Инженерный вестник Дона, №10 (2025)
ivdon.ru/ru/magazine/archive/n10y2025/10517

Обеспечение информационной и кибербезопасности военнослужащих в цифровую эпоху при проведении специальной военной операции

П. С. Шевчук[1], А.П. Зверев[2], М.С. Пазин[3]

[1]Ростовский государственный университет путей сообщения
[2]Академии государственной противопожарной службы, Москва
[3]Донской государственный технический университет

Аннотация: В статье анализируются современные угрозы информационной безопасности военнослужащих в зоне проведения специальной военной операции, в том числе методы социальной инженерии, разведка по открытым источникам кибершпионажа. На основе систематизации реальных инцидентов, нормативно-правового анализа и международного опыта предлагаются комплексные меры по защите персональных данных и противодействию киберугрозам — от технических решений и протоколов цифровой гигиены до организационных и правовых механизмов. Результаты исследования направлены на повышение осведомлённости личного состава, снижение влияния человеческого фактора как основной уязвимости и формирование устойчивой системы информационной безопасности в полевых условиях. Разработанные рекомендации могут быть использованы при подготовке военнослужащих, совершенствовании уставов и внедрении стандартов кибербезопасности в Вооружённых силах Российской Федерации.
Ключевые слова: информационная безопасность, военнослужащие, специальная военная операция, персональные данные, киберугрозы, цифровая гигиена, социальная инженерия, кибербразведка, безопасность связи, военная кибербезопасность.

Введение

Современная военная деятельность всё больше интегрируется в цифровое пространство, что открывает новые возможности для управления, связи и координации, но в то же время создаёт серьёзные риски для информационной безопасности (ИБ) личного состава. Военнослужащие, особенно те, кто находится в зоне проведения специальной военной операции (СВО), становятся крайне уязвимыми для кибератак, сбора разведывательных данных и манипуляций через цифровые каналы.

Особую остроту проблема приобретает в условиях СВО, где противник активно применяет методы гибридной войны, включая кибербразведку, дезинформацию и социальную инженерию. Цифровое поле боя становится не менее важным, чем физическое, а военнослужащий — не только носителем

оружия, но и источником ценной информации, которую стремятся добыть противоборствующие стороны [1-3].

Целью данной статьи является разработка концептуальных и практических рекомендаций по обеспечению информационной безопасности военнослужащих в условиях специальной военной операции с акцентом на защиту персональных данных и противодействие современным киберугрозам в полевых условиях.

Анализ угроз информационной безопасности военнослужащих

Информационная безопасность в военной сфере представляет собой состояние защищённости военной информации, информационных систем и цифровой инфраструктуры, при котором обеспечивается конфиденциальность, целостность, доступность и неотрекаемость данных, критически важных для выполнения боевых задач, управления войсками и обеспечения национальной безопасности [4, 5].

В отличие от гражданской сферы, где ИБ преимущественно направлена на защиту персональных данных и корпоративных активов, военная информационная безопасность имеет стратегический характер и напрямую связана с боеспособностью, живучестью подразделений и исходом операций.

Особенность военной ИБ заключается в том, что она охватывает не только технические системы, но и человеческий фактор, процедуры управления и психологическую устойчивость личного состава. Утечка данных может произойти не через взлом сервера, а через неосторожный пост в социальной сети — что делает ИБ в военной сфере многоуровневой и комплексной дисциплиной.

Цифровая среда в зоне вооружённого конфликта кардинально отличается от мирного времени по уровню угроз, динамике, ограничениям и целям использования.

Основные характеристики цифровой среды в зоне конфликта:

1. Гибридный характер угроз. Современные конфликты носят гибридный характер, где кибератаки, информационная война, психологические операции и традиционные боевые действия тесно взаимосвязаны. Противник использует разведку по открытым источникам (open source intelligence) - OSINT-разведку, социальную инженерию, фейковые рассылки и кибершпионаж как часть тактики поражения.

2. Высокая уязвимость личного состава. Военнослужащие в зоне СВО часто используют личные устройства (смартфоны, планшеты) из-за недостатка специализированной техники или желания связаться с родными.

