ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ И ТЕЛЕКОММУНИКАЦИИ
INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

УДК 004.056
DOI: 10.21822/2073-6185-2025-52-4-49-62

Оригинальная статья/ Original article

Оптимизация структуры ИСПДн объектов КИИ на основе теории рисков

Э.В. Бирих, И.И. Фадеев, Е.Н. Николаев, Д.В. Сахаров, П.А. Лужников
Санкт-Петербургский государственный университет телекоммуникаций
имени профессора М.А. Бонч-Бруевича,
193232, г. Санкт-Петербург, пр. Большевиков, 22, к. 1, Россия

Резюме. Цель. Целью исследования является снижение актуальных рисков ИБ важных активов на основе анализа и систематизации значимых недостатков, выявленных в результате аудита ИБ ИСПДн в двадцати организациях КИИ. **Метод.** Обобщение и анализ результатов контрольно-надзорной деятельности ИСПДн объектов КИИ, выявление наиболее опасных угроз на основе теории рисков. **Результат.** Выявлены опасные угрозы ИБ объектов КИИ, предложены решения по усилению защищенности ИСПДн путем изменения топологии, повышения защищенности сервера с ПДн за счет сегментации сети, многоуровневой фильтрации трафика и комплексного мониторинга. Проведен расчет эффективности предложенных мер. **Вывод.** Выявлены опасные типовые угрозы ИБ объектов КИИ, предложены решения по усилению защищенности в информационных системах персональных данных.

Ключевые слова: информационная система персональных данных, объекты критической информационной инфраструктуры, защита информации, модель угроз, модель нарушителя, информационная безопасность, теория рисков, сетевая инфраструктура

Для цитирования: Э.В. Бирих, И.И. Фадеев, Е.Н. Николаев, Д.В. Сахаров, П.А. Лужников. Оптимизация структуры ИСПДн объектов КИИ на основе теории рисков. Вестник Дагестанского государственного технического университета. Технические науки. 2025;52(4):49-62. DOI:10.21822/2073-6185-2025-52-4-49-62.

Optimization of the structure of the information system of personal data of critical information infrastructure objects based on risk theory

E.V. Birikh, I.I. Fadeev, E.N. Nikolaev, D.V. Sakharov, P.A. Luzhnikov
M.A. Bonch-Bruevich Saint Petersburg State University of Telecommunications,
22 Bolshevikov Ave., build. 1, St Petersburg 193232, Russia

Abstract. Objective. The purpose of the study is to reduce the actual risks of information security of important assets based on the analysis and systematization of significant deficiencies identified as a result of the ISPDn information security audit in twenty CII organizations. **Method.** Generalization and analysis of the results of the control and supervisory activities of ISPs of CII facilities, identification of the most dangerous threats based on risk theory. **Result.** Dangerous threats to the information security of CII facilities have been identified, and solutions have been proposed to enhance the security of ISPs by changing the topology, increasing the security of the server with PD through network segmentation, multi-level traffic filtering and integrated monitoring. The effectiveness of the proposed measures has been calculated. **Conclusion.** Dangerous typical threats to the information security of CII facilities have been identified, and solutions have been proposed to enhance security in personal data information systems.

Keywords: personal data information system, critical objects, information protection, threat model, intruder model, information security, risk theory, network infrastructure

For citation: E.V. Birikh, I.I. Fadeev, E.N. Nikolaev, D.V. Sakharov, P.A. Luzhnikov. Optimization of the structure of the information system of personal data of critical information infrastructure objects based on risk theory. Herald of Daghestan State Technical University. Technical Sciences. 2025; 52(4):49-62. (In Russ) DOI:10.21822/2073-6185-2025-52-4-49-62.

Введение. В современном цифровом обществе защита персональных данных (ПДн) является одной из важнейших задач как для государственных, так и для частных организаций. Указанная категория информации обрабатывается в информационных системах персональных данных (ИСПДн) [1-7]. Основным компонентом обеспечения безопасности ПДн является правильно спроектированная и защищённая сетевая инфраструктура, которая позволяет контролировать потоки данных и предотвращать несанкционированный доступ к информации [8-13]. Не случайно законодатель ввел новые нормы в статью 272 УК РФ и усилил уголовную ответственность за незаконное использование и передачу персональных данных. Изменения вступили в силу 11 декабря 2024 года [14].

Нормативно-правовая база, регламентирующая защиту ПДн в РФ, включает в себя ряд ключевых документов, таких как приказы ФСТЭК России № 21 от 18 февраля 2013 года и № 31 от 14 марта 2014 года [15, 16] в дополнение к приказу № 239 от 25 декабря 2017 г. Эти нормативные документы устанавливают требования к защите информации в ИСПДн и определяют основные меры, которые должны быть реализованы для обеспечения защиты данных, а также могут применятся на незначимых объектах КИИ.

Несмотря на обязательность исполнения требований указанных приказов ФСТЭК России, при проведении контрольных мероприятий федеральными органами исполнительной власти на объектах КИИ регулярно фиксируются многочисленные нарушения в области защиты ИСПДн, в типовой структуре которых присутствуют различные уровни сетевого взаимодействия, включающие сегменты обработки, хранения и передачи персональных данных, а также элементы контроля и защиты доступа. Выявляемые нарушения указывают на недостатки в реализации защитных мер, которые, хотя и прописаны в нормативной документации, часто остаются недостаточно реализованными на практике. Систематическое выявление таких нарушений подчёркивает необходимость совершенствования на предприятиях технических и организационных мер защиты, а также проведение регулярного контроля за соблюдением требований нормативных актов в сфере ИБ.

Постановка задачи. Задачей исследования является проведение анализа типовых нарушений безопасности, выявленных в ходе контрольно-надзорных мероприятий в двадцати организациях КИИ, и разработка подхода к повышению безопасности типовой инфраструктуры ИСПДн на основе оценки рисков.

Методы исследования. В работе использованы методы обобщения и анализа данных аудитов информационной безопасности ИСПДн, теория рисков на основе стандарта NIST SP 800-30 с использованием смешанного качественно-количественного подхода к оценке вероятности угроз, сочетающего экспертные оценки и статистические данные из отчетов Kaspersky [17-22]. Проведен расчет коэффициента эффективности защитных мер путем сравнения количества угроз до и после внедрения мер защиты. Выполнено моделирование защищенной сетевой топологии с учетом требований сегментации и многоуровневой фильтрации трафика. Осуществлен сравнительный анализ снижения рисков после внедрения предложенных защитных мер.

Обсуждение результатов. Аудит безопасности показывает, что многие компании сталкиваются с трудностями уже на этапе практической реализации требований к защите сетевой инфраструктуры [23-28]. Топология структуры типовой ИСПДн представлена на рис. 1.

Уровень сетевой инфраструктуры в контексте ИБ относится к физическим и логическим компонентам, которые составляют сеть для передачи данных. Это включает в себя все элементы, обеспечивающие коммуникацию и функционирование сети, такие как маршрутизаторы, коммутаторы, серверы, каналы связи, протоколы передачи данных и устройства защиты информации [29-35].

Рис. 1 – Топология типовой ИСПДн
Fig. 1 – Topology of a typical personal data information system

На основе анализа аудита ИБ ИСПДн выявлены нарушения защиты информации на уровне сетевой инфраструктуры, приведенные в табл. 1.

