Юрчак Владислав Витальевич, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М.Штеменко

Недошивин Кирилл Андреевич, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М.Штеменко

Золотарев Александр Сергеевич, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М.Штеменко

Петренко Алексей Павлович, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М.Штеменко

Симоненко Евгений Евгеньевич, курсант
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М.Штеменко

Научный руководитель:
Коломейцев Александр Эдуардович
кандидат технических наук
Краснодарское высшее военное орденов Жукова и Октябрьской Революции
Краснознамённое училище имени генерала армии С.М.Штеменко

КРИПТОГРАФИЧЕСКАЯ БЕЗОПАСНОСТЬ ТАКТИЧЕСКОГО ЗВЕНА: ИМПЕРАТИВЫ ЭКСТРЕННОГО РЕАГИРОВАНИЯ ПРИ ЗАХВАТЕ ЛИЧНОГО СОСТАВА

Аннотация. Данное исследование посвящено проблеме обеспечения криптографической устойчивости военной связи в условиях физического захвата личного состава, имеющего при себе носимые средства коммуникации. В работе анализируется многоуровневая природа угроз, возникающих при попадании радиоэлектронного оборудования в руки противника.

Ключевые слова: Экстренная смена ключей, компрометация средств связи, динамическое исправление ключами, аппаратный модуль безопасности, тактическая криптографическая устойчивость.

Введение: экзистенциальный вызов современной тактической связи

Эволюция вооруженных конфликтов последних десятилетий неумолимо движется в сторону тотальной цифровизации поля боя, где каждый военнослужащий, от отделенного стрелка до командира батальона, становится не просто боевой единицей, но и узлом сложной информационной сети. Носимые средства связи, некогда выполнявшие исключительно функцию голосовой коммуникации, трансформировались в многофункциональные терминалы, обеспечивающие передачу данных целеуказания, видеопотоков с разведывательных дронов, координат позиционирования и команд управления. Эта глубокая интеграция электроники в тактические процессы порождает критическую уязвимость: пленение военнослужащего с исправным терминалом связи создает ситуацию, при которой противник получает не просто трофейное оборудование, а полноценный инструмент проникновения в защищенный контур управления своими войсками.

Парадокс современной войны заключается в том, что чем совершеннее становятся средства криптографической защиты каналов передачи, тем более привлекательной целью для противника становится физический носитель ключевой информации. Если ранее, в эпоху аналоговой связи и простых кодовых таблиц, захват радиостанции требовал от противника значительных усилий по дешифровке перехваченных материалов, то сегодня получение доступа к действующему устройству с активированными ключами шифрования открывает врагу мгновенный доступ ко всем текущим коммуникациям подразделения. Противник, завладевший такой радиостанцией, получает способность не только пассивно прослушивать переговоры, но и активно вмешиваться в управление войсками, имитируя голос захваченного командира и отдавая ложные приказы, ведущие подразделения в огневые мешки или провоцирующие огонь по своим позициям.

Разработка эффективных регламентов экстренной смены ключей в таких условиях перестает быть сугубо технической задачей и превращается в комплексную проблему, лежащую на пересечении криптографии, тактической психологии, эргономики боевых систем и военного права. Требуется создать такую систему реагирования, которая, будучи запущенной в считанные секунды после фиксации факта пленения, обеспечит мгновенную изоляцию скомпрометированного устройства и перестройку всей сети связи на новые криптографические параметры, при этом сохраняя управляемость подразделений, продолжающих выполнять боевую задачу. Как показывает опыт современных конфликтов, включая боевые действия на территории Украины, где система управления боем "Дельта" ежедневно подвергается массированным хакерским атакам, физические ключи безопасности становятся критическим элементом защиты наряду с программными средствами шифрования.