Эти устройства:

– не защищены от вредоносного программное обеспечение (ПО);
– передают геолокацию в фоновом режиме;
– содержат метаданные в фото и видео;
– подключаются к ненадёжным сетям.

3. Ограниченная инфраструктура и связь. В полевых условиях отсутствуют стабильные каналы связи, централизованные серверы, резервное питание. Это затрудняет:

– применение сложных систем шифрования;
– обновление ПО и антивирусов;
– централизованный мониторинг и управление устройствами.

4. Активное использование противником цифрового пространства. Противоборствующая сторона целенаправленно:

– мониторит соцсети и мессенджеры;
– создаёт фейковые аккаунты для вербовки;
– распространяет дезинформацию через поддельные каналы;
– использует искусственный интеллект (ИИ) для автоматического анализа открытых данных.

5. Психологический и эмоциональный фактор. Стресс, усталость, желание поделиться переживаниями — всё это снижает бдительность. Военнослужащий может непреднамеренно нарушить правила ИБ, не осознавая последствий. Это делает психологическую подготовку и цифровую гигиену неотъемлемой частью общей безопасности.

Цифровая среда в условиях вооружённого конфликта — это динамичное, враждебное и многогранное пространство, где угрозы исходят не только извне, но и изнутри системы. Эффективная защита возможна только при учёте этих особенностей: сочетании технических решений, жёсткой дисциплины, непрерывного обучения и психологической устойчивости. Без этого даже самые современные технологии окажутся бесполезными [6, 7].

Сравнительная характеристика информационной безопасности в мирное и военное время представлена в табл.1. Как видно из табл. 1, ИБ в военное время принципиально отличается от мирной парадигмы не только масштабом угроз, но и характером последствий. Если в мирное время утечка данных ведёт к финансовым потерям, то в зоне СВО — к прямой угрозе жизни. Это требует пересмотра всех подходов к защите: от технических решений до психологической подготовки личного состава [8, 9].

В зоне СВО военнослужащие сталкиваются с многоуровневой системой угроз. К внешним источникам относятся государственные разведки противника, хакерские группы, а также организованные преступные группировки, использующие военных как источник информации для шантажа или продажи.

Внутренние угрозы связаны с человеческим фактором: неосторожностью, недостаточной подготовкой по ИБ, а в редких случаях — сознательной утечкой данных. Именно внутренние угрозы становятся причиной более 60% инцидентов.

Таблица 1.

Сравнительная характеристика ИБ в мирное и военное время

Критерий	Мирное время	Военное время
Основная цель ИБ	Защита конфиденциальности данных, предотвращение финансовых потерь	Обеспечение боеспособности, сохранение жизни личного состава, защита оперативных планов
Источники угроз	Хакеры, киберпреступники, инсайдеры, конкуренты	Государственные разведки, хакерские группы противника, дезинформаторы, вербовщики
Типичные угрозы	Фишинг, вредоносное ПО, DDoS, утечки баз данных	OSINT-разведка, геотрекинг, социальная инженерия, вербовка, дезинформация, кибершпионаж
Объекты защиты	Корпоративные сети, персональные данные клиентов, ИС управления	Персональные данные военнослужащих, дислокация подразделений, каналы связи, тактические данные
Человеческий фактор	Ошибки, неосторожность, недостаток обучения	Стресс, усталость, эмоциональные публикации, желание связаться с родными высокая уязвимость
Используемые устройства	Корпоративные компьютеры, защищённые смартфоны, контролируемые сети	Личные смартфоны, гражданские мессенджеры, незащищённые Wi-Fi, ограниченная инфраструктура
Уровень последствий	Финансовые убытки, штрафы, репутационный ущерб	Потери личного состава, срыв операций, артиллерийские удары по координатам, деморализация
Реакция на инциденты	Расследование, восстановление систем, уведомление регуляторов	Немедленные тактические меры: смена дислокации, блокировка каналов, психологическая поддержка
Подход к защите	Реактивный и профилактический	Прогнозирующий и превентивный (в идеале); часто — вынужденно реактивный из-за условий

Основными уязвимыми местами цифровой инфраструктуры являются:

– использование гражданских мессенджеров без шифрования;

– отсутствие контроля за личными устройствами;

– низкая осведомлённость личного состава о принципах цифровой гигиены.

