

СИСТЕМА КОМПЛЕКСНОЙ ЗАЩИТЫ СИТУАЦИОННОГО ЦЕНТРА

© А. В. Фурсова¹, А. В. Яковлев¹✉

¹ *Кафедра «Информационные системы и защита информации»,
yava73@bk.ru; ФГБОУ ВО «ТГТУ», Тамбов, Российская Федерация*

Ключевые слова: защита информации; сертифицированные средства защиты; ситуационный центр; технические каналы.

Аннотация: Представлено описание подхода к защите ситуационных центров, как одной из целей атак злоумышленников для получения информации ограниченного доступа. Комплексная защита включает в себя построение защищаемого программно-аппаратного контура в соответствии с требованиями ФСТЭК России, а также меры защиты конфиденциальных переговоров от утечки по техническим каналам. Рассмотрены структура и состав аппаратных и программных средств защиты информации типового ситуационного центра и требования нормативно-правовых актов в данной предметной области. Определены уровни применения сертифицированных средств защиты и обоснована технология реализации подхода. Данный подход предусматривает интеграцию средств защиты при соблюдении нормативных требований и позволяет создать среду, устойчивую к современным угрозам информационной безопасности, для ситуационного центра.

Введение

Российская группа компаний «Солар», специализирующаяся на предоставлении услуг и сервисов в области информационной безопасности, представила отчет о кибератаках на российские компании в 2024 году, согласно которому большинство инцидентов информационной безопасности зафиксированы в государственном секторе [1]. Заинтересованность злоумышленников государственными структурами вызвана стремлением в получении доступа к информации ограниченного доступа, обрабатываемым персональным данным, а также к важным государственным документам. Внедренная на всех уровнях государственной власти – от федерального до муниципального – сеть распределенных ситуационных центров, обеспечивающая оперативный мониторинг и анализ информации, может выступать в качестве цели атаки злоумышленников [2].

Структура и состав средств ситуационного центра

Ситуационный центр состоит из аппаратных и программных составляющих, необходимых для сбора, обработки и визуализации данных о наблюдаемых объектах [3]. Аппаратная часть ситуационного центра включает в себя следующие компоненты [4, 5]:

- экраны коллективного пользования (видеостены);
- средства видеоконференцсвязи;

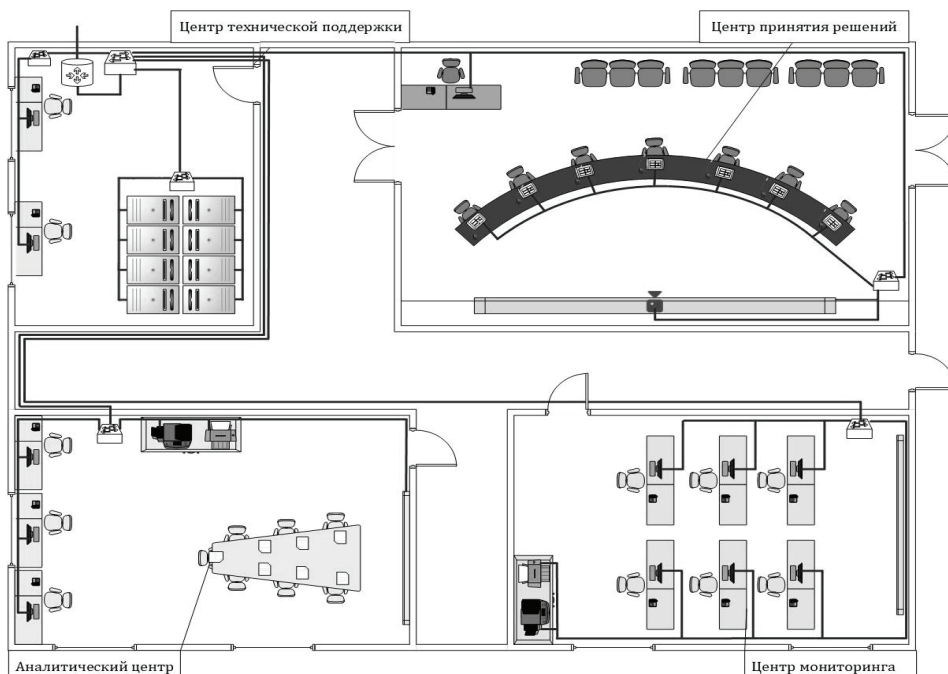


Рис. 1. Структура ситуационного центра

- серверное оборудование различного целевого назначения;
- стационарные автоматизированные рабочие места;
- коммуникационное оборудование.

Роль экрана коллективного пользования выполняет видеостена, на которой демонстрируется информация в виде графиков, схем, изображений и т. д. В качестве источников для исходных данных выступают системы видеонаблюдения, SCADA-системы и каналы вещания. Видеостена представляет собой модули отображения (например, светодиодных экранов), которые формируют единый экран, и контроллер, отвечающий за обработку и распределение сигналов от источников на модули отображения.

Система видеоконференцсвязи ситуационного центра предназначена для оперативного проведения совещаний и удаленных переговоров в режиме реального времени, что критически важно для анализа данных и принятия коллективных решений [6]. Средства видеоконференцсвязи включают в себя готовые программно-аппаратные решения – это комплекс из специального клиентского программного обеспечения для подключения к видеоконференции, сервера управления и сервера видеосвязи.

Назначение серверного оборудования для функционирования ситуационного центра определяет количество приобретаемого аппаратного компонента. Ситуационный центр предполагает обработку больших информационных потоков, поэтому внедряется сервер хранения данных, который чаще всего включает в себя несколько дисковых хранилищ, объединенных, например, с помощью RAID. Доменная структура, где автоматизированные рабочие места объединены общими политиками и логически разделены по подсетям, создается с помощью сервера контроллера домена. Отдельно выделяется сервер на прикладные задачи, связанные с визуализацией информации, мониторинга и прогнозирования на основании получаемых данных, то есть на обработку больших данных.

Оборудованные стационарные автоматизированные рабочие места необходимы не только специалистам центра мониторинга и аналитики для получения, обработки и подготовки информации, но и непосредственно специалистам технической поддержки и сотруднику центра принятия решения для управления отображением информационных потоков, а также для отслеживания работы оборудования ситуационного центра. Техническое оснащение включает в себя рабочие станции, интегрированные в локальную сеть ситуационного центра, а также мониторы, МФУ и телефоны для оперативного взаимодействия.

В состав коммуникационного оборудования входят коммутаторы, маршрутизаторы, кабельные линии, необходимые для формирования сетевой инфраструктуры ситуационного центра.

Организация защиты информации в ситуационном центре

Поскольку ситуационный центр предназначен для анализа больших потоков данных, то ключевым элементом центра становится программное обеспечение, способное формировать целостную и понятную картину для управления из разрозненной информации, полученной из различных источников. Причем данное программное обеспечение может представлять собой как самостоятельную сборку необходимых компонентов для выполнения целей ситуационного центра, начиная от программного обеспечения для автоматизированных рабочих мест и заканчивая системой прогнозирования и принятия решений, так и готовые программные решения коммерческих компаний. Примерами таких решений, зарегистрированных в реестре российского программного обеспечения, являются [7]:

- ситуационный центр «Джет»;
- центр управления / ситуационный центр руководителя;
- информационно-аналитическая платформа ситуационных центров OODM.

Кроме применения системного, прикладного и информационно-аналитического программного обеспечения, применяются программные решения для обеспечения защиты информации ограниченного доступа. В соответствии с требованиями Приказа ФСТЭК России № 17 ситуационный центр, обрабатывающий информацию высокого уровня значимости (УЗ 1) в масштабах регионального, относится к классу защищенности К1 [8]. Для обеспечения защиты циркулирующей в нем информации необходимо внедрение комплекса сертифицированных средств защиты информации, представленных в табл. 1.

Сертифицированные средства защиты формируют собой защищенный контур для ситуационного центра:

- превентивный уровень – антивирусная защита и контроль доступа;
- уровень обнаружения – системы обнаружения вторжений и SIEM-системы;
- уровень обеспечения устойчивости – средства виртуализации и обеспечение целостности.

Таким образом, достижение класса защищенности К1 для ситуационного центра становится возможным при интеграции приведенных выше сертифицированных средств в единый программно-аппаратный комплекс. Но при этом защищенность информации достигается не только за счет внедрения этих решений, но и благодаря правильной настройке и согласованному взаимодействию.

Ситуационный центр – это не только мощный аналитический и визуальный комплекс, но и место проведения закрытых совещаний, где обсуждается стратегически важная информация. При этом рассмотренные ранее методы защиты информации не учитывают возможность утечки информации по акустиковибрационному каналу. В связи с этим необходимо выполнение требований СТР-К в части защиты конфиденциальной речевой информации [9].

Таблица 1

Сертифицированные средства защиты информации

Меры защиты информации	Примеры сертифицированных средств
Идентификация и аутентификация субъектов доступа и объектов доступа	Специальные конфигурации сертифицированных операционных систем. Средство защиты информации Secret Net Studio
Управление доступом субъектов доступа к объектам доступа	Специальные конфигурации сертифицированных операционных систем. Средство защиты информации Secret Net Studio. Программа контроля полномочий доступа к информационным ресурсам «Ревизор-2 XP»
Регистрация событий безопасности	Программный комплекс «Система мониторинга и управления событиями безопасности Ankey SIEM. Система управления событиями информационной безопасности U-SIEM. Программный комплекс «Система мониторинга и управления событиями безопасности Smart Monitor»
Антивирусная защита	Dr.Web Enterprise Security Suite. Kaspersky Endpoint Security
Обнаружение вторжений	Межсетевой экран и система обнаружения вторжений «Рубикон». Межсетевой экран с системой обнаружения вторжений IdecuUTM. Программный комплекс обнаружения вторжений «Ребус-СОВ». Программное средство обнаружения вторжений «Кречет»
Обеспечение целостности информационной системы и информации	Средство защиты информации Secret Net Studio. Программа фиксации и контроля исходного состояния программного комплекса «ФИКС» версия 2.0.2
Защита средств виртуализации	Программное обеспечение «Защищенная среда виртуализации zVirt Max». Программное обеспечение «Система серверной виртуализации «Р-Виртуализация». Программный комплекс «Средства виртуализации «Брест»
Защита информационной системы, ее средств, систем связи и передачи данных	Программно-аппаратный комплекс ViPNet Coordinator HW 4. Аппаратно-программный комплекс шифрования «Континент». Версия 3.9. Средство защиты информации Secret Net Studio

Согласно данному документу, реализация требований в части защиты речевой информации от утечки по акустическому каналу предполагает комплексный подход: применение организационно-режимных мер и внедрение инженерно-технических средств защиты.

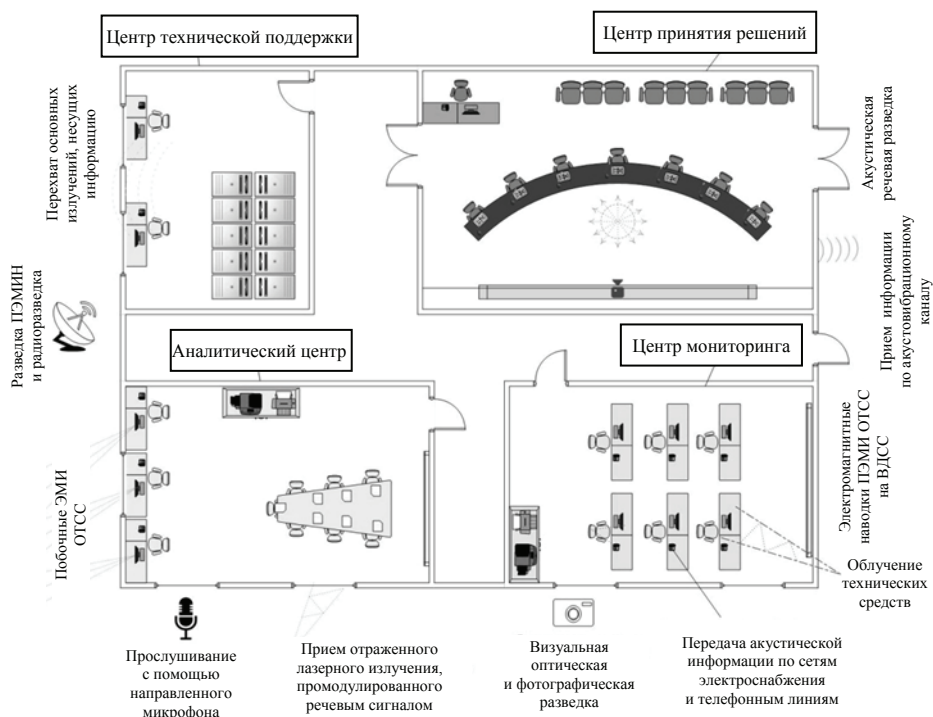


Рис. 2. Технические каналы утечки информации ситуационного центра

Организационно-режимные меры защиты включают в себя требования к помещениям и доступу к ним, а также работу с персоналом по противодействию утечки информации. Основой этих мер выступает строгий пропускной режим и контроль доступа, который распространяется как на сотрудников ситуационного центра, так и на посетителей. Это позволяет предотвратить не только несанкционированный доступ в защищаемое помещение, но и минимизировать риск установки акустических закладок [10, 11]. Помещения необходимо размещать в пределах контролируемой зоны, но при этом следует учитывать следующие рекомендации:

- удаленность от границы контролируемой зоны;
- отсутствия смежных стен с организациями-соседями;
- размещение не на первом этаже.

При проведении конфиденциальных мероприятий запрещается применение любых средств связи, а также аудио- и видеозаписывающих устройств. Если же в помещении находятся стационарные телефонные и факсимильные аппараты, то они в обязательном порядке отключаются от сети на весь период поведения мероприятия.

Не менее значимым элементом организационно-режимных мер защиты является работа с персоналом, которая включает в себя проведение регулярных инструктажей и обучающих мероприятий по работе в защищаемых помещениях.

Инженерно-технические средства представляют собой комплекс решений, состоящий из внедрения сертифицированных активных средств защиты от утечки по акустическому каналу и применения пассивных средств, включающих строительные решения для уменьшения распространения звуковых волн. Установка звукопоглощающих панелей в ограждающие конструкции помещений ситуационного центра является одним из способов эффективной звукоизоляции. Кроме это-

го, возможно оборудование тамбура на входах в защищаемое помещение ситуационного центра, создающее дополнительные барьеры для распространяемых конфиденциальных сведений, минимизирующих перехват по акустическому каналу утечки информации при открывании двери. Для защиты наиболее уязвимых элементов – оконных проемов (при наличии) – применяются различные способы, начиная от количества стекол и заканчивая внедрением нескольких стекол разной толщины и дистанций между ними в оконной раме [12]. Данные пассивные методы обеспечивают надежную защиту при перехвате информации по акустическому каналу за счет многоуровневого физического барьера на пути распространения звуковых волн.

Активные средства защиты осуществляют маскировку информативного речевого сигнала и представляют собой систему акустической и виброакустической защиты конфиденциальной информации. Данная система состоит из следующих элементов: генератора или нескольких генераторов, виброизлучателей и акустоизлучателей [13, 14]. Генератор шума, как основа системы, формирует маскирующие помехи, используя для этого разные виды шумов, которые затрудняют выделение полезной речевой информации: «белый», «окрашенный» или «речеподобные» помехи. Виброакустические излучатели устанавливаются на ограждающие конструкции и создают механические вибрации, а акустоизлучатели формируют направленные акустические помехи в сторону, откуда может вестись перехват информации.

Поскольку в защищаемом помещении должны быть использованы только сертифицированные средства защиты информации, то в качестве системы акустической и виброакустической защиты конфиденциальной информации могут быть использованы следующие системы [15]:

- активной акустической и вибрационной защиты акустической речевой информации «Соната-АВ» модель 4Б;
- виброакустической защиты «Муссон»;
- постановки виброакустических и акустических помех «ЛГШ-404»;
- акустических и виброакустических помех «БУРАН»;
- акустической и виброакустической защиты «КЕДР-А»;
- виброакустической защиты «Гамма СВА3-01»;
- виброакустической защиты «Камертон-5».

Кроме систем акустической и виброакустической защиты, ситуационный центр оснащается системой защиты от побочных электромагнитных излучений и наводок (**ПЭМИН**) [16]. Система включает пассивные и активные средства. К пассивным относятся экранирующие конструкции самого помещения (стены, пол, потолок, двери, окна), экранированные кабельные каналы и сетевые фильтры. Активные средства предназначены для подавления или искажения полезного сигнала, содержащего конфиденциальную информацию, и включают в себя следующие типы систем: зашумления, виртуального зашумления и активного компенсационного подавления, работающие по принципу «антишума».

Выбор конкретных средств, их мощности и конфигурации осуществляется на основе предварительного инструментального обследования ситуационного центра на соответствие требованиям стандартов по защите от ПЭМИН (например, ГОСТ Р 51624–2000 или ведомственных требований).

Заключение

Таким образом, ситуационный центр представляет собой цель для злоумышленников, поэтому требуется комплексный подход к защите конфиденциальной информации. Безопасность формируется из построения программно-аппаратной

защиты на базе сертифицированных средств для информации, циркулирующей в системах ситуационного центра, и внедрения сертифицированных активных систем виброакустического шумления для защиты конфиденциальных переговоров. Грамотная интеграция всех систем безопасности, их настройка, а также соблюдение требований нормативных документов позволяют создать защищенную среду для обработки информации ограниченного доступа ситуационного центра.

Традиционные методы защиты от конкретных угроз и атак, как правило, включают набор программных и аппаратных компонентов, функционирующих независимо друг от друга. Они обладают ограниченными адаптивными возможностями, используют пассивные механизмы обнаружения атак, что приводит к высокому уровню ложных срабатываний, ухудшению производительности из-за большого объема ресурсов, необходимых для защиты. Подход с использованием интеллектуальных многоагентных систем представляет собой перспективный метод построения комплексных систем защиты информации в компьютерных сетях, который позволяет преодолеть перечисленные недостатки. Эта технология способствует значительному повышению эффективности защиты информации, обеспечивая адекватность, устойчивость к деструктивным действиям, универсальность и гибкость.

Список литературы

1. Кибератаки на российские компании в 2024 году // SOLAR. – URL : <https://rt-solar.ru/analytics/reports/5320> (дата обращения: 08.10.2025).

2. Ситуационные центры и центры управления для органов государственной власти // POLYMEDIA. – URL : <https://solutions.polymedia.ru/gov> (дата обращения: 08.10.2025).

3. ГОСТ Р 56875–2016. Информационные технологии. Системы безопасности комплексные и интегрированные. Типовые требования к архитектуре и технологиям интеллектуальных систем мониторинга для обеспечения безопасности предприятия и территорий: национальный стандарт Российской Федерации : введен 2017-010-01 / Федеральное агентство по техническому регулированию и метрологии. – Москва : Стандартинформ, 2019. – 46 с.

4. Фурсова, А. В. Анализ актуальных угроз ситуационного центра регионального уровня/ А. В. Фурсова, А. В. Яковлев // Актуальные проблемы кибербезопасности. Противодействие экстремизму и терроризму в информационной молодежной среде : сборник докладов I межрегиональной научно-практической конференции, Брянск, 29 апреля 2025 года. – Брянск, 2025. – С. 220–224.

5. Симанков, В. С. Программное и аппаратное обеспечение подсистем интеллектуального ситуационного центра / В. С. Симанков, В. А. Шарай // Вестник Адыгейского государственного университета. Серия 4: Естественно-математические и технические науки. – 2021. – № 3(286). – С. 63–72.

6. Комплекс решений для ситуационного центра предприятия // JETINFO. – URL : <https://www.jetinfo.ru/complex-of-decisions-for-situational-center-of-enterprise> (дата обращения: 08.10.2025).

7. Поиск программного обеспечения // Реестр программного обеспечения. – URL : <https://reestr.digital.gov.ru> (дата обращения: 08.10.2025).

8. Приказ ФСТЭК от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» // Официальный сайт Федеральной службы по техническому и экспортному контролю. – URL : <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (дата обращения: 08.10.2025).

9. Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) // Wikisec. – URL : <https://wikisec.ru/images/2/2c/Str-k-.pdf> (дата обращения: 08.10.2025).
10. Акустические закладки // Акустические закладки. – URL : http://rfanat.qrz.ru/s17/spy_aku-zakl.html (дата обращения: 08.10.2025).
11. Системный подход к построению программно-аппаратного комплекса для подготовки специалистов по информационной безопасности / В. В. Алексеев, В. А. Гриднев, А. В. Яковлев, О. С. Машкова, У. А. Савилова, Д. А. Шибков, Д. А. Яковлева // Вестник Тамбовского государственного технического университета. – 2021. – Т. 27. № 1. – С. 20–30. doi: 10.17277/vestnik.2021.01.pp.020-030
12. Фурсова, А. В. Влияние параметров светопрозрачных поверхностей на акустооптический канал утечки информации / А. В. Фурсова, А. В. Яковлев, М. В. Волчихина // Информатика: проблемы, методы, технологии : материалы XXIV Международной научно-практической конференции им. Э. К. Алгазинова, Воронеж, 14–15 февраля 2024 года. – Воронеж: Воронежский государственный университет, 2024. – С. 814–820.
13. Системы виброакустической маскировки // Техника для спецслужб. – URL : <http://www.bnti.ru/showart.asp?aid=595&lv1=04.03.01.01>. (дата обращения: 08.10.2025).
14. Волчихина, М. В. Метод адаптации параметров средств защиты информации на основе дискретного изменения амплитуды и тембра субъектов переговоров // Вестник Тамбовского государственного технического университета. – 2022. – Т. 28, № 2. – С. 226–234.
15. Государственный реестр сертифицированных средств защиты информации // Реестры ФСТЭК России. – URL : <https://reestr.fstec.ru/reg3> (дата обращения: 08.10.2025).
16. Методы защиты информации от утечки через ПЭМИН // ИНТУИТ. – URL : <https://intuit.ru/studies/courses/4647/591/lecture/12704?ysclid=mgzac48736572768115> (дата обращения: 08.10.2025).

Integrated Security System for the Situation Center

© A. V. Fursova¹, A. V. Yakovlev¹✉

¹ *Department of Information Systems and Information Security,
yava73@bk.ru; TSTU, Tambov, Russian Federation*

Keywords: information security; certified security tools; situation center; technical channels.

Abstract: This article describes an approach to protecting situation centers, which are one of the targets of malicious attacks aimed at obtaining restricted information. Integrated security includes the construction of a secure hardware and software system in accordance with the requirements of the Federal Service for Technical and Export Control of Russia, as well as measures to protect confidential communications from leakage via technical channels. The structure and composition of hardware and software for information security in a typical situation center and the requirements of regulatory legal acts in this subject area are discussed. The application levels of certified security tools have been defined, and the technology for implementing the approach has been substantiated. This approach involves integrating

security tools while adhering to regulatory requirements and enables the creation of an environment for the situation center that is resilient to modern information security threats.

References

1. Available at: <https://rt-solar.ru/analytics/reports/5320> (accessed 8 October 2025).
2. Available at: <https://solutions.polymedia.ru/gov> (accessed 8 October 2025).
3. GOST R 56875-2016. *Informatsionnye tekhnologii. Sistemy bezopasnosti kompleksnye i integrirovannye. Tipovye trebovaniya k arkhitekture i tekhnologiyam intellektualnykh sistem monitoringa dlya obespecheniya bezopasnosti predpriyatiya i territorij: natsionalnyj standart Rossijskoj Federatsii: data vvedeniya 2017-010-01 / Federalnoe agentstvo po tekhnicheskomu regulirovaniyu i metrologii.*– Moscow: Standartinform, 2019. – 46 s.
4. Fursova A.V., Yakovlev A.V. *Analiz actual nykh ugroz situatsionnogo tsentra regionalnogo urovnya: Sbornik dokladov I mezhregionalnoj nauchno-prakticheskoy konferentsii* [Analysis of current threats to the regional-level situation center: Collection of Papers from the First Interregional Scientific and Practical Conference], Bryansk, 29 April, Bryansk, 2025, pp. 220-224.
5. Simankov V.S., Sharaj V.A. [Software and hardware for the subsystems of the intelligent situation center], *Vestnik Adygejskogo gosudarstvennogo universiteta. Seriya 4: Estestvenno-matematicheskie i tekhnicheskije nauki*, [Bulletin of Adyghe State University. Series 4: Natural, mathematical and technical sciences], 2021, no. 3, pp. 63-72. doi: 10.53598/2410-3225-2021-3-286-63-72
6. Available at: <https://www.jetinfo.ru/complex-of-decisions-for-situational-center-of-enterprise> (accessed 8 October 2025).
7. Available at: <https://reestr.digital.gov.ru> (accessed 8 October 2025).
8. Available at: <https://fstec.ru/dokumenty/vse-dokumenty/prikazy/prikaz-fstek-rossii-ot-11-fevralya-2013-g-n-17> (accessed 8 October 2025).
9. Available at: <https://wikisec.ru/images/2/2c/Str-k-.pdf> (accessed 8 October 2025)
10. Available at: http://rfanat.qrz.ru/s17/spy_aku-zakl.html (accessed 8 October 2025).
11. Alekseev V.V., Gridnev V.A., Yakovlev A.V., Mashkova O.S., Savilova U.A., Shibkov D.A., Yakovleva D.A. [A System Approach to the Construction of the Software and Hardware Complex for Training Information Security Specialists], *Transactions of the Tambov State Technical University*, 2021, vol. 27, no. 1, pp. 20-30. doi: 10.17277/vestnik.2021.01.pp.020-030 (In Russ., abstract in Eng.)
12. Fursova A.V., Yakovlev A.V., Volchikhina M.V. *Vliyanie parametrov svetoprozrachnykh poverkhnostej na akustoopticheskij kanal utechki informatsii: Materialy XXIV Mezhdunarodnoj nauchno-prakticheskoy konferentsii im. E.K. Algazinova* [The effect of translucent surface parameters on the acousto-optical information leakage channel: Materials of the XXIV International Scientific and Practical Conference named after E.K. Algazinov], Voronezh, 14-16 February, 2024, Voronezh, 2024, pp. 814-820. (In Russ., abstract in Eng.)
13. Available at: <http://www.bnti.ru/showart.asp?aid=595&lvl=04.03.01.01> (accessed 8 October 2025).
14. Volchikhina M. V. [A Method for Adapting the Parameters of Information Security Tools Using a Discrete Change in the Amplitude and Timbre of the Subjects of Negotiations], *Transactions of the Tambov State Technical University*, 2022, vol. 28, no. 2, pp. 226-234. doi: 10.17277/vestnik.2022.02.pp.226-234 (In Russ., abstract in Eng.)
15. Available at: <https://reestr.fstec.ru/reg3> (accessed 8 October 2025).
16. Available at: <https://intuit.ru/studies/courses/4647/591/lecture/12704?ysclid=mgzac48736572768115> (accessed 8 October 2025).

Systeme des umfassenden Schutzes des Lagezentrums

Zusammenfassung: Dieser Artikel beschreibt einen Ansatz zum Schutz von Lagezentren, die Ziel von Angreifern sind, die auf den Zugriff auf vertrauliche Informationen abzielen. Ein umfassender Schutz beinhaltet den Aufbau einer sicheren Hardware- und Softwareinfrastruktur gemäß den Anforderungen des russischen Föderalen Dienstes für technische und Exportkontrolle (FSTEC) sowie Maßnahmen zum Schutz vertraulicher Kommunikation vor Datenleck über technische Kanäle. Der Artikel untersucht die Struktur und Zusammensetzung der in einem typischen Lagezentrum zum Schutz von Informationen eingesetzten Hardware und Software sowie die Anforderungen der einschlägigen Rechtsvorschriften. Die Anwendungsstufen zertifizierter Sicherheitstools sind bestimmt und die Implementierungstechnologie dieses Ansatzes begründet. Dieser Ansatz integriert Sicherheitstools unter Einhaltung der regulatorischen Anforderungen und ermöglicht die Schaffung einer Umgebung für das Lagezentrum, die gegenüber modernen Bedrohungen der Informationssicherheit widerstandsfähig ist.

Système de la protection intégrée du centre de situation

Résumé: Est décrite l'approche pour la protection des centres de situation comme l'une des cibles des attaques visant à obtenir des informations d'accès restreint. La protection complète comprend la construction d'un circuit logiciel et matériel protégé conformément aux exigences du Service fédéral de contrôle technique et des exportations de la Russie, ainsi que des mesures de protection des négociations confidentielles contre les fuites par les canaux techniques. Sont examinées la structure et la composition des outils matériels et logiciels de la protection de l'information du centre de situation modèle et les exigences des actes juridiques et réglementaires dans ce domaine. Sont définis les niveaux de l'application des protections certifiées; est justifiée la technologie de mise en œuvre de l'approche. Cette approche intègre les protections dans le respect de la réglementation et permet de créer un environnement résistant aux menaces actuelles en matière de sécurité de l'information pour le centre de situation.

Авторы: *Фурсова Арина Викторовна* – аспирант кафедры «Информационные системы и защита информации»; *Яковлев Алексей Вячеславович* – кандидат технических наук, доцент кафедры «Информационные системы и защита информации», ФГБОУ ВО «ТГТУ», Тамбов, Российская Федерация.