

Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

**59-я научная конференция
аспирантов, магистрантов и студентов**

Сборник материалов докладов

17–21 апреля 2023 года
Минск, БГУИР

УДК 004:378
ББК 32.81+74.48
И66

Инновационные технологии в образовательном процессе: материалы 59-ой конференции аспирантов, магистрантов и студентов учреждения образования «Белорусский государственный университет информатики и радиоэлектроники», 17-21 апреля 2023 г., Минск, Беларусь. – Минск : БГУИР, 2023. – 92 с.; ил.

В сборнике опубликованы материалы докладов, представленных на 59-й научной конференции аспирантов, магистрантов и студентов БГУИР. Материалы одобрены оргкомитетом и публикуются в авторской редакции.

Для научных и инженерно-технических работников, преподавателей, аспирантов, магистрантов и студентов вузов.

МЕТОДИКА КАЛИБРОВКИ ВОЛЬТМЕТРА ЦИФРОВОГО УНИВЕРСАЛЬНОГО В7-65/2

Белоус А.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Дмитренко А. А. – канд. техн. наук

Актуальность разработки методики калибровки обусловлена тем, что она является одним из самых распространённых видов метрологических работ, представляет собой один из факторов, обеспечивающих доверие к результатам измерений и испытаний продукции, что играет не последнюю роль в подтверждении её пригодности.

Калибровка средства измерений – проведение работ по метрологической оценке, в ходе которых устанавливается соотношение между значением величины, полученным с использованием средства измерений или эталона единицы величины, и значением величины, воспроизводимой и (или) хранимой национальным эталоном единицы величины, эталоном единицы величины того же рода или стандартным образцом, в целях определения действительных метрологических характеристик средства измерений [1].

Хотя поверка и калибровка включают в себя одни и те же операции, результаты калибровки могут быть более информативными. В отличие от поверки, осуществляемой аккредитованными в соответствии с законодательством об аккредитации юридическими лицами и индивидуальными предпринимателями, калибровка не подлежит обязательному государственному контролю и надзору и может проводиться любой метрологической службой, имеющей для этого надлежащие условия. Однако эта процедура, несмотря на добровольность, подразумевает соблюдение всех необходимых требований. Главное из этих требований – обязательная прослеживаемость к государственному (национальному) эталону, так называемая привязка к нему. Поскольку измерения являются частью технологических процессов и оказывают прямое влияние на качество проводимых работ, необходимо сравнение полученных результатов, чему служит эталонная размерная единица. Таким образом, калибровку следует рассматривать как составную часть государственной системы обеспечения единства измерений, а кроме того, и как часть мировой системы обеспечения единства измерений, ведь принципы национальной системы должны быть гармонизированы с международными правилами и нормами. Следует отметить, что за основу при разработке методик калибровки могут быть взяты действующие методики поверки, которые тем не менее не предоставляют всей возможной информации о средстве измерения.

Разработки методик калибровки представляется наиболее актуальной для тех предприятий, на которых такие методики отсутствуют, но которые в таких методиках нуждаются. Они должны разрабатываться в целях повышения качества калибровочных работ и, в конечном итоге, для повышения эффективности проводимых работ.

Классификация вольтметров.

Измерители напряжения являются самой многочисленной группой среди средств измерения, применяемых в радиоэлектронике. В основу классификаций вольтметров положены следующие признаки:

– вид измеряемого напряжения: вольтметры-калибраторы (В1), постоянного тока (В2), переменного тока (В3), импульсного тока (В4), фазочувствительные (В5), селективные (В6), универсальные (В7);

– тип применяемых измерительных преобразователей: электромеханические и электронные;

– тип отсчетного устройства: стрелочные (аналоговые) и цифровые вольтметры. Парк аналоговых приборов характеризуется единой конструктивной базой, идентичностью расположения органов управления, удобством эксплуатации, метрологической обеспеченностью;

– тип структурной схемы: приборы прямого преобразования и уравнивающего преобразования. Приборы уравнивающего преобразования разделяют на приборы с автоматическим и ручным уравниванием;

– значение измеряемого напряжения: пиковое (амплитудное), среднеквадратическое и средневыпрямленное;

– частотный диапазон: низкочастотные, высокочастотные, сверхвысокочастотные, широкополосные вольтметры.

Назначение и область применения В7-65/2.

Вольтметр универсальный В7-65/2 предназначен для измерения постоянного напряжения, среднеквадратического значения переменного напряжения произвольной формы, сопротивления постоянному току, постоянному и переменному токам, частоты и периода синусоидального и импульсного сигналов, он обеспечивает математическую и логическую обработку результатов измерений по программам, заложенным в вольтметре. Вольтметр В7-65/2 обеспечивает обмен информацией по последовательному асинхронному интерфейсу типа "Стык С2" в соответствии с ГОСТ 18145-81 с использованием цепей стыка 102, 103, 104, 106, 107, 108.2, 109. Может быть использован для контроля и измерения электрических параметров при поверке, настройке и эксплуатации измерительной аппаратуры.

Рабочими условиями являются:

- диапазон температуры окружающего воздуха от 5 до 40°С;
- относительная влажность воздуха до 80% при температуре 25°С;
- атмосферное давление 84 – 106,7 кПа (630 – 800 мм.рт.ст.).

Принцип действия вольтметра основан на преобразовании измеряемой величины в нормированное постоянное напряжение с последующим преобразованием методом широтно-импульсной модуляции. При измерении временных характеристик переменного напряжения (частота, период) входной сигнал преобразуется в последовательность прямоугольных импульсов эталонной частоты за период их следования. Результаты измерения представляются в форме индикации 5,5 и 4,5 десятичных разрядов.

Нормируемыми метрологическими характеристиками вольтметра универсального цифрового В7-65/2 являются:

- пределы и диапазон измерения постоянного напряжения, а так же пределы допускаемой основной погрешности;
- пределы и диапазон измерения переменного напряжения, диапазон его частот и пределы допускаемой основной погрешности;
- пределы и диапазон измерения постоянного тока, пределы его допускаемой основной погрешности;
- пределы и диапазон измерения переменного тока, диапазон его частот, а так же пределы допускаемой основной погрешности;
- пределы и диапазон измерения сопротивления постоянному току, а так же пределы его допускаемой основной погрешности;
- диапазон измерения частоты синусоидальных сигналов и пределы допускаемой основной погрешности;
- диапазон измерения частоты импульсных сигналов и пределы допускаемой основной погрешности;
- диапазон измерения периода синусоидальных и импульсных сигналов и пределы допускаемой основной погрешности.

При этом важно учитывать, что пределы допускаемой дополнительной погрешности, вызванной отклонением температуры окружающего воздуха от нормальных условий на каждые 10°С, не более значения основной погрешности.

Общие сведения о калибровке средств измерений и порядок проведения.

Калибровка измерительных приборов заключается в установлении зависимости между показаниями прибора и размером измеряемой (входной) величины. Под калибровкой часто понимают процесс подстройки показаний выходной величины или индикации измерительного инструмента до достижения согласования между эталонной величиной на входе и результатом на выходе (с учётом оговоренной точности). Например, калибровкой медицинского термометра, показывающего в ванне с температурой 36,6°С результат на дисплее 36,3°С будет добавление 0,3°С. При этом неважно, будет ли эта величина внесена в память прибора или написана на приклеенной к термометру бумаге.

Средства измерений подвергаются первичной, периодической и внеочередной калибровке. Первичной калибровке подлежат средства измерений при выпуске из ремонта и при ввозе по импорту. Периодическую калибровку должны проходить все средства измерений через определенные межкалибровочные интервалы, кроме средств измерений, находящихся на длительном хранении. Средства измерений, находящиеся в эксплуатации (на хранении), могут подвергаться внеочередной калибровке при:

- повреждении калибровочного клейма или в случае утери сертификата о калибровке;
- вводе в эксплуатацию средств измерений после длительного хранения (более одного межкалибровочного интервала);
- неудовлетворительной работе средств измерений.

Калибровка средств измерений производится в соответствии с нормативными документами, регламентирующими проведение калибровочных (поверочных) работ. Калибровка средств измерений

осуществляется физическим лицом, аттестованным на право проведения калибровочных работ, в порядке, установленном в электроэнергетике. Представлять средства измерений на калибровку следует в сроки, установленные графиками калибровки. Средства измерений, представляемые на калибровку, должны быть очищены от грязи, пыли и наружной смазки. Положительные результаты калибровки средств измерений действительны в течение межкалибровочного интервала. Метрологические службы обязаны вести учет результатов калибровки и разрабатывать рекомендации по корректировке межкалибровочных интервалов. Расчет межкалибровочных интервалов должен производиться в соответствии с МИ 2187-92 и РД 34.11.403 (МУ 34-70-023-82). Средства измерений, признанные по результатам калибровки непригодными к применению, должны направляться на ремонт. Критерием пригодности средств измерений к применению является соответствие технических и метрологических характеристик средств измерений указанным в техническом описании и инструкции по эксплуатации. При выдаче средств измерений из калибровки необходимо проверить комплектность, наличие клейм, пломб, сертификата о калибровке, записи в паспорте.

Выделяют четыре метода поверки (калибровки) средств измерений:

– метод непосредственного сличения средства измерения. Основан на использовании образцового и проверяемого приборов, а также источника физического сигнала. На входы каждого прибора подается одинаковый сигнал и одновременно осуществляется фиксация показаний. После чего путем вычислений определяется абсолютная погрешность, а затем и приведенная;

– метод сличения средства измерения с эталоном, используя компаратор. При возникновении сложности реализации предыдущего метода, схема дополняется прибором сравнения – компаратором, после чего производится поверка (калибровка). На практике есть два способа осуществления этого метода. Замещение и противопоставление. В первом случае сигнал подается поочередно на один вход компаратора, а во втором одновременная подача на два входа. В результате производится анализ полученного разностного сигнала;

– метод прямого измерения. Аналогичен первому методу, но отличие заключается в поверке всех реперных точек. Определение погрешности реализуется двумя способами: регулирование величины сигнала источника для совпадения реперной точки с указателем прибора и установление физического сигнала номинального значения, соответствующего данной реперной точке;

– метод поверки (калибровки) косвенным измерением. В данном случае производятся измерения параметров, напрямую связанных сверяемым. После чего с помощью расчетов и учета их однозначной зависимости друг с другом выявляются необходимые значения. Нужно помнить, что в этом случае, погрешность метода включает и погрешность при прямых измерениях.

Чтобы минимизировать неточности в процессе перенаправления размеров единиц измерений от эталонов рабочим устройствам, применяют специальные схемы. Их называют поверочными. Они представляют собой спецификацию, которая определяет неточности и соподчиняет все СИ, задействованные в передаче размера единицы физической величины от эталона рабочим измерительным приборам, основанном на соответствующей методике. Схемы поверки утверждают метрологическое подчинение государственного эталона, его разрядных аналогов и СИ. Государственные поверочные схемы распространяются на все СИ определенного вида, применение которых ограничено пределами страны.