Меры защиты персональных данных и противодействия киберугрозам

На рис. 1 представлена четырёхкомпонентная модель обеспечения информационной безопасности военнослужащих, действующих в условиях

специальной военной операции (СВО).

Модель строится вокруг центрального элемента — «Комплексная модель защиты военнослужащих в цифровой среде», который символизирует интеграцию всех мер в единую систему.

Каждое направление представлено отдельным блоком с перечнем конкретных мероприятий, реализуемых на уровне подразделений и личного состава. Все компоненты модели взаимосвязаны и направлены на минимизацию рисков, связанных с утечкой персональных данных, социальной инженерией, геолокационным трекингом и другими киберугрозами.

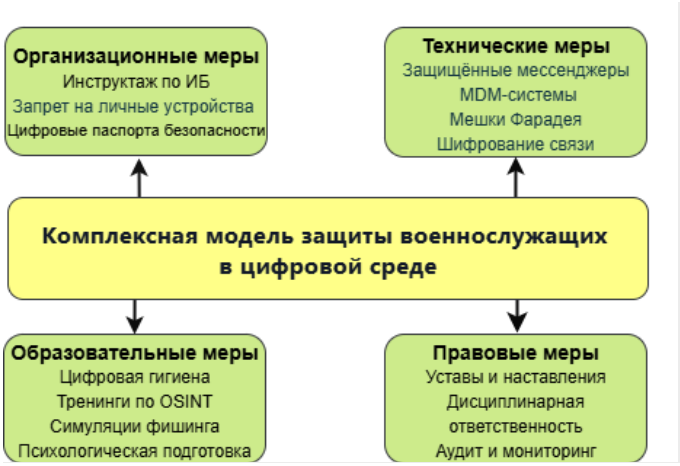

Рис. 1. - Модель обеспечения информационной безопасности

Детализация компонентов модели.

1. Организационные меры. Этот блок охватывает управленческие и процедурные аспекты обеспечения ИБ:

– инструктаж по информационной безопасности - обязательное обучение перед отправкой в зону СВО, включающее основы OSINT, фишинга, цифровой гигиены;

– запрет на использование личных устройств - исключение возможности утечки данных через смартфоны, планшеты, ноутбуки;

– цифровые паспорта безопасности - индивидуальные профили, содержащие уровень допуска, разрешённые приложения, историю нарушений

и результаты тестирования;

2. Технические меры направлены на обеспечение защищённой цифровой инфраструктуры:

– защищённые мессенджеры - внедрение военных аналогов Telegram/WhatsApp с end-to-end шифрованием («КриптАТ», «Аврора»);

– мешки Фарадея - физическая изоляция устройств от радиосигналов, предотвращение слежки и удалённого взлома;

– шифрование связи - применение протоколов передачи данных в реальном времени для голосовой и текстовой связи.

3. Образовательные меры фокусируются на формировании культуры цифровой безопасности:

– цифровая гигиена - правила поведения в сети: что можно публиковать, как распознавать фишинг, как настраивать устройства.

– тренинги по OSINT - обучение личного состава «думать, как разведчик» — понимать, какие данные они сами выдают в открытых источниках.

– симуляции фишинга - практические занятия, имитирующие реальные атаки для отработки реакции.

– психологическая подготовка - работа с когнитивными искажениями, устойчивостью к манипуляциям, вербовке и дезинформации.

4. Правовые меры обеспечивают нормативно-дисциплинарную основу:

– уставы и наставления - включение требований ИБ в официальные документы (строевой устав, наставления по боевой подготовке);

– дисциплинарная ответственность — введение санкций за нарушения (предупреждения, лишение премий, уголовная ответственность);

– аудит и мониторинг — регулярные проверки, анализ логов, отчётность командиров, внедрение «тайных покупателей».

Модель является интегрированной и синергетической:

– без организационных мер технические средства не будут использоваться должным образом;

– без образовательных мер даже самые совершенные технологии окажутся бесполезными;

– без правовых норм нет механизма принуждения и контроля;

– без технических решений невозможно защититься от высокотехнологичных атак.

