МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ им. А. И. ГЕРЦЕНА»

Институт информационных технологий и технологического образования

кафедра информационных технологий и электронного обучения

Основная профессиональная образовательная программа

Направление подготовки 09.03.01 Информатика и вычислительная техника

Направленность (профиль) «Технологии разработки программного обеспечения»

форма обучения – очная

Отчет

по вариативной самостоятельной работе.

Анализ различных источников по теме " Безопасность ИТ (System security and privacy)"

Обучающегося 4 курса

Стецук Максима Николаевича

Санкт-Петербург
2024

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

В последние десятилетия информационные технологии стали неотъемлемой частью жизни как частных пользователей, так и организаций по всему миру. Почти все аспекты жизни, включая личные, финансовые, образовательные и профессиональные данные, теперь сохраняются и обрабатываются в цифровом виде. В результате, безопасность информационных технологий (ИТ) становится ключевым фактором для обеспечения безопасности данных, их доступности и конфиденциальности. Поскольку интернет и другие цифровые технологии продолжают развиваться, возрастает и количество угроз, которые могут привести к утечке данных, разрушению информационных систем или даже нарушению функционирования критически важных инфраструктур.

Одним из наиболее серьезных вызовов является рост числа кибератак, нацеленных на корпоративные сети, банковские системы, государственные учреждения, а также частных пользователей. Все чаще проблемы информационной безопасности выходят за рамки технических аспектов и затрагивают персональные данные и иную информацию пользователей.

Современные угрозы информационной безопасности можно разделить на несколько категорий. Основными из них являются: вредоносное ПО, нацеленное на получение доступа к личной или корпоративной информации, разрушение данных или извлечение финансовой выгоды, фишинг и социальная инженерия, направленные на манипуляцию людьми с целью получения конфиденциальной информации, атаки на сети и системы, перегружающие серверы или системы, делающие их недоступными для пользователей, а также утечки данных, приводящие к распространению конфиденциальной информации.

Цель данной работы - провести всесторонний анализ текущего состояния проблемы безопасности информационных технологий. Для этого будет рассмотрено множество аспектов, включая виды угроз, методы защиты, роль законодательных и этических норм, а также реальные примеры инцидентов в области информационной безопасности.

1 Современные угрозы безопасности ИТ

В современном цифровом мире угрозы информационной безопасности становятся все более разнообразными и сложными. С развитием технологий и увеличением зависимости от ИТ-систем возрастает и количество различных угроз, способных нанести значительный ущерб как организациям, так и частным пользователям. Рассмотрим основные виды современных угроз безопасности ИТ.

1.1 Вирусы и вредоносное ПО

Одной из наиболее распространенных угроз информационной безопасности являются вирусы и другие виды вредоносного ПО (вредоносные программы). Эти угрозы могут привести к повреждению данных, потере информации или потере контроля над устройствами.

- Вирусы - это программы, которые могут самовоспроизводиться и распространяться на другие устройства, заражая их. Вирусы могут быть использованы для различных целей, таких как сбор данных, вмешательство в нормальную работу систем или разрушение информации;
- Трояны - это вид вредоносных программ, которые маскируются под безвредные приложения или файлы. Троян может открывать backdoor для удаленного доступа к системе злоумышленников;
- Программы-вымогатели (ransomware) - это вредоносные программы, которые шифруют данные на компьютере пользователя и требуют выкуп за восстановление доступа к этим данным.

1.2 Фишинг и социальная инженерия

Фишинг и социальная инженерия являются одними из самых опасных угроз, поскольку они не требуют технической подготовки со стороны злоумышленников, а опираются на психологические манипуляции с пользователями.

- Фишинг - это метод обмана, при котором злоумышленники создают поддельные веб-сайты или электронные письма, которые выглядят как официальные сообщения от банков, социальных сетей или других доверенных источников. Основная цель фишинга — заставить пользователя раскрыть свои конфиденциальные данные, такие как логины, пароли или данные банковских карт;

- Социальная инженерия - это техника, при которой злоумышленник использует психологические методы для получения доступа к защищенным системам. Это может включать в себя звонки пользователям, отправку ложных сообщений или манипуляции с сотрудниками организаций.