Ведомственные поверочные схемы охватывают СИ заданной физической величины. При установлении для СИ одинаковых физических величин должно быть исключено их противоречие государственным аналогам. Данная разновидность устанавливается при отсутствии государственных схем поверки с возможностью указания определенных типов СИ.

Локальные поверочные схемы применяются министерскими метрологическими службами, охватывая СИ подчиненных предприятий. Они обязательно должны быть согласованы с требованиями соподчиненности, утвержденными государственными схемами поверки, разработчиками которых являются обладатели государственных эталонов - НИИ Госстандарта РФ.

Ведомственные и локальные разновидности выполняются в форме чертежей. Госстандарт устанавливает государственные схемы поверки, тогда как их локальные версии определяются службами метрологии или главами предприятий.

Данным нормативным документом определяется регламент передачи размера одной и более единиц измерений физических величин от эталонов рабочим устройствам. В нем обязательно должны содержаться, как минимум, две ступени передачи.

Список использованных источников:

1. Постановление Государственного комитета по стандартизации Республики Беларусь от 23 апреля 2021 г. № 42 «Об утверждении Правил осуществления метрологической оценки в виде работ по калибровке средств измерений».

СИСТЕМА БОРЬБЫ С БПЛА «ГРОЗА-Р»

Босак Д.И.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Лавринчик Н.Н.

Гроза-Р (белор. Навальніца-Р) — белорусское радиоэлектронное ружьё для борьбы с мультикоптерами, разработанное ОАО «КБ Радар». Создавалось в рамках серии комплексов и средств радиоэлектронной борьбы «Гроза».

Впервые разработка была представлена на выставке IDEX-2017 в ОАЭ. В 2018 году 12 ружей «Гроза-Р2» поступили на вооружение в 387-й центр технического контроля и обеспечения защиты информации Вооружённых Сил Республики Беларусь.

Как всем известно, беспилотные летательные аппараты уже давно активно используются во время проведения боевых кампаний по всему миру. Разведка, огневая поддержка, доставка грузов — у роботов весьма широкий спектр задач. Разумеется, эта проблема не осталась незамеченной, а потому инженеры уже вовсю создают оружие, направленное на уничтожение вражеской беспилотной робототехники. Основой для «Грозы-Р» стала пневматическая винтовка Сума СМ.011, используемая для страйкбольных состязаний.

Ружьё для беспилотных летательных аппаратов разборное, так что во время транспортировки аккумулятор и антенну-глушитель нужно переносить отдельно, они подключаются к корпусу непосредственно перед стрельбой с помощью кабеля. Принцип работы «Грозы-Р» довольно прост. На винтовке установлены 3 антенны, суммарно охватывающие 30 сектор. Их задача заключается в заглушении вражеских сигналов: радиосигналы глушатся на расстоянии до 2 км, а сигналы со спутников — до 5 км.

Лишившись связи с оператором, дрон теряет управление, после чего или разбивается от падения с высоты (если он летающий), или становится добычей противника. Для прицела используется оптика Sturman 1x38 RD. «Гроза-Р» — винтовка не из легких: если сам корпус весит всего 2 кг, то вот система заглушки и зарядная станция — все 10. А заряжать придется часто, особенно во время длительной «охоты», поскольку заряда аккумулятора хватает на 1 час постоянно работы. Стоит отметить, что мы уже писали про подобные разработки: DroneGun (на видео ниже), военная противодронная винтовка США была представлена общественности еще осенью прошлого года. Также обращаем внимание на еще более раннюю разработку — Drone Defender, одно из первых ружей подобного назначения.

23 октября 2020 года пограничники заставы «Знаменка» Брестской погрангруппы с помощью радиоэлектронного ружья «Гроза-Р2» перехватили гексакоптер, который использовался для переброски сигарет через белорусско-польский участок границы. 22 февраля 2021 года ещё один дрон с грузом контрабандных сигарет был перехвачен пограничниками в Каменецком районе близ деревни Чижевичи. 6 апреля на белорусско-польской границе в Брестском районе недалеко от деревни Сычи перехвачен третий беспилотник.

Винтокрылый летательный аппарат предназначался для незаконной переправки табачных изделий. 18 мая на границе с Литвой радиоэлектронным ружьём сбит беспилотник НАТО. Отмечалось, что это уже не первый случай, когда делается попытка использования беспилотников-шпионов вблизи границ Белоруссии.

Как заявил заместитель начальника Генерального штаба Вооружённых Сил Республики Беларусь Игорь Король, в течение недели делается около 30 попыток незаконного использования дронов Североатлантического альянса. При всех своих преимуществах, самоходный комплекс «Гроза-С» имеет определенный недостаток в виде габаритов и массы. В некоторых случаях войскам или спецслужбам нужна аналогичная система с меньшими размерами, пригодная для переноски силами оператора. В ответ на подобные нужды потенциальных эксплуатантов был разработан комплекс «Гроза-Р». В связи с характерным обликом эта система уже получила прозвище «радиоэлектронная винтовка».

Главной задачей проекта «Гроза-Р» было максимальное сокращение габаритов всех систем, в том числе ценой некоторого ухудшения характеристик в сравнении с полноценным самоходным комплексом РЭБ. Поставленные задачи были успешно решены при помощи нескольких оригинальных идей. Результат проектных работ был впервые представлен широкой публике всего несколько дней назад. Площадкой для первой демонстрации «радиоэлектронной винтовки» стала международная выставка IDEX-2017, проходившая в Объединённых Арабских Эмиратах.

С целью упрощения процесса разработки и производства с одновременным получением приемлемых результатов авторы проекта «Гроза-Р» решили использовать некоторые готовые компоненты. В качестве основного элемента комплекса, отвечающего за удобство эксплуатации, был

выбран корпус страйкбольной автоматической винтовки Сума SM0011 китайского производства, имитирующей немецкую Heckler & Koch G36C.

При переделке готовое изделие лишилось всех внутренних устройств и некоторых других деталей. Вместо исходных компонентов в корпусе были смонтированы новые, такие как клавиша включения на бывшей шахте магазина и т.д. Для установки антенных устройств, сошки и прицела предлагается использовать штатные планки Пикатинни, изначально имеющиеся на базовом изделии. На передней части «винтовки» крепятся три сравнительно крупных радиопрозрачных кожуха с антеннами. Имеются два кожуха с вертикальной ориентацией, помещенные справа и слева от основного корпуса. Третий кожух, отличающийся меньшим сечением, находится ниже двух других. Ввиду наличия кожухов конфигурация антенн неизвестна.

Учитывая известные сведения о других подобных проектах, можно предположить, что внутри радиопрозрачных изделий находятся антенны типа волновой канал. В приемную шахту магазина помещена заглушка, имеющая разъем для подключения кабеля подачи сигналов. Фактически сама «винтовка» является лишь антенным устройством, не имеющим собственных средств генерации сигнала. За формирование радиосигнала отвечает т.н. блок нелинейных искажений, помещенный в отдельном защищенном корпусе. С винтовкой-излучателем он соединяется при помощи кабеля. Блок имеет собственные аккумуляторные батареи, а также набор необходимой радиоэлектронной аппаратуры.

Предлагаемый комплекс «Гроза-Р» может работать в двух режимах, отличающихся характером выдаваемых помех. Возможно простое «глушение» определенных диапазонов или подавление сигналов спутниковых систем навигации. В первом режиме оператор может выставить подавление в диапазонах 2,4-2,485 ГГц или 5,76-5,88 ГГц.

Такой режим предназначен для подавления радиоканалов управления беспилотных летательных аппаратов. Вторым вариантом использования блока нелинейных искажений позволяет подавить рабочие частоты систем GPS, ГЛОНАСС, Galileo и «Бэйдоу». По имеющимся данным, продемонстрированный в ОАЭ образец «радиоэлектронной винтовки» белорусской разработки получил коллиматорный прицел типа Sturman 1x38 RD. Это устройство закреплено на верхней планке Пикатинни и предназначается для наведения «оружия» на беспилотный летательный аппарат.

За счет большого диаметра входного зрачка и иных особенностей конструкции такой прицел должен обеспечивать сравнительную простоту и удобство использования «винтовки». Помимо самой «винтовки» и связанных с ней приборов комплекс РЭБ «Гроза-Р» имеет в своем составе рюкзак для транспортировки, складную двуногую сошку и зарядное устройство. Общая масса комплекса – около 10 кг. Из них 2 кг приходится на винтовку-антенное устройство.

Блок нелинейных искажений весит менее 8 кг. При переводе в походное положение блок с электроникой отсоединяется от «винтовки». С последней могут сниматься антенны вместе с кожухами. Все это обеспечивает правильную укладку в транспортный ранец, облегчающую переноску силами оператора. В боевом положении «винтовка» переносится в руках, тогда как электронный блок остается в ранце за спиной оператора.

Принцип работы оригинального комплекса достаточно прост. При визуальном или ином обнаружении БПЛА противника, оператор должен включить блок нелинейных искажений и выбрать требуемый режим работы, после чего следует навести «оружие» на цель. Электромагнитное воздействие в течение определенного времени (зависит от ряда факторов, в первую очередь, от типа БПЛА) приводит к подавлению канала управления, из-за чего оператор теряет возможность контролировать беспилотный летательный аппарат.

Для борьбы с автономно работающими аппаратами следует использовать подавление сигналов спутниковой навигации, не позволяющее технике продолжать работу по заложенной программе. Утверждается, что одна зарядка аккумуляторов позволяет комплексу «Гроза-Р» выполнять подавление радиоканалов (при непрерывной работе передатчика) в течение 1 часа. Помехи распространяются в секторе шириной 30°. Максимальная дальность подавления каналов управления – 5 км, «глушения» спутниковой навигации – 3 км.

Бурное развитие беспилотных летательных аппаратов и широкое распространение подобных систем делает актуальным вопрос борьбы с такой техникой. В разных странах предпринимаются различные попытки создания специализированных «противодроновых» систем или адаптации существующих комплексов к решению новых задач.

Список использованных источников:

1. <https://bte.by/katalog/sredstva-radioelektronnay-borby/radioelektronnnoe-ruzhe.html>.

ПРОБЛЕМАТИКА БОРЬБЫ С БПЛА

Бутевич П.А.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Назаров Д.Г.

Аннотация. Проблематика борьбы с беспилотными летательными аппаратами, приоритетные направления в борьбе с дронами.

Беспилотный летательный аппарат (дрон) – летательный аппарат без пилота на борту.

Дроны могут решать разный перечень задач, связанных с их основными особенностями – автономностью управления, относительной дешевизной производства. За счёт этого они стали крайне востребованы в вооруженных силах различных государств и стали неотъемлемой частью любого вооруженного конфликта. В результате этого проблема борьбы с ними очень остро стала в РЭТ ВВС и войсках ПВО нашего государства.

Главными проблемами для ПВО являются малозаметность дронов, их дешевизна производства и многозадачность. Из опыта локальных войн и вооруженных конфликтов можно отметить, что БПЛА боевого предназначения обнаруживаются либо визуальным способом наблюдения, либо на дальних подступах, но уничтожение дрона экономически нецелесообразно из-за отношения цены ракеты и беспилотника. Также аппараты без пилота работают в основном на крайне низких высотах, что ещё больше затрудняет их обнаружение. Как итог для РТВ важнейшей задачей являются разработка успешных систем обнаружения беспилотников на предельно низких высотах и повышения незаметности радиолокационных станций (РЛС).

