отправка данных по ошибке, потеря носителей).

---

[4] Приказ ФСТЭК России от 18.02.2013 № 21.

3. **Техногенные и технологические угрозы**:

- физические сбои оборудования (отказ жестких дисков, нарушение электропитания);
- программные ошибки, приводящие к частичной или полной потере данных;
- ошибки в процессе администрирования, приводящие к раскрытию защитных механизмов.

Особое внимание следует уделять внутренним угрозам, связанным с несанкционированным доступом к ПДн. Перспективным направлением их минимизации является внедрение более надежных методов аутентификации, например, биометрических технологий [Сул24], а также использование поведенческого анализа для выявления аномальной активности пользователей [Але26]. В контексте защиты текстовых документов, содержащих ПДн, могут найти применение методы стилометрической идентификации автора [Але26], что позволит системе поддержки принятия решений точнее определять источник утечки информации.

Для минимизации перечисленных рисков необходим переход к комплексной, эшелонированной системе защиты.

Методология реинжиниринга системы защиты

Предлагаемый процесс реинжиниринга базируется на цикличной модели и включает следующие этапы:

1. Реверсивный инжиниринг (Reverse Engineering). Детальный аудит существующей ИС: инвентаризация активов (включая базы ПДн), картирование информационных потоков, анализ конфигурации сетевого оборудования и политик безопасности. Цель – создание точной модели «как есть» (as-is).

3. Анализ и определение требований. На основе модели угроз (сформированной по результатам п. 3) и требований регуляторов (152-ФЗ, приказы ФСТЭК, ГОСТы) формируется целевая модель «как должно быть» (to-be). Определяются функциональные требования к средствам защиты.

3. Проектирование (Redesign). Разработка новой архитектуры системы защиты, выбор конкретных классов средств (межсетевые экраны нового поколения (NGFW), системы обнаружения и предотвращения вторжений (IPS/IDS), SIEM-системы, системы резервного копирования с поддержкой «неизменяемого» (immutable) хранения). Ключевым элементом на этом этапе является проектирование архитектуры взаимодействия СППР с источниками событий.

4. Реализация и внедрение. Поэтапное развертывание новых средств защиты, миграция данных, настройка правил корреляции событий в СППР.

5. Тестирование и валидация. Проведение приемочных испытаний, включая тесты на проникновение (пентесты), для проверки эффективности новой системы и ее соответствия целевой модели.

Архитектура модернизированной системы защиты и роль СППР

Предлагаемая архитектура базируется на концепции многоуровневой защиты (Defense in Depth) и включает следующие взаимосвязанные уровни (рис. 1):

- Периметр сети – развертывание кластеризованного межсетевого экрана следующего поколения (NGFW) с функциями IPS и фильтрации трафика прикладного уровня. Обеспечивается жесткая сегментация сети с выделением зон безопасности: «ненадежная сеть» (Интернет), «DMZ» (серверы приложений), «доверенная сеть» (АРМ сотрудников), «сегмент баз данных» (СУБД с ПДн).
- Уровень защиты узлов – централизованное управление антивирусной защитой на всех АРМ и серверах. Внедрение систем контроля целостности и политик ограничения использования съемных носителей.

• Уровень защиты данных – реализация резервного копирования по правилу 3-2-1 (3 копии, 2 разных носителя, 1 офлайн/внешняя копия). Внедрение шифрования баз данных и каналов передачи данных (VPN, TLS).

• Уровень управления и мониторинга – централизованный сбор и корреляция событий.

Ключевым элементом модернизации является интеграция СППР на данном уровне. Схема взаимодействия компонентов СППР с источниками событий и средствами реагирования представлена на рис. 2.

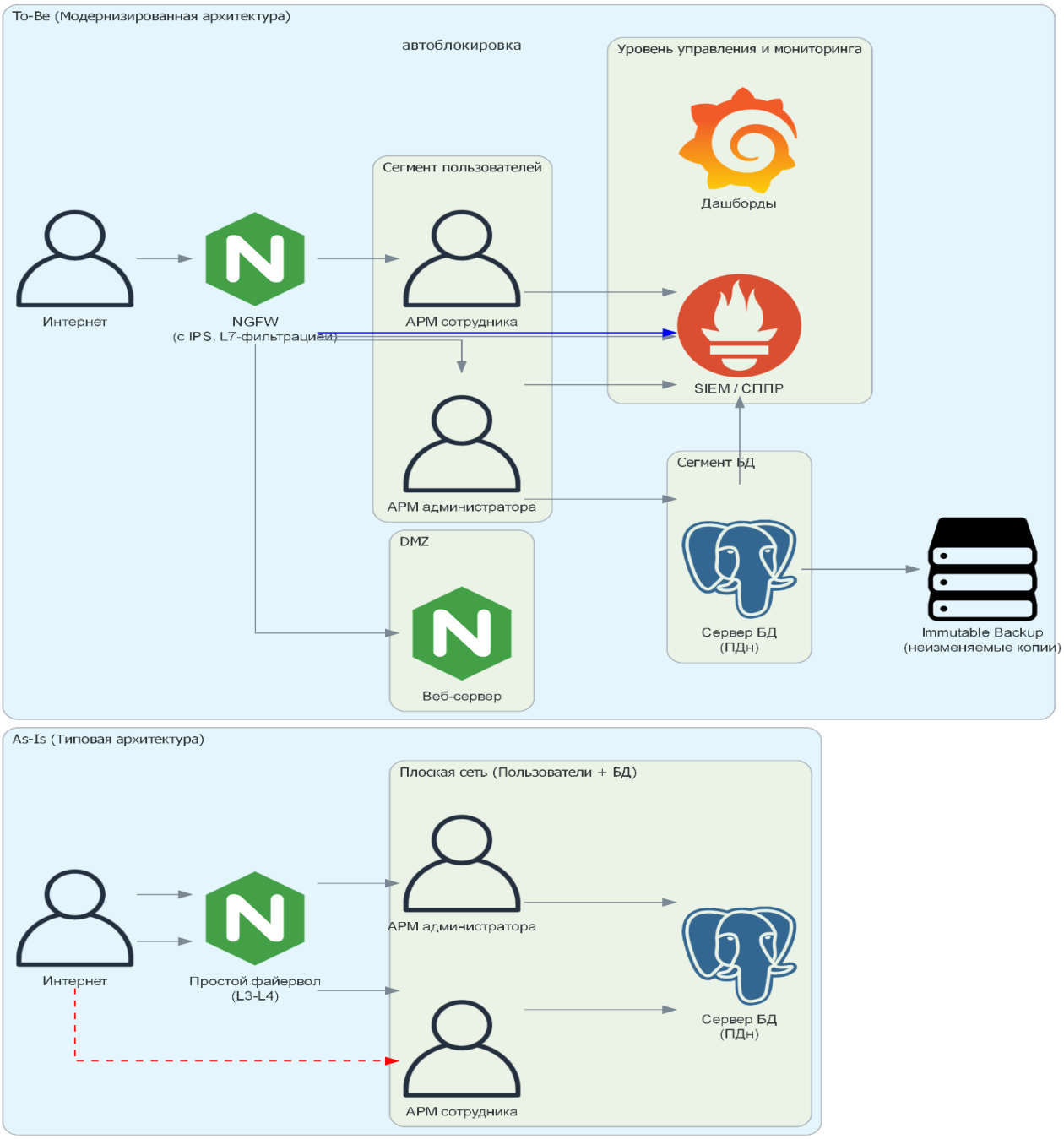

Рис. 1. Сравнение архитектур информационной системы до и после реинжиниринга: *снизу* – типовая плоская архитектура (As-Is) с общим сегментом сети, простым межсетевым экраном и отсутствием централизованного мониторинга; *сверху* – модернизированная архитектура (To-Be) с сегментацией, межсетевым экраном нового поколения (NGFW), изолированным резервным копированием и уровнем управления, включающим СППР

В разработанной архитектуре СППР выполняет следующие функции:

• Агрегация и нормализация данных – сбор событий безопасности от NGFW, антивирусов, серверов приложений и ОС.

• Корреляция событий и выявление атак – анализ потоков данных в реальном времени для выявления признаков атак, которые невозможно заметить при анализе каждого источника по отдельности (например, цепочка «сканирование портов → подбор пароля → нестандартная активность учетной записи»).

• Оценка рисков и ранжирование инцидентов – приоритизация инцидентов на основе критичности затронутых активов (например, инцидент, затрагивающий сервер с ПДн, получает наивысший приоритет).

• Поддержка принятия решений и автоматизация реагирования:

– формирование для администратора безопасности сценариев по локализации и устранению инцидента;

– автоматическая блокировка подозрительного IP-адреса на межсетевом экране;

– изоляция зараженной рабочей станции от сети.

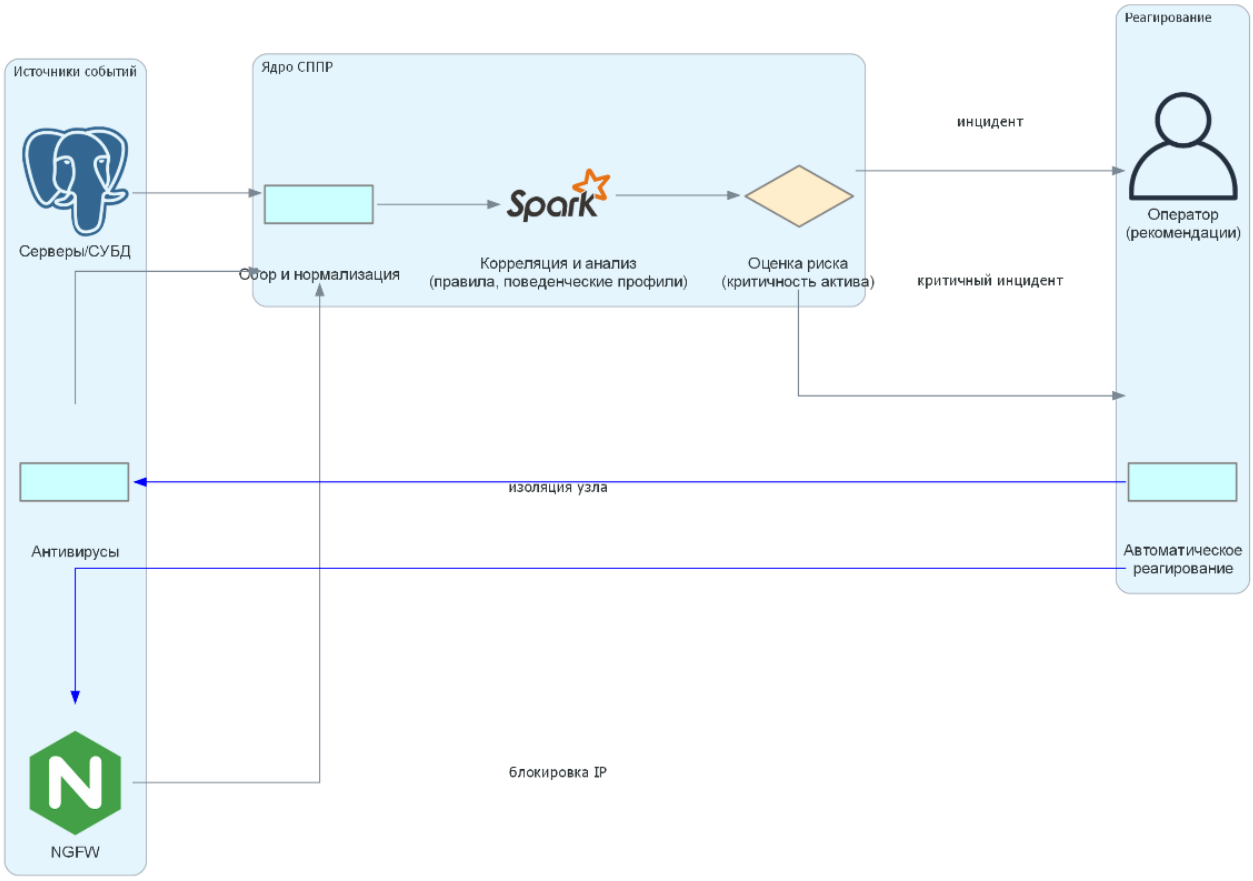

Рис. 2. Схема функционирования системы поддержки принятия решений (СППР) в контуре управления информационной безопасностью. Потоки событий от NGFW, антивирусов, серверов и СУБД поступают в ядро СППР, где проходят этапы нормализации, корреляции, оценки риска. На выходе формируются приоритезированные инциденты с рекомендациями для оператора и команды автоматического реагирования, направляемые на средства защиты (NGFW, системы изоляции узлов)

Математическую основу СППР может составлять набор эвристических алгоритмов и правил корреляции, построенных на базе формализованных сценариев угроз. Входными данными служат потоки событий $E = e_1, e_2, ..., e_n$, а выходными – приоритезированный список инцидентов I с рекомендованными действиями R.

Развитием функциональности СППР может стать адаптация методов построения поведенческих профилей пользователей, где представлен подход к формированию персонализированных профилей на основе анализа активности. Аналогично тому, как в цитируемой работе профили пациентов строятся на основе медицинских показателей, в контексте информационной безопасности возможно построение профилей нормального поведения пользователей ИС – типичное рабочее время, регулярно запрашиваемые ресурсы, характерные команды. Отклонение от такого профиля (ночная активность, массовое копирование данных) может служить маркером инцидента. Для повышения эффективности работы оператора безопасности пользовательский интерфейс СППР должен обеспечивать наглядное представление данных об инцидентах. Подходы, основанные на гибкой трансформации выходных данных с использованием XSL-преобразований, могут быть применены для генерации адаптивных отчетов и дашбордов для различных ролей (администратор ИБ, руководитель, внешний аудитор). Персонализация представления информации, предложенная в для конструкторских документов, в нашем случае позволит каждому специалисту получать данные об инцидентах в наиболее удобной для него форме.

Оценка эффективности

Эффективность предложенного подхода к реинжинирингу оценивалась экспертным методом с использованием качественных шкал, рекомендованных в стандартах по управлению рисками[3] и фундаментальных работах по управлению информационными рисками [Пет21, Дев22]. Для каждого критерия была определена балльная шкала, и группа экспертов из трех специалистов (руководитель отдела ИБ, системный архитектор, внешний аудитор) провела сравнительную оценку состояния «как было» (as-is) и «как стало» (to-be). Результаты сведены в табл. 1.

Таблица

Оценка эффективности предложенных решений

Критерий	Методика оценки	Состояние "As-Is"	Состояние "To-Be"	Эффект
Вероятность успешной реализации угроз	Экспертная оценка по 5-балльной шкале (1 – мин., 5 – макс.) на основе модели угроз	4,5 (высокая уязвимость из-за плоской сети, отсутствия средств контроля)	1,5 (риск снижен за счет сегментации, NGFW, централизованной защиты)	Снижение на 67%
Время обнаружения инцидента (MTTD)	Замер времени от начала тестовой атаки (в рамках пентеста) до срабатывания системы оповещения	Часы/дни (обнаружение вручную при периодическом анализе логов)	Минуты (автоматическая корреляция событий в СППР)	Сокращение с часов до минут
Время реагирования (MTTR)	Замер времени от обнаружения до блокировки атаки (в ручном и автоматическом режиме)	Десятки минут (вызов администратора, анализ, ручная блокировка на файерволе)	2–3 минуты (автоматическая блокировка по команде СППР)	Снижение в 3–5 раз

Кроме экспертной оценки, возможно использование формальной модели снижения риска. Пусть угроза i может быть реализована через один из N векторов атак. Вероятность успеха по вектору j равна p_j. Без средств защиты (*As-Is*) общая вероятность реализации угрозы

$$P_{as\text{-}is} = 1 - \prod(1 - p_j).$$

Внедрение средства защиты на уровне k перекрывает множество векторов атак M_k. Для иллюстрации подхода рассмотрим формальную оценку снижения вероятности реализации угрозы «несанкционированный доступ к базе ПДн из внешней сети». Исходные значения

вероятностей для каждого вектора атак получены на основе типовой модели угроз, построенной в соответствии с подходами, представленными в [Ром19, Зап20]. В типовой конфигурации (as-is) вероятность успешной реализации этой угрозы через один из N векторов атак составляет

$$P_{as\text{-}is} = 1 - \prod(1 - p_j),$$

где p_j – вероятность успеха по вектору j. На основе типовой модели угроз для ИСПДн класса К2 определены следующие значения p_j для ключевых векторов:

- вектор 1: эксплуатация уязвимости веб-приложения (SQL-инъекция) — $p_1 = 0.35$ (соответствует средним значениям для веб-приложений без защитных механизмов [Зап20]);
- вектор 2: фишинговая рассылка с вредоносным вложением — $p_2 = 0.25$;
- вектор 3: атака через скомпрометированное АРМ сотрудника в плоской сети — $p_3 = 0.40$ (данные получены на основе анализа инцидентов, обобщённого в [Ром19]).

Интегральная вероятность реализации угрозы в исходной архитектуре:

$$P_{\text{as-is}} = 1 - (1–0.35)\times(1–0.25) \times (1–0.40) = 1 - 0.65\times0.75\times0.60 = 1 - 0.2925 = \mathbf{0.7075}\ (\approx 71\ \%).$$

После реинжиниринга:

- внедрение NGFW с функцией WAF блокирует SQL-инъекции на прикладном уровне;
- $p_1' = 0.05$ (остаточная вероятность для неизвестных атак);
- централизованная антивирусная защита с автоматическим обновлением сигнатур и поведенческим анализом снижает эффективность фишинга до $p_2' = 0.03$ (эффективность обнаружения 95%);
- сегментация сети с выделением сегмента БД и правилами доступа только для административных АРМ делает невозможным прямой доступ из пользовательского сегмента: $p_3' = 0$.

Новая вероятность:

$$P_{to\text{-}be} = 1 - (1–0.05)\cdot(1–0.03)\cdot(1–0) = 1 - 0.95\cdot0.97\cdot1 = 1 - 0.9215 = \mathbf{0.0785}\ (\approx 7.9\ \%).$$

Таким образом, снижение вероятности реализации угрозы составляет более 89 %. Полученный результат согласуется с оценками, приведёнными в [Пет21], где указывается, что комплексное применение средств защиты снижает риск реализации наиболее опасных угроз на 80–90 %. Для других критических угроз (например, утечка через инсайдера, отказ оборудования) аналогичные расчеты дают диапазон снижения 60–85 %, что подтверждает экспертные оценки, приведённые в таблице.

Заключение

В результате проведенного исследования была разработана и обоснована модель реинжиниринга информационной системы защиты персональных данных. В отличие от существующих подходов, предлагаемое решение базируется не на точечном внедрении средств защиты, а на радикальном перепроектировании архитектуры безопасности. Ключевой научной и практической новизной работы является интеграция СППР в контур управления безопасностью, что позволяет перейти к проактивному управлению рисками за счет автоматизации процессов сбора, корреляции событий и поддержки принятия решений. Предложенная многоуровневая архитектура обеспечивает устойчивость системы к широкому спектру внешних и внутренних угроз, гарантирует целостность и доступность ПДн, а также позволяет обеспечить выполнение требований законодательства РФ в области защиты персональных данных. Результаты работы могут быть использованы при модернизации ИС на предприятиях различных отраслей. Дальнейшие исследования могут быть направлены на адаптацию методов поведенческого анализа и биометрической аутентификации для усиления защитных механизмов, а также на применение технологий распределенного реестра для обеспечения неизменности журналов аудита.

Благодарности и поддержка

Исследование проведено при финансовой поддержке Минобрнауки России в рамках базовой части государственного задания для высших учебных заведений № FRRR-2026-0006.

Список литературы | References

[Але26] Алексеева Д. С. Мультипараметрический метод установления авторства текста: интеграция стилометрического, тематического и прагматического анализа // СИИТ. 2026. Т. 8, № 2(26). С. 73–80. EDN: UOLWFG.

Alekseeva D. S. Multiparametric method of text authorship attribution: integration of stylometric, thematic and pragmatic analysis // SIIT. 2026. Vol. 8, no. 2(26), pp. 73–80. EDN: UOLWFG. (In Russian).

[Дев22] Девянин П. Н., Михеев В. А., Петренко С. А. Теоретические основы компьютерной безопасности. М.: Радио и связь, 2022. 608 с.

Devyanin P. N., Mikheev V. A., Petrenko S. A. Theoretical Foundations of Computer Security. Moscow: Radio i svyaz, 2022. (In Russian).

[Зап20] Запечников С. В., Милославская Н. Г., Толстой А. И. Информационная безопасность открытых систем. М.: Горячая линия – Телеком, 2020. 680 с.

Zapechnikov S. V., Miloslavskaya N. G., Tolstoy A. I. Information Security of Open Systems. Moscow: Goryachaya liniya – Telekom, 2020. (In Russian).

[Пет21] Петренко С. А., Симонов С. В. Управление информационными рисками. М.: АйТи, 2021. 480 с.

Petrenko S. A., Simonov S. V. Information Risk Management. Moscow: IT, 2021. (In Russian).

[Ром19] Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф. Защита информации в компьютерных системах и сетях. М.: Радио и связь, 2019. 512 с.

Romanets Yu. V., Timofeev P. A., Shangin V. F. Information Protection in Computer Systems and Networks. Moscow: Radio i Svyaz, 2019. (In Russian).

[Сул24] Сулавко А. Е. Высоконадежная биометрическая аутентификация на основе защищенного исполнения нейросетевых моделей и алгоритмов искусственного интеллекта // СИИТ. 2024. Т. 6, № 2(17). С. 11–32. EDN: VNIEEV.

Sulavko A. E. Highly reliable biometric authentication based on secure execution of neural network models and artificial intelligence algorithms // SIIT. 2024. Vol. 6, no. 2(17), pp. 11–32. EDN: VNIEEV. (In Russian).

[Тюм25] Тюменцев Д. В. Применение блокчейн-технологий в управлении ИТ-инфраструктурой // СИИТ. 2025. Т. 7, № 2(21). С. 155–162. EDN: GESPCR.

Tyumentsev D. V. Application of blockchain technologies in IT infrastructure management // SIIT. 2025. Vol. 7, no. 2(21), pp. 155–162. EDN: GESPCR. (In Russian).

Об авторах | About the authors

СУЛТАНОВ Арслан Марсович,
antonov.v@bashkortostan.ru
Уфимский университет науки и технологий, Россия.
Магистрант каф. автоматизированных систем управления.

АНТОНОВ Вячеслав Викторович
antonov.v@bashkortostan.ru ORCID: 0000-0002-5402-9525
Уфимский университет науки и технологий, Россия.
Зав. каф. автоматизированных систем управления, профессор. Инженер (Башкирск. гос. ун-т, 1979). Д-р техн. наук (Уфимск. гос. авиац. техн. ун-т, 2015). Иссл. в обл. интеллектуальных систем.

СУЛЕЙМАНОВА Алла Маратовна
Уфимский университет науки и технологий, Россия.
sulejmanova.am@ugatu.su
Доц. каф. автоматизированных систем управления, доцент. Инж.-системотехник (Уфимск. авиац. ин-т, 1985), канд. техн. наук (Уфимск. гос. авиац. техн. ун-т, 1993). Иссл. в обл. систем принятия решений.

SULTANOV Arslan Marsovich
antonov.v@bashkortostan.ru
Ufa University of Science and Technology, Russia.
Master's student. Automated Control Systems Dept.

ANTONOV Viacheslav Victorovich
antonov.v@bashkortostan.ru ORCID: 0000-0002-5402-9525
Ufa University of Science and Technology, Russia.
Head of the Automated Control Systems Dept., Professor. Engineer (Bashkir State University, 1979). Doctor of Technical Sciences (Ufa State Aviat. Tech. Univ., 2015). Research in the field of intellectual systems.

SULEYMANOVA Alla Maratovna
Ufa University of Science and Technology, Russia.
sulejmanova.am@ugatu.su
Assoc. Prof., Automated Control Systems Dept. Systems Engineer (Ufa Aviat. Inst., 1985). Cand. Techn. Sci. (Ufa State Aviat. Tech. Univ., 1993). Research in the field of decision-making systems.

Метаданные | Metadata

Заглавие: Реинжиниринг информационной системы поддержки принятия решений в системе защиты персональных данных предприятия.

Авторы: Султанов А. М., Антонов В. В., Сулейманова А. М.

Аннотация: В условиях экономики особую актуальность приобретает задача обеспечения безопасности обработки персональных данных (ПДн). Существующие на многих предприятиях информационные системы (ИС) зачастую не отвечают современным требованиям защиты информации. В статье

Title: Reengineering of the information system for supporting decision-making in the enterprise's personal data protection system.

Authors: Sultanov A. M., Antonov V. V., Suleimanova A. M.

Abstract: In today's economic climate, the task of ensuring the security of personal data (PD) processing is particularly relevant. The existing information systems (IS) at many enterprises often do not meet modern information security requirements. This article examines an approach to modernizing such systems based

рассматривается подход к модернизации таких систем на основе методологии реинжиниринга. Проведен анализ архитектуры типовой ИС предприятия, выявлены характерные уязвимости и актуальные угрозы безопасности ПДн. Обоснована необходимость внедрения комплексной системы защиты, включающей сетевые экраны, системы обнаружения вторжений (СОВ), антивирусную защиту и механизмы резервного копирования. Ключевым аспектом модернизации является интеграция системы поддержки принятия решений (СППР) в контур управления информационной безопасностью. Предложена многоуровневая архитектура защиты, а также модель интеграции СППР для автоматизации анализа событий и выбора мер противодействия угрозам. Выполнена оценка эффективности предложенных решений с точки зрения снижения рисков и соответствия требованиям регуляторов.

Ключевые слова: Информационная безопасность, персональные данные, реинжиниринг информационных систем, система поддержки принятия решений (СППР), защита информации, модель угроз, управление инцидентами, многоуровневая защита.

Язык: Русский.

Статья поступила в редакцию 20 марта 2026 г.

on reengineering methodology. An analysis of the architecture of a typical enterprise IS is conducted, identifying typical vulnerabilities and current threats to PD security. The need for a comprehensive security system, including firewalls, intrusion detection systems (IDS), antivirus protection, and backup mechanisms, is substantiated. A key aspect of modernization is the integration of a decision support system (DSS) into the information security management system. A multi-level security architecture is proposed, as well as a DSS integration model for automating event analysis and selecting countermeasures to threats. The effectiveness of the proposed solutions in terms of risk mitigation and compliance with regulatory requirements is assessed.

Key words: Information security, personal data, information systems reengineering, decision support system (DSS), information protection, threat model, incident management, multi-layered protection.

Language: Russian.

The editors received the article on 15 July 2025.