Таблица 1. Типовые нарушения в ИСПДн на сетевом уровне
Table 1. Typical violations in the ISPD at the network level

№	Тип нарушения Violation Type	Описание нарушения Violation Description
1	Отсутствие сегментации сети Lack of network segmentation	Не используется логическая или физическая сегментация сети для разделения зон с разным уровнем защиты. No logical or physical network segmentation is used to separate zones with different levels of protection.
2	Недостаточные меры по мониторингу сетевой активности Insufficient network activity monitoring	Отсутствие систем для анализа и мониторинга сетевых пакетов и подозрительной активности внутри сети. Lack of systems for analyzing and monitoring network packets and suspicious activity within the network.
3	Недостаточная защита от DDoS-атак Insufficient protection against DDoS attacks	Не реализованы механизмы защиты от распределённых атак на отказ в обслуживании, что увеличивает риск перегрузки сети. Distributed denial-of-service attack protection mechanisms are not implemented, which increases the risk of network overload.
4	Использование устаревших версий программного обеспечения Using outdated software versions	На некоторых узлах сети используются уязвимые версии ПО, что открывает потенциальные дыры в защите. Some network nodes are running vulnerable versions of software, which opens potential security holes.

Данные нарушения существенно снижают конфиденциальность, целостность, доступность ПДн и могут привести к утечке, несанкционированному доступу или блокировке конфиденциальной информации. Рассмотрим их подробнее:

1. Отсутствие сегментации сети – это нарушение, при котором не проводится разделение сети на логические или физические сегменты. Такое разделение позволяет ограничить доступ к разным зонам сети на основе уровня их критичности и степени конфиденциальности данных. Например, персонал, работающий с некритическими ресурсами, не должен иметь доступ к базам данных с персональной информацией. Без сегментации нарушитель, получивший доступ к одной части сети, может легко проникнуть в другие её зоны, включая те, которые содержат критически важные данные.

2. Недостаточные меры по мониторингу сетевой активности означают, что в организации либо отсутствуют, либо слабо настроены системы мониторинга и анализа сетевых пакетов. Это затрудняет своевременное обнаружение подозрительной активности, такой как несанкционированные подключения или сканирование портов. Без регулярного мониторинга сетевой активности администраторы могут не заметить кибератаку или внутреннюю утечку данных.

3. Недостаточная защита от DDoS-атак – это распространённое нарушение, которое связано с отсутствием механизмов противодействия распределённым атакам на отказ в обслуживании. В случае успешной атаки сеть может быть перегружена искусственно созданным трафиком, что приведёт к её недоступности для легитимных пользователей, а также увеличит уязвимость перед дальнейшими атаками, пока сеть отключена.

4. Использование устаревших версий программного обеспечения на сетевых узлах и устройствах создаёт серьёзные уязвимости, поскольку такие версии ПО могут содержать известные уязвимости, для которых уже выпущены обновления. Нарушители могут использовать эти уязвимости для проникновения в сеть, захвата контроля над сетевыми ресурсами или внедрения вредоносного кода. Для минимизации этих рисков организациям рекомендуется предпринять конкретные шаги, направленные на модернизацию сетевой инфраструктуры и оптимизацию процессов защиты данных [33-36]. Эти меры должны быть

реализованы в соответствии с требованиями, установленными законодательством, и передовыми практиками в области информационной безопасности. В табл. 2, были приведены рекомендации, которые помогут устранить наиболее распространённые нарушения.

Таблица 2. Рекомендации по устранению наиболее частых нарушений
Table 2. Recommendations for eliminating the most common violations

№	Тип нарушения Violation Type	Рекомендации по устранению Recommendations for elimination
1	Отсутствие сегментации сети Lack of network segmentation	Внедрить сегментацию сети с помощью VLAN, разделяя сетевые зоны на основе чувствительности данных. Implement network segmentation using VLANs, separating network zones based on data sensitivity.
2	Недостаточные меры по мониторингу сетевой активности Insufficient network activity monitoring	Внедрить системы обнаружения и предотвращения вторжений (IDS/IPS) и настроить регулярный мониторинг сетевой активности. Implement intrusion detection and prevention systems (IDS/IPS) and set up regular monitoring of network activity.
3	Недостаточная защита от DDoS-атак Insufficient protection against DDoS attacks	Установить системы фильтрации трафика и использования CDN для распределения нагрузки, настроить защиту от DDoS. Install traffic filtering systems and use CDN for load distribution, configure DDoS protection.
4	Использование устаревших версий программного обеспечения Using outdated software versions	Настроить регулярное обновление программного обеспечения и внедрить систему управления патчами (patch management). Set up regular software updates and implement a patch management system.

В современной цифровой среде информационные системы организаций постоянно подвергаются различным угрозам. Чтобы минимизировать возможные убытки и обеспечить защиту данных, используется теория рисков, которая позволяет оценить вероятность возникновения инцидента и его потенциальное влияние на организацию [17-18]. Согласно методике NIST 800-30, расчет коэффициента риска производится по следующей формуле:

$$R = P(t) \times S,$$

где R – значение риска, P – вероятность реализации угрозы информационной безопасности (применяется смесь качественной и количественной шкалы), S – степень влияния угрозы на актив (цена актива в качественной и количественной шкале).

Чтобы оценить вероятность P(t) с использованием смешанного подхода, разделим оценку на качественную и количественную составляющие:

1. Качественная оценка:

Будет использоваться метод анализа исторических данных. Вероятности выбираются на основе частоты возникновения угроз в прошлом, оценивая, насколько часто происходили инциденты, связанные с каждой угрозой. Оценка основана на данных отчётов, указывающих на количество инцидентов, а также на текущих тенденциях. Для качественной оценки используются следующие вероятности:

Высокая вероятность (0.7-1.0): Угроза реализовывалась часто (например, несколько инцидентов за последний год или больше 30% инцидентов связано с этой угрозой).

Средняя вероятность (0.4-0.6): Угроза реализовывалась время от времени (например, один или два инцидента за год или около 20-30%).

Низкая вероятность (0.1-0.3): Инциденты редки или незначительны (менее 20%).

2. Количественная оценка:

Количественная оценка основана на реальных данных о частоте инцидентов из отчётов. Используются данные из отчётов Kaspersky 2023 и 2024 годов. Таким образом, выполнен расчет вероятности P(t) для каждого типа нарушения:

1) Отсутствие сегментации сети:

Качественная оценка: высокая (0.7) – часто встречается в инцидентах.

Количественная оценка: согласно отчетам Kaspersky, около 30% всех атак были связаны с отсутствием сегментации. Это даёт количественную вероятность 0.3.

Итоговая вероятность P(t) – среднее арифметическое качественной и количественной оценок: $P(t) = (0.7 + 0.3)/2 = 0.5.$

2) Недостаточные меры по мониторингу сетевой активности:

Качественная оценка: средняя (0.5) – инциденты редки, но возможны.

Количественная оценка: в отчётах Kaspersky указано, что около 25% инцидентов связаны с недостаточным мониторингом. Это даёт количественную вероятность 0.25.

Итоговая вероятность: $P(t) = (0.5 + 0.25)/2 = 0.375$.

3) Недостаточная защита от DDoS-атак:

Качественная оценка: средняя (0.5) – случаи не часты, но возможны.

Количественная оценка: в отчетах отмечается, что около 15% инцидентов связаны с DDoS-атаками. Количественная вероятность – 0.15.

Итоговая вероятность: $P(t) = (0.5 + 0.15)/2 = 0.325$.

4) Использование устаревших версий ПО:

Качественная оценка: высокая (0.7) – часто встречается.

Количественная оценка: согласно отчетам, около 40% атак связаны с уязвимостями в устаревшем ПО. Количественная вероятность – 0.4.