Как одним из способов достижения поставленной задачи является усовершенствование систем передачи информации и принятия решения, для ускорения процесса выдачи данных по цели и скорейшего поражения аппарата противника. Для этого необходимо создать закрытые каналы передачи информации между подразделениями РТВ и обеспечивающих их эффективное уничтожение группировкой войск, а также систему быстрой передачи информации на пункты принятия решения. Важным моментом хочу отметить, что пересмотр системы в целом может принести значительные результаты, но это требует время на рассмотрение проекта, что, перспективно, но не решит проблему в ближайшее время.

Разработка новых систем связи или модернизация старых может привести к ускорению процесса доведения информации, что, в будущем, тоже может привести к успехам в данном вопросе. Одним из вопросов является перевод стационарной системы связи на цифровые способы передачи и обработки информации, модернизация имеющихся на вооружении подвижных комплексов связи для повышения их качественных показателей, разработка и внедрение современных средств и комплексов связи в различных звеньях управления, создание унифицированной автоматизированной системы управления связью на всех уровнях военного управления, обеспечение информационной безопасности системы связи. Все работы проводятся с использованием передовых информационно-телекоммуникационных технологий и направлены на достижение условий для интеграции доступа и услуг, высокой пропускной способности и устойчивости при обеспечении управления войсками (силами) и оружием во всех звеньях управления в любых условиях обстановки.

С целью дальнейшего развития территориальной системы связи Вооруженных Сил, резервирования сети электросвязи общего пользования Республики Беларусь, удовлетворения потребностей в цифровых каналах связи в настоящее время спроектированы и построены стационарные магистральные цифровые радиорелейные линии связи 1-й очереди и выполняются работы по строительству 2-й очереди, общая протяженность которых составит более 1.000 километров. Результатом строительства магистральных цифровых радиорелейных линий связи станет выход системы связи Вооруженных Сил на принципиально новый, более высокий уровень развития. В целом это позволит значительно повысить устойчивость и пропускную способность системы связи Вооруженных Сил, а также снизить финансовые затраты на аренду каналов связи.

При этом, порядка 50% ОКР выполняется в интересах войск связи за счет денежных средств инновационных фондов Госкомвоенпрома, а также предприятий Республики Беларусь. Для управления современной цифровой системой связи Вооруженных Сил создана автоматизированная система, решающая задачи мониторинга и автоматизации управления, контроля и отображения информации о состоянии цифровых систем связи и их элементов. Эта система позволяет в короткий срок принимать оптимальные решения при кризисных ситуациях и доводить распоряжения до подчиненных пунктов управления связью в реальном масштабе времени [1].

Также не менее важной проблемой является обнаружение БПЛА на предельно низких высотах. Кроме того, беспилотники обладают низкими характеристиками, обусловленные их выполнением из композитных материалов и пластика со специальной окраской с особой комбинацией слоев, небольшими бензиновыми и тем более электрическими двигателями, мало излучающие тепло, и

работающие почти бесшумно для из обнаружения, что делает их выявление ещё труднее. Поэтому, для эффективного выполнения задачи необходимо одновременное использование нескольких способов обнаружения. Наибольшую уязвимость МБЛА обуславливает наличие у них электромагнитного излучения.

К ЭМ демаскирующим признакам относятся: сигналы бортового ответчика; сигналы радиолокационных станций, отраженные от корпуса и агрегатов МБЛА; сигналы телевизионных ретрансляторов, широкоэмитерных станций, базовых станций сотовой связи, отраженные от МБЛА; команды и «доклады» канала управления между наземным пунктом управления и МБЛА, а также между МБЛА и спутником-ретранслятором системы навигации; сигналы бортовой РЛС бокового обзора; каналы обмена разведывательной информацией; сигналы системы автоматической посадки на аэродром. Основными способами обнаружения МБЛА в электромагнитном спектре являются: использование тепловизора инфракрасного диапазона ЭМ волн; использование камер оптического диапазона ЭМ волн; использование радиолокационных станций; осуществление радиомониторинга. Для выявления объектов с отличающейся от окружающей среды температурой используются инфракрасные тепловизионные камеры, что позволяет вести наблюдение с помощью за МБЛА даже в условиях ограниченной видимости и в темное время суток. Для получения наиболее информативных и стабильных результатов возможно точное совмещение тепловизионных снимков с видимым изображением.

Для этого применяется тепловизор и фотокамера для одновременного ведения аэрофотосъемки в видимом диапазоне. Получаемые инфракрасные изображения в оттенках серого могут быть преобразованы в псевдоцветные, где темным оттенкам соответствуют низкие температуры, а светлым – высокие. Для обнаружения МБЛА в оптическом диапазоне ЭМ волн существует активные и пассивные методы. Активными методами считается метод анаглифов и метод определения координат МБЛА в пространстве. Пассивные методы включают в свой состав метод визуального наблюдения и метод комбинированного стереоэффекта. Основным средством обнаружения БПЛА являются радиолокационные станции. В ряде случаев МБЛА являются сложной целью для существующих РЛС. Эти аппараты имеют малую эффективную площадь рассеяния (ЭПР), из-за чего их обнаружение становится достаточно сложной задачей. В частности, снижается максимальная дальность обнаружения [2]. Однако несмотря на данные недостатки дальности обнаружения дронов остаются крайне малы для РЛС всех диапазонов. Увеличение дальности обнаружения беспилотников требует использование комбинированных методов, что приводит к увеличению стоимости систем обнаружения.

В следствии необходимо производить модернизацию образцов для повышения дальности обнаружения малозаметных целей. Создание небольших и мощных систем приведёт к повышению обороноспособности против дронов, однако данные разработки требуют больших финансов и крайне неэффективны, так как не применимы в ближайшее время. Данные системы требуют время на процесс разработки, обкатку, ввод в эксплуатацию, что перспективно на будущее время. Также не стоит забывать про то, что РЛС должны эффективно работать не только по одному конкретно виду целей. Как результат необходимо производить модернизацию или разработку, не ухудшая характеристики обнаружения по остальным высотам и целям. Однако к значительному успеху в ближайшее время не приведёт, что оставит проблему.

В результате необходимость разработки способа координации между пунктами выдачи информации и штабами, обусловленная малой дальностью обнаружения возрастает.

Как один из методов борьбы с дронами хочу отметить повышение маскирующих характеристик РЛС. Не смотря на высокую разрешающую способность при съёмке беспилотниками, БПЛА управляются операторами. Ошибки при считывании информации человеком не исключены. В результате этого уменьшение визуальной заметности приведёт к снижению эффективности обнаружения дронами радиолокационных станций, что приведёт к обнаружению беспилотника раньше, чем обнаружится станция. Уменьшение габаритов антенных систем и покраска в цвет местности, нанесение защитных камуфляжей, использование специальных приспособлений для уменьшения визуальной заметности, выбор позиции РЛС в лесах – всё это приведёт к повышению маскирующих свойств станций. Однако нецелесообразный выбор позиции приведёт к уменьшению дальности обнаружения. Как итог БПЛА не выполнит свою задачу по предназначению что приведёт к снижению эффективности дронов.

Как итог совокупность решения данных проблем позволит улучшить систему борьбы против беспилотников и повысит эффективность обнаружения и скорость выдачи информации, что закономерно приведёт к усилению обороноспособности государства и выводу из «игры» дроны.

Список использованных источников:

1. https://www.mil.by/special/ru/news/press_center/press_releases/8439_
2. <https://russiandrone.ru/publications/metody-obnaruzheniya-malorazmernykh-besplotnykh-letatelnykh-apparatov-na-osnove-analiza-elektromagn/>

БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ РЕСПУБЛИКИ БЕЛАРУСЬ

Войтович Б.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь.

Хожевец О.А.

Аннотация. Современные виды беспилотных летательных аппаратов Республики Беларусь.

Hunter (с англ. «охотник») — белорусский разведывательно-ударный беспилотный вертолёт производства КБ «Беспилотные вертолёты». Может применяться в составе российского беспилотного авиационного комплекса БАС-750.



Рисунок 1 – Белорусский разведывательно-ударный беспилотный вертолёт «Hunter».

Аппарат был презентован 23 июня 2021 года, в первый день международной оружейной выставке «MILEX—2021» в Минске. Вместе с ним дебют был и у броневика Volat V2. На первом показе символическую ленточку перерезали Председатель Госкомвоенпрома Дмитрий Пантус, главный конструктор КБ «Беспилотные вертолёты» Владимир Чудаков и Председатель Президиума НАН Беларуси Владимир Гусаков.

Испытания дрона, по состоянию на июнь 2022 года, все ещё продолжались. Беспилотник предназначен для работы в городских условиях. Основной задачей является уничтожение огневых точек противника в труднодоступных местах.

К бортовой защите дрона относятся станция защиты от радиолокационных ракет, станция радиационного предупреждения и барьерный радар. Навигация осуществляется оптико-электронной инерциальной системой, метеорологической радиолокационной станцией и радиовысотометром. Управление аппарата осуществляется на наземной станции управления (НСК). Она способна управлять двумя беспилотными вертолётами одновременно для выполнения парных боевых вылетов, а также реализовать уникальные программные средства обработки и представления информации. В станцию входят передвижной пункт, внешний источник питания с бензиновым генератором и заправочная станция на 800 литров бензина.

Машина полностью роботизирована, оснащена 52 микроконтроллерами, внутри неё организована нейросеть. Для выполнения задачи ей нужно только задать цель и направление. Однако применение оружия дроном возможно исключительно при контроле человека.

«Hunter» оснащён 7,62-мм пулемётом Калашникова танковой модификации с боекомплектом в 550 патронов, восемью 57-мм неуправляемыми ракетами и 16 противотанковыми бомбами. Пулемёт способен вести стрельбу до 1,5 км. Ракеты осуществляют залп на расстоянии 1,8 км.

Продолжительность полёта составляет 9 часов при максимальной скорости 180 км/ч. Предельная масса для взлета — 750 кг, из которых 200 может составлять полезный груз. Аппарата дрона, в зависимости от типа и расположения камеры, распознает транспорт на расстоянии 7—9,2 км, а человека — 4,5—6,2. Дальность целеуказания составляет 3 км.

В июне 2022 года СМИ сообщили о грядущем появлении у ВС России ударных вертолётных беспилотников. Газета «Московский комсомолец» писала, что масса аппарата составит 750 кг при 200 кг полезной нагрузки. Как отметил главный редактор издания «Беспилотная авиация» Денис Федутин, поскольку в России таких дронов нет, то речь может идти о закупке зарубежных моделей,

а именно, беспилотного летательного аппарата «Hunter», который как раз подходит под опубликованные характеристики. По его словам, за последние годы белорусские разработчики сумели существенно развить свои компетенции в области беспилотной техники, поэтому для россиян их опыт был бы ценен в развитии отечественной продукции. Федутинов упомянул, что ранее специалисты из Белоруссии привлекались к работе над более лёгким российским вертолётным дроном БАС-200.