1.3 Утечка и потеря данных

Утечка данных и потеря информации представляют собой серьезные угрозы для организаций и отдельных пользователей. В последние годы случаи утечек личных и корпоративных данных стали все более частыми и могут привести к значительным финансовым и репутационным потерям, как организаций, так и отдельно взятых личностей.

- Утечка данных может происходить по разным причинам, например, из-за недостаточной защиты данных, ошибок сотрудников или злонамеренных действий хакеров;
- Потеря данных может произойти из-за неисправностей в оборудовании, ошибках пользователей или атак, таких как программы-вымогатели.

1.4 Атаки на системы и сети

Атаки на системы и сети могут иметь серьезные последствия для функционирования организаций и пользователей. Существуют различные виды атак, направленных на нарушение нормальной работы систем и сетей.

- DDoS-атаки (Distributed Denial of Service) - это атаки, при которых злоумышленники используют распределенную сеть зараженных устройств (ботнет) для перегрузки сервера или сети, делая его недоступным для пользователей;
- Эксплойты - это уязвимости в программном обеспечении, которые злоумышленники используют для получения несанкционированного доступа к системе или сети.

2 Методы и технологии защиты информации

В условиях постоянно растущего спектра угроз безопасности ИТ, для обеспечения защиты данных и систем от несанкционированного доступа и повреждения, используется широкий спектр методов и технологий. Эти методы можно разделить на несколько основных категорий: криптография и шифрование данных, аутентификация и авторизация, безопасные сетевые протоколы, системы обнаружения и предотвращения вторжений, а также защита данных в облачных сервисах. Рассмотрим каждый из этих методов более подробно.

2.1 Криптография и шифрование данных

Криптография является основой для защиты информации в современных информационных системах. Этот метод использует математические алгоритмы для преобразования данных в такой формат, который невозможен для прочтения без соответствующего ключа. Криптография применяется как для защиты данных при передаче, так и для хранения.

- Шифрование данных позволяет защитить информацию от несанкционированного доступа. Для этого используются два основных подхода:
    - Симметричное шифрование: алгоритм, при котором один и тот же ключ используется как для шифрования, так и для дешифрования данных;
    - Асимметричное шифрование: использует пару ключей - публичный (для шифрования) и приватный (для дешифрования), что позволяет обмениваться информацией безопасно.
- Цифровые подписи и хеширование также являются важными инструментами криптографии, обеспечивающими проверку целостности данных и аутентичность отправителя.

2.2 Аутентификация и авторизация

Аутентификация и авторизация - это процессы, которые помогают удостовериться в том, что пользователи и устройства имеют право доступа к информации или системе.

- Аутентификация - это процесс проверки подлинности пользователя или устройства. Наиболее распространенные методы аутентификации включают

использование пароля и логина, но в последние годы широко применяются более надежные технологии, такие как биометрия и токены безопасности;

- Авторизация - это процесс предоставления прав доступа после успешной аутентификации.

Двухфакторная аутентификация (2FA) стала стандартом в обеспечении безопасности. Она добавляет дополнительный уровень защиты путем использования двух различных факторов для подтверждения личности.

2.3 Безопасные сетевые протоколы

Основные виды:

- SSL (Secure Sockets Layer) и TLS (Transport Layer Security) - это криптографические протоколы, предназначенные для защиты данных, передаваемых по сети. Они обеспечивают шифрование данных и проверку подлинности серверов, что предотвращает их перехват и модификацию;
- VPN (Virtual Private Network) - это технология, создающая защищенное соединение через публичную сеть. VPN шифрует данные, передаваемые между клиентом и сервером, и предоставляет анонимность, что позволяет защитить информацию от перехвата в открытых сетях;
- IPsec (Internet Protocol Security) - это набор протоколов для защиты данных, передаваемых по интернет-протоколу. IPsec используется для шифрования и аутентификации данных на уровне сетевого слоя и применяется в различных виртуальных частных сетях и при организации безопасных соединений.

Эти протоколы обеспечивают защиту данных при их передаче, снижая риски утечек информации и атак, таких как «man-in-the-middle» (кража данных путем проксирования соединения).

2.4 Системы обнаружения и предотвращения вторжений

Системы обнаружения вторжений (IDS) и системы предотвращения вторжений (IPS) предназначены для мониторинга сетевой активности и обнаружения подозрительных действий, которые могут указывать на попытки вторжения или нарушения безопасности.

- IDS анализирует трафик и данные, чтобы выявить аномалии или шаблоны, характерные для атак, и уведомить администраторов о возможных угрозах. Система IDS не блокирует атаки, а лишь информирует о них;

- IPS выполняет ту же функцию, но с возможностью активной блокировки подозрительных действий в реальном времени, предотвращая вторжения и минимизируя ущерб.

2.5 Защита данных в облачных сервисах

С развитием облачных технологий, все больше данных и приложений переносятся в облачные сервисы. Однако это также вызывает вопросы безопасности, так как данные находятся за пределами традиционных корпоративных сетей и могут быть подвержены различным угрозам.

Для защиты данных в облаке используются следующие методы:

- Шифрование данных в облаке - необходимо, чтобы данные, хранящиеся в облаке, были зашифрованы, чтобы даже в случае утечки информации они не были доступны для посторонних лиц. Многие облачные сервисы предоставляют встроенные функции шифрования;
- Контроль доступа - системы управления доступом (IAM) обеспечивают, что только авторизованные пользователи могут получить доступ к данным. Управление правами доступа позволяет ограничивать доступ к данным в зависимости от ролей сотрудников или приложений;
- Резервное копирование и восстановление - для защиты от потери данных облачные провайдеры часто предлагают услуги резервного копирования и восстановления, что гарантирует сохранность информации в случае сбоя или атаки.

Таким образом, методы и технологии защиты информации играют ключевую роль в обеспечении безопасности данных в современном мире. Криптография, аутентификация, безопасные сетевые протоколы, системы предотвращения вторжений и защита данных в облачных сервисах - все эти инструменты необходимы для создания многоуровневой системы безопасности, способной эффективно защищать от различных угроз, включая кибератаки, утечки данных и несанкционированный доступ.

3 Примеры крупных происшествий, связанных с информационной безопасностью

Киберугрозы и инциденты в области информационной безопасности с каждым годом становятся более масштабными и сложными. Ряд крупных происшествий, связанных с информационной безопасностью, продемонстрировали не только уязвимости в отдельных компаниях, но и системные проблемы в защите данных на глобальном уровне. В этом разделе мы рассмотрим несколько ярких примеров таких инцидентов, включая операцию "Триангуляция" с участием компании Apple, шпионский софт Pegasus и уязвимости в продукции Microsoft.

3.1 Операция "Триангуляция"

Операция "Триангуляция" (Triangulation) стала известной после того, как в 2010 году было раскрыто, что компания Apple хранит и отправляет данные о местоположении пользователей на серверы, что вызвало огромные вопросы по безопасности и конфиденциальности. Проблема была связана с приложением Location Services, которое использует GPS, Wi-Fi и сотовые вышки для определения местоположения пользователей. Однако приложение собирало эти данные, даже если пользователь отключал функцию отслеживания местоположения на своем устройстве.

Это привело к утечке огромного количества информации о перемещениях пользователей iPhone и iPad, которая сохранялась в незащищенном виде. Эти данные могли быть использованы для отслеживания поведения пользователей и составления их подробных профилей, что ставило под угрозу конфиденциальность.

3.2 Шпионский софт Pegasus

Pegasus - это шпионский софт, разработанный израильской компанией NSO Group, предназначенный для слежки за мобильными устройствами, включая iPhone и Android. Программа была использована для незаконного взлома смартфонов политиков, журналистов, правозащитников и других высокопрофильных целей по всему миру.

Pegasus имеет способность без ведома пользователя устанавливать шпионское ПО на устройства через уязвимости в операционных системах, используя нулевые уязвимости (zero-day exploits). Эти уязвимости позволяют использовать уязвимости в коде операционной системы, которые еще не были исправлены производителями. Программное

обеспечение может активировать камеру и микрофон устройства, считывать сообщения, отслеживать местоположение и перехватывать звонки, не оставляя следов на телефоне.

Самым громким случаем использования Pegasus стала утечка данных из проекта The Pegasus Project, в котором участвовали такие издания, как The Guardian и The Washington Post. В результате расследования выяснилось, что эта программа использовалась для слежки за тысячами людей, включая журналистов, политических активистов, а также даже глав государств, таких как президент Франции Эммануэль Макрон.

3.3 Уязвимости в продукции Microsoft

Вопрос уязвимостей в продуктах Microsoft стал особенно актуален после ряда инцидентов, когда уязвимости в операционных системах Windows и других продуктах компании были использованы хакерами для атак на крупные организации, включая государственные учреждения.

Одним из самых громких случаев стала утечка инструментов хакеров из Equation Group (группа, связанная с АНБ США), когда в 2017 году в сеть попали данные о том, как Microsoft не успела вовремя закрыть уязвимости в своем программном обеспечении. Это привело к тому, что атаки с использованием уязвимостей в Windows SMB (Server Message Block) стали распространенными и привели к вирусу WannaCry, который поразил более 200 тысяч компьютеров по всему миру. Атака использовала уязвимость, о которой Microsoft знала, но которую не успела исправить до того, как она была использована злоумышленниками.

Примеры крупных происшествий, подчеркивают важность информационной безопасности в современном мире. Эти инциденты не только выявляют уязвимости в технологических системах, но и показывают, как важна защита конфиденциальных данных и их доступности. Каждое из этих происшествий стало сигналом для организаций, правительств и пользователей о необходимости улучшать свои практики безопасности, чтобы предотвратить возможные атаки и утечки данных в будущем.

4 Проблемы конфиденциальности и приватности

С развитием информационных технологий и цифровых сервисов возникает множество вопросов и проблем, связанных с защитой конфиденциальности и приватности данных пользователей. Вопросы безопасности и конфиденциальности в цифровую эпоху становятся все более актуальными, поскольку интернет и мобильные устройства проникают в каждый аспект нашей жизни. В данном разделе будут рассмотрены ключевые проблемы конфиденциальности и приватности, такие как регулирование безопасности данных, вызовы цифровой эпохи и трудности с обработкой и сбором личных данных.

4.1 Регулирование безопасности данных

В последние годы вопрос защиты личных данных стал одной из самых обсуждаемых тем в области информационной безопасности, особенно в свете внедрения таких нормативных актов, как GDPR (General Data Protection Regulation) в Европейском Союзе и аналогичных законов по всему миру.

- GDPR был принят в мае 2018 года и стал значимым инструментом в регулировании конфиденциальности данных. Этот закон направлен на усиление контроля над данными пользователей, установленное обязательство для организаций собирать, обрабатывать и хранить персональную информацию в соответствии с высокими стандартами безопасности;
- В России аналогом GDPR является Федеральный закон о защите персональных данных (№ 152-ФЗ), который регулирует сбор, хранение и обработку личных данных. Он требует от организаций соблюдения стандартов безопасности данных и установления строгих норм по защите персональной информации пользователей, особенно в случае обработки чувствительных данных.

4.2 Конфиденциальность в цифровую эпоху

Современные технологии неизбежно связаны с компромиссами между удобством и конфиденциальностью. С ростом использования интернета и мобильных устройств вопросы конфиденциальности становятся все более важными, особенно в контексте социальных сетей и иных популярных сервисов.

- Мониторинг и сбор данных - современные технологические компании собирают огромные объемы данных о своих пользователях, включая информацию об их предпочтениях, поведении, интересах и взаимодействиях с сервисами. Эта информация используется для улучшения услуг и таргетирования рекламы, однако возникает вопрос, насколько этично и безопасно собирать такие данные;
- Этические вопросы - в цифровую эпоху важными становятся не только вопросы безопасности, но и этики в обработке данных. Например, компании могут использовать личные данные для манипулирования пользовательскими предпочтениями или для воздействия на их решения;
- Приватность и социальные сети - в эпоху социальных сетей приватность становится относительно понятием. Пользователи делятся личной информацией в публичных профилях, не всегда осознавая, как эта информация может быть использована.

4.3 Проблемы с обработкой и сбором личных данных

Обработка и сбор личных данных затрагивает многие аспекты цифровой жизни и вызывает серьезные опасения среди пользователей и экспертов в области безопасности. Основные проблемы, связанные с этим процессом, включают следующее:

- Мониторинг - одной из главных угроз конфиденциальности является постоянный мониторинг пользователей. Все больше компаний и сервисов отслеживают поведение пользователей в сети, собирая данные о его действиях;
- Реклама - сбор данных с целью таргетированной рекламы стал важным инструментом для многих интернет-компаний. Эти данные включают в себя информацию о привычках пользователей, интересах, поисковых запросах и покупках;
- Социальные сети - различные платформы собирают огромное количество информации о пользователях, которая используется не только для предоставления персонализированного контента, но и для продажи рекламных услуг.

Проблемы конфиденциальности и приватности данных в цифровую эпоху становятся все более актуальными и требуют комплексного подхода, а также регулирования безопасности данных через законодательные акты.

5 Перспективы и будущее безопасности ИТ

Будущее информационной безопасности представляет собой вызовы и возможности, которые обусловлены стремительным развитием технологий, таких как искусственный интеллект (ИИ), большие данные, Интернет вещей (IoT) и другие инновации. Эти технологии, с одной стороны, способствуют улучшению защиты информации, с другой - создают новые риски и уязвимости. В данной части работы рассматриваются основные перспективы и проблемы, с которыми потенциально может столкнуться безопасность ИТ в будущем, а также роль новых технологий в борьбе с угрозами.

5.1 Роль искусственного интеллекта и машинного обучения в области безопасности

Искусственный интеллект (AI) и машинное обучение (ML) становятся важными инструментами в сфере безопасности информационных технологий. Их применение в защите данных позволяет значительно улучшить способность к обнаружению и предотвращению угроз.

- Обнаружение угроз в реальном времени - AI и ML могут анализировать огромные объемы данных в реальном времени, выявляя аномалии и отклонения от обычной активности;
- Адаптация к новым угрозам - AI способен учиться на основе предыдущих атак и автоматически адаптировать алгоритмы защиты к новым типам угроз. Это становится важным в условиях постоянного развития методов атак, таких как использование нулевых уязвимостей (zero-day exploits) или новых вирусов;
- Автоматизация и снижение человеческого фактора - AI и ML могут автоматизировать процессы защиты, уменьшая влияние человеческого факторы и скорость реакции на инциденты.

5.2 Проблемы и возможности защиты в эпоху больших данных и Интернета вещей (IoT)

С развитием технологий большие данные (Big Data) и Интернет вещей (IoT) создают новые вызовы и возможности в области информационной безопасности.

- Большие данные и защита данных: Большие данные включают в себя огромные объемы разнообразной информации, которая может быть использована для различных целей - от улучшения услуг до прогнозирования поведения пользователей. Однако с ростом объемов данных увеличиваются и риски утечек или утрат информации;
- Интернет вещей (IoT): С каждым годом число устройств, подключенных к Интернету, продолжает расти, что создает дополнительные риски для безопасности. Устройства IoT часто имеют недостаточную защиту, а также могут быть использованы как входные точки для атак.

Кроме того, безопасность IoT связана с проблемой стандартизации, так как в настоящее время нет единого стандарта безопасности для устройств IoT, что создает дополнительные уязвимости и значительно расширяет потенциальную площадь атаки.

5.3 Прогнозы развития угроз и методов защиты в ближайшие годы

В ближайшие годы угрозы безопасности ИТ, скорее всего, будут становиться более разнообразными и сложными, требуя новых подходов к защите данных.

- Рост киберпреступности - преступные организации будут продолжать использовать новые технологии для разработки более совершенных атак. Это может включать кибероружие, основанное на ИИ, атаки на критически важные инфраструктуры и массовые утечки данных;
- Угрозы от квантовых компьютеров - квантовые вычисления могут стать важным прорывом в области технологий, но они также представляют угрозу для безопасности, поскольку способны разрушить многие современные методы шифрования, такие как RSA и ECC;
- Развитие защиты с помощью ИТ-автоматизации - в ответ на растущие угрозы, ожидается дальнейшее внедрение автоматизированных систем безопасности на базе ИИ и машинного обучения. Компании будут внедрять более продвинутые системы защиты, способные самостоятельно адаптироваться к новым угрозам и обеспечивать более высокую скорость реакции на инциденты;
- Совершенствование методов аутентификации - с увеличением числа угроз также возрастает потребность в более сложных методах аутентификации. В ближайшие годы ожидается развитие биометрических технологий, таких как распознавание лиц и отпечатков пальцев;

- Ужесточение регуляций - в ответ на глобальные угрозы безопасности и утечки данных мы также можем ожидать более жесткие меры по контролю за обработкой данных.

Будущее безопасности информационных технологий будет зависеть от того, как человечество адаптируется к новым вызовам, связанным с развитием технологий и угроз. Искусственный интеллект и машинное обучение играют важную роль в обеспечении безопасности, но также несут новые риски. Развитие больших данных и Интернета вещей открывает как возможности для улучшения защиты, так и новые уязвимости.

ЗАКЛЮЧЕНИЕ

В ходе анализа состояния проблемы безопасности информационных технологий было выявлено, что эта область продолжает оставаться одной из самых актуальных и динамично развивающихся. В условиях стремительного роста использования цифровых технологий и интернета новые угрозы становятся все более сложными и разнообразными. Основными вызовами в сфере безопасности ИТ являются вирусы и вредоносное ПО, фишинг, утечка данных, атаки на системы и сети, а также угрозы, возникающие в связи с развитием Интернета вещей и больших данных. В ответ на эти угрозы активно разрабатываются новые методы защиты, включая криптографию, аутентификацию, использование безопасных протоколов и современных систем мониторинга.

Однако для эффективной защиты данных необходимо применять комплексный подход. Это означает интеграцию различных технологий и методик защиты, включая использование искусственного интеллекта для анализа угроз, развитие стандартов безопасности для Интернета вещей, а также усиление контроля за обработкой личных данных в рамках регулирования, как, например, GDPR. Комплексный подход также требует от организаций постоянного обновления знаний в области безопасности и применения самых современных методов защиты.

Таким образом, безопасность информационных технологий является многоуровневой и многогранной проблемой, решение которой возможно только в условиях постоянного совершенствования как технологий защиты, так и систем регулирования, обучения и обмена опытом среди профессионалов.

ЛИТЕРАТУРА

1. Сарыгулов С. Х., Сарыев Н. Г. РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В БУДУЩЕМ КИБЕРБЕЗОПАСНОСТИ //Символ науки. – 2023. – №. 10-2. – С. 54-56.
2. Муниров Д. Д. ВАЖНОСТЬ КИБЕРБЕЗОПАСНОСТИ В ЦИФРОВУЮ ЭПОХУ //PSIXOLOGIYA VA SOTSIOLOGIYA ILMIY JURNALI. – 2024. – Т. 2. – №. 7. – С. 35-42.
3. Kaur J., Ramkumar K. R. The recent trends in cyber security: A review //Journal of King Saud University-Computer and Information Sciences. – 2022. – Т. 34. – №. 8. – С. 5766-5781.
4. Stamp M. Information security: principles and practice. – John Wiley & Sons, 2011.
5. Авраменко В. С., Бобрешов-Шишов Д. И., Маликов А. В. Способ выявления уязвимостей" нулевого дня" на основе анализа поведения эксплойтов //Проблемы технического обеспечения войск в современных условиях. – 2018. – С. 45-48.
6. Коваль К. О. Цель для хакеров, или уязвимость нулевого дня //Бизнес-инжиниринг сложных систем: модели, технологии, инновации. – 2020. – С. 154-157.
7. Антонова Т. С., Смирнов В. М. Фишинг как неизученное киберпреступление //StudNet. – 2021. – Т. 4. – №. 6. – С. 69-75.
8. Hadnagy C. Social engineering: The art of human hacking. – John Wiley & Sons, 2010.
9. Mattei T. A. Privacy, confidentiality, and security of health care information: Lessons from the recent Wannacry cyberattack //World neurosurgery. – 2017. – Т. 104. – С. 972-974.
10. Намиот Д. Е., Ильюшин Е. А., Чижов И. В. Искусственный интеллект и кибербезопасность //International Journal of Open Information Technologies. – 2022. – Т. 10. – №. 9. – С. 135-147.
11. Шаньгин В. Информационная безопасность. – Litres, 2022.