Итоговая вероятность: $P(t) = (0.7 + 0.4)/2 = 0.55$.

Для того, чтобы посчитать R – итоговое значение риска, требуется определить S – стоимость актива. Для оценки рисков, связанных с утечками и компрометацией ПДн, важно учитывать различные факторы, влияющие на безопасность информационных систем. Каждый из этих факторов может оказывать значительное воздействие на конфиденциальность, целостность и доступность ПДн, что в свою очередь определяет уровень риска и последствий для организации. Подход к оценке S – стоимости актива, для каждого нарушения оценивается по шкале от 1 до 3, где:

1. Минимальные последствия (например, утечка некритичных ПДн, которая не оказывает значительного влияния на операции компании или нарушает права ограниченного числа субъектов данных).
2. Мредние последствия (например, компрометация ПДн сотрудников или клиентов, что может привести к финансовым убыткам, штрафам, утрате доверия и умеренным репутационным рискам).
3. Максимальные последствия (например, утечка конфиденциальной информации клиентов, такой как финансовые данные, медицинские данные или биометрические сведения, что может повлечь за собой значительные убытки, штрафы и серьезные репутационные потери).

Расчет оценки S – ценность актива (ПДн). Отсутствие сегментации сети: если сеть не сегментирована, нарушители могут беспрепятственно перемещаться по ней, получая доступ к персональным данным, таким как данные клиентов или сотрудников. Это может привести к нарушению конфиденциальности, целостности и доступности этих данных. Последствия оцениваются как максимальные, поскольку утечка или компрометация может повлечь за собой значительные репутационные и финансовые потери S = 3.

Недостаточные меры по мониторингу сетевой активности: мониторинг сетевой активности позволяет обнаруживать подозрительные действия и предотвращать утечки ПДн на ранних этапах. Отсутствие мониторинга может привести к утечке данных, однако последствия будут умеренными, так как угроза может затронуть ограниченное количество данных или субъектов S = 2.

Недостаточная защита от DDoS-атак: DDoS-атаки могут вызвать сбой в работе сервисов, которые обрабатывают или хранят персональные данные. В результате могут быть нарушены процессы, связанные с доступом к данным, что повлечет за собой значительные убытки для организаций, особенно тех, которые зависят от постоянного доступа к данным S = 3.

Использование устаревших версий ПО: Устаревшее программное обеспечение может содержать уязвимости, которые могут быть использованы для компрометации ПДн, таких как финансовая или медицинская информация. Это может привести к серьезным последствиям для конфиденциальности, целостности и доступности данных, создавая высокий уровень риска S =3. На основе полученных данных составлена табл. 3, в которой

содержаться сведения по типам нарушений, качественной оценки, количественной оценки, итоговой вероятности P(t), ценности актива S, а также итогового значения риска R.

Таблица 3. Результаты расчетов
Table 3. Calculation results

Тип нарушения Violation Type	**Качественная оценка Qualitative**	**Количественная оценка Quantitative**	**Вероятность P(t) Probability**	**S (ценность актива/ asset value)**	**R (значение риска/risk significance)**
Отсутствие сегментации сети/ Lack of network segmentation	0.7	0.3	0.5	3	0.9
Недостаточные меры по мониторингу сетевой активности/ Insufficient network activity monitoring	0.5	0.25	0.375	2	0.75
Недостаточная защита от DDoS-атак/ Insufficient protection against DDoS attacks	0.5	0.15	0.325	3	0.975
Использование устаревших версий программного обеспечения/ Using outdated software versions	0.7	0.4	0.55	3	1.65

Использование смешанной оценки вероятности, учитывающей как качественные, так и количественные показатели, позволяет более точно определить вероятность угроз. Наибольший риск (R = 1.65) наблюдается при использовании устаревших версий ПО, так как их уязвимости широко используются нарушителями. Согласно полученным данным, предложена защищенная сеть, которая может быть внедрена на предприятиях, занимающихся обработкой ПДн [34 - 29]. Топология данной сети представлена на рис. 2.

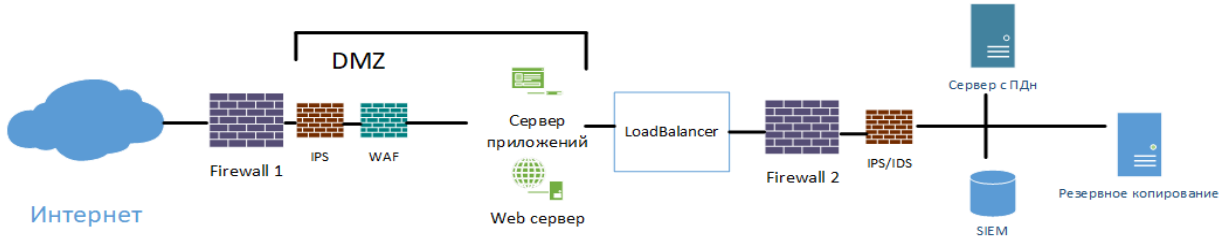

Рис. 2 – Топология защищенной сети
Fig. 2 – Topology of a secure network

Данная сеть включает несколько ключевых компонентов, каждый из которых выполняет определенные функции для защиты и обработки данных. Интернет-трафик сначала поступает на первый межсетевой экран (Firewall 1), который фильтрует входящие соединения и ограничивает доступ к демилитаризованной зоне (DMZ). В DMZ расположены веб-серверы и серверы приложений, которые обрабатывают запросы внешних пользователей. Также в DMZ размещен WAF (Web Application Firewall), который защищает веб-приложения от угроз на уровне приложений, таких как SQL-инъекции и XSS-атаки, фильтруя вредоносный HTTP-трафик.

Второй межсетевой экран (Firewall 2) изолирует внутреннюю сеть от DMZ, предоставляя дополнительный уровень безопасности. Внутренняя сеть содержит серверы с ПДн, доступ к которым контролируется более строгими правилами. Эти серверы поддерживаются системами мониторинга безопасности, такими как SIEM для анализа событий и IPS/IDS для предотвращения вторжений. Также между вторым firewall и внутренней сетью находится балансировщик нагрузки, который распределяет трафик между серверами и защищает от перегрузок.

Более подробное описание данной сети представлено в табл. 4.