Буревестник МБ — белорусский военный беспилотный летательный аппарат, разработанный научно-производственным центром «Беспилотные авиационные комплексы и технологии» при Физико-техническом институте НАН РБ.



Рисунок 2 – Беспилотный летательный аппарат «Буревестник»

Работа началась в 2011 году [1]. Разработка военного дрона белорусскими учёными и инженерами-конструкторами велась на базе гражданского беспилотного летательного аппарата модели «Буревестник». За счёт этого удалось существенно сократить стоимость проекта, а также сроки его создания. Фактически, беспилотный летательный аппарат модели. Первым лётным испытаниям дрон подвергся в 2016 году. Аппарат успешно справился с поставленными задачами, а проект стал подготавливаться к началу своего производства [2].

БПЛА выполнен по двухбалочной схеме с толкающим воздушным винтом. Его масса — до 300 килограммов, максимальная скорость — до 200 километров в час, крейсерская — 80–120, диапазон рабочих высот — от 200 до 3500 метров. Взлетает со взлетно-посадочной полосы или хорошо утрамбованных грунтовых площадок. Важной характеристикой является гарантированная дальность передачи информации и связи на расстоянии до 290 километров. При этом задержка сигнала практически не ощущается. В автономном режиме полёта по заранее составленной программе его дальность может достигать более 1000 километров при продолжительности полета до 10 часов^[3].

Дрон может нести гиростабилизированную платформу с фото-, видео- и инфракрасными камерами. Они могут снимать качественное видео и фото с расстояния до 3000 метров. Зум позволяет увеличивать объект съёмки в двадцать раз. На аппарат можно устанавливать модуль радиационного мониторинга. Он измеряет радиационный фон на высоте до 300 метров. Вся собранная информация в режиме реального времени передается оператору на экран наземного пункта управления. Также БПЛА может взять на борт до 60 килограммов другой полезной нагрузки^[3].

«Буревестник МБ» представляет собой самостоятельную боевую единицу, способную наносить точные удары по позициям противника, для чего на вооружении дрона находятся несколько ракет, способных наносить серьёзный ущерб как живой силе противника, так и бронированной технике [1].

На борту БПЛА могут быть размещены два барражирующих боеприпаса выполненных в виде малых дронов одноразового действия («дроны-камикадзе») массой 26 кг каждый, способных во время автономного полета вести разведку и наблюдение для обнаружения цели. Каждый такой миниатюрный аппарат имеет боевую часть массой 10 кг взрывчатого вещества. Для наведения на цель БПЛА использует оптико-электронный и вычислительный комплексы, позволяющие ему поражать заданный объект с точностью до 1-2 м. При старте с носителя на высоте 3,5 км дальность удара составит не менее 36 км. Причем после запуска барражирующего боеприпаса в цель команду на поражение можно отменить и аппарат вернется на заданную высоту для продолжения разведки и перенацеливания [3].

Оптимальный состав команды для запуска «Буревестника» — 3-5 человек. В эту группу входят оператор, специалист по бортовому оборудованию, техник самолёта, водитель и начальник расчёта. Разработано несколько вариантов пункта управления: переносной, передвижной на базе МАЗа и стационарный. В каждом по три рабочих места: оператора дрона, оператора целевой нагрузки и начальника расчёта [3].

Роль беспилотников в качестве ударного средства в современных военных конфликтах сложно переоценить. Они проявили себя как универсальное оружие, способное поражать наземные и

морские цели, а также выполнять попутно ряд других военных задач, таких как разведка и корректировка огня. Особого внимания заслуживают дроны-камикадзе, или барражирующие снаряды. Это сравнительно новый вид ударных БПЛА, которые обладают рядом преимуществ. Ввиду высокой эффективности этого оружия, его стали разрабатывать многие страны. В частности, в прошлом году свои дроны-камикадзе представила и Беларусь. Предлагаем далее подробнее разобраться что это за аппараты, какими характеристиками обладают и для каких целей могут использоваться.

Как не сложно догадаться из названия, дроны-камикадзе — это БПЛА одноразового использования. По сути, они представляют собой обычный небольшой беспилотник, в корпусе которого содержится снаряд. Поэтому их еще называют “барражирующими снарядами”. Запустить такой беспилотник можно только один раз.

В чем преимущества этого оружия? Дроны-камикадзе имеют компактные размеры, они незаметны для систем РЛС, при этом летят практически беззвучно. В результате сбить такой дрон крайне сложно, хотя возможно. Беспилотник способен поражать цели на больших расстояниях, вести разведку, а также барражировать и ожидать подходящего момента для нанесения удара, к примеру, пока цель выйдет из укрытия.

Главное отличие от ракет или, к примеру, артиллерии, заключается в том, что барражирующий снаряд может найти цель после запуска. То есть дрон может выйти в зону нахождения цели и затем провести доразведку для нанесения точного удара. При этом система наведения барражирующего снаряда гораздо более простая и дешевая, чем самонаводящиеся головки ракет. Разумеется, сам дрон тоже недорогой, поэтому его не страшно потерять, в отличие от таких БПЛА, как Байрактар или Орион.

Единственный минус этого оружия — оно требует связи с оператором, в отличие от тех же ракет. Поэтому дальность полета ограничена. Правда, некоторые модификации израильских беспилотников-камикадзе HERO способны поражать цели на расстоянии более 100 км. Кроме того, мощность заряда дронов значительно меньше чем у ракет, так как грузоподъемность у них обычно невысокая.

Дроны-камикадзе могут поражать живую силу противника, легкобронированную технику, а также, как показывают последние события, даже промышленные объекты. Очевидно, роль беспилотников-камикадзе в военных конфликтах со временем будет только возрастать.

ОАО “558 Авиационный ремонтный завод” впервые представили ударные беспилотники “Чекан” и “Ловчий” в июне 2021 года. Информации о них еще не так много, тем не менее некоторые данные уже известны.

УБЛА-25 “Чекан” представляет собой тактический авиационный комплекс с БПЛА одноразового применения. Он классифицируется как тактический разведывательно-ударный комплекс малой дальности, который предназначен для поиска, обнаружения и поражения живой силы и легкоуязвимой техники противника в светлое время суток.

В состав комплекса входит наземный пункт управления, а также два ударных одноразовых барражирующих снаряда и пусковое устройство. Дальность действия дрона составляет 25 км. На борту беспилотника может быть установлен осколочно-фугасный либо кумулятивный боеприпас.

Максимальная взлетная масса БПЛА составляет 12 кг, при этом сама боевая часть весит 2 кг. “Чекан” способен подниматься на высоту до 200 метров. Его крейсерская скорость составляет 90 км/ч.

Дрон камикадзе “Ловчий”, или “Охотник”, (не путать с российским тяжелым ударным беспилотником “Охотник”, о котором мы рассказывали ранее) более тяжелый и мощный, чем «Чекан». Он способен нести полезную нагрузку весом до 20 кг, при этом радиус его действия тоже значительно выше — достигает 70 километров.

Ранее я также рассказывал о российских дронах-беспилотниках “Куб” и “Ланцет”, разработанных концерном Калашникова. Эти аппараты сильно отличаются от американских аналогов, при этом обладают впечатляющими характеристиками. К примеру, “Ланцет” оснащен четырьмя парами крыльев, что обеспечивает высокую маневренность БПЛА.

Как я писал выше, свой дрон-камикадзе также разработал Израиль, а точнее израильская компания UVision Air. HERO 120 аналогично российскому “Ланцету” имеет восемь крыльев. К слову, на момент разработки российского БЛА эта технология была уникальной. Масса аппарата составляет 12,5 кг, при этом он может нести боеголовку весом 4,5 кг. Также свои дроны-камикадзе разрабатывают и другие некоторые страны.

Список использованных источников:

1. https://ru.wikipedia.org/wiki/%D0%91%D0%B5%D1%81%D0%BF%D0%B8%D0%BB%D0%BE%D1%82%D0%BD%D1%8B%D0%B9_%D0%BB%D0%B5%D1%82%D0%B0%D1%82%D0%B5%D0%BB%D1%8C%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BF%D0%BF%D0%B0%D1%80%D0%B0%D1%82
2. https://ru.wikipedia.org/wiki/%D0%91%D1%83%D1%80%D0%B5%D0%B2%D0%B5%D1%81%D1%82%D0%BD%D0%B8%D0%BA_%D0%9C%D0%91
3. <https://hi-news.ru/technology/beloruskie-drony-kamikadze-chekan-i-lovchij.html>

МЕТОДИКА КАЛИБРОВКИ НИЗКОЧАСТОТНОГО ГЕНЕРАТОРА

Гладков А.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Дмитренко А. А.– канд. техн. наук

Развитие многих направлений науки и техники определяются точностью измерения времени и частоты. Из семи основных физических величин (длина, масса, время, сила электрического тока, термодинамическая температура, сила света и количество вещества) эталоны времени и частоты являются самыми точными. Это свидетельствует о том внимании, которое проявляет общество в процессе научной и производственной деятельности к вопросам измерения времени и его производной – частоты. Государственный первичный эталон времени и частоты, базирующийся на группе квантовых мер частоты (водородных, цезиевых, рубидиевых генераторов), обеспечивает воспроизведение единицы времени – секунды и единицы частоты – герца.

Измерения частоты – наиболее точный и быстро развивающийся вид измерений. Во-первых, единица времени (частоты) является основной единицей системы СИ; во-вторых, определение секунды связано с пересчетом событий, а пересчет является самым точным методом измерений; в-третьих, повышение точности измерений частоты необходимо для прикладного использования в телекоммуникациях, навигации, космической отрасли.

Устройство и принцип действия. Генератор является радиоэлектронным устройством, в зависимости от вида сигнала содержащий разные функциональные узлы. Общими узлами, для разных видов генераторов, являются: источник исходного сигнала (перестраиваемый автогенератор или кварцевый синтезатор частоты), усилители, выходные формирователи сигнала, выходной аттенюатор, цепи управления, цепи стабилизации выходного уровня и блок питания. Дополнительно в составе генератора могут быть различные модуляторы, формирователи временных интервалов и другие компоненты. В некоторых генераторах форма выходного сигнала синтезируется цифровым методом, с помощью ЦАП. Существуют также генераторы сигнала оптического диапазона, их работа основана на принципах квантовой электроники

Измерительный генератор – это источник электрических колебаний с заранее известными параметрами, предназначенный для исследования, настройки и проверки функционирования электрических цепей и устройств [1].

Они отличаются от обычных генераторов:

- возможностью установки высокой точности частоты и уровня выходного напряжения;
- регулировкой выходных параметров в широких пределах;
- высокой стабильностью и наличием измерительных приборов, контролирующих эти параметры;
- возможностью совместной работы с другими электронными средствами.

Измерительные генераторы характеризуются следующими параметрами:

- частотные параметры (характеризуют диапазон частот генерируемых колебаний, точность установки частоты и ее стабильность);
- параметры выходного напряжения или мощности (определяют напряжение на входе аттенюатора – опорное);
- пределы плавного или ступенчатого изменения выходного напряжения;
- сопротивление нагрузки, а также точность и стабильность установленного уровня выходного напряжения.