Природа угрозы: системный анализ последствий захвата носимых средств связи

Осмысление проблемы экстренной смены ключей невозможно без глубокого понимания тех угроз, которые порождает ситуация пленения военнослужащего, имеющего при себе действующую радиостанцию. Противник, захвативший устройство, получает в свое распоряжение инструмент, атакующий информационную безопасность своих войск сразу на нескольких уровнях. Первый и наиболее очевидный уровень – это компрометация криптографических ключей, хранящихся в памяти устройства. Современные аппаратные модули безопасности, защищенные от инженерного анализа и соответствующие стандартам TEMPEST, значительно затрудняют извлечение ключевой информации, однако не делают этот процесс абсолютно невозможным при наличии у противника соответствующей лабораторной базы и времени. Противник, располагая захваченным образцом, может применить методы крипто атаки, анализ побочных электромагнитных излучений или прямой съем информации с микросхем памяти, постепенно восстанавливая полную картину ключевого расписания подразделения.

Второй уровень угрозы, значительно более опасный в тактическом масштабе времени, – это атака на доверие, или маскарад. Даже если криптографические ключи надежно защищены и самоуничтожаются при первой попытке несанкционированного доступа, сам факт наличия у противника устройства, аутентифицированного в сети и признаваемого легитимным абонентом, создает катастрофическую ситуацию. Противник, используя захваченную радиостанцию, может инициировать ложные вызовы, передавать дезинформацию, запрашивать огневую поддержку по координатам расположения своих подразделений или, напротив, отменять уже согласованные удары по выявленным целям противника. Особую опасность представляет возможность использования захваченного устройства для внедрения вредоносного программного обеспечения в ретрансляционные узлы или командирские машины, что позволяет противнику получить долгосрочный контроль над элементами системы управления.

Третий уровень угрозы связан с нарушением синхронизации и целостности сети связи. Экстренная ситуация, вызванная пленением, неизбежно порождает информационный хаос. Командиры подразделений, не имеющие четкого алгоритма действий, могут получать противоречивые распоряжения по разным каналам связи, теряя способность к адекватной

оценке обстановки. Противник, понимая это, может искусственно инициировать множественные ложные сигналы о компрометации, перегружая систему управления и вызывая эффект отказа в обслуживании. В такой ситуации подразделение, лишенное надежной связи, становится легкой добычей для противника, действующего по отработанным схемам радиоэлектронного подавления и дезинформации.

Четвертый уровень угрозы, актуализировавшийся с распространением биометрических методов аутентификации, связан с возможностью использования противником физиологических параметров захваченного военнослужащего. Современные системы доступа, использующие отпечатки пальцев или сканирование сетчатки глаза, могут быть обмануты при прямом принуждении пленного к разблокировке устройства. Именно поэтому, как показывает практика использования системы "Дельта", украинские военные применяют комплексный подход, комбинируя физические ключи YubiKey с ограничением функциональности для передовых подразделений и системами искусственного интеллекта, отслеживающими аномальное поведение пользователей.

Архитектура реагирования: трехуровневая система действий при пленении

Эффективный регламент экстренной смены ключей должен строиться как иерархическая система, в которой каждому уровню военной вертикали соответствуют четко определенные функции, а время реакции на инцидент минимизируется за счет автоматизации ключевых процессов. Нижний уровень этой системы представлен самим военнослужащим, непосредственно владеющим радиостанцией и находящимся в зоне боевого соприкосновения. Именно этот уровень является критически важным, поскольку только боец, осознающий неизбежность пленения или потери сознания вследствие ранения, способен предпринять действия, которые невозможно автоматизировать. Регламент предписывает военнослужащему в такой ситуации активировать процедуру гарантированного стирания ключевой информации, используя механические или электронные средства, встроенные в конструкцию радиостанции.

Современные требования к аппаратному обеспечению тактической связи включают обязательное наличие физического элемента управления аварийным стиранием, такого как выдергиваемый тросик, поворотный переключатель под защитной крышкой или две одновременно нажимаемые кнопки, расположенные на значительном удалении друг от друга для предотвращения случайной активации. Эта механика должна срабатывать даже при полном отсутствии электропитания, используя энергию, запасенную в суперконденсаторах, и гарантированно уничтожать содержимое энергонезависимой памяти криптомодуля. После активации стирания или параллельно с ним военнослужащий обязан произвести максимально возможное физическое повреждение устройства, извлекая аккумулятор, деформируя корпус, разбивая антенный тракт и вынимая съемные криптографические модули, чтобы лишить противника возможности даже исследовать конструкцию аппарата.

