УДК 681.5

АДАПТАЦИЯ СИСТЕМ УПРАВЛЕНИЯ ИНФОРМАЦИОННЫМИ РИСКАМИ К НОВЫМ КИБЕРУГРОЗАМ В ЭПОХУ ГЛОБАЛЬНОЙ НЕСТАБИЛЬНОСТИ

Плохута К.Д., аспирант, Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)

Шашина Н.С., д-р экон. наук, проф., зав. кафедрой «Экономика технологического предпринимательства», Санкт-Петербургский государственный электротехнический университет «ЛЭТИ» имени В.И. Ульянова (Ленина)

В статье рассматриваются вопросы обеспечения безопасности информационных систем в условиях усиления киберугроз, связанных с эксплуатацией устаревшего программного обеспечения, ростом количества целевых атак и технологическими ограничениями.

В работе применялись методы анализа нормативных документов в области информационной безопасности, выполнен обзор передовых технических решений по своевременному выявлению и предотвращению кибератак, а также использован метод оценки влияния человеческого фактора, включающий анализ рисков, связанных с возможными ошибками сотрудников.

Результаты исследования показывают, что эффективная защита информационных ресурсов достигается за счет своевременной модернизации инфраструктуры, внедрения интеллектуальных систем мониторинга и своевременного реагирования на угрозы, а также формирования организационной культуры, направленной на повышение осведомленности сотрудников по вопросам информационной безопасности.

На основании полученных данных сделан вывод о необходимости комплексного подхода, включающего развитие национальных технологий защиты, совершенствование нормативной базы и систематическое обучение персонала как обязательные условия для обеспечения стабильного функционирования организаций в период глобальной нестабильности.

Ключевые слова: кибербезопасность, устаревшие системы, Advanced PersistentThreats, MITRE ATT&CK, XDR, искусственный интеллект, блокчейн, постквантовая криптография, социальная инженерия, культура безопасности.

Цитирование: Плохута К.Д., Шашина Н.С. Адаптация систем управления информационными рисками к новым киберугрозам в эпоху глобальной нестабильности // Информационно-экономические аспекты стандартизации и технического регулирования. 2025. № 3(84). С. 52–58.

ВВЕДЕНИЕ И ОБЗОР ЛИТЕРАТУРЫ

Санкции, дефицит актуальных обновлений программного обеспечения, устаревшая инфраструктура и рост числа целенаправленных атак усложняют задачу выстраивания надежной системы защиты. Теоретические и прикладные исследования в области информационной безопасности подтверждают, что классические подходы, ориентированные лишь на базовый набор инструментов, таких как антивирусы, межсетевые экраны и стандартные регламенты информационной безопасности, уже не способны эффективно противостоять высокотехнологичным угрозам, эксплуатирующим уязвимости в операционных системах, зачастую давно снятых с поддержки [1, 2, 3].

Возникает необходимость в пересмотре и адаптации существующих подходов к управлению информационными рисками с учетом актуальных угроз и специфики текущей ситуации. Особое внимание следует уделять распространению методов социальной инженерии, увеличению количества и сложности целенаправленных атак класса Advanced Persistent Threats (APT), а также технологическим ограничениям, вызванным санкционными мерами, ограничивающими доступ организаций к зарубежному программному и аппаратному обеспечению.

Отсутствие своевременных обновлений программного обеспечения и эксплуатация устаревшей инфраструктуры существенно повышают уровень уязвимостей, кото-

рые могут быть успешно использованы злоумышленниками. Ряд исследований указывает на то, что накопленный «технологический долг» и недостаточная осведомленность сотрудников о современных киберугрозах значительно увеличивают вероятность успешных атак со стороны злоумышленников [4].

В отечественных исследованиях подчеркивается, что традиционный набор мер, таких как антивирусы, сегментация сети, регламенты, перестает быть достаточным. Злоумышленники активно применяют уязвимости нулевого дня, методики социальной инженерии и методы обхода сигнатурных средств защиты. Обзор литературы по этой проблеме свидетельствует о том, что многие авторы сосредоточены на базовых аспектах и не учитывают новых киберугроз, связанных с санкционными ограничениями и ограниченными возможностями обновления оборудования. С другой стороны, делается акцент на информационно-экономических аспектах, подчеркивая, что организации нередко стремятся к экономии, что приводит к замедлению процессов модернизации ИТ-инфраструктуры [3, 5].