Основными нормируемыми метрологическими характеристиками измерительных генераторов являются:

- пределы и диапазон частот;
- пределы и диапазон уровней воспроизводимых сигналов;
- погрешность установки частоты;
- нестабильность частоты;
- погрешность установки выходного напряжения.

Структурная схема измерительного генератора представлена на рисунке 1.

Задающий генератор (ЗГ) – это основной функциональный узел, определяющий частоту и форму генерируемых сигналов. В зависимости от вида измерительного генератора это может быть:

- генератор синусоидальных колебаний;
- генератор периодической последовательности импульсов;
- генератор шума.

Преобразователь в зависимости от вида измерительного генератора может выполнять следующие функции:

- повышение уровня сигнала (усилитель напряжения или мощности);
- придавать сигналу определенную форму (модулятор).

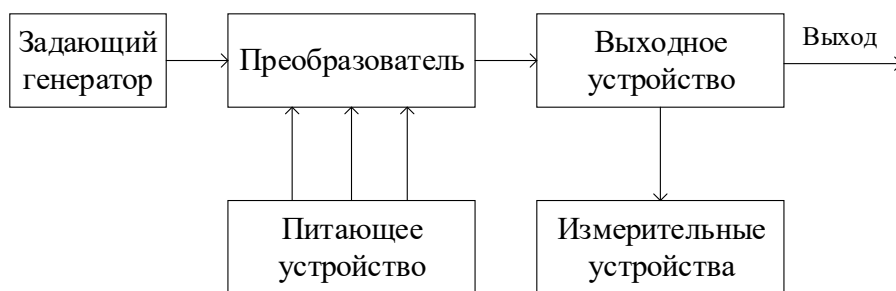


Рисунок 1 – Обобщенная структурная схема измерительного генератора

Классификация. По ГОСТ 15094 генераторы подразделяются на 6 видов: низкочастотные, высокочастотные, импульсные, сигналов специальной формы, шумовых сигналов и качающейся частоты. Однако, следует учитывать, что классификационные границы условны, некоторые генераторы занимают промежуточное положение между низко- и высокочастотными, некоторые бывают комбинированными по виду сигнала. Для оптических генераторов существует аналогичная классификация. Кроме генераторов стандартизованных видов бывают генераторы отраслевого назначения (в составе контрольно-измерительной аппаратуры).

Виды генераторов. Генератором радиосигнала называется устройство, в котором энергия одного или нескольких внешних источников преобразуется в энергию высокочастотных колебаний (радиосигнала). Генератор всегда включает в себя нелинейный генераторный прибор, в котором и происходит это преобразование, внешние электрические цепи источники питания.

Виды генераторов:

1. По форме выходного сигнала:

- синусоидальных сигналов (генератор Мейснера, генератор Хартли (индуктивная трёхточка), генератор Колпитца (ёмкостная трёхточка) и др.);

- прямоугольных импульсов — мультивибратор;

- функциональный генератор — прямоугольных, треугольных и синусоидальных импульсов.

2. По частотному диапазону:

- низкочастотные;

- высокочастотные.

3. По принципу работы:

- кварцевым резонатором;

- блокинг-генератор;

- RC-генератор.

Исследуемый генератор. Генератор ГЗ-109 предназначен для регулировки, испытания и ремонта различных радиотехнических и радиоэлектронных устройств в телевидении, радиовещании, акустике, технике связи. Чаще всего используется для проверки приборов с меньшим классом точности.

Применяется генератор ГЗ-109 в лабораторных и цеховых условиях. Так же радиотехнические устройства нуждаются в пуско-наладочных и ремонтных работах. Для этого необходимо использование низкочастотного генератора сигналов. К такому виду приборов относится генератор сигнала ГЗ-109 (RC-типа), который обладает четырьмя поддиапазонами, в пределах которых возможна плавная установка частоты (что является необходимым и крайне удобным в работе с радиотехническими устройствами). Представленный генератор ГЗ-109 имеет как несимметричный, так и симметричный выходы, которые рассчитаны на подключение ряда согласованных нагрузок. Также генератор ГЗ-109 имеет повышенную мощность на выходе и стабилизатор выходного напряжения. Это все обеспечивает большую универсальность генератора.

ГЗ-109 характеризуется низким уровнем гармонических искажений, имеет достаточно широкий диапазон генерируемых частот от 20 Гц до 200 кГц, что в свою очередь даёт обширный спектр использования донного устройства, повышенная выходная мощность обеспечивают универсальность генератора, так же обеспечивается выходной сигнал прецизионной (обладающий высокой точностью или созданный с соблюдением высокой точности параметров) формы. Измерительный генератор сигналов низкой частоты ГЗ-109 имеет функцию памяти на сохранение настроек. Это позволяет сэкономить время, затрачиваемое на настройку прибора.

На замену ГЗ-109 выступает ряд модифицированных низкочастотных генераторов различной конфигурации, таких как ГЗ-102, ГЗ-118, ГЗ-119, ГЗ-122. Поверка устройства производится по техническому описанию, для чего необходим ряд сторонних (Электронный частотомер ЧЗ-54 для измерения выходной частоты генератора, вольтметр Ф5263, В7-28 для определения выходного напряжения генератора) приборов, имеющих соответствующие требования для проведения поверки. В данном случае нас интересует только измерения погрешности частоты на всех 4 (множители $1, 10, 10^2, 10^3$) диапазонах с плавной установкой частоты.

Калибровка. Калибровка представляет собой набор действий, определяющих взаимосвязь между значениями измеряемой величины, указанной калибруемым измерительным прибором, и соответствующими значениями физических величин, осуществляемых с помощью стандартных единиц измерения и с учетом неопределенности измерения. В простейшем случае эта процедура заключается в определении разницы между показанием стандарта и показанием калибруемого прибора с учетом неопределенности измерений. Целью калибровки является определение метрологических свойств калибруемого прибора, определение его пригодности для проведения измерений или подтверждение того, что калиброванный прибор соответствует определенным метрологическим требованиям (поверка). Доказательством, подтверждающим метрологические свойства откалиброванного прибора, является документ, выданный лабораторией, и именуемый как сертификат о калибровке (поверке) с указанными символами аккредитации. Во время калибровки необходимо поддерживать согласованность измерений, также известную как Прослеживаемость, составляющую непрерывную привязку калибруемого прибора по национальному или международному стандарту.

Что такое калибровка? Многие проводят в полевых условиях сравнение двух измерителей и называют их "калиброванными", если они дают одинаковые показания. Это не калибровка. Это всего лишь проверка в полевых условиях. Она может показать наличие проблемы, но не позволит узнать, какой из приборов дает правильные показания. Если нарушена калибровка обоих измерителей, на одинаковую величину и в одном направлении, то сравнение ничего не даст. Для эффективной калибровки ее стандарт должен быть точнее, чем испытываемый прибор. У большинства из нас имеется микроволновка или другой бытовой прибор, отображающий время в часах и минутах. Большинство из нас живет в местах, где часы переводят как минимум два раза в год, да еще после отключения электричества. Устанавливая время на таком бытовом приборе, что вы используете в качестве эталонного хронометра? Вы используете часы с индикацией секунд? Метрологическая лаборатория действует по тому же принципу. Они проверяют, насколько точно ваши "полные минуты" совпадают с правильным количеством секунд. Обычно для калибровки требуется стандарт, точность которого как минимум в 10 раз выше испытываемого прибора. В противном случае вы проводите калибровку в пределах пересекающихся допусков, и допуски вашего стандарта превращают правильно откалиброванный прибор в неправильно откалиброванный, или наоборот.

Периодичность калибровки. Рассмотрим следующие интервалы калибровки:

- Интервал калибровки, рекомендуемый производителем. В спецификациях производителя указано, как часто требуется выполнять калибровку приборов, однако для наиболее важных измерений могут потребоваться другие интервалы.

- Перед наиболее критичным проектом измерений. Предположим, что вы останавливаете предприятие для проведения испытаний, в которых требуются исключительно точные измерения. Определите, какие приборы вы будете использовать для этих испытаний. Отправьте их на калибровку, после чего "заприте в кладовке", чтобы их не использовали до начала испытаний.

- После наиболее критичного проекта измерений. Если вы зарезервировали откалиброванные измерительные приборы для конкретных испытаний, отправьте это оборудование на калибровку после окончания испытаний. Получив результаты калибровки, вы узнаете - можно ли считать результаты испытаний полными и надежными.

- После события. Если ваш прибор подвергался ударным воздействиям — что-то привело к срабатыванию внутренней защиты от перегрузки или прибор подвергся резкому удару — отправьте его на калибровку и проверьте заодно целостность защитного контура.

- По необходимости. Для некоторых измерительных задач требуется откалиброванное сертифицированное измерительное оборудование — независимо от масштабов проекта. Обратите внимание, что это требование может быть не указано явным образом, а просто ожидается — обратитесь к спецификациям до начала испытаний.

Измерительное оборудование, точно также, как и электрооборудование, требует испытаний:

- Ежемесячно, ежеквартально или раз в полгода. Если вы выполняете важные измерения и делаете это часто, то сокращение интервала калибровки означает снижение вероятности постановки под сомнение результатов испытаний.

- Ежегодно. Если вы выполняете как очень важные, так и малозначимые измерения, то ежегодная калибровка - это оптимальный баланс между осторожностью и затратами.

- Раз в два года. Если вы редко проводите критически важные измерения и не подвергаете прибор неблагоприятным воздействиям, то калибровка с большим интервалом позволит сэкономить средства.

Список использованных источников:

1. Газпром колледж Волгоград [Электронный ресурс]. – Режим доступа <https://volgogradcollege.gazprom.ru/d/textpage/53/339/izmeritelnye-generatory.pdf>.

РАЗВИТИЕ РЭТ ВВС И ВОЙСК ПВО

Крижик В.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Маргель А.Б.

Аннотация. Преимущества и тактико-технические характеристики белорусской радиолокационной станции "РЛС П-18БМА".

В настоящее время ВВС и войска ПВО продолжают развиваться как важнейший вид Вооруженных Сил Республики Беларусь, основной задачей которого является завоевание и удержание господства в воздухе при отражении любой военной угрозы в отношении Беларуси. Прикрытие от ударов с воздуха становится важнейшей государственной задачей, а противовоздушная оборона приобретает новое качество и, наряду с силами ответного удара, становится решающим фактором сдерживания агрессии.

Ежедневно к несению боевого дежурства по противовоздушной обороне в ВВС и войсках ПВО привлекается более 500 военнослужащих и лиц гражданского персонала. Личный состав, задействованный на боевом дежурстве, ежедневно сопровождает более 400 воздушных судов. Активно ведется разработка и внедрение в войска автоматизированных систем управления ВВС и войсками ПВО. Применение автоматизированных систем управления увеличивает эффективность боевого управления ВВС и войсками ПВО. Приоритетным направлением развития вооружения и военной техники на ближайшую перспективу будет оставаться модернизация основных образцов, как авиационной техники, так и техники зенитных ракетных и радиотехнических войск, имеющих для этого потенциал. Одним из таких образцов ВВСТ является РЛС П-18. РЛС П-18 является двухкоординатной РЛС метрового диапазона волн и предназначена для обнаружения ВО, определения их текущих координат (наклонной дальности, азимута) и принадлежности. Кроме того, при сопряжении с высотомерами с ВИКО обеспечивается полуавтоматическое целеуказание на высотомеры по азимуту и наклонной дальности для определения высоты полета ВО.