Модель наглядно демонстрирует, что современная информационная безопасность военнослужащих — это не набор отдельных мер, а целостная система, объединяющая управление, технологии, образование и правовые рамки [10]. Только такой комплексный подход позволяет противостоять многоуровневым киберугрозам в условиях гибридной войны и обеспечивать сохранность жизни, боеспособности и секретности военных операций. Каждый компонент играет свою роль, но лишь их синергия создаёт устойчивую защиту в цифровой среде.

Перспективы и предложения по совершенствованию системы информационной безопасности военнослужащих

Современные вызовы цифровой эпохи требуют трансформации подходов к обеспечению ИБ личного состава ВС РФ. В условиях СВО недостаточно реактивного реагирования на инциденты — необходима системная и технологически обоснованная стратегия. В этой связи целесообразно реализовать следующие направления развития системы ИБ:

1. Разработка единых стандартов информационной безопасности для вооружённых сил в цифровую эпоху.

На сегодняшний день нормативно-методическая база в области ИБ военнослужащих носит фрагментарный характер и не охватывает специфику полевых условий. Представляется необходимым разработать и утвердить Единый стандарт информационной безопасности военнослужащего (ЕСИБ-

ВС), который должен включать требования к цифровому поведению, техническим средствам связи, процедурам реагирования на инциденты и минимальному уровню подготовки по ИБ для всех категорий личного состава.

2. Создание специализированных подразделений кибербезопасности в полевых условиях.

Эффективное противодействие киберугрозам в зоне боевых действий невозможно без наличия штатных специалистов на местах. Целесообразно формировать мобильные группы кибербезопасности (МГКБ) в составе бригад и полков, участвующих в СВО. В их задачи должны входить оперативный аудит цифровой гигиены личного состава, мониторинг открытых источников на предмет утечек, обучение военнослужащих и реагирование на инциденты.

3. Интеграция искусственного интеллекта и машинного обучения для детектирования угроз в реальном времени.

Объём цифровых данных, генерируемых в зоне конфликта, превышает возможности ручного анализа. Перспективным направлением является внедрение систем на основе искусственного интеллекта (ИИ) и машинного обучения (МО), способных автоматически выявлять аномалии в поведении пользователей, анализировать метаданные изображений и текстов в социальных сетях, а также прогнозировать возможные векторы атак. Такие системы могут быть интегрированы в существующие АСУ и обеспечивать командованию оперативную картину цифровой угрозы.

Заключение

Проведённое исследование подтверждает высокую актуальность и практическую значимость обеспечения информационной безопасности военнослужащих в условиях специальной военной операции. Цифровая среда, ранее воспринимавшаяся как вспомогательный инструмент, сегодня стала театром активных боевых действий, где утечка данных, геолокации или

неосторожный пост в соцсети могут стоить жизни не только одному солдату, но и целому подразделению.

Человеческий фактор остаётся главной уязвимостью. Технические средства и запреты неэффективны без осознанности, дисциплины и культуры цифровой гигиены среди личного состава.

Комплексный подход — единственный путь к эффективной защите. Необходимо синхронное применение организационных, технических, образовательных и правовых мер — ни один из этих элементов по отдельности не даст устойчивого результата.

Будущее военной кибербезопасности - за адаптивными интеллектуальными системами. ИИ, МО, квантовое шифрование, нейроинтерфейсы — это не фантастика, а ближайшие технологические рубежи, которые потребуют пересмотра всех существующих подходов.

Таким образом, ИБ военнослужащего — это не просто пункт в инструкции. Это элемент боеготовности, компонент живучести подразделения и фактор победы на цифровом поле боя. Инвестировать в неё — значит инвестировать в жизнь солдат, в успех операций и в технологический суверенитет государства.

Литература

1. Менциев А.У., Чебиева Х.С. Современные угрозы безопасности в сети Интернет и контрмеры (обзор) // Инженерный вестник Дона, 2019, № 3. URL: ivdon.ru/ru/magazine/archive/N3y2019/5859.

2. Антонов В. В., Пальчевский Е. В., Еникеев Р. Р. Прогнозирование на основе искусственной нейронной сети второго поколения для поддержки принятия решений в особо значимых ситуациях // Программные продукты и системы. 2022. № 3. С. 384-395.

3. Карасев М. А., Котлярова Л. Д. Информационное обеспечение процесса принятия управленческих решений // Экономика и

предпринимательство. 2022. № 4(141). С. 745-748.

4. Селиверстов В.В., Корчагин С.А. Анализ актуальности и состояния современных фишинг-атак на объекты критической информационной инфраструктуры // Инженерный вестник Дона. 2024. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9277.

5. Butakova M.A., Chernov A.V., Shevchuk P.S. An approach for distributed reasoning on security incidents in critical information infrastructure with intelligent awareness systems. Advances in Intelligent Systems and Computing. - 2019. T. 1046. pp. 248-255.

6. Butakova M.A., Chernov A.V., Shevchuk P.S., Vereskun V.D. Neural fuzzy adaptive control for mobile smart objects. 2018 International Symposium on Consumer Technologies, ISCT 2018. - 2018. pp. 45-48.

7. Butakova M.A., Chernov A.V., Shevchuk P.S., Vereskun V.D. Complex event processing for network anomaly detection in digital railway communication services. 2017 25th Telecommunications Forum, TELFOR 2017 - Proceedings. 25. - 2018. pp. 1-4.

8. Баланов А.Н. Биометрия. Разработка и внедрение систем идентификации. – Санкт-Петербург. – Изд-во Лань., 2024. – с. 228.

9. Лебедев Б. К., Лебедев О. Б., Черкасов Р. И. Использование нейронных сетей для решения задач компьютерного зрения // Инженерный вестник Дона. – 2025. – № 2. – URL: ivdon.ru/ru/magazine/archive /n2y2025/9870/.

10. Большаков М.А., Ходаковский В.А. Подход к повышению качества моделей машинного обучения в задачах мониторинга сложных систем на основе применения метрических пространств // Инженерный вестник Дона. 2024. № 11. URL: ivdon.ru/magazine/archive/n11y2024/9630.

References

1. Menciev A.U., Chebieva H.S. Inzhenernyj vestnik Dona, 2019, № 3.

URL: ivdon.ru/ru/magazine/archive/N3y2019/5859.

2. Antonov V. V., Pal'chevskiy E. V., Enikeev R. R. Programmnye produkty i sistemy. 2022. № 3. pp. 384-395.

3. Karasev M. A., Kotlyarova L. D. Ekonomika i predprinimatel'stvo. 2022. № 4(141). pp. 745-748.

4. Seliverstov V.V., Korchagin S.A. Inzhenernyj vestnik Dona. 2024. № 6. URL: ivdon.ru/ru/magazine/archive/n6y2024/9277.

5. Butakova M.A., Chernov A.V., Shevchuk P.S. An approach for distributed reasoning on security incidents in critical information infrastructure with intelligent awareness systems. Advances in Intelligent Systems and Computing. 2019. T. 1046. pp. 248-255.

6. Butakova M.A., Chernov A.V., Shevchuk P.S., Vereskun V.D. Neural fuzzy adaptive control for mobile smart objects. 2018 International Symposium on Consumer Technologies, ISCT 2018. 2018. pp. 45-48.

7. Butakova M.A. Chernov A.V., Shevchuk P.S., Vereskun V.D. Complex event processing for network anomaly detection in digital railway communication services. 2017 25th Telecommunications Forum, TELFOR 2017. Proceedings. 25. 2018. pp. 1-4.

8. Balanov A.N. Biometriya. Razrabotka i vnedrenie sistem identifikacii. [Development and implementation of identification systems]. Sankt Peterburg. Izd-vo Lan`, 2024. p. 228.

9. Lebedev B. K., Lebedev O. B., Cherkasov R. I. Inzhenernyj vestnik Dona. 2025. № 2. URL: ivdon.ru/ru/magazine/archive/n2y2025/9870/.

10. Bol'shakov M.A., Khodakovskiy V.A. Inzhenernyj vestnik Dona. 2024. № 11. URL: ivdon.ru/magazine/archive/n11y2024/9630.

Авторы согласны на обработку и хранение персональных данных.

Дата поступления: 3.09.2025

Дата публикации: 26.10.2025