Таблица 4. Описание топологии сети
Table 4. Description of network topology

Элемент Element	**Рекомендации по СЗИ Recommendations for information security system**	**Функциональная роль Functional role**	**Примеры защиты от атак Examples of protection against attacks**
Firewall	InfoWatch ARMA Industrial Firewall, InfoWatch ARMA Стена, Ideco NGFW (Ideco UTM), PT NGFW, другие отечественные аналоги	Ограничение доступа между внутренними и внешними сетями, фильтрация пакетов, защита от несанкционированного доступа.	-Lateral Movement (Латеральное движение) – ограничивает передвижение злоумышленника между сегментами сети. -Man-in-the-Middle (MitM) – блокирует атаки путем фильтрации трафика. -Privilege Escalation – фаерволы помогают предотвратить атаки с повышением привилегий.
DMZ	Отечественные решения для физической и логической сегментации	Сегментация сети. DMZ размещает публичные сервисы, изолируя их от внутренней сети и предотвращая прямой доступ к критичной информации.	-Internal Reconnaissance – ограничивает доступ атакующих к внутренним системам. -SQL Injection – защищает от попыток эксплуатации уязвимостей через веб-сервисы, размещенные в DMZ. -WannaCry – ограничивает распространение вируса в защищенные сегменты сети.
Load-Balancer	TrafficSoft ADC, DS Proxima Отечественные решения (в том числе за счёт кластеризации)	Балансировка нагрузки между серверами, повышение доступности сервисов и защита от DDoS-атак.	-SYN Flood – балансировщики нагрузки могут фильтровать SYN-пакеты и предотвращать перегрузку серверов. -UDP Flood – ограничивают трафик для защиты от атак, направленных на исчерпание пропускной способности. -Botnet Attacks – помогают распределить трафик, снижая эффект DDoS.
WAF	PT Application Firewall, InfoWatch ARMA, UserGate WAF Qrator (Cloud), MITIGATOR, ServicePipe (Cloud), Kaspersky AntiDDOS (Cloud)	Защита веб-приложений от атак на уровне HTTP(S), таких как SQL-инъекции, XSS, CSRF и другие уязвимости веб-приложений.	-SQL Injection – фильтрация запросов с потенциальными инъекциями. -Cross-Site Scripting (XSS) – предотвращение внедрения вредоносных скриптов в страницы веб-приложений. -Cross-Site Request Forgery (CSRF) – защита от подделки запросов.
IPS/IDS	В составе имеющихся отечественных средств типа Континент 4, ViPNet IDS 3, ViPNet IDS HS	Обнаружение и предотвращение вторжений, мониторинг сетевой активности, выявление аномального поведения в трафике.	-Brute Force Attack – мониторинг и предотвращение попыток перебора паролей. -Denial-of-Service (DoS) – обнаружение и блокировка атак на сетевые ресурсы. -Exploitation of Zero-Day Vulnerabilities – выявление и предотвращение атак на уязвимости, не имеющие патчей.
SIEM	PT MaxPatrol SIEM, RuSIEM, KUMA, R-Vision SIEM, KOMRAD	Централизованный сбор и анализ данных о событиях безопасности, мониторинг сетевойактивности и системы обнаружения угроз.	-Port Scanning – анализирует журналы и оповещает о сканировании портов. -Brute Force Attack – мониторит попытки массового перебора паролей. -DNS Spoofing – выявление аномальных изменений в DNS-записях, что может свидетельствовать о атаке.
Сервер с ПДн	Контроль баз данных с решениями продуктов классов DAM/DBF (Гарда БД)	Хранение ПДн и их защита от утечек и несанкционированного доступа.	-Ransomware – защита от программ-вымогателей, использующих уязвимости в старых версиях ПО для шифрования данных. -Buffer Overflow – предотвращение выполнения вредоносного кода через переполнение буфера. -SQL Injection – защита от инъекций в базы данных.
Backup Systems	Кибер Бэкап, RuBackup, ROC Backup	Регулярное создание резервных копий данных, обеспечение восстановления данных при сбоях или атаках.	-Ransomware – защита от потери данных в случае атаки программами-вымогателями, путем регулярного создания резервных копий. -Buffer Overflow – резервные копии помогут восстановить данные, если были повреждены из-за уязвимости в приложении. -WannaCry – восстановление данных после заражения вирусом.

При выборе СЗИ следует опираться на отечественные сертифицированные решения. Для углубленного анализа состояния защищённости ИСПДн объектов КИИ произведена систематизация выявленных в ходе аудита типов нарушений и соответствующих угроз безопасности. В рамках исследования осуществлён сбор данных о зарегистрированных угрозах, произведена оценка их количества за год по четырём основным типам выявленных нарушений. В табл. 5 определено количество угроз, зафиксированных в организациях без наличия защиты от соответствующих типов нарушений.

Таблица 5. Организации без защиты от соответствующих типов нарушений
Table 5. Organizations without protection against the corresponding types of violations

Тип нарушения Violation Type	**Количество организаций без защиты Number of organizations without protection**	**Количество угроз Number of threats**
Отсутствие сегментации сети/ Lack of network segmentation	2	54
Недостаточные меры по мониторингу сетевой активности/ Insufficient network activity monitoring	3	33
Недостаточная защита от DDoS-атак/ Insufficient protection against DDoS attacks	1	25
Использование устаревших версий программного обеспечения/ Using outdated software versions	4	14

В табл. 6 представлены данные об организациях, использующих меры защиты, а также количество зарегистрированных угроз.

Таблица 6. Организации с применением средств защиты
Table 6. Organizations using protective equipment

Тип нарушения Violation Type	**Количество организаций с защитой Number of organizations with protection**	**Используемые средства защиты Protective equipment used**	**Количество угроз Number of threats**
Отсутствие сегментации сети/ Lack of network segmentation	2	Firewall	10
Недостаточные меры по мониторингу сетевой активности/ Insufficient network activity monitoring	3	IPS/IDS	8
Недостаточная защита от DDoS-атак/ Insufficient protection against DDoS attacks	1	LoadBalancer	5
Использование устаревших версий программного обеспечения/ Using outdated software versions	4	Backup Systems	8

Для оценки эффективности применяемых мер защиты информационной безопасности в сети было решено рассмотреть изменения риска, связанного с выявленными нарушениями, до и после внедрения соответствующих защитных механизмов. Методология расчета основана на сочетании количественного анализа угроз и применения коэффициента эффективности мер защиты. Для этого использовался стандарт NIST 800-30.

Такой подход позволяет четко формализовать понятие риска и облегчает проведение дальнейших расчетов, учитывая изменения вероятности реализации угрозы после внедрения мер защиты. Для оценки влияния внедренных мер защиты на вероятность P, был введен коэффициент эффективности защитных мер Кэфф. Этот коэффициент характеризует степень снижения количества угроз в результате использования различных защитных механизмов. Такой подход позволяет количественно оценить эффективность защиты для каждого типа нарушений. Расчет коэффициента эффективности для каждого нарушения производится по следующей формуле:

$$К\text{эфф} = \frac{U\text{бз} - U\text{сз}}{U\text{бз}},$$

где Кэфф – коэффициент эффективности, Uбз – количество угроз до внедрения защиты, Uсз – количество угроз после внедрения защиты.

Произведен расчет показателей коэффициента для каждого типа нарушений:

1) Отсутствие сегментации сети:

$$K\text{эфф} = \frac{54 - 10}{54} = \frac{44}{54} = 0.815$$

2) Недостаточные меры по мониторингу сетевой активности:

$$K\text{эфф} = \frac{33 - 8}{33} = \frac{25}{33} = 0.758$$

3) Недостаточная защита от DDoS-атак:

$$K\text{эфф} = \frac{25 - 5}{25} = \frac{20}{25} = 0.8$$

4) Использование устаревших версий ПО:

$$K\text{эфф} = \frac{14 - 8}{14} = \frac{6}{14} = 0.429$$

Для учета влияния мер защиты вероятность реализации угрозы P была пересчитана на основе коэффициента эффективности. Это позволило перейти от исходной вероятности Pстар к скорректированной вероятности Pнов. Такой подход позволяет учитывать не только статистические данные, но и влияние защитных мер, что важно при анализе сетей с различными уровнями защиты. После внедрения мер защиты новая вероятность угрозы $P_{нов}$ определяется как:

$$P\text{нов} = P\text{стар} \times (1 - K\text{эфф}),$$

где $P_{нов}$ – вероятность после внедрения средства защиты, $P_{стар}$ – исходная вероятность до внедрения защиты, Kэфф – коэффициент эффективности защиты.