РЛС П-18 может использоваться для:

- обнаружения воздушных целей при автономной работе, а также для наращивания радиолокационного поля при сопряжении с РЛС 5Н84А, П-19 и П-37;
- ввода данных о воздушных целях в автоматизированные системы управления (АСУ);
- полуавтоматического целеуказания (по азимуту, углу места и дальности) зенитным ракетным комплексам (ЗРК) при сопряжении с радиовысотомером ПРВ-13;
- определения трех координат воздушных целей (наклонной дальности, азимута и высоты) при работе в составе РЛК, состоящего из РЛС П-18 и радиовысотомера ПРВ-16;
- расширения возможностей по обнаружению и проводке маловысотных целей при сопряжении с РЛС П-19 с отображением радиолокационной информации на одном индикаторе;
- обеспечения наведения и полетов истребительной авиации в приаэродромных подразделениях, а также совмещенных с ПНА.

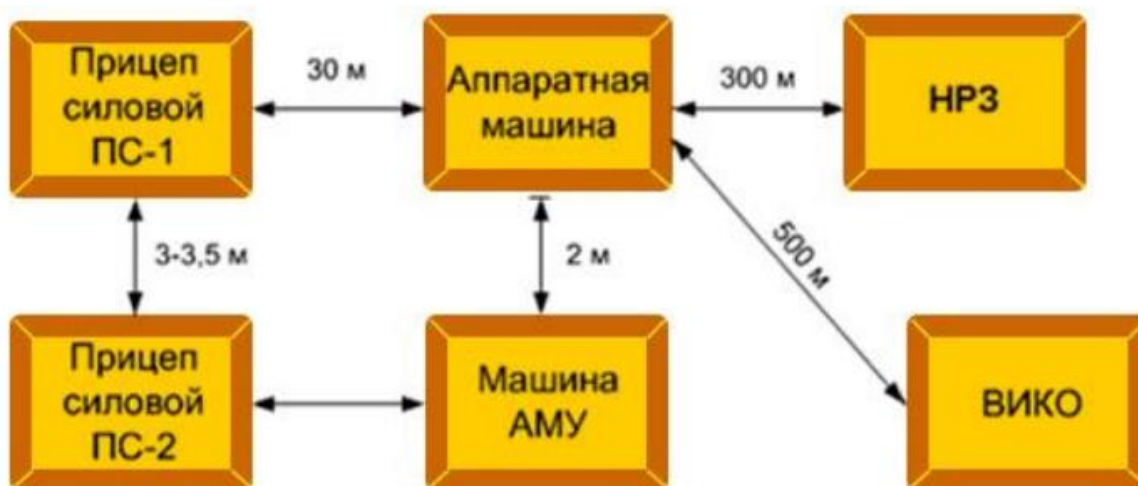


Рисунок 1 - Схема размещения элементов РЛС П-18 на позиции.

РЛС П-18БМА – РЛС метрового диапазона волн, предназначена для определения координат (азимут, дальность, высота при сопряжении с подвижным высотомером ПРВ-16БМ-А) и характеристик целей (скорость, курс, государственная принадлежность, пеленг источника помех), их автоматического сопровождения и выдачи РЛИ автоматизированным способом на комплексы средств автоматизации 7В960 (7В970) «РИФ-Р» («РИФ-В») по аппаратуре передачи данных (2С07, 2С06) и неавтоматизированным способом (считывания РЛИ голосом по цифровым данным формуляров или табло АРМ (автоматизированное рабочее место)) в координатах «азимут – дальность» или квадратах сетки ПВО, приема, отображения и обработки РЛИ от другой аналогичной РЛС или от РЛС, оснащенной экстрактором. Общий вид РЛС представлен на рисунке 2.

В состав РЛС входят:

- аппаратная машина, в которой размещается основная электронная аппаратура РЛС, – машина № 1;
- машина с антенно-мачтовым устройством (АМУ) – машина № 2;
- прицеп силовой (ПС)-1-3 и ПС-2-3;
- комплект кабелей внешнего подключения.



Рисунок 2 - Внешний вид РЛС П-18БМА

Боевые возможности РЛС.

Зона обнаружения РЛС в вертикальной плоскости формируется в соответствии с диаграммой направленности антенны (ДНА) и характеризуется:

- пределами обнаружения по углу места и радиусом «мертвой воронки»;
- потолком беспровального сопровождения;
- максимальной дальностью обнаружения.

Пределы обнаружения по углу места характеризуются следующими данными:

- нижняя граница зоны обнаружения (\min) составляет десятки минут;
- верхняя граница (\max) составляет 30° при горизонтальном положении антенны;
- радиус «мертвой воронки» $R_{m.v} = 2H_c$.

Список использованных источников:

1. Боевое применение средств радиолокации военного назначения : учеб. пособие / В. В. Навойчик [и др.]. – Минск : БГУИР, 2022. – 290 с. : ил. ISBN 978-985-543-615-8.

РАДИОЛОКАЦИОННАЯ СТАНЦИЯ «ТРАССОВЫЙ РАДИОЛОКАЦИОННЫЙ КОМПЛЕКС «СОПКА»»

Некрасов Н.С.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Беккеров Д.Э.

Аннотация. Преимущества и тактико-технические характеристики радиолокационной станции "Сопка".

Трассовый радиолокационный комплекс (ТРЛК) «Сопка» S-диапазона предназначен для использования в качестве источника радиолокационной информации для систем управления воздушным движением и контроля воздушного пространства.

Одновременно в ТРЛК организован отдельный канал для получения метеорологической информации аналогичной информации, получаемой от специализированных метеолокаторов.

ТРЛК «Сопка» обеспечивает обнаружение воздушных объектов (ВО), измерение дальности, азимута и угла места (высоты) целей, определение государственной принадлежности; получение дополнительной информации по каналу МВРЛ/НРЗ, передаваемой бортовыми ответчиками, объединение радиолокационной информации (РЛИ), получаемой от ПОРЛ, ВРЛ и НРЗ, а также выдает обработанную информацию потребителям по согласованным протоколам на средства отображения. По желанию Покупателя ТРЛК может комплектоваться аппаратурой АЗН-В.

Антенное устройство первичного радиолокатора - фазированная антенная решетка (ФАР) с частотным управлением положения луча в вертикальной плоскости; антенны МВРЛ и НРЗ - моноимпульсные антенные решетки, расположенные с тыльной стороны антенны ПОРЛ («спина-к-спине»). Вращение по азимуту обеспечивается безредукторным приводом вращения.

Передающее устройство ПОРЛ - твердотельное, с синфазным суммированием мощности 64 модулей с воздушным охлаждением, средняя излучаемая мощность на выходе передатчика не менее 4 кВт. Амплитудно-фазовая стабильность передающего устройства обеспечивает коэффициент подавления отражений от местных предметов не менее 50 дБ. Передатчик работает в режиме «мягкого отказа», замена отказавших модулей может производиться в процессе работы без выключения излучения

Приемное устройство ПОРЛ многоканальное, состоит из 4 основных и 4 резервных каналов (100% резервирование). Каждый канал имеет однократное преобразование частоты с коэффициентом шума не более 3 дБ.

Динамический диапазон приемного устройства не менее 60 дБ по выходу промежуточной частоты. Каждый канал выполнен в виде отдельного интегрированного блока (модуля), выход из строя одного или нескольких приемных каналов не приведет к отказу ПОРЛ, т.к. в этом случае происходит автоматическое переключение на резервный комплект. Замена неисправных приемных модулей возможна в процессе работы ПОРЛ.

ОСНОВНЫЕ ОСОБЕННОСТИ ТРЛК «СОПКА»:

- трехкоординатный твердотельный цифровой радиолокационный комплекс;
- высокие тактико-технические и эксплуатационные характеристики;
- возможность работы без постоянного присутствия персонал-Высокая надежность с автоматическим резервированием;
- автоматизированная система диагностики и контроля;
- современные методы обработки сигналов и информации;
- встроенный метеоканал;
- сопряжение с любыми центрами УВД.

ПРЕИМУЩЕСТВА ПО ИСПОЛЬЗОВАНИЮ ВАРИАНТА ТРЛК «СОПКА» С ПЕРЕВОЗИМЫМ АНТЕННЫМ МОДУЛЕМ:

- сокращаются сроки ввода ТРЛК в эксплуатацию и замена существующих РЛС типа П-35/ П-37 с использованием ранее созданных радиолокационных позиций без существенных затрат;
- сокращается трудоемкость технического обслуживания антенного модуля; - Ветровые нагрузки до 50 м/с обеспечиваются без дополнительных работ по креплению прицепа на горке;
- антенный модуль проходит приемо-сдаточные испытания (ПСИ) непосредственно на заводе-изготовителе и транспортируется без разборки; - Исключается необходимость проведения проектно-изыскательских и строительных работ для установки башни;
- возможность использования существующей инфраструктуры РЛП старого парка РЛС типа П-35/ П-37 и других с минимальной подготовкой площадки и коммуникаций;

– появляется возможность изменения места развертывания ТРЛК «Сопка-2» и его транспортирования на другую позицию

ТРЛК «Сопка» обеспечивает:

- обнаружение воздушных судов, измерение дальности, азимута и высоты целей;
- получения через канал МОВРЛ/ОСЧ дополнительных данных,
- передаваемых бортовыми ответчиками, объединения РЛИ, получаемой от ПОРЛ, ВОРЛ и РЛС ОСЧ, а также выдачи обработанной информации пользователям с использованием согласованных протоколов на средства отображения.



Рисунок 1 – Сопка

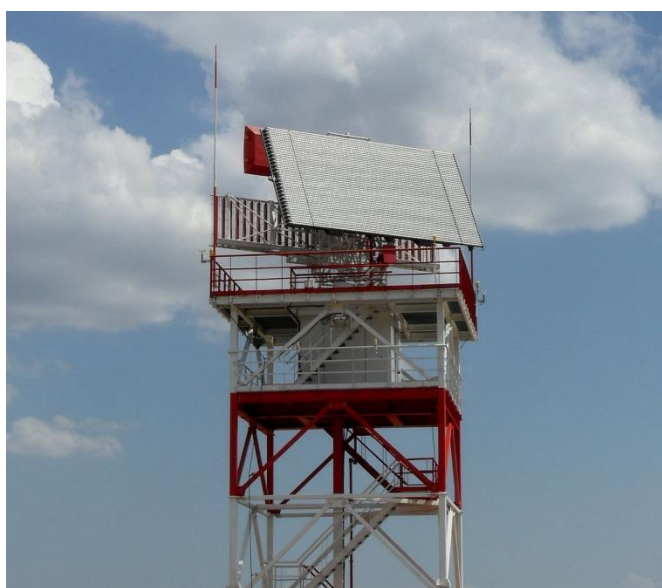


Рисунок 2 – Сопка-2

Список использованных источников:

1. <https://lemz.ru/%D1%81%D0%BE%D0%BF%D0%BA%D0%B0-2/>

ТРАССОВЫЙ РАДИОЛОКАЦИОННЫЙ КОМПЛЕКС «СОПКА-2»

Никулин Н.С.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Лавринчик Н.Н.