Средний уровень реагирования представлен командиром взвода или роты, который, получив сигнал о потере связи с подчиненным или зафиксировав иные признаки его пленения, обязан инициировать первый этап цифровой изоляции скомпрометированного абонента. Действия командира должны быть максимально алгоритмизированы и не требовать аналитического осмысления в стрессовой ситуации боя. Получив подтверждение факта пленения от соседних подразделений или зафиксировав резкое прекращение передачи данных, командир направляет в вышестоящий штаб формализованное донесение, содержащее уникальный идентификатор пропавшего устройства, и, если позволяет тактическая обстановка, отдает приказ на запуск дистанционной блокировки. Одновременно с этим командир переводит свое подразделение на использование резервных каналов связи или запасных частот, заранее определенных в плане связи на данный период боя.

Верхний уровень системы реагирования представлен штабом батальона или бригады, который располагает наиболее полной информацией о состоянии сети и имеет полномочия для проведения общесистемных мероприятий. Получив подтвержденный сигнал о компрометации, оперативный дежурный или начальник связи вносит идентификатор захваченной радиостанции в общевойсковой список отзыва сертификатов, который

автоматически синхронизируется со всеми пограничными коммуникационными узлами, ретрансляторами и командирскими машинами. Одновременно с этим инициируется процедура массовой эфирной рассылки новых ключей шифрования для всего подразделения, к которому принадлежал захваченный боец. Важнейшим требованием к этой процедуре является ее селективность: новые ключи должны получать только легитимные абоненты, а скомпрометированное устройство, будучи внесенным в черный список, автоматически исключается из процесса аутентификации и лишается возможности синхронизироваться с обновленной сетью. Такой подход, реализованный, например, в системе Tactical Key Management, разработанной MIT Lincoln Laboratory, позволяет выводить устройства в поле вообще без предварительно загруженных ключей и генерировать их динамически непосредственно в ходе миссии.

Технологические решения: от предустановленных ключей к динамическому управлению

Традиционный подход к управлению криптографическими ключами в тактическом звене основывался на принципе предварительной загрузки: перед началом боевых действий все радиостанции насыщались ключевой информацией на определенный период, и в ходе операции смена ключей производилась лишь в плановом порядке или не производилась вовсе. Этот подход, обеспечивавший относительную простоту реализации, обладал фатальным недостатком: при пленении военнослужащего противник получал доступ ко всем ключам, действующим на протяжении всего периода, на который была произведена загрузка. Современные технологические решения направлены на преодоление этого ограничения через внедрение систем динамического управления ключами, позволяющих генерировать, распределять и отзывать ключи в реальном масштабе времени.

Одним из перспективных направлений является внедрение систем асимметричной криптографии на тактическом уровне, когда каждое устройство обладает уникальной парой ключей, а аутентификация абонентов производится через централизованный удостоверяющий центр. При таком подходе захват отдельного устройства не компрометирует всю сеть, поскольку скомпрометированный сертификат может быть мгновенно отозван, а все остальные абоненты продолжат работу с использованием своих индивидуальных ключей. Однако реализация инфраструктуры открытых ключей в тактическом звене сопряжена со значительными сложностями, связанными с необходимостью постоянного доступа к удостоверяющему центру, что проблематично в условиях нарушения связности и активного радиоэлектронного противодействия.

Альтернативным решением, активно развиваемым в последние годы, является использование технологий симметричной криптографии с динамическим согласованием ключей, таких как платформа Symmetric Key Agreement, разработанная компанией Arqit. Эта технология позволяет концевым устройствам самостоятельно генерировать сеансовые ключи в партнерстве с любым количеством других абонентов без необходимости предварительной загрузки ключевого материала. Ключи создаются локально на устройстве и могут обновляться с любой периодичностью, вплоть до нескольких раз в минуту. При таком подходе даже захват устройства не дает противнику доступа к будущим сеансам связи, поскольку каждый последующий сеанс будет использовать новые ключи, сгенерированные уже после компрометации.