Расчет снижения вероятности по каждому типу нарушений:

1) Отсутствие сегментации сети:

$$P\text{нов} = 0.5 \times (1 - 0.815) = 0.0925$$

2) Недостаточные меры по мониторингу сетевой активности:

$$P\text{нов} = 0.375 \times (1 - 0.758) = 0.09075$$

3) Недостаточная защита от DDoS-атак:

$$P\text{нов} = 0.325 \times (1 - 0.8) = 0.065$$

4) Использование устаревших версий ПО:

$$P\text{нов} = 0.55 \times (1 - 0.429) = 0.31405$$

После пересчета вероятности Pнов был выполнен расчет нового уровня риска Rнов с учетом изменений вероятности реализации угрозы. Такой шаг позволил сравнить исходный уровень риска с уровнем после внедрения защитных мер. Кроме того, данный расчет помогает количественно оценить, насколько эффективно снижена угроза для каждого типа нарушения. Новый риск рассчитывается по следующей формуле:

$$R\text{нов} = P\text{нов} \times S,$$

где $R_{нов}$ – риск после снижения вероятности возникновения угрозы, $P_{нов}$ – вероятность после внедрения средства защиты, S – ценность актива.

Расчёт риска возникновения угрозы для каждого типа нарушения:

1) Отсутствие сегментации сети:

$$R\text{нов} = 0.0925 \times 3 = 0.2775$$

2) Недостаточные меры по мониторингу сетевой активности:

$$R\text{нов} = 0.09075 \times 2 = 0.1815$$

3) Недостаточная защита от DDoS-атак:

$$R\text{нов} = 0.065 \times 3 = 0.195$$

4) Использование устаревших версий ПО:

$$R\text{нов} = 0.31405 \times 3 = 0.94215$$

Для финальной оценки влияния внедренных мер защиты был рассчитан параметр снижения риска ΔR. Это значение отражает разницу между исходным и корректированным риском, которая напрямую зависит от коэффициента эффективности защиты. Таким образом, ΔR показывает, насколько значимым является вклад защитных мер в уменьшение угроз. Расчёт снижения риска производится по следующей формуле:

$$\Delta R = R\text{стар} - R\text{нов},$$

где ΔR – параметр снижения риска, $R_{стар}$ – исходное значение риска, $R_{нов}$ – риск после снижения вероятности возникновения угрозы.

Произведён расчет снижения риска для каждого типа нарушения:

1) Отсутствие сегментации сети:

$$\Delta R = 0.9 - 0.2775 = 0.6225$$

2) Недостаточные меры по мониторингу сетевой активности:

$$\Delta R = 0.75 - 0.1815 = 0.5685$$

3) Недостаточная защита от DDoS-атак:

$$\Delta R = 0.975 - 0.195 = 0.78$$

4) Использование устаревших версий ПО:

$$\Delta R = 1.65 - 0.94215 = 0.70785$$

Таким образом, предложенная топология сети обеспечивает надежную защиту сервера с ПДн за счет сегментации сети, многоуровневой фильтрации трафика и комплексного мониторинга.

Вывод. В статье исследована типовая топология ИСПДн, проведен анализ аудита таких систем в двадцати организациях КИИ, выделены и систематизированы значимые недостатки, влекущие серьёзные риски ИБ важных активов. На основе анализа выявляемых нарушений безопасности и оценки рисков по смешанной модели предложена топология сети, обеспечивающая повышенную защиту типовой инфраструктуры ИСПДн организации.

Проведённая количественная оценка рисков информационной безопасности продемонстрировала существенное снижение уровня угроз после внедрения защитных мер. Результаты расчётов показали значительное уменьшение показателей риска по всем рассматриваемым категориям. Полученные данные подтверждают эффективность реализованных защитных механизмов, выражающуюся в существенном снижении расчётных значений рисков по всем исследуемым направлениям. Цель работы достигнута.

Результаты работы могут быть использованы разработчиками активного сетевого оборудования и сетевых средств защиты информации, сотрудниками служб информационной безопасности в целях защиты корпоративных ИСПДн объектов КИИ.

Дальнейшей задачей в рамках данного исследования является оптимизация сетевой инфраструктуры ИСПДн с учетом перспективных методов защиты и современных угроз информационной безопасности на основе разработки адаптивных механизмов защиты, способных динамически реагировать на изменения в структуре атак и минимизировать риски для критически важных активов.

Благодарности. Исследование выполнено при финансовой поддержке Минцифры России («Грант ИБ МТУСИ № 40469 №22/21-к и №10/22-к»).

Acknowledgments. The study was carried out with the financial support of the Ministry of Digital Development of the Russian Federation (Grant IB MTUCI No. 40469 No. 22/21-k and No. 10/22-k).

Библиографический список:

1. Миняев А.А., Красов А.В., Сахаров Д.В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных. Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29-33 (15.08.2024).
2. Красов А.В., Лансере Н.Н., Фадеев И.И., Гельфанд А.М., Лесневский М.В. Типовые офтальмологические информационные системы, являющиеся объектами критической информационной инфраструктуры. Офтальмохирургия. 2022. № S4. С. 85-91 (15.08.2024).
3. Миняев А.А. Моделирование угроз безопасности информации в территориально-распределенных информационных системах. Наукоемкие технологии в космических исследованиях Земли. 2021. Т. 13. № 2. С. 52-65.
4. Lipatnikov V., Tikhonov V., Shevchenko A., Saharov D., Polyanicheva A.Security management in large-scale heterogeneous network systems based on intelligent information security services. В сборнике: ACM International Conference Proceeding Series. 5, The Premier Conference on Smart Next Generation Networking Technologies. Сер. "ICFNDS 2021 - 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies" 2021. С. 562-567 (19.08.2024).

5. Korshunov G.A., Lipatnikov V.A., Shevchenko A.A. Decision support systems for information protection in the management of the information network. В сборнике: Fuzzy Technologies in the Industry - FTI 2018. Proceedings of the II International Scientific and Practical Conference. Сер. "CEUR Workshop Proceedings" 2018. С. 418-426.
6. Ковцур М.М., Сахаров Д.В., Бирих Э.В., Дрепа В.Е. Метод обнаружения wlan точек доступа нарушителя в распределенной ИСПДн // Электросвязь. 2024. № 12-2. С. 60-69 (22.08.2024).
7. Сахаров Д.В., Штеренберг С.И., Левин М.В., Колесникова Ю.А. Разработка модели обеспечения отказоустойчивости сети передачи данных. Известия высших учебных заведений. Технология легкой промышленности. 2016. Т. 34. № 4. С. 14-20 (25.08.2024).
8. Синельщиков В. С., Цветков А. Ю. Защита персональных данных на предприятии //Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2021). – 2021. – С. 653-657 (26.08.2024).
9. Бирих Э.В. Разработка программного модуля для автоматизации определения уровня защищенности в ИСПДн / Булова М.Д., Казанцев А.А., Миняев А.А. //В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). Материалы XIII Международной научно-технической и научно-методической конференции. Санкт-Петербург, 2024. С. 122-127 (27.08.2024).
10. Лаврова Д.С., Попова Е.А., Штыркина А.А., Штеренберг С.И. Предупреждение Dos-атак путем прогнозирования значений корреляционных параметров сетевого трафика. Проблемы информационной безопасности. Компьютерные системы. – 2018. – №. 3. – С. 70-77.
11. Kovtsur M., Minyaev A., Khramtsov D., Abramenko G. Investigation of attacks and methods of protection of wireless networks during authorization using the ieee 802.1x protocol. В сборнике: ACM International Conference Proceeding Series. 5, The Premier Conference on Smart Next Generation Networking Technologies. Сер. "ICFNDS 2021 - 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies" 2021. С. 555-561 (4.09.2024).
12. Minyaev A.A., Krasov A.V., Saharov D.V. The method and methodology of efficiency assessment of protection system of distributed information systems. В сборнике: 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2020. Brno, 2020. С. 291-295 (6.09.2024).
13. Сахаров Д.В., Ковцур М.М., Бахтин Д.В. Модель защиты от эксплойтов и руткитов с последующим анализом и оценкой инцидентов. Наукоемкие технологии в космических исследованиях Земли. 2019. Т. 11. № 5. С. 22-31.
14. Федеральный закон «О внесении изменений в Уголовный кодекс Российской Федерации» от 30.11.2024 № 421-ФЗ.
15. Приказ ФСТЭК России "Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 18.02.2013 № 21. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21. - 2013 г. - с изм. и допол. в ред. от 25.11.2022. (20.09.2024).
16. Приказ ФСТЭК России "Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды" от 14.03.2014 № 31. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31. - 2014 г. - с изм. и допол. в ред. от 16.01.2023. (20.09.2024).
17. Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology: NIST 800-30. – Введ. 06.01.2002. – США. – 2002. – 56 с. (22.09.2024).
18. Информационные технологии. Методы и средства обеспечения безопасности. Ч. 3. Методы менеджмента безопасности информационных технологий: ГОСТ Р ИСО/МЭК ТО 13335-3-2007. – Введ. 01.09.2007. – М.: Стандартинформ, 2007. – 76 с (23.09.2024).
19. Андрианов В.И., Красов А.В., Липатников В.А. Инновационное управление рисками информационной безопасности. Учебное пособие / Санкт-Петербург, 2012 (24.09.2024).
20. Аналитический отчёт: Ландшафт киберугроз для России и СНГ 2024 // Лаборатория Касперского. URL: https://go.kaspersky.com/rs/802-IJN-240/images/Report_Threat_Landscape_RU.pdf (24.01.2025).
21. Every third cyber incident was due to ransomware, Kaspersky reports // Лаборатория Касперского URL: https://securelist.com/state-of-ransomware-2023/112590/ (дата обращения: 24.10.2024).
22. Отчеты от центров экспертизы «Лаборатории Касперского»: комплексный анализ актуальных угроз, технологий и трендов - всё для усиления вашей кибербезопасности. // Лаборатория Касперского URL: https://www.kaspersky.ru/enterprise-security/resources/white-papers (25.01.2025).
23. Бирих Э.В. К вопросу об аудите персональных данных / Ферапонтова С.С. // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 111-114. (27.01.2025).
24. Korshunov G.I., Lipatnikov V.A., Omarov R.G., Varzhapetian A.G. Prevention of attacks with distributed denial of service for information networks of cyberphysical systems. В сборнике: JOP Conference Series: Metrological Support of Innovative Technologies. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Krasnoyarsk, Russia, 2020. С. 32060. (27.01.2025).
25. Как устаревшие технологии ставят под угрозу безопасность и эффективность бизнеса // vc.ru — бизнес, технологии, идеи, модели роста, стартапы URL: https://vc.ru/u/2040785-gruppa-kompanii-x-com/1417550-kak-ustarevshie-tehnologii-stavyat-pod-ugrozu-bezopasnost-i-effektivnost-biznesa (25.10.2024).
26. Бирих Э.В., Ферапонтова С.С. К вопросу об аудите персональных данных // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2018). VII Международная научно-техническая и научно-методическая конференция. Сборник научных статей. В 4-х томах. Под редакцией С.В. Бачевского. 2018. С. 111-114.
27. Yurkin D.V., Livshitz I.I., Minyaev A.A. Formation of the instantaneous information security audit concept. Communications in Computer and Information Science. 2016. Т. 678. С. 314-324. Kashevnik A., Ponomarev A., Krasov A.

Human-computer threats classification in intelligent transportation systems. Conference of Open Innovations Association, FRUCT. 2020. № 26. С. 151-157. (27.01.2025).
28. Doynikova E.V., Fedorchenko A.V., Novikova E.S., Ushakov I.A., Krasov A.V. Security decision support in the control systems based on graph models. В сборнике: Proceedings of 2021 IV International Conference on Control in Technical Systems (CTS). IEEE, 2021. С. 224-227. (28.01.2025).
29. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning. Studies in Computational Intelligence. 2020. Т. 868. С. 350-355. (2.02.2025).
30. Vitkova L., Saenko I., Tushkanova O. An approach to creating an intelligent system for detecting and countering inappropriate information on the internet. Studies in Computational Intelligence. 2020. Т. 868. С. 244-254. (4.02.2025).
31. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure. В сборнике: Proceedings - 2019 International Russian Automation Conference, RusAutoCon 2019. 2019. С. 8867699.
32. Kotenko I., Vitkova L., Saenko I., Tushkanova O., Branitskiy A. The intelligent system for detection and counteraction of malicious and inappropriate information on the internet. AI Communications. 2020. -Т. -33. № 1. -С. 13-25.
33. Zhernova K., Chechulin A. Overview of vulnerabilities of decision support interfaces based on virtual and augmented reality technologies. Lecture Notes in Networks and Systems. 2022. Т. 330 LNNS. С. 400-409. (7.02.2025).
34. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders. В сборнике: ACM International Conference Proceeding Series. 4. Сер. "Proceedings of the 4th International Conference on Future Networks and Distributed Systems, ICFNDS 2020" 2020. С. 3442619. (7.02.2025).
35. Бирих Э.В., Паскенова А.У. Комплексная защита объекта информатизации // В сборнике: Технологии информационного общества. Сборник трудов XIX Международной отраслевой научно-технической конференции. Москва, 2025. С. 136-138. (8.02.2025).
36. IPS/IDS — системы обнаружения и предотвращения вторжений // Selectel — аренда IT-инфраструктуры для бизнеса URL: https://selectel.ru/blog/ips-and-ids/ (25.10.2024).
37. Сегментация сети в парадигме результативной кибербезопасности // Результативная кибербезопасность URL: https://rezbez.ru/article/segmentacziya-seti-v-paradigme-rezultativnoj-kiberbezopasnosti (дата обращения: 25.01.2024).
38. Липатников В.А., Сахаров Д.В., Кузнецов И.А. Управление безопасностью распределенной ивс на основе прогноза заражения компьютерным вирусом. Электросвязь. 2017. № 1. С. 53-59. (9.02.2025).
39. Медведева И.М., Бирих Э.В. Методы защиты от утечек конфиденциальной информации и персональных данных // Актуальные проблемы социально-гуманитарного и научно-технического знания. 2025. № 1(41). С. 5-8.
40. Бирих Э.В., Булова М.Д., Казанцев А.А., Миняев А.А. Разработка программного модуля для автоматизации определения уровня защищенности в ИСПДН // В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2024). Материалы XIII Международной научно-технической и научно-методической конференции. Санкт-Петербург, 2024. С. 122-127 (14.02.2025).
41. Махмутова Н.Ф., Бирих Э.В., Сахаров Д.В., Кривец А.С., Дегтярев М.А. Исследование способов повышения безопасности корпоративных сетей. Вестник Дагестанского государственного технического университета. Технические науки. 2024;51(3):110-116. https://doi.org/10.21822/2073-6185-2024-51-3-110-116 (17.02.2025).
42. Ковцур М.М., Сахаров Д.В., Бирих Э.В., Дрепа В.Е. Метод обнаружения wlan точек доступа нарушителя в распределенной ИСПДН // Электросвязь. 2024. № 12-2. С. 60-69. (18.02.2025).
43. Сахаров Д.В., Красов А.В., Ушаков И.А., Орлов Г.А. Защищенная модель программно-определяемой сети в среде виртуализации KVM. Электросвязь. 2020. № 3. С. 26-32. (23.02.2025).
44. Андрианов В.И., Бухарин В.В., Кирьянов А.В., Липатников В.А., Санин И.Ю., Сахаров Д.В., Стародубцев Ю.И. Способ защиты информационно-вычислительных сетей от компьютерных атак // Патент на изобретение RU 2472211 C1, 10.01.2013. Заявка № 2011147613/08 от 23.11.2011 (24.02.2025).