Аннотация. Преимущества и тактические характеристики белорусской радиолокационной станции «Сопка-2».

Трассовый радиолокационный комплекс (ТРЛК) «Сопка-2» S-диапазона предназначен для использования в качестве источника радиолокационной информации для систем управления воздушным движением и контроля воздушного пространства.

Одновременно в ТРЛК организован отдельный канал для получения метеорологической информации аналогичной информации, получаемой от специализированных метеолокаторов.

ТРЛК «Сопка-2» обеспечивает обнаружение воздушных объектов (ВО), измерение дальности, азимута и угла места (высоты) целей, определение государственной принадлежности; получение дополнительной информации по каналу МВРЛ/НРЗ, передаваемой бортовыми ответчиками, объединение радиолокационной информации (РЛИ), получаемой от ПОРЛ, ВРЛ и НРЗ, а также выдает обработанную информацию потребителям по согласованным протоколам на средства отображения.

По желанию Покупателя ТРЛК может комплектоваться аппаратурой АЗН-В.

Антенное устройство первичного радиолокатора - фазированная антенная решетка (ФАР) с частотным управлением положения луча в вертикальной плоскости; антенны МВРЛ и НРЗ - моноимпульсные антенные решетки, расположенные с тыльной стороны антенны ПОРЛ («спина-к-спине»). Вращение по азимуту обеспечивается безредукторным приводом вращения.

Передающее устройство ПОРЛ - твердотельное, с синфазным суммированием мощности 64 модулей с воздушным охлаждением, средняя излучаемая мощность на выходе передатчика не менее 4 кВт. Амплитудно-фазовая стабильность передающего устройства обеспечивает коэффициент подавления отражений от местных предметов не менее 50 дБ. Передатчик работает в режиме «мягкого отказа», замена отказавших модулей может производиться в процессе работы без выключения излучения.



Рисунок 1 - Трассовый радиолокационный комплекс «Сопка-2»

Приемное устройство ПОРЛ многоканальное, состоит из 4 основных и 4 резервных каналов (100% резервирование). Каждый канал имеет однократное преобразование частоты с коэффициентом шума не более 3 дБ.

Динамический диапазон приемного устройства не менее 60 дБ по выходу промежуточной частоты. Каждый канал выполнен в виде отдельного интегрированного блока (модуля), выход из

стройка одного или нескольких приемных каналов не приведет к отказу ПОРЛ, т.к. в этом случае происходит автоматическое переключение на резервный комплект. Замена неисправных приемных модулей возможна в процессе работы ПОРЛ.

Многоканальная аппаратура цифровой обработки сигналов построена на цифровых сигнальных процессорах и программируемых логических интегральных схемах (ПЛИС). Аналого-цифровое преобразование принятого сигнала производится на промежуточной частоте с формированием амплитудно-частотной характеристики с помощью цифровых фильтров, обеспечивающих высокую идентичность характеристик каналов и их фазовую стабильность. Внутрипериодная обработка сигналов (сжатие, подавление несинхронных импульсных помех) реализуется на ПЛИС.

Межпериодная обработка (селекция движущихся целей, адаптация к скорости ветра, виду и параметрам пассивных помех) осуществляется на сигнальных процессорах. Процессор первичной обработки осуществляет формирование пакетов и вычисление координат воздушных объектов, формирование пеленгов постановщиков активных помех, формирование карт пассивных помех.

Процессор вторичной обработки осуществляет траекторную обработку и отождествление информации ПОРЛ с данными МВРЛ/НРЗ. Сопровождение траекторий воздушных объектов возможно по информации, получаемой из любого канала (ПОРЛ или МВРЛ / НРЗ).

Встроенный моноимпульсный вторичный радиолокатор «Лири-ВМ» соответствует нормам ИКАО (Приложение 10), ГОСТ Р 51845- 2001 и обеспечивает определение координат и получение дополнительной (полетной) информации по каналу МВРЛ, передаваемой бортовыми ответчиками по стандарту RBS, в том числе и в режиме «S», а также государственное опознавание ВО во всех режимах системы «Пароль».

Встроенная система управления позволяет в автоматическом режиме реализовывать программы обзора, производя обнаружение и сопровождение ВО, оборудованных соответствующими приемоответчиками.

Отличительной особенностью построения аппаратуры МВРЛ является использование полностью цифровой резервированной аппаратуры обработки ответных сигналов с кодированием на промежуточной частоте и цифровым фазовым детектированием.

Управление включением и чередованием режимов запроса осуществляется автоматически по данным процессора вторичной обработки информации.

Автоматизированная система контроля и управления обеспечивает диагностирование устройств РЛК с целью локализации неисправностей и отказов с точностью до сменного элемента (типового элемента замены) и автоматическую или ручную реконфигурацию систем по результатам контроля работоспособности РЛК, дистанционное включение (выключение) и управление режимами работы.

Высокая надежность обеспечивается полным дублированием оборудования с автоматическим резервированием, наличие контроля и дистанционного управления обеспечивает возможность работы без постоянного присутствия обслуживающего персонала.

Аппаратура ТРЛК смонтирована в контейнере типа «Универсал», имеющем все необходимые условия для работы аппаратуры и персонала (вентиляция, кондиционирование воздуха, отопление, освещение, пожарная и охранная сигнализация, система автоматического пожаротушения и т.д.).

Основные технические характеристики:

Пределы работы:	
по дальности, км (ПРЛ/МВРЛ)	370 / 450
По азимуту, град.	360
По углу места, град.	45
по высоте, км	35
Точность определения координат (СКО)	
для ПРЛ: по дальности, м	10
по азимуту, угл. мин	15
по углу места, угл. мин	50
для МВРЛ / НРЗ: по дальности, м	6
по азимуту, угл. мин	
Разрешающая способность:	
для ПРЛ: по дальности, м	250
По азимуту, град.	1,3
для ВРЛ: по дальности, м	100
По азимуту, град.	0,6
Вероятность объединения координат ПРЛ и ВРЛ с выхода АПОИ:	
по одному самолету, не менее	0,95
полетной информации	0,96
Темп обновления информации, с	10
Количество одновременно сопровождаемых трасс целей, не менее	300
Энергопотребление, кВА, не более	40
Среднее время наработки на отказ, ч	20 000

Основные особенности:

Трехкоординатный твердотельный цифровой радиолокационный комплекс;
Высокие тактико-технические и эксплуатационные характеристики;
Возможность работы без постоянного присутствия персонала;
Высокая надежность с автоматическим резервированием;
Автоматизированная система диагностики и контроля;
Современные методы обработки сигналов и информации;
Встроенный метеоканал; Сопряжение с любыми центрами УВД.



Рисунок 2 - Шкаф МОВРЛ



Рисунок 3 - Передатчик ТРЛК «Сопка-2»



Рисунок 4 - Трассовый радиолокационный комплекс «сопка-2» в перевозимом варианте исполнения

ТРЛК «Сопка-2» с перевозимым антенным модулем разработан для реализации возможности Заказчика использовать существующую инфраструктуру радиолокационных позиций (РЛП) от старого парка РЛС (типа П-35/ П-37 и других) с минимальной подготовкой площадки и коммуникаций

Преимущества по использованию варианта трлк «сопка-2» с перевозимым антенным модулем:

- Сокращаются сроки ввода ТРЛК в эксплуатацию и замена существующих РЛС типа П-35/ П-37 с использованием ранее созданных радиолокационных позиций без существенных затрат;
- Сокращается трудоемкость технического обслуживания антенного модуля;
- Ветровые нагрузки до 50 м/с обеспечиваются без дополнительных работ по креплению прицепа на горке;
- Антенный модуль проходит приемо-сдаточные испытания (ПСИ) непосредственно на заводеизготовителе и транспортируется без разборки;
- Исключается необходимость проведения проектно-изыскательских и строительных работ для установки башни;
- Возможность использования существующей инфраструктуры РЛП старого парка РЛС типа П-35/ П-37 и других с минимальной подготовкой площадки и коммуникаций;
- Появляется возможность изменения места разворачивания ТРЛК «Сопка-2» и его транспортирования на другую позицию.

Список использованных источников:

1.. <https://lemz.ru/wp-content/uploads/2019/10/%D0%A2%D0%A0%D0%9B%D0%9A-%D0%A1%D0%9E%D0%9F%D0%9A%D0%90-2-%D0%A0%D0%A3%D0%A1.pdf>

МЕТОДИКА КАЛИБРОВКИ ОСЦИЛЛОГРАФА УНИВЕРСАЛЬНОГО

Парахневич А. В.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Дмитренко А. А. – канд. техн. наук

В настоящее время всё больше развиваются и совершенствуются различные приборы для измерения. Повышение их точности, надежности и степени автоматизации приводят к необходимости создания новых методов и средств контроля их метрологических характеристик. Это, в свою очередь, требует разработки новых технологий и средств их метрологической поверки, калибровки и сертификации.

Калибровка средства измерений – проведение работ по метрологической оценке, в ходе которых устанавливается соотношение между значением величины, полученным с использованием средства измерений или эталона единицы величины, и значением величины, воспроизводимой и (или) хранимой национальным эталоном единицы величины, эталоном единицы величины того же рода или стандартным образцом, в целях определения действительных метрологических характеристик средства измерений.

Поскольку калибровка является добровольной, а не обязательной метрологической процедурой, то межкалибровочный интервал не регламентируется. Вместе с тем, в методике калибровки могут содержаться рекомендации по установлению межкалибровочного интервала.

Калибровка средств измерений не заменяет поверку, которой в обязательном порядке подлежат все средства измерений, предназначенные для использования в сфере государственного регулирования обеспечения единства измерений.

Калибровка проводится по методикам, предоставленным Заказчиком.

Калибровка может осуществляться по методикам поверки, утвержденным в рамках проведения испытаний в целях утверждения типа, а также по методикам, приведенным в международных, региональных, межгосударственных или национальных стандартах.

Нередко методику калибровки приходится разрабатывать специально под конкретные задачи исследования.

При необходимости методики калибровки разрабатываются с учетом требований постановления Государственного комитета по стандартизации Республики Беларусь 23 апреля 2021 г. № 42 «Об утверждении Правил осуществления метрологической оценки в виде работ по калибровке средств измерений».

Однако калибровка как процедура метрологического контроля, осуществляемая аккредитованной метрологической службой юридического лица, в ряде случаев отличается от поверки.

Например, при калибровке возможно определение характеристик погрешности средства измерений в одной точке диапазона измерений в условиях, отличающихся от нормальных, что принципиально отличает ее от поверки как операции допускового контроля основной погрешности средства измерений в нормальных условиях.

Средство измерения признается пригодным, если действительные значения его метрологических характеристик соответствуют ранее установленным техническим требованиям. Вывод о пригодности средства измерения в этом случае делает калибровочная лаборатория.