Подходы к комплексному обеспечению информационной безопасности широко отражены в пособии по комплексному обеспечению информационной безопасности автоматизированных систем, где рассматривается необходимость многослойной защиты с учетом технических, организационных и правовых мер [6]. Однако, несмотря на существующие рекомендации и подходы, на практике остается нерешенной задача эффективного объединения профилактических и проактивных мер защиты от современных угроз.

С одной стороны, необходимы своевременные обновления операционных систем и переход на отечественные программные продукты, с другой – внедрение решений, которые способны проактивно выявлять и предотвращать атаки на ранних этапах. Особенно актуальной становится интеграция решений, способных заблаговременно выявлять признаки угроз и предотвращать их развитие в инциденты. Важную роль здесь играют методы анализа тактик, техник и процедур злоумышленников, основанные на классификации фреймворка MITRE ATT&CK и использующие отечественные разработки в области информационной безопасности. Такие подходы позволяют повысить эффективность систем защиты и своевременно противодействовать современным угрозам [5].

Санкционные ограничения и последствия технологического разрыва привели к усилению зависимости от отечественных решений и необходимости развивать собственные средства защиты, сертифицированные ФСТЭК [7]. В то же время зарубежные авторы указывают на растущую сложность кибератак и необходимость динамического пересмотра модели риска [8]. Их идея пересекается с отечественными разработками, где на первый план выходит учет человеческого фактора, так как одной из причин успешности атак становится недостаточная информированность персонала или несоблюдение регламентов. Анализ материалов Infars и RTM Group подтверждает, что доля неправильных действий сотрудников может достигать 30–40% в организациях, не внедривших программы обучения [9, 10].

Проблема, которую решает настоящая статья, заключается в том, что устаревшие системы в условиях глобальной нестабильности и санкционных барьеров создают новые вызовы для управления информационными рисками. Традиционные сугубо технические меры устаревают, необходимо сочетать инновационные методы, такие как фреймворк MITRE ATT&CK, XDR, машинное обучение, распределенные реестры, постквантовая криптография, с организационными подходами в виде тренингов и стандартов корпоративной культуры безопасности.

При этом важно учитывать экономические ограничения и приоритизировать меры, дающие максимальный эффект при минимуме затрат. Таким образом, цель данной работы – показать, каким образом возможно адаптировать системы управления информационными рисками к новым киберугрозам, обусловленным устареванием инфраструктуры, санкционными ограничениями и человеческим фактором, и тем самым повысить уровень защищенности организаций.

МЕТОДЫ ИССЛЕДОВАНИЯ

Методы исследования включают теоретический анализ, основанный на критическом разборе действующих стандартов, научных статей и конференционных материалов в области риск-менеджмента и статистического моделирования, а также сопоставление российских нормативных актов с международными стандартами информационной безопасности. Проводился сбор и анализ статистических данных о кибератаках, применялся факторный анализ, эксплораторный и конфирматорный, для выявления латентных факторов, определяющих взаимосвязи между переменными риска. Использовался сравнительно-аналитический подход при изучении современных средств обнаружения угроз, включая XDR-платформы, фреймворк MITRE ATT&CK и системы машинного обучения. Особое внимание уделялось человеческому фактору на основе социологических методов.

РЕЗУЛЬТАТЫ И ОБСУЖДЕНИЯ

В контексте данного исследования информационный риск можно определить как совокупность вероятных неблагоприятных последствий, возникающих при реализации угроз, эксплуатирующих уязвимости в информационных технологиях и системах.

В соответствии со стандартами ISO/IEC 27005, ГОСТ Р ИСО/МЭК 27005–2010 информационный риск трактуется как потенциальная опасность, возникающая при реализации конкретной угрозы, которая использует уязвимость в информационной системе [11,12]. Ущерб может быть выражен в финансовых потерях, репутационных издержках,

срыве технологических процессов или утечке конфиденциальных данных [7].

Также риск рассматривают как произведение или совокупность вероятности угрозы и величины возможного ущерба. Однако в реальности, особенно когда речь идет об устаревших ОС и приложениях, вероятность атаки может стремительно возрастать, а ущерб от инцидента – выходить за рамки простых материальных потерь, включая правовые санкции, блокировку деятельности, а в некоторых случаях – вывод из строя критически важных систем [6]. Эту точку зрения разделяют и зарубежные авторы [8], подчеркивающие, что в эпоху глобальной взаимозависимости и санкционного давления риск становится многоплановым, затрагивая и аспекты технологического суверенитета.

Подобная трактовка согласуется с мнением некоторых отечественных авторов, что информационные риски – «опасность возникновения убытков или ущерба в результате применения компанией информационных технологий». Иными словами, ИТ-риски связаны с созданием, передачей, хранением и использованием информации с помощью электронных носителей и иных средств связи [13].

При этом в современных условиях, характеризующихся глобальной взаимозависимостью и стремительным ростом киберугроз, ущерб от инцидентов нередко выходит за рамки простой материальной оценки, затрагивая правовые аспекты, блокируя деятельность организаций или выводя из строя критически важные системы. Именно поэтому информационный риск все чаще рассматривается как многоплановое явление, способное оказывать комплексное воздействие на финансовую стабильность, деловую репутацию и технологический суверенитет компаний.

Для России проблема усугубляется тем, что многие компании продолжают использовать Windows 7 и даже более старые версии Windows XP, чей цикл поддержки давно завершен, и при этом не имеют ресурсов или возможности перейти на обновленные продукты [14,15]. Уязвимости таких систем детально изучены злоумышленниками, которые активно применяют уже задокументированные эксплойты без необходимости вкладываться в разработку новых инструментов взлома [16, 17]. Вдобавок к этому санкционные барьеры могут ограничивать доступ к зарубежным средствам ИБ, особенно если вендоры уходят с рынка или отказываются поддерживать более старые ОС.

Статистические данные Positive Technologies [17], а также отчеты StatCounter [15] указывают, что каждая четвертая атака на инфраструктуру в России связана с эксплуатацией устаревших версий программного обеспечения. Не случайно Федеральная служба по техническому и экспортному контролю в своих методических рекомендациях настоятельно призывает к постепенной модернизации программно-аппаратной базы организаций [7]. Однако на практике такой процесс часто затруднен экономическими и организационными причинами. Для минимизации связанных с этим рисков важно развивать адекватные методы защиты.

Классические меры кибербезопасности, описанные в ряде учебных пособий, включающие аутентификацию, разграничение доступа, антивирусные программы и межсетевые экраны, формировались во времена, когда скорость эволюции кибератак была значительно ниже, а целевые APT-угрозы не были столь распространены. Сегодня актуальность приобретают инновационные методы.

Во-первых, фреймворк MITRE ATT&CK [5, 16] предоставляет открытую базу знаний о тактиках, техниках и процедурах злоумышленников, что дает возможность систематизировать потенциальные сценарии взлома по этапам и строить многоуровневую защиту.

Во-вторых, подход Extended Detection and Response объединяет данные от рабочих станций, серверов, сетевых экранов и облачных сервисов в единый центр корреляции, акцентируя внимание на автоматизации анализа и ускоренном реагировании.

В отчетах FinCERT [9] отмечается, что российские финансовые институты внедряют XDR-платформы для снижения времени обнаружения атак, эксплуатирующих уязвимости устаревшего ПО. Алгоритмы машинного обучения и искусственного интеллекта, например в Kaspersky Anti Targeted Attack Platform [20] или Solar Dozor [14], позволяют в режиме реального времени обрабатывать большие объемы логов и сетевых пакетов, выявляя аномалии даже при отсутствии актуальных сигнатур; это особенно важно, если система не получает обновлений от производителя. Блокчейн и распределенные реестры [17] находят применение в финансовых сервисах для надежного хранения транзакций и упрощения аудита, хотя они не решают всех проблем безопасности операционных систем.

Наконец, постквантовая криптография, учитывающая будущие возможности квантовых компьютеров и разрабатываемая отечественными специалистами, становится критически значимой для стратегических систем с долгим сроком хранения данных. Эффективность перечисленных мер оценивается с помощью комплексной системы метрик [2,6,18]: среднее время обнаружения, влияющее на способность быстро выявлять скрытые APT; среднее время реагирования MTTR, зависящее как от технических средств, включая автоматизацию в XDR, так и от организационной готовности к инцидентам ложноположительных и ложноотрицательных срабатываний, напрямую влияющих на загруженность специалистов и риск пропустить реальную атаку, а также объем предотвращенного ущерба, который дает экономическое обоснование инвестиций в безопасность. При этом особую угрозу представляет че-

ловеческий фактор: по данным Infars [9] и RTM Group [10], от 30 до 40% сотрудников, не обученных в организациях, готовы переходить по фишинговым ссылкам, поскольку не осознают возможных последствий.

Причины такого поведения анализируются в исследованиях по психологии безопасности [19], где подчеркивается роль когнитивных и социальных факторов, включая доверчивость, спешку и неверное понимание внутренних регламентов. Систематическое обучение, практические фишинг-симуляции и меры повышения осведомленности позволяют уменьшить число ошибок на 40–50% [10], что, в свою очередь, улучшает среднее время обнаружения атак и укрепляет общую киберустойчивость организации. Дополнительно в рамках современных концепций, таких как «нулевое доверие», рекомендуется предполагать скомпрометированность любого элемента инфраструктуры по умолчанию и использовать строгую верификацию всех взаимодействий, что еще более повышает значимость комплексного подхода к защите и согласованных действий персонала.

В научно-практических работах по управлению рисками неоднократно подчеркивается важность человеческого фактора при оценке эффективности систем защиты информации: если сотрудник вводит свои учетные данные на фишинговом сайте, даже самые современные антивирусные решения не способны предотвратить кражу [14]. Следовательно, доля неправильных действий персонала становится одной из ключевых метрик в анализе того, насколько быстро средства защиты могут отреагировать на угрозу и насколько серьезными окажутся последствия пробоя.

При этом ряд исследований указывает, что даже при ограниченном бюджете организация способна повышать уровень киберзащиты путем приоритизации рисков и использования методов на основе нечеткой логики и эволюционных алгоритмов. Нечеткая логика позволяет учитывать неопределенность исходных данных и применять качественные экспертные оценки при расчете рисков (например, высокий риск потери данных, средняя эффективность межсетевого экрана и эффективности защитных мер).

Эволюционные алгоритмы обеспечивают автоматизированный перебор различных комбинаций инструментов и помогают выбрать оптимальное соотношение «риск –затраты – эффективность», что особенно ценно в условиях ограниченных финансовых и временны́х ресурсов. Данное исследование позиционируется в общем научном поле информационной безопасности как попытка объединить несколько аспектов:

- рассмотрение устаревшей инфраструктуры как критического фактора риска;
- учет санкционных ограничений, затрудняющих выбор зарубежных решений;
- интеграцию современных технологий (MITRE ATT&CK, XDR, ML, блокчейн, постквантовая криптография);
- формирование корпоративной культуры, повышающей осведомленность сотрудников.

Такой многоуровневый подход показывает, почему классические требования, например соответствие ГОСТ, без учета поведенческих особенностей персонала больше не дают должного результата.

В работах по комплексному обеспечению ИБ [6], а также в отраслевых журналах и зарубежной литературе подчеркивается, что инновационные технические средства должны дополняться организационными мерами. Существенную роль играет опыт ведущих отечественных вендоров ([20], «Ростелеком-Солар» [14]), разработчиков отечественных ОС, таких как Astra Linux, и государственных структур (ФСТЭК [7], Роскомнадзор [21], ФинЦЕРТ [9]), которые формируют актуальные стандарты и требования с учетом современных киберугроз.

В исследовании трактуется информационный риск как совокупность вероятности атаки, множества уязвимостей и масштаба потенциального ущерба.

Рассмотренные методы защиты способны компенсировать слабые места старого ПО и закрытых экосистем, обеспечивая, к примеру, поведенческий анализ, не зависящий от патчей, и обнаружение аномалий в режиме реального времени. Для оценки эффективности противодействия кибератакам широко применяют показатели Mean time to detect и Mean time to respond. Чем быстрее организация выявляет факт взлома и реагирует на него, тем ниже совокупные потери. Однако даже наиболее продвинутые системы мониторинга XDR и SIEM с модулями машинного обучения теряют эффективность, если сотрудники не соблюдают базовые правила безопасности.

Эмпирические данные свидетельствуют, что без регулярного обучения 30–40 % персонала склонны переходить по фишинговым ссылкам, открывать вредоносные вложения или разглашать конфиденциальные сведения. Подобные действия часто «обходят» технические барьеры, поскольку исходят от легитимных пользователей сети.

Напротив, систематически обучающие программы и регулярные симуляции фишинговых атак способны почти вдвое сократить долю неправильных действий [11, 15], что повышает общую бдительность сотрудников и ускоряет выявление инцидентов, а также улучшает координацию при реагировании (сокращается MTTR).

В условиях современных угроз и глобальной нестабильности целесообразно модернизировать программно-аппаратное окружение, постепенно переводя устаревшие ОС

на отечественные аналоги, сертифицированные ФСТЭК [7]. Параллельно необходимо внедрять динамические методы обнаружения, что даст возможность вовремя противодействовать даже неизвестным сценариям атак, направленным на «открытые» узлы инфраструктуры. Наряду с этим следует активно развивать человеческий капитал: формировать культуру безопасности, проводить регулярные тренинги, учитывать KPI (долю ошибок в фишинг-тестах, степень вовлеченности персонала, качество соблюдения регламентов).

ЗАКЛЮЧЕНИЕ

На основании проведенного анализа данных и обзора существующих исследований можно сделать вывод о том, что только многоуровневый подход, сочетающий технологические решения, нормативную поддержку и непрерывное обучение сотрудников, позволит российским организациям преодолеть уязвимости, связанные с устаревшим ПО, и существенно повысить киберустойчивость на долгосрочную перспективу.

Список использованных источников и литературы

1. Милославская Н.Г. Управление рисками информационной безопасности. Учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. – Москва: Горячая Линия – Телеком, 2013. – 130 с. – ISBN 978-5-9912-0272-5. – URL: https://ibooks.ru/bookshelf/334011/reading (дата обращения: 13.03.2025). – Текст: электронный.
2. Аникин И.В. Метод управления рисками информационной безопасности в корпоративных информационных сетях // Инфокоммуникационные технологии. 2015. Т. 13. № 2. С. 215–221.
3. Прохорова О.В. Информационная безопасность и защита информации : учебник для вузов / О. В. Прохорова. – 6-е изд., стер. – Санкт-Петербург: Лань, 2025. – 124 с. – ISBN 978-5-507-52899-8. – Текст: электронный // Лань: электронно-библиотечная система. – URL: https://e.lanbook.com/book/462293 (дата обращения: 13.03.2025). – Режим доступа: для авториз. пользователей.
4. Бурый А.С., Усцелемов В.Н. Информационная безопасность автоматизированных систем // Информационно-экономические аспекты стандартизации и технического регулирования. 2023. № 2 (72). С. 31–37.
5. Смирнов Д.В., Евсютин О.О. Методика сбора данных об активности вредоносного программного обеспечения под ОС Windows на базе MITRE ATT&CK // Информатика и автоматизация. 2024. Т. 23. № 3. С. 642–683.
6. Мещеряков Р.В., Шелупанов А.А. Комплексное обеспечение информационной безопасности автоматизированных систем. Томск: В-Спектр, 2007. 350 с.
7. ФСТЭК России. Сертификация средств защиты информации [Электронный ресурс]. URL: https://fstec.ru
8. Wangen G., Hallstensen C., Snekkenes E. Cybersecurity risk management: A systematic review of current approaches // Computers & Security. 2020. Vol. 93. Article 101694.
9. Infars. «Социальная инженерия: как предотвратить атаки на сотрудников» [Электронный ресурс]. URL: https://infars.ru/blog/hs/cta/cta/redirect/1789215/b8c3de1c-229f-4f86-8000-4928a6b7a3e1/
10. RTM Group. «Противодействие социальной инженерии: обучение сотрудников» [Электронный ресурс]. URL: https://rtmtech.ru/services/obuchenie-personala-sotsialnoj-inzhenerii/
11. ISO/IEC 27005:2022. Информационные технологии. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности: руководство. – Женева: ISO, 2022.
12. ГОСТ Р ИСО/МЭК 27005–2010. Информационная технология. Методы и средства обеспечения безопасности. Управление рисками информационной безопасности [Текст]: национальный стандарт Российской Федерации. – Введ. 2012-01-01. – М.: Стандартинформ, 2011. – 35 с.
13. Исаев И.В. ИТ-РИСКИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ // Современные наукоемкие технологии. 2014. № 7-1. С. 184–184; URL: https://top-technologies.ru/ru/article/view?id=34276
14. Ростелеком-Солар. Solar Dozor [Электронный ресурс]. URL: https://rt-solar.ru/products/solar_dozor/
15. StatCounter. Использование Windows 7 в России 2023 [Электронный ресурс]. URL: https://overclockers.ru/blog/Scorpion81/show/123332/poyavilas-statistika-sistem-windows-ot-statcounter-za-noyabr-2023
16. Positive Technologies. Анализ применения MITRE ATT&CK в российских компаниях [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/
17. Positive Technologies. Актуальные киберугрозы: итоги 2022 года [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022/ (дата обращения: 07.02.2025).
18. Марков А.С., Барабанов А.В., Цирлов В.Л. Методы оценки несоответствия средств защиты информации. – М.: Радио и связь, 2012. – 192 с.
19. Smith J., Brown A. Cybersecurity risks and human factors // Cybersecurity Journal. 2018. Vol. 14. P. 45–57.
20. Kaspersky Anti Targeted Attack Platform [Электронный ресурс] // Лаборатория Касперского: [сайт]. – URL: https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform
21. Роскомнадзор. Проверки операторов персональных данных [Электронный ресурс]. URL: https://pd.rkn.gov.ru/operators-registry/operators-list/

ADAPTING INFORMATION RISK MANAGEMENT SYSTEMS TO NEW CYBER THREATS IN AN ERA OF GLOBAL INSTABILITY

Plokhuta K.D., postgraduate student, Saint Petersburg Electrotechnical University «LETI» ETU

Shashina N.S., Doctor of Economics, Professor Head of the Department of Economics of Technological Entrepreneurship of the Saint Petersburg Electrotechnical University «LETI» ETU

The article discusses the issues of ensuring the security of information systems in the context of increasing cyber threats associated with the use of outdated software, an increase in the number of targeted attacks and technological limitations.

The work used methods for analyzing regulatory documents in the field of information security, reviewed advanced technical solutions for the timely detection and prevention of cyber-attacks, and used a method for assessing the impact of the human factor, including risk analysis related to possible errors by employees.

The results of the study show that effective protection of information resources is achieved through timely modernization of infrastructure, the introduction of intelligent monitoring systems and timely response to threats, as well as the formation of an organizational culture aimed at raising awareness of information security issues among employees.

Based on the data obtained, it is concluded that an integrated approach is necessary, including the development of national protection technologies, improvement of the regulatory framework and systematic training of personnel as prerequisites for ensuring the stable functioning of organizations in a period of global instability.

Keywords: cybersecurity, legacy systems, Advanced Persistent Threats, MITRE ATT&CK, XDR, artificial intelligence, blockchain, post-quantum cryptography, social engineering, security culture.

For citation: Plokhuta K.D., Shashina N.S. Adapting information risk management systems to new cyber threats in an era of global instability. Information and economic aspects of standardization and technical regulation. 2025. No. 3 (84), p. 52–58.

References

1. Miloslavskaya N.G. Information security risk management. Textbook for universities / N.G. Miloslavskaya, M.Y. Senatorov, A.I. Tolstoy. – Moscow: Hotline–Telecom, 2013. – 130 p. – ISBN 978-5-9912-0272-5. – URL: https://ibooks.ru/bookshelf/334011/reading (date of access: 02/07/2025). – Text: electronic.
2. Anikin I.V. Method of information security risk management in corporate information networks // Infocommunication technologies. – 2015. – Vol. 13. – No. 2. – P. 215–221.
3. Prokhorova O.V. Information security and information protection: a textbook for universities / O. V. Prokhorova. – 6th ed., ster. – Saint Petersburg: Lan, 2025. – 124 p. – ISBN 978-5-507-52899-8. – Text: electronic // Lan: electronic library system. – URL: https://e.lanbook.com/book/462293 (date of access: 02/07/2025).
4. Buriy A.S., Usselemov V.N. Information Security Of Automated Systems// Information and economic aspects of standardization and technical regulation. – 2023. – No. 2 (72). – Pp. 31–37.
5. Meshcheryakov R.V., Shelupanov A.A. Integrated information security of automated systems. Tomsk: V-Spektr. – 2007. – 350 p.
6. Smirnov D.V., Evsyutin O.O. Methodology for collecting data on the activity of malicious software for Windows based on MITRE ATT&CK // Informatics and Automation. – 2024. – Vol. 23. – No. 3. – P. 642–683.
7. FSTEC of Russia. Certification of information security tools [Electronic resource]. – URL: https://fstec.ru (date of access: 02/07/2025).
8. Wangen G., Hallstensen C., Snekkenes E. Cybersecurity risk management: A systematic review of current approaches // Computers & Security. – 2020. – Vol. 93. – Article 101694.

9. Infars. «Social Engineering: how to prevent attacks on employees» [Electronic resource]. – URL: https://infars.ru/blog/hs/cta/cta/redirect/1789215/b8c3de1c-229f-4f86-8000-4928a6b7a3e1 / (date of access: 02/07/2025).
10. RTM Group. «Countering social engineering: employee training» [Electronic resource]. – URL: https://rtmtech.ru/services/obuchenie-personala-sotsialnoj-inzhenerii / (date of access: 02/07/2025).
11. ISO/IEC 27005:2022. Information technology. Methods and means of ensuring security. Information Security Risk Management: a guide. Geneva: ISO, 2022.
12. GOST R ISO/IEC 27005–2010. Information technology. Methods and means of ensuring security. Information Security Risk Management [Text]: national standard of the Russian Federation. – Introduction. 2012-01-01. Moscow: Standartinform. – 2011. – 35 p.
13. Isaev I.V. IT-risks and information security // Modern high-tech technologies. – 2014. – No. 7-1. – Pp. 184–184.
14. Rostelecom-Solar. Solar Dozor [Electronic resource]. – URL: https://rt-solar.ru/products/solar_dozor / (date of access: 02/07/2025).
15. StatCounter. Using Windows 7 in Russia 2023 [Electronic resource]. – URL: https://overclockers.ru/blog/Scorpion81/show/123332/poyavilas-statistika-sistem-windows-ot-statcounter-za-noyabr-2023 (date of access: 02/07/2025).
16. Positive Technologies. Analysis of the application of MITRE ATT&CK in Russian companies [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru / (date of access: 02/07/2025).
17. Positive Technologies. Actual cyber threats: results of 2022 [Electronic resource]. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022 / (date of access: 02/07/2025).
18. Markov A.S., Barabanov A.V., Cirlov V.L. Methods for assessing the inconsistency of information security tools. Moscow: Radio and Communications. – 2012. – 192 p.
19. Smith J., Brown A. Cybersecurity risks and human factors // Cybersecurity Journal. – 2018. – Vol. 14. – Pp. 45–57.
20. Kaspersky Anti Targeted Attack Platform [Electronic resource] // Kaspersky Lab: [website]. – URL: https://www.kaspersky.ru/enterprise-security/anti-targeted-attack-platform (date of access: 02/07/2025).
21. Roskomnadzor. Verification of personal data operators [Electronic resource]. – URL: https://pd.rkn.gov.ru/operators-registry/operators-list / (date of access: 02/07/2025).