Особого внимания заслуживает опыт применения физических ключей безопасности YubiKey в системе управления боем "Дельта", где развернуто более 30 тысяч таких устройств, из которых 22 тысячи используются исключительно в военных целях. Эти ключи, работающие на основе криптографии с открытым ключом и поддерживающие стандарт FIDO2, обеспечивают двухфакторную аутентификацию, практически неуязвимую для фишинговых атак. Важным уроком, извлеченным из боевого применения, стала необходимость учета физических ограничений: USB-версии ключей приводили к поломке портов планшетов в полевых условиях, что потребовало перехода на беспроводные версии с технологией NFC и внедрения программных версий ключей на смартфонах военнослужащих.

Интеграция с системами искусственного интеллекта и биометрического контроля.

Развитие технологий искусственного интеллекта открывает новые возможности для автоматизации обнаружения фактов компрометации и реагирования на них. Традиционные регламенты основывались на предположении, что факт пленения будет своевременно обнаружен и подтвержден командиром, однако в условиях высокодинамичного боя это предположение часто не выполняется. Противник, захвативший радиостанцию, может продолжать использовать ее в течение длительного времени, имитируя нормальную работу и передавая ложные данные, прежде чем его действия вызовут подозрения.

Системы искусственного интеллекта, обученные на моделях нормального поведения абонентов в сети, способны автоматически выявлять аномалии, свидетельствующие о возможной компрометации. Такие системы анализируют множество параметров: характер трафика, географическое местоположение устройства, частоту и продолжительность сеансов связи, используемые протоколы и даже голосовые характеристики оператора. При обнаружении значительных отклонений от нормальной модели система автоматически повышает уровень тревоги и предлагает командиру проверить подозрительного абонента или временно ограничить его доступ к критическим функциям сети.

В украинской системе "Дельта" подобные механизмы уже активно применяются: искусственный интеллект помогает выявлять и маркировать подозрительные системы, а командиры на местах получают возможность оперативно блокировать доступ для конкретных военнослужащих при появлении признаков компрометации. Такой подход позволяет нейтрализовать угрозу даже в тех случаях, когда сам захваченный боец не успел или не смог уничтожить свою радиостанцию, а командир подразделения временно утратил контроль над ситуацией.

Перспективным направлением является интеграция носимых средств связи с биометрическими датчиками, непрерывно мониторящими состояние военнослужащего. Резкое изменение физиологических параметров, характерное для ранения или экстремального стресса, может служить триггером для автоматического запуска процедур защиты. Например, при фиксации критического падения пульса или остановки дыхания устройство может самостоятельно инициировать стирание ключей и подачу сигнала тревоги, не дожидаясь действий самого бойца или его командира. Развитие таких технологий позволит создать систему защиты, работающую на опережение, блокирующую устройство еще до того, как противник получит к нему физический доступ.

Психологические и правовые аспекты имплементации регламентов.

Наиболее сложным препятствием на пути внедрения эффективных регламентов экстренной смены ключей является человеческий фактор. Военнослужащий, воспитанный в духе бережного отношения к вверенному имуществу и осознающий высокую стоимость носимой радиостанции, в критической ситуации может испытать психологический ступор, не решаясь уничтожить дорогостоящую технику. Этот ступор, длящийся всего несколько секунд, может оказаться фатальным, позволив противнику захватить устройство в полностью работоспособном состоянии.

Преодоление этого психологического барьера требует комплексной работы по нескольким направлениям. Во-первых, необходима регулярная тренировка действий по уничтожению радиостанции в ходе тактико-специальных учений, доводящая соответствующие навыки до уровня безусловного рефлекса, не требующего аналитического осмысления. Во-вторых, требуется создание четкой правовой базы, освобождающей военнослужащего от материальной ответственности за уничтожение или повреждение средств связи, если эти действия были совершены с целью предотвращения захвата секретной информации противником.

Правовая защита должна распространяться не только на самого военнослужащего, но и на его командиров, отдающих приказы на уничтожение оборудования. В условиях боевой обстановки решения часто приходится принимать на основе неполной информации, и командир, приказавший заблокировать и списать устройство, которое впоследствии могло

оказаться просто потерявшим связь, но не захваченным, не должен подвергаться дисциплинарному или материальному преследованию. Только наличие таких гарантий способно создать атмосферу, в которой командиры всех уровней будут действовать решительно, не опасаясь негативных последствий для своей карьеры.

Важным элементом психологической подготовки является разъяснение личному составу причинно-следственных связей между захватом исправной радиостанции и гибелью их товарищей. Осознание того, что промедление с уничтожением аппаратуры может привести к тому, что противник, используя захваченное устройство, наведет артиллерию на позиции своего же подразделения, должно стать более сильным мотиватором, чем страх перед дисциплинарным взысканием. Регулярные беседы, разбор боевых эпизодов и моделирование ситуаций позволяют сформировать у военнослужащих правильное понимание приоритетов: жизнь товарищей и выполнение боевой задачи важнее сохранности любой, даже самой дорогой техники.

Эргономические требования и стандарты аппаратного обеспечения.

Реализация описанных регламентов предъявляет жесткие требования к конструкции носимых средств связи, которые должны проектироваться с учетом специфики их применения в экстремальных условиях. Аппаратное обеспечение должно соответствовать стандартам TEMPEST, гарантирующим отсутствие утечек информации через побочные электромагнитные излучения и наводки, что особенно критично в момент генерации новых ключей, когда устройство наиболее уязвимо для перехвата. Кроме того, конструкция должна обеспечивать аппаратное разделение "красной" (незашифрованной) и "черной" (зашифрованной) частей схемы, исключающее возможность случайного смешивания разнородных сигналов.

Критически важным требованием является наличие механических элементов управления аварийным стиранием ключей, доступных для активации в условиях ограниченной видимости, сильного стресса и, возможно, ранения оператора. Эти элементы должны быть защищены от случайного срабатывания, но при этом располагаться в зоне легкой досягаемости и иметь тактильно различимую фактуру, позволяющую идентифицировать их на ощупь без визуального контроля. Цветовая маркировка таких элементов должна соответствовать общепринятым стандартам опасности, например, ярко-красному цвету с предупреждающими надписями, видимыми в приборах ночного видения.

Опыт боевого применения выявил еще одну важную проблему: использование USB-портов для подключения физических ключей аутентификации приводит к их быстрому механическому износу и поломкам в полевых условиях. Вибрация при движении техники, удары, попадание пыли и влаги – все это снижает надежность разъемных соединений. Решением становится переход на беспроводные интерфейсы, такие как NFC, или резервирование ключей в виде программных приложений на защищенных смартфонах военнослужащих. При проектировании новых образцов носимых средств связи необходимо предусматривать встроенные аппаратные модули аутентификации, не требующие внешних подключаемых устройств.

Важным требованием к современным криптографическим устройствам является их функциональная совместимость с различными типами радиостанций и оборудования связи, производимого разными поставщиками. В условиях ведения коалиционных действий или при использовании разнородной техники в рамках одного подразделения способность устройств взаимодействовать друг с другом становится критическим фактором боеспособности. Соответствие стандартам НАТО и национальным криптографическим стандартам позволяет обеспечить необходимый уровень интероперабельности без снижения требований безопасности.

Перспективные направления развития: постквантовая криптография и автономные системы.

Заглядывая в будущее, необходимо учитывать стремительное развитие квантовых вычислений, которые в обозримой перспективе способны поставить под угрозу всю

современную криптографию, основанную на сложности факторизации больших чисел или дискретного логарифмирования. Уже сегодня ведущие производители криптографического оборудования, такие как Yubico, демонстрируют прототипы устройств, поддерживающих постквантовые криптографические алгоритмы. Переход на постквантовую криптографию потребует увеличения вычислительных мощностей и объемов памяти, поскольку новые алгоритмы имеют значительно больший размер ключей и подписей, однако этот переход неизбежен для обеспечения долгосрочной защиты информации.

Компания Arqit уже предлагает коммерческие решения, обеспечивающие квантово-безопасную симметричную криптографию для тактического звена, позволяющие динамически генерировать ключи между доверенными конечными точками без использования инфраструктуры открытых ключей. Такие решения особенно перспективны для применения в беспилотных летательных аппаратах и роботизированных системах, где ограничения по размеру, весу и энергопотреблению (SWaP) не позволяют использовать традиционные аппаратные криптомодули. Возможность создавать эфемерные ротируемые ключи непосредственно на борту беспилотника открывает новые горизонты для безопасного управления группами дронов, действующих в условиях активного противодействия противника.

Другим перспективным направлением является развитие технологий распределенного реестра для аудита и синхронизации истории смены ключей в подразделении. Блокчейн-подобные структуры позволяют создать неизменяемую запись всех событий, связанных с генерацией, распределением и отзывом ключей, что критически важно для расследования инцидентов и восстановления хронологии событий после боя. Кроме того, такие технологии могут быть использованы для автоматизации доверительных отношений между подразделениями различных родов войск, не имеющих предварительно согласованных ключевых расписаний.

Развитие автономных систем управления ключами, не требующих участия человека в процессе реагирования на инциденты, представляет собой естественную эволюцию описанных регламентов. Автоматические системы, анализирующие данные от множества датчиков и принимающие решения о блокировке устройств на основе заданных критериев, способны реагировать на угрозы на порядки быстрее человека. Однако внедрение таких систем требует решения сложных этических и правовых проблем, связанных с передачей машине права принимать решения, потенциально влияющие на жизнь военнослужащих и выполнение боевых задач. Баланс между скоростью автоматической реакции и необходимостью человеческого контроля останется предметом дискуссий на долгие годы.

Заключение.

Проблема экстренной смены ключей при пленении личного состава не имеет простых решений и не может быть сведена к закупке более совершенной техники или написанию идеального регламента. Только системный подход, объединяющий передовые технологические решения, продуманную организационную структуру, глубокую психологическую подготовку личного состава и адекватную правовую базу, способен обеспечить тот уровень криптографической устойчивости, который требуется в современной высокотехнологичной войне.

Технологическая составляющая системы должна включать аппаратные модули гарантированного стирания, средства динамического управления ключами, интеграцию с биометрическими датчиками и искусственным интеллектом, а также защиту от будущих квантовых угроз. Организационная составляющая требует четкого распределения ответственности между всеми уровнями военной иерархии, от рядового бойца до штаба бригады, и отработки взаимодействия между ними в ходе регулярных учений. Психологическая подготовка должна формировать у военнослужащих правильные приоритеты и устойчивые навыки действий в экстремальных ситуациях, а правовая база – обеспечивать защиту тех, кто действует решительно, пусть и с риском для сохранности дорогостоящего имущества.

Опыт современных конфликтов убедительно доказывает, что противник будет постоянно искать и находить новые способы использования захваченных средств связи для проникновения в информационное пространство своих войск. Система защиты не может оставаться статичной; она должна непрерывно развиваться, адаптируясь к новым угрозам и используя новые технологические возможности. Только в этом случае можно гарантировать, что даже в условиях тяжелых потерь и тактического хаоса управляемость подразделений будет сохранена, а противник не получит ожидаемого преимущества от захвата наших средств связи

Список литературы:

1. Arqit Quantum Inc. Launches SKA Edge Controller for Quantum-Safe Deployed Military Operations. Nasdaq, July 2025.
2. Ukraine uses 30,000 physical security keys to protect DELTA combat system from cyberattacks. Mezha Media, October 2025.
3. Ukrainian army relies on YubiKeys to prevent Russian hacks. Biometric Update, October 2025.
4. Tactical Key Management. MIT Lincoln Laboratory.
5. R&S®MMC3000: Устройство шифрования повышенной прочности. Rohde & Schwarz