Таким образом, калибровка отличается от поверки по техническому и организационному содержанию. Калибровка по своему техническому содержанию может быть шире или уже, чем поверка, в зависимости от конкретных требований заказчика. Кроме того, результаты периодической поверки действительны в течение межповерочного интервала. Результаты калибровки действительны только на момент калибровки, а решение о дальнейшей эксплуатации и установлении межкалибровочного интервала принимает лицо, эксплуатирующее средство измерения.

В организационном содержании поверка является обязательной функцией, осуществляемой органами государственного метрологического надзора, другими уполномоченными на то органами, организациями, а калибровка является добровольной функцией, осуществляемой как государственными научными метрологическими институтами или органами государственного метрологического надзора, так и метрологическими службами юридических лиц. Аккредитация на право проведения калибровки средств измерений осуществляется только в соответствии с желанием заинтересованной метрологической службы юридического лица.

Электронные осциллографы являются одним из самых важных инструментов для любого инженера в радиоэлектронике. Они позволяют измерять и анализировать различные электрические сигналы, которые используются в радиоэлектронике.

Применение электронных осциллографов в радиоэлектронике имеет множество преимуществ.

Во-первых, они обладают высокой точностью измерений, что является важным фактором в работе с электронными сигналами.

Во-вторых, они позволяют измерять широкий спектр частот, что позволяет исследовать различные типы сигналов, включая как низкочастотные, так и высокочастотные.

Кроме того, электронные осциллографы обладают возможностью быстрого анализа сигналов, что позволяет исследовать их характеристики в реальном времени. Это особенно важно при работе с сигналами, которые изменяются во времени, такими как сигналы в радиосвязи или в системах управления.

Еще одним преимуществом использования электронных осциллографов в радиоэлектронике является возможность быстрого и точного обнаружения и измерения помех и сигналов низкой амплитуды, которые могут быть трудными для обнаружения с помощью других методов измерения.

Электронные осциллографы также широко применяются при отладке и исправлении неисправностей в радиоэлектронной аппаратуре. Они позволяют инженерам быстро определить местонахождение проблемы и вносить необходимые корректировки для ее устранения.

Однако, для того чтобы электронные осциллографы работали с требуемой точностью, необходимо периодически калибровать их.

В процессе эксплуатации, могут возникнуть сбои в работе или изменения в точности измерений, поэтому калибровка необходима для правильности измерений и получения точных результатов измерений.

Калибровка осциллографа включает в себя несколько этапов, таких как калибровка коэффициента отклонения, коэффициента развертки. Для выполнения этих калибровок может потребоваться использование калибровочных сигналов и калибровочных схем.

В состав обобщенной структурной схемы осциллографа входят, ЭЛТ со схемой управления лучом, канал вертикального отклонения (канал Y), канал горизонтального отклонения (канал X), канал управления яркостью (канал Z) и калибраторы амплитуды и длительности.

В осциллографах применяют широкополосные ЭЛТ с электростатическим управлением лучом. Они могут иметь один или несколько лучей.

Номенклатура основных параметров канала Y включает основную погрешность измерения напряжения, параметры коэффициента отклонения, параметры переходной характеристики и параметры входа Y. По определению, коэффициент отклонения – это постоянная канала Y обратная его чувствительности. Он характеризуется диапазоном калиброванных значений и основной погрешностью. Основная погрешность нормируется для различных классов точности осциллографов в соответствии стандартом.

В связи с тем, что современные осциллографы, как правило, используются для исследования импульсных сигналов, их характеризуют не АЧХ, а переходной характеристикой. Ей соответствует изображение на экране ЭЛТ, получаемое при подаче на вход Y перепада напряжения с длительностью фронта 0,3 и менее от времени нарастания характеристики.

К основным параметрам канала X относятся основная погрешность измерения временных интервалов, параметры коэффициента развертки и параметры синхронизации. Основная погрешность измерения временных интервалов нормируется в соответствии стандарта и также определяет класс точности осциллографа. Коэффициент развертки характеризуется диапазоном калиброванных значений и основной погрешностью.

Важно отметить, что калибровка должна проводиться только уполномоченными юридическими лицами на калибровку. Так же калибровка должна осуществляться в соответствии с методиками калибровки, в качестве которых могут использоваться методики калибровки, установленные международными, межгосударственными и государственными стандартами, а также методики калибровки, разработанные уполномоченными юридическими лицами на калибровку на основе иерархической схемы калибровки.

Таким образом, регулярная калибровка электронных осциллографов является необходимым шагом для обеспечения точности измерений и надежности средства измерения. Это позволяет получать более точные результаты и сохранять высокую эффективность работы в течение всего периода эксплуатации.

Актуальность разработки методики калибровки обусловлена тем, что калибровка, является одним из самых распространенных видов метрологических работ, представляет собой один из факторов, обеспечивающих доверие к результатам измерений.

Список использованных источников:

1. ГОСТ 8.009-84 Государственная система обеспечения единства измерений. Нормируемые метрологические характеристики средств измерений.
2. ГОСТ 8.311-78 Государственная система обеспечения единства измерений. Осциллографы электронно-лучевые универсальные. Методы и средства поверки.

ТРЕХКООРДИНАТНАЯ РАДИОЛОКАЦИОННАЯ СТАНЦИЯ «ВОСТОК 3D»

Салей Ф.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Назаров Д.Г.

Аннотация. Преимущества и тактико-технические характеристики радиолокационной станции «Восток 3D».

РЛС семейства «Восток» разрабатываются конструкторским бюро «Радар», являющимся управляющей компанией холдинга «Системы радиолокации». Результатом достаточно длительных работ уже стало появление нескольких проектов радиолокационных станций разного назначения, отличающихся друг от друга теми или иными особенностями. Последними на данный момент представителями семейства являются станции «Восток-3D» и «Восток-3D VHF». Они были созданы на основе более старых образцов, однако имеют заметные отличия. В частности, благодаря расширенной функциональности одна такая станция может заменить сразу два образца техники предыдущей модели.

Как мы можем понять из названия, целью проекта «Восток-3D» было создание трехкоординатной радиолокационной станции, способной определять все параметры воздушной цели: ее высоту и дальность до нее. Для решения подобной задачи было предложено монтировать на одной самоходной антенно-аппаратной машине обновленный комплекс оборудования, представляющий собой доработанный вариант аппаратуры предыдущих РЛС семейства. Таким образом, новое антенное устройство строится на основе агрегатов двух существующих радиолокационных комплексов, что позволяет решать поставленные задачи, но при этом не приводит к значительному усложнению или удорожанию станции.

В состав РЛС «Восток-3D» входят три основных компонента: антенно-аппаратная машина, выносное автоматизированное рабочее место и автономная дизельная электростанция. Все компоненты станции базируются на автомобильных шасси, что позволяет быстро перебрасывать весь комплекс на нужную позицию. В качестве базы для РЛС используются грузовые шасси белорусского производства. Комплекс может перемещаться по автомобильным дорогам, а также имеет возможность движения по пересеченной местности.

Антенно-аппаратная машина оснащается приводами с дистанционным управлением, что упрощает и ускоряет развертывание станции на позиции. Широкое применение гидравлики позволяет расчету из трех человек подготовить РЛС к работе за минимальное время. После этого комплекс может работать в течение длительного времени, осуществляя поиск воздушных целей, выполняя их сопровождение и выдавая информацию потребителям.

Главным элементом комплекса «Восток-3D» является т.н. антенно-аппаратная машина, несущая главные элементы радиоэлектронного оборудования. Представленные образцы такой техники были построены на трехосном автомобильном шасси белорусского производства. Базовая машина оснащена грузовой платформой нового типа, на которой устанавливается необходимое оборудование. Так, в передней части платформы имеется крупный кожух для части аппаратуры, а в задней находятся крепления для подъемной мачты с антеннами. По периметру платформы располагаются гидравлические домкраты, необходимые для стабилизации машины во время развертывания и работы.

Как следует из имеющихся материалов, при разработке антенного устройства РЛС «Восток-3D» самым активным образом использовались наработки по двухкоординатной станции «Восток-Э/Д». Непосредственно на платформе машины-носителя помещается подъемная телескопическая мачта с креплениями для антенных устройств. Определение координат цели по азимуту и дальности предлагается осуществлять при помощи крупной антенны, выполненной в виде решетки большой ширины с дополнительными боковыми элементами. На уровне мачты располагается наклонная антенна высотомера, которую, вероятно, тоже заимствовали из существующего проекта.

Антенны перспективной РЛС выполнены складными. При переводе в походное положение общие габариты антенного устройства значительно сокращаются. Мачта вместе со сложенными антеннами укладывается на платформу поворотом вперед. Все подобные действия выполняются по командам с пульта дистанционного управления и без непосредственного участия человека.

Максимальная дальность обнаружения воздушных целей заявлена на уровне 360 км. На таких расстояниях, в зависимости от разных факторов, РЛС «Восток-3D» может обнаружить крупные или средние самолеты. Кроме того, как утверждается, метровый диапазон позволяет находить и стелс-самолеты. Так, для ударного самолета типа F-117A заявленная дальность обнаружения достигает 350 км. При использовании противником активных помех максимальная дальность обнаружения

подобных целей заметно снижается. Утверждается, что путем модернизации передатчиков максимальная дальность обнаружения может быть увеличена.



Рисунок 1 – Один из пультов на борту самоходной машины

Главным элементом комплекса «Восток-3D» является т.н. антенно-аппаратная машина, несущая главные элементы радиоэлектронного оборудования. Представленные образцы такой техники были построены на трехосном автомобильном шасси белорусского производства. Базовая машина оснащена грузовой платформой нового типа, на которой устанавливается необходимое оборудование. Так, в передней части платформы имеется крупный кожух для части аппаратуры, а в задней находятся крепления для подъемной мачты с антеннами. По периметру платформы располагаются гидравлические домкраты, необходимые для стабилизации машины во время разворачивания и работы.

Как следует из имеющихся материалов, при разработке антенного устройства РЛС «Восток-3D» самым активным образом использовались наработки по двухкоординатной станции «Восток-Э/Д». Непосредственно на платформе машины-носителя помещается подъемная телескопическая мачта с креплениями для антенных устройств. Определение координат цели по азимуту и дальности предлагается осуществлять при помощи крупной антенны, выполненной в виде решетки большой ширины с дополнительными боковыми элементами. На уровне мачты располагается наклонная антенна высотомера, которую, вероятно, тоже заимствовали из существующего проекта.

Антенны перспективной РЛС выполнены складными. При переводе в походное положение общие габариты антенного устройства значительно сокращаются. Мачта вместе со сложенными антеннами укладывается на платформу поворотом вперед. Все подобные действия выполняются по командам с пульта дистанционного управления и без непосредственного участия человека.

Максимальная дальность обнаружения воздушных целей заявлена на уровне 360 км. На таких расстояниях, в зависимости от разных факторов, РЛС «Восток-3D» может обнаружить крупные или средние самолеты. Кроме того, как утверждается, метровый диапазон позволяет находить и стелс-самолеты. Так, для ударