УДК 338.24:004.056 **DOI: 10.34670/AR.2026.40.68.004**

Внедрение сквозной системы управления безопасностью в межотраслевой корпоративной среде

Козырь Наталья Сергеевна

Кандидат экономических наук, доцент,
Кубанский государственный технологический университет,
350072, Российская Федерация, Краснодар, ул. Московская, 2;
e-mail: n_k_@mail.ru

Ильина Татьяна Владимировна

Кандидат экономических наук, доцент,
Кубанский государственный технологический университет,
350072, Российская Федерация, Краснодар, ул. Московская, 2;
e-mail: ilina666666@mail.ru

Аннотация

Статья посвящена анализу особенностей внедрения сквозной системы управления безопасностью (ССУБ) в межотраслевой корпоративной среде, характеризующейся высокой неоднородностью ИТ-инфраструктуры, различиями в зрелости процессов и сложившимися организационными ограничениями. Показано, что фрагментарный подход к информационной безопасности приводит к увеличению транзакционных издержек, росту операционной неопределенности и повышению вероятности каскадных сбоев, затрагивающих ключевые бизнес-процессы предприятия. В ходе исследования выявлены структурные барьеры, оказывающие существенное экономическое влияние на внедрение ССУБ: наличие устаревших технологических компонентов, отсутствие актуализированного реестра активов, разрыв между функциями ИТ и ИБ, формализованный характер политик, не отражающих реальных процессов, а также дефицит специалистов в областях GRC, SOC и DevSecOps. Эти факторы ограничивают управляемость и усложняют построение прозрачной модели рисков, необходимой для принятия обоснованных управленческих решений. Проведен межотраслевой сравнительный анализ, показывающий, что финансовый сектор, промышленность, медицина, образование и ИТ-компании формируют различающиеся нормативные требования, профили угроз и экономические приоритеты. Полученные результаты подтверждают необходимость адаптации архитектуры безопасности к отраслевой специфике, особенностям регулирования и доступным ресурсам. Предложена масштабируемая модель внедрения, позволяющая согласовать глубину организационных регламентов, объем мониторинга и уровень автоматизации с размером и зрелостью предприятия. Обоснована пятиэтапная схема внедрения, основанная на логике PDCA, включающая формирование нормативного контура, построение модели рисков, реализацию технических мер, организацию мониторинга и корректирующий цикл

развития. Показано, что применение сквозной системы управления безопасностью способствует снижению операционных рисков, повышению прозрачности корпоративных процессов и укреплению экономической устойчивости предприятий вне зависимости от отрасли.

Для цитирования в научных исследованиях

Козырь Н.С., Ильина Т.В. Внедрение сквозной системы управления безопасностью в межотраслевой корпоративной среде // Экономика: вчера, сегодня, завтра. 2025. Том 15. № 11А. С. 34-42. DOI: 10.34670/AR.2026.40.68.004

Ключевые слова

Экономическая безопасность, информационная безопасность, региональная экономика, отраслевая экономика, архитектура безопасности, PDCA-цикл, организационное развитие, организационная зрелость, управление рисками, ИТ-инфраструктура.

Введение

Цифровизация региональных хозяйственных систем усиливает зависимость предприятий от устойчивости информационной инфраструктуры, что делает безопасность значимым фактором экономической стабильности и развития территорий [Айларова, 2024]. Усложнение корпоративных ИТ-ландшафтов и потребность в надежной инфраструктуре отмечаются как в государственных, так и в муниципальных структурах, что подтверждается исследованиями организационных моделей управления информационными ресурсами [Грязнова, Михеева, 2015]. В этих условиях безопасность становится ключевым элементом обеспечения управляемости, снижая транзакционные издержки и повышая устойчивость процессов [Шереметьева, Веролайнен, 2024].

В научной литературе широко представлены исследования, посвященные экономике информационной безопасности, оценке затрат и эффективности защитных мер [Власенко и др., 2020]. При этом сохраняются структурные барьеры цифрового развития организаций, влияющие на формирование безопасной инфраструктуры, включая социально-организационные и технологические ограничения [Иванов, 2025]. Несмотря на значительное внимание к вопросам регулирования и нормативного обеспечения защиты информации [Метельков, 2024], интеграция безопасности в сквозные управленческие контуры предприятий остается исследованной недостаточно. Организационно-экономические механизмы поддержки инфраструктуры требуют дальнейшего развития с точки зрения воспроизводимости управленческих решений [Регуш, Маркова, 2017].

С экономической точки зрения актуальными остаются вопросы согласования процессов цифровизации бизнеса с требованиями безопасности [Резниченко, 2024], оценки экономической эффективности корпоративных систем и инструментов управления [Сунгатуллин, 2025], а также выбора оптимальных средств мониторинга и контроля при ограниченных ресурсах предприятий [Табункова, Оганесян, 2023]. В этих условиях сквозная система управления безопасностью (ССУБ) выступает инструментом снижения операционных рисков и обеспечения прозрачности процессов в межотраслевой корпоративной среде.

Структурные барьеры внедрения сквозной системы безопасности

Внедрение ССУБ осложняется рядом факторов, характерных для большинства российских организаций: наследием устаревших технологий, отсутствием актуального реестра активов, несогласованностью процессов ИТ и ИБ, формальным характером политик и дефицитом квалифицированных кадров (таблица 1).

Таблица 1 – Ключевые проблемы внедрения сквозных систем управления безопасностью

Проблема	Проявления	Последствия
Наследие инфраструктуры	Устаревшие системы, отсутствие обновлений	Рост уязвимостей, ограниченный контроль
Несогласованность процессов	Разрыв ИТ/ИБ, отсутствие регламентов	Потеря инцидентов, низкая управляемость
Отсутствие реестра активов	Неактуальные данные о системах и записях	Ошибочная оценка рисков, некорректное реагирование
Формальный характер политики	Документы не отражают реальные процессы	Формальное соответствие без защиты
Кадровый дефицит	Недостаток специалистов, зависимость от подрядчиков	Ошибки конфигураций, медленное реагирование

Проблемы характерны для большинства российских предприятий и требуют адаптации внедрения ССУБ к их исходным условиям.

Масштабирование архитектуры с учетом отраслевых различий организаций

Межотраслевая корпоративная среда различается масштабом, структурой и уровнем зрелости процессов, поэтому сквозная система безопасности должна адаптироваться к условиям конкретного предприятия. В таблице 2 представлены варианты масштабирования сквозной архитектуры ССУБ, отражающие адаптацию единого подхода к условиям предприятий разного размера и уровня технологической зрелости.

Таблица 2 – Масштабирование сквозной архитектуры безопасности в организациях различного масштаба

Тип организации	Характеристика	Подход к внедрению
Малые	10–50 человек, ограниченный бюджет	Минимальный контур: учет активов, базовый контроль доступа, аудит логов
Средние	50–500 сотрудников, собственные серверы	Реализация 3–4 уровней ССУБ, внедрение SIEM и Service Desk
Крупные/ холдинги	Сложные распределенные системы	Полноценная пятиуровневая архитектура, интеграция GRC+SOC

Представленные данные показывают, что масштабирование сквозной архитектуры безопасности носит не линейный, а адаптивный характер: при сохранении общей логики ССУБ глубина и состав уровней изменяются в зависимости от ресурсов, организационной структуры и характера ИТ-ландшафта предприятия, что позволяет применять единый подход в малых, средних и крупных организациях без потери функциональности.

Отраслевая специфика определяет набор регуляторных требований, доминирующих угроз и приоритетов защиты, что напрямую влияет на конфигурацию сквозной системы безопасности. В таблице 3 обобщены ключевые особенности внедрения ССУБ в наиболее распространенных секторах экономики. Для каждой отрасли выделены приоритетные направления защиты и типовые технологические средства, формирующие основу архитектуры безопасности в данных средах.

Таблица 3 – Отраслевые особенности внедрения сквозной системы безопасности

Отрасль	Ключевые приоритеты безопасности	Типовые технологии и средства
Финансовая сфера	Защита транзакций; управление привилегированным доступом; антифрод.	Банковские SIEM; DLP; криптография; PAM-системы.
Образование	Защита персональных данных; контроль сетевого трафика; снижение теневого ИТ.	Astra Linux; UserGate; FreeIPA.
Промышленность / КИИ	Сегментация OT/IT; контроль команд SCADA; физическая безопасность.	Континент-АП; Prometheus; специализированные шлюзы безопасности.
Медицина	Защита ЭМК; контроль доступа; криптографическая защита данных.	VipNet; CryptoPro; DLP; Service Desk.
ИТ-компании	Защита CI/CD; безопасность исходного кода; контроль контейнерной среды.	GitLab CI/CD; SonarQube; Kubernetes; Vault.

Представленные данные показывают, что отраслевые различия определяют набор нормативных требований, профиль угроз и приоритеты защиты, что напрямую влияет на конфигурацию сквозной системы безопасности. Архитектура ССУБ остается единой по принципам, но ее реализация должна адаптироваться к отраслевой специфике, учитывая доступные ресурсы и характер критичных процессов, что обеспечивает корректное распределение мер защиты и повышение управляемости безопасности в конкретных условиях предприятия.

Последовательные этапы формирования сквозного контура безопасности

Процесс внедрения сквозной системы управления безопасностью (ССУБ) в действующей ИТ-инфраструктуре требует строго детерминированной последовательности. Каждая стадия формирует обязательные входные данные для следующей, что исключает фрагментарность, характерную для стихийных внедрений. Представленная модель опирается на принципы PDCA, но адаптирована к условиям гетерогенных корпоративных ИТ-ландшафтов (таблица 4).

Таблица 4 – Последовательность формирования сквозной системы управления безопасностью (ССУБ)

Этап	Содержание этапа	Ключевые результаты
1. Политико-управленческий	Установление целей и порогов риска; утверждение политики и регламентов; распределение ролей; формирование RACI.	Нормативный контур и формализованная структура ответственности.
2. Инвентаризационно-аналитический	Создание реестра активов и их критичности; построение модели угроз и рисков; определение приоритетных мер контроля.	Актуальный реестр активов, модель рисков и приоритеты защиты.
3. Технологический	Внедрение мер защиты (IAM/PAM, сегментация, криптография, журналирование, контроль целостности,	Техническая база ССУБ, согласованная с политикой и моделью рисков.

Этап	Содержание этапа	Ключевые результаты
	управление уязвимостями); разработка эксплуатационных процедур.	
4. Мониторингово-операционный	Развёртывание SOC/SIEM; интеграция телеметрии; настройка корреляции; управление инцидентами; автоматизация реагирования.	Наблюдаемость инфраструктуры и управляемое реагирование.
5. Контрольно-корректирующий (PDCA)	Аудит и анализ эффективности; сопоставление метрик с моделью рисков; корректировка политик и регламентов; планирование развития.	Замкнутый контур управления и повышение зрелости ССУБ.

Этап 1. Формирование нормативного контура и распределение ответственности. На первом этапе формируется нормативно-управленческая платформа ССУБ, определяющая границы и правила функционирования всей системы. Актуализируются политика безопасности с учётом отраслевых и регуляторных требований, устанавливаются пороги риска и критерии критичности активов. Роли участников закрепляются в виде RACI-матрицы, обеспечивающей однозначность полномочий и исключение дублирования функций. Одновременно утверждаются базовые регламенты – управления доступом, активами, инцидентами и аудита, – формирующие обязательные требования, к которым впоследствии приводятся технические и операционные механизмы защиты.

Этап 2. Инвентаризация активов и построение модели рисков. На втором этапе формируется аналитический базис ССУБ, обеспечивающий корректность технических и мониторинговых решений. Проводится инвентаризация ИТ-активов – систем, сервисов, сетевых сегментов, облачных ресурсов и учётных записей – с присвоением каждому объекту однозначной идентификации и функционального назначения. Активы классифицируются по критичности в соответствии с заранее установленными критериями ущерба и влияния на бизнес-процессы, что позволяет сформировать целостную структуру взаимосвязей и потоков данных. На основе актуализированного перечня активов разрабатывается модель угроз и рисков, включающая оценку вероятности реализации угроз и потенциальных последствий для предприятия. Эта модель определяет приоритеты защиты и перечень контрольных мероприятий, которые далее транслируются в технический контур. Итогом этапа становится формализованный реестр активов и структурированная модель рисков, обеспечивающие воспроизводимость проектных решений и определяющие исходные параметры для внедрения технических мер, мониторинга и реагирования.

Этап 3. Реализация технических мер защиты и формирование эксплуатационного контура. Третий этап направлен на перевод нормативных и аналитических требований в функционирующий технический контур ССУБ. На основе реестра активов и модели рисков внедряются ключевые механизмы защиты: управление доступом (IAM/PAM), многофакторная аутентификация, принцип минимальных привилегий и сегментация ИТ-среды с выделением защищённых зон. Одновременно реализуются криптографические меры, средства контроля целостности, журналирование событий и системы обнаружения уязвимостей, обеспечивающие техническую наблюдаемость инфраструктуры. Параллельно формируются эксплуатационные регламенты, определяющие порядок обновления, резервного копирования, управления изменениями и восстановления после сбоев. Эти документы обеспечивают воспроизводимость технических операций и согласование фактических процессов с требованиями политики и модели рисков. Результатом этапа является целостный технический контур ССУБ, включающий

реализованные механизмы защиты, регламентированные процедуры их эксплуатации и формализованные каналы телеметрии, необходимой для последующего мониторинга и реагирования.

Этап 4. Формирование мониторингово-операционного контура (SOC/SIEM). На четвёртом этапе создаётся мониторингово-операционный контур, обеспечивающий наблюдаемость инфраструктуры и управляемое реагирование на инциденты. На основе реестра активов и модели рисков интегрируются источники телеметрии – серверы, сетевые устройства, приложения, облачные сервисы и подсистемы доступа. Для каждого источника определяется глубина и формат журналирования, что формирует единый поток данных для анализа. Центральным элементом этапа является развёртывание SIEM, выполняющего агрегирование, нормализацию и корреляцию событий. Корреляционные правила опираются на модели угроз и позволяют трансформировать разрозненные низкоуровневые события в структурированные инциденты с заданным приоритетом. Для сокращения времени реагирования внедряются механизмы автоматизации (SOAR) и формализованные плейбуки, задающие воспроизводимые сценарии обработки типовых событий. Мониторинговый контур формирует систему метрик – время обнаружения и реагирования, стабильность логирования, повторяемость инцидентов, полнота покрытия критичных активов. Эти показатели становятся ключевым источником информации для корректирующего управления на следующем этапе. Результатом этапа является функционирующий SOC/SIEM-контур, обеспечивающий непрерывное наблюдение, структурированную интерпретацию событий и оперативное реагирование, что повышает устойчивость инфраструктуры и управляемость рисков.

Этап 5. Контрольно-корректирующий цикл (PDCA) и оценка эффективности системы защиты. Финальный этап формирует корректирующий контур, обеспечивающий устойчивость и адаптивность сквозной системы безопасности к изменению угроз, конфигураций инфраструктуры и организационных условий. На основе данных мониторинга, телеметрии SOC/SIEM и эксплуатационных регламентов проводится регулярный аудит, включающий проверку конфигураций, анализ журналов событий, оценку полноты корреляции и работоспособности автоматизированных плейбуков реагирования. Полученные метрики – время обнаружения и реагирования, полнота покрытия активов, стабильность логирования, частота повторяющихся инцидентов – сопоставляются с моделью рисков, что позволяет выявлять отклонения, указывать на системные ошибки и определять зоны недостаточной защищённости. На основании анализа обновляются политика безопасности, регламенты, параметры технических механизмов и приоритеты развития инфраструктуры. Одновременно корректируется модель рисков и критерии критичности активов, что обеспечивает точное согласование требований с фактической архитектурой предприятия.

Завершающим элементом этапа становится стратегическое планирование повышения зрелости процессов, включая внедрение улучшений по CMMI-подходам, оптимизацию регламентов и расширение автоматизации. В результате формируется замкнутый цикл PDCA, в рамках которого система безопасности поддерживает способность к саморегуляции и развитию, обеспечивая непрерывную адаптацию к внешним и внутренним изменениям.

Заключение

Предложенная методология демонстрирует применимость ССУБ в организациях различных масштабов и отраслей. Этапный подход снижает риски неуспешной интеграции, а адаптация к

отраслевым и инфраструктурным особенностям позволяет формировать устойчивые контуры управления безопасностью. Ключевым фактором остается поддержка руководства, обеспечивающая согласованность процессов и закрепление ролей в системе.

Библиография

1. Айларова З.А. Цифровизация бизнеса в целях обеспечения экономически безопасного региона. Экономика и управление: проблемы, решения. 2024. Т. 7. № 8(149). С. 81-87. DOI 10.36871/ek.up.p.r.2024.08.07.010. https://doi.org/10.36871/ek.up.p.r.2024.08.07.010
2. Власенко А.В., Макарян А.С., Шарай В.А., Швырев Б.А. Информационная безопасность. Краснодар: Новация, 2020. 190 с.
3. Грязнова Е.В., Михеева В.В. Информационная инфраструктура деятельности муниципального управления. NB: Административное право и практика администрирования. 2015. № 6. С. 1-9. DOI 10.7256/2306-9945.2015.6.18389. https://doi.org/10.7256/2306-9945.2015.6.18389
4. Иванов С.Л. Социально-инфраструктурные барьеры цифровизации бизнеса в РФ и способы их преодоления. Проблемы современной экономики. 2025. № 1(93). С. 148-151.
5. Метельков А.Н. Цифровая информационная инфраструктура как объект технического регулирования в концепте ее защиты. Вестник Воронежского института ФСИН России. 2024. № 4. С. 116-124.
6. Регуш В.В., Маркова Г.В. Понятие и сущность организационно-экономического механизма воспроизводства материально-технических и производственных ресурсов. Экономика, труд, управление в сельском хозяйстве. 2017. № 1(30). С. 40-48.
7. Резниченко П.Ю. Особенности и подходы к цифровизации бизнеса. Экономика и управление: научно-практический журнал. 2024. № 5(179). С. 28-35. DOI 10.34773/EU.2024.5.5. https://doi.org/10.34773/EU.2024.5.5
8. Сунгатуллин Р.Г. Автоматизированные системы управления предприятием (ERP): анализ экономической эффективности. Экономика и управление: проблемы, решения. 2025. Т. 2. № 3(156). С. 40-49. DOI 10.36871/ek.up.p.r.2025.03.02.005. https://doi.org/10.36871/ek.up.p.r.2025.03.02.005
9. Табункова М.П., Оганесян Л.Л. Технико-экономическое обоснование выбора оптимальных средств обнаружения атак (вторжений) для нужд центров мониторинга Российской Федерации. Инженерный вестник Дона. 2023. № 11(107). С. 189-200.
10. Шереметьева Н.Г., Веролайнен С.И. Информационная инфраструктура: сущность и особенности оценки. International Law Journal. 2024. Т. 7. № 3. С. 182-188. DOI 10.58224/2658-5693-2024-7-3-182-188. https://doi.org/10.58224/2658-5693-2024-7-3-182-188

Implementation of an End-to-End Security Management System in a Cross-Industry Corporate Environment

Natal'ya S. Kozyr'

PhD in Economic Sciences, Associate Professor,
Kuban State Technological University,
350072, 2, Moskovskaya str., Krasnodar, Russian Federation;
e-mail: n_k_@mail.ru

Tat'yana V. Il'ina

PhD in Economic Sciences, Associate Professor,
Kuban State Technological University,
350072, 2, Moskovskaya str., Krasnodar, Russian Federation;
e-mail: ilina666666@mail.ru

Abstract

The article analyzes the features of implementing an end-to-end security management system in a cross-industry corporate environment characterized by high heterogeneity of IT infrastructure, differences in process maturity, and established organizational constraints. It is shown that a fragmented approach to information security leads to increased transactional costs, growth of operational uncertainty, and a higher probability of cascading failures affecting key business processes of the enterprise. During the research, structural barriers having a significant economic impact on the implementation of the system were identified: the presence of outdated technological components, the lack of an updated asset register, the gap between IT and information security functions, the formalized nature of policies that do not reflect real processes, and a shortage of specialists in the areas of GRC, SOC, and DevSecOps. These factors limit manageability and complicate the construction of a transparent risk model necessary for making informed management decisions. A cross-industry comparative analysis is conducted, showing that the financial sector, industry, medicine, education, and IT companies form differing regulatory requirements, threat profiles, and economic priorities. The obtained results confirm the need to adapt the security architecture to industry specifics, regulatory features, and available resources. A scalable implementation model is proposed, allowing for the alignment of the depth of organizational regulations, the scope of monitoring, and the level of automation with the size and maturity of the enterprise. A five-stage implementation scheme based on the PDCA logic is justified, including the formation of a regulatory framework, building a risk model, implementing technical measures, organizing monitoring, and a corrective development cycle. It is shown that the application of an end-to-end security management system contributes to the reduction of operational risks, increased transparency of corporate processes, and strengthened economic resilience of enterprises regardless of the industry.

For citation

Kozyr' N.S., Il'ina T.V. (2025) Vnedreniye skvoznoy sistemy upravleniya bezopasnost'yu v mezhotraslevoy korporativnoy srede [Implementation of an End-to-End Security Management System in a Cross-Industry Corporate Environment]. *Ekonomika: vchera, segodnya, zavtra* [Economics: Yesterday, Today and Tomorrow], 15 (11A), pp. 34-42. DOI: 10.34670/AR.2026.40.68.004

Keywords

Economic security, information security, regional economy, industry economy, security architecture, PDCA cycle, organizational development, organizational maturity, risk management, IT infrastructure.

References

1. Ailarova, Z. A. (2024). Tsifrovizatsiia biznesa v tseliakh obespecheniia ekonomicheski bezopasnogo regiona [Digitalization of business to ensure an economically secure region]. *Ekonomika i Upravlenie: Problemy, Resheniia*, 7(8), 81–87. https://doi.org/10.36871/ek.up.p.r.2024.08.07.010
2. Griaznova, E. V., & Mikheeva, V. V. (2015). Informatsionnaia infrastruktura deiatel'nosti munitsipal'nogo upravleniia [Information infrastructure of municipal governance]. *NB: Administrativnoe Pravo i Praktika Administrirovaniia*, 6, 1–9. https://doi.org/10.7256/2306-9945.2015.6.18389
3. Ivanov, S. L. (2025) Sotsial'no-infrastrukturnye bar'ery tsifrovizatsii biznesa v RF i sposoby ikh preodoleniia [Socio-infrastructural barriers to business digitalization in the Russian Federation and ways to overcome them]. *Problemy Sovremennoi Ekonomiki*, 1(93), 148–151.

4. Metel'kov, A. N. (2024). Tsifrovaia informatsionnaia infrastruktura kak ob"ekt tekhnicheskogo regulirovaniia v kontsepte ee zashchity [Digital information infrastructure as an object of technical regulation in the context of its protection]. *Vestnik Voronezhskogo Instituta FSIN Rossii*, 4, 116–124.
5. Regush, V. V., & Markova, G. V. (2017). Poniatie i sushchnost' organizatsionno-ekonomicheskogo mekhanizma vosproizvodstva material'no-tekhnicheskikh i proizvodstvennykh resursov [Concept and essence of the organizational-economic mechanism of reproduction of technical and production resources]. *Ekonomika, Trud, Upravlenie v Sel'skom Khoziaistve*, 1(30), 40–48.
6. Reznichenko, P. Y. (2024). Osobennosti i podkhody k tsifrovizatsii biznesa [Features and approaches to business digitalization]. *Ekonomika i Upravlenie: Nauchno-Prakticheskii Zhurnal*, 5(179), 28–35. https://doi.org/10.34773/EU.2024.5.5
7. Sheremet'eva, N. G., & Verolainen, S. I. (2024). Informatsionnaia infrastruktura: sushchnost' i osobennosti otsenki [Information infrastructure: Essence and assessment specifics]. *International Law Journal*, 7(3), 182–188. https://doi.org/10.58224/2658-5693-2024-7-3-182-188
8. Sungatullin, R. G. (2025) Avtomatizirovannye sistemy upravleniia predpriiatiem (ERP): analiz ekonomicheskoi effektivnosti [Enterprise resource planning (ERP) systems: Economic efficiency analysis]. *Ekonomika i Upravlenie: Problemy, Resheniia*, 2(3), 40–49. https://doi.org/10.36871/ek.up.p.r.2025.03.02.005
9. Tabunkova, M. P., & Oganesian, L. L. (2023). Tekhniko-ekonomicheskoe obosnovanie vybora optimal'nykh sredstv obnaruzheniia atak (vtoryzhenii) dlia nuzhd tsentrov monitoringa Rossiiskoi Federatsii [Techno-economic justification for the selection of optimal intrusion-detection tools for monitoring centers of the Russian Federation]. *Inzhenernyi Vestnik Dona*, 11(107), 189–200.
10. Vlasenko, A. V., Makarian, A. S., Sharai, V. A., & Shvyrev, B. A. (2020). *Informatsionnaia bezopasnost'* [Information security]. Novatsiia.