References:

1. Minyaev A.A., Krasov A.V., Sakharov D.V. A method for evaluating the effectiveness of the information protection system of geographically distributed personal data information systems. *Bulletin of the St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences.* 2020; 1: 29-33. (08/15/2024) (In Russ).
2. Krasov A.V., Lancere N.N., Fadeev I.I., Gelfand A.M., Lesnevsky M.V. Typical ophthalmological information systems that are objects of critical information infrastructure. *Ophthalmosurgery*. 2022; S4: 85-91. (08/15/2024). (In Russ).
3. Minyaev A.A. Modeling of information security threats in geographically distributed information systems. High-tech technologies in space exploration of the Earth. 2021; 13(2):52-65. (In Russ).
4. Lipatnikov V., Tikhonov V., Shevchenko A., Saharov D., Polyanicheva A.Security management in large-scale heterogeneous network systems based on intelligent information security services. In the collection: ACM International Conference Proceeding Series. 5, The Premier Conference on Smart Next Generation Networking Technologies. Cer. "ICFNDS 2021 - 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies" 2021: 562-567. (08/19/2024).
5. Korshunov G.A., Lipatnikov V.A., Shevchenko A.A. Decision support systems for information protection in the management of the information network. In the collection: Fuzzy Technologies in the Industry - FTI 2018. Proceedings of the II International Scientific and Practical Conference. Ser. "CEUR Workshop Proceedings" 2018: 418-426.
6. Kovtsur M.M., Sakharov D.V., Birikh E.V., Drepa V.E. Method of detecting wlan access points of an intruder in a distributed ISPDn. *Telecommunication.* 2024;12-2: 60-69 (08/22/2024). (In Russ).
7. Sakharov D.V., Shterenberg S.I., Levin M.V., Kolesnikova Yu.A. Development of a data transmission network fault tolerance model. News of higher educational institutions. *Technology of light industry*. 2016; 34(4):14-20. (08/25/2024). (In Russ).
8. Sinelshchikov V. S., Tsvetkov A. Yu. Protection of personal data at the enterprise. *Actual problems of infotelec communications in science and education* (APINO 2021). 2021:653-657 (08/26/2024). (In Russ).
9. Birikh E.V. Development of a software module for automating the determination of the security level in ISPs / Bulova M.D., Kazantsev A.A., Minyaev A.A. // In the collection: Actual problems of infotelec communications in science and

education (APINO 2024). Proceedings of the XIII International Scientific, Technical, Scientific and Methodological Conference. Saint Petersburg, 2024:122-127 (08/27/2024). (In Russ).
10. Lavrova D.S., Popova E.A., Shtyrkina A.A., Shterenberg S.I. Prevention of Dos attacks by predicting the values of correlation parameters of network traffic. *Information security issues. Computer systems*. 2018;3:70-77. (In Russ).
11. Kovtsur M., Minyaev A., Khramtsov D., Abramenko G. Investigation of attacks and methods of protection of wireless networks during authorization using the ieee 802.1x protocol.In the collection: ACM International Conference Proceeding Series. 5, The Premier Conference on Smart Next Generation Networking Technologies. Cer. "ICFNDS 2021 - 5th International Conference on Future Networks and Distributed Systems: The Premier Conference on Smart Next Generation Networking Technologies" 2021:555-561. (094/2024).
12. Minyaev A.A., Krasov A.V., Saharov D.V. The method and methodology of efficiency assessment of protection system of distributed information systems. In the collection: 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops, ICUMT 2020. Brno, 2020: 291-295. (09/6/2024).
13. Sakharov D.V., Kovtsur M.M., Bakhtin D.V. A model of protection against exploits and rootkits with subsequent analysis and assessment of incidents. *High-tech technologies in space exploration of the Earth*. 2019;11(5):22-31. (In Russ).
14. Federal Law "On Amendments to the Criminal Code of the Russian Federation" dated 11/30/2024 No. 421-FZ.
15. Order of the FSTEC of Russia "On Approval of the Composition and Content of Organizational and Technical Measures to Ensure the Security of Personal Data during their Processing in Personal Data Information Systems" dated 02/18/2013 No. 21. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 . - 2013 - with amendments and additions. ed. dated 11/25/2022. (09/20/2024). (In Russ).
16. Order of the FSTEC of Russia "On Approval of Requirements for Information Security in Automated Control Systems for Production and Technological Processes at Critical Facilities, Potentially Dangerous Facilities, as well as Facilities that pose an Increased Danger to Human Life and Health and to the Environment" dated 03/14/2014 No. 31. URL: https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-14-marta-2014-g-n-31 - 2014 - with amendments and additions. ed. from 01/16/2023. (09/20/2024). (In Russ).
17. Risk management guide for information technology systems. Recommendations of the National Institute of Standards and Technology: NIST 800-30. – Introduction. 06.01.2002. – USA. – 2002: 56 (09/22/2024).
18. Information technology. Methods and means of ensuring security. Part 3. Methods of information technology security management: GOST R ISO/IEC TO 13335-3-2007. – Introduction. 09/01/2007. Moscow: Standartinform, 2007:76 (09/23/2024). (In Russ).
19. Andrianov V.I., Krasov A.V., Lipatnikov V.A. Innovative information security risk management. Textbook / Saint Petersburg, 2012 (09/24/2024). (In Russ).
20. Analytical report: The Cyber Threat Landscape for Russia and the CIS 2024 // Kaspersky Lab. URL: https://go.kaspersky.com/rs/802-IJN-240/images/Report_Threat_Landscape_RU.pdf (24.01.2025). (In Russ).
21. Every third cyber incident was due to ransomware, Kaspersky reports // Kaspersky Lab URL: https://securelist.com/state-of-ransomware-2023/112590 / (accessed: 10/24/2024).
22. Reports from Kaspersky Lab's Expertise Centers: Comprehensive analysis of current threats, technologies, and trends - everything to enhance your cybersecurity. // Kaspersky Lab URL: https://www.kaspersky.ru/enterprise-security/resources/white-papers (01/25/2025).
23. Birikh E.V. On the issue of personal data audit / Ferapontova S.S. In the collection: Actual problems of infotelec communications in science and education (APINO 2018). VII International Scientific, Technical, Scientific and Methodological Conference. Collection of scientific articles. In 4 volumes. Edited by S.V. Bachevsky. 2018:111-114 (01/27/2025). (In Russ).
24. Korshunov G.I., Lipatnikov V.A., Omarov R.G., Varzhapetian A.G. Prevention of attacks with distributed denial of service for information networks of cyberphysical systems. In the collection: JOP Conference Series: Metrological Support of Innovative Technologies. Krasnoyarsk Science and Technology City Hall of the Russian Union of Scientific and Engineering Associations. Krasnodar, Russia, 2020. pp. 32060. (01/27/2025).
25. How outdated technologies jeopardize business security and efficiency // vc.ru — business, technology, ideas, growth models, startups URL: https://vc.ru/u/2040785-gruppa-kompanii-x-com/1417550-kak-ustarevshie-tehnologii-stavyat-pod-ugrozu-bezopasnost-i-effektivnost-biznesa (10/25/2024). (In Russ).
26. Birikh E.V., Ferapontova S.S. On the issue of personal data audit. In the collection: Actual problems of infotelec communications in science and education (APINO 2018). VII International Scientific, Technical, Scientific and Methodological Conference. Collection of scientific articles. In 4 volumes. Edited by S.V. Bachevsky. 2018:111-114. (In Russ).
27. Yurkin D.V., Livshitz I.I., Minyaev A.A. Formation of the instantaneous information security audit concept. Communications in Computer and Information Science. 2016. Vol. 678. pp. 314-324. Kashevnik A., Ponomarev A., Krasov A. Human-computer threats classification in intelligent transportation systems. *Conference of Open Innovations Association, FRUCT.* 2020; 26:151-157. (01/27/2025).
28. Doynikova E.V., Fedorchenko A.V., Novikova E.S., Ushakov I.A., Krasov A.V. Security decision support in the control systems based on graph models. In the collection: Proceedings of the 2021 IV International Conference on Control in Technical Systems (CTS). IEEE, 2021: 224-227. (01/28/2025).
29. Balueva A., Desnitsky V., Ushakov I. Approach to detection of denial-of-sleep attacks in wireless sensor networks on the base of machine learning. *Studies in Computational Intelligence*. 2020; 868: 350-355. (2.02.2025).
30. Vitkova L., Saenko I., Tushkanova O. An approach to creating an intelligent system for detecting and countering inappropriate information on the internet. *Studies in Computational Intelligence*. 2020; 868: 244-254. (02/14/2025).
31. Krasov A., Vitkova L., Pestov I. Behavioral analysis of resource allocation systems in cloud infrastructure. In the collection: Proceedings - 2019 International Russian Automation Conference, RusAutoCon 2019. 2019:.8867699.
32. Kotenko I., Vitkova L., Saenko I., Tushkanova O., Branitskiy A. The intelligent system for detection and counteraction of malicious and inappropriate information on the internet. *AI Communications.* 2020; 33(1):13-25.
33. Zhernova K., Chechulin A. Overview of vulnerabilities of decision support interfaces based on virtual and augmented reality technologies. *Lecture Notes in Networks and Systems*. 2022; 330 LNNS:400-409 (02/7/2025).

34. Buinevich M., Izrailov K., Kotenko I., Ushakov I., Vlasov D. Approach to combining different methods for detecting insiders. In the collection: ACM International Conference Proceeding Series. 4. Proceedings of the 4th International Conference on Future Networks and Distributed Systems, ICFNDS 2020, 2020: 3442619. (02/7/2025).
35. Birich E.V., Paskenova A.U. Complex protection of the informatization object // In the collection: Information Society Technologies. Proceedings of the XIX International Industrial Scientific and Technical Conference. Moscow, 2025. pp. 136-138 (02/08/2025). (In Russ).
36. IPS/IDS - intrusion detection and prevention systems. Selectel - rental of IT infrastructure for business URL: https://selectel.ru/blog/ips-and-ids / (10/25/2024). (In Russ).
37. Network segmentation in the effective cybersecurity paradigm. Effective cybersecurity URL: https://rezbez.ru/article/segmentacziya-seti-v-paradigme-rezultativnoj-kiberbezopasnosti (date of reference: 01/25/2024).
38. Lipatnikov V.A., Sakharov D.V. Kuznetsov I.A. Security management of a distributed IVS based on the prediction of infection with a computer virus. *Telecommunications*. 2017;1:53-59. (02/9/2025). (In Russ).
39. Medvedeva I.M., Birikh E.V. Methods of protection against leaks of confidential information and personal data. *Actual problems of socio-humanitarian and scientific-technical knowledge.* 2025;1 (41): 5-8. (In Russ).
40. Birikh E.V., Bulova M.D., Kazantsev A.A., Minyaev A.A. Development of a software module for automating the determination of the security level in ISPS // In the collection: Current problems of infotelec communications in science and education (APINO 2024). Proceedings of the XIII International Scientific, Technical, Scientific and Methodological Conference. Saint Petersburg, 2024. pp. 122-127 (02/14/2025). (In Russ).
41. Makhmutova N.F., Birikh E.V., Sakharov D.V., Krivets A.S., Degtyarev M.A. Investigation of ways to improve the security of corporate networks. *Herald of Daghestan State Technical University. Technical Sciences.* 2024;51(3):110-116. https://doi.org/10.21822/2073-6185-2024-51-3-110-116 (02/17/2025). (In Russ).
42. Kovtsur M.M., Sakharov D.V., Birikh E.V., Drepa V.E. A method for detecting an intruder's wlan access points in a distributed ISPDN. *Telecommunications.* 2024;12-2: 60-69 (02/18/2025). (In Russ).
43. Sakharov D.V., Krasov A.V., Ushakov I.A., Orlov G.A. A secure model of a software-defined network in a KVM virtualization environment. *Telecommunications*. 2020; 3:26-32 (02/23/2025). (In Russ).
44. Andrianov V.I., Bukharin V.V., Kiryanov A.V., Lipatnikov V.A., Sanin I.Yu., Sakharov D.V., Starodubtsev Yu.I. A method for protecting information and computing networks from computer attacks. Patent for invention RU 2472211 C1, 10.01.2013. Application No. 2011147613/08 dated 11/23/2011 (02/24/2025). (In Russ).

Сведения об авторах:

Бирих Эрнест Владимирович, старший преподаватель, кафедра защищенных систем связи; be1982@mail.ru. ORCID.org/0000-0003-4808-9422

Фадеев Илья Игоревич, ассистент, кафедра защищенных систем связи; fadeev.collapse@yandex.ru. ORCID.org/0009-0003-0256-2330

Николаев Ефим Николаевич, студент, кафедра информационной безопасности компьютерных сетей; nickolaev.efim@yandex.ru. ORCID.org/0009-0005-7805-4249

Сахаров Дмитрий Владимирович, кандидат технических наук, доцент, доцент, кафедра защищенных систем связи; sguard7@mail.ru. ORCID.org/0000-0002-6130-5321

Лужников Павел Алексеевич, кандидат технических наук, старший научный сотрудник, доцент, кафедра защищенных систем связи; Pavel_oreshek1@mail.ru. ORCID.org/0009-0000—0693-0960

Information about the authors:

Ernest V. Birikh, Senior Lecturer, Department of Secure Communication Systems; be1982@mail.ru. ORCID.0000-0003-4808-9422

Ilya I. Fadeev, Assistant, Department of Secure Communication Systems; fadeev.collapse@yandex.ru. ORCID.0009-0003-0256-2330

Efim N. Nikolaev, Student, Department of Information Security of Computer Networks; nickolaev.efim@yandex.ru. ORCID.0009-0005-7805-4249

Dmitrii V. Sakharov, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof. of the Department of Secure Communication Systems; sguard7@mail.ru. ORCID.0000-0002-6130-5321

Pavel A. Luzhnikov, Cand. Sci. (Eng.), Assoc. Prof., Assoc. Prof. of the Department of Secure Communication Systems; Pavel_oreshek1@mail.ru. ORCID.0009-0000—0693-0960

Конфликт интересов/Conflict of interest.

Авторы заявляют об отсутствии конфликта интересов/The authors declare no conflict of interest.

Поступила в редакцию/Received 15.09.2025.

Одобрена после рецензирования/Reviced 21.10.2025.

Принята в печать/Accepted for publication 29.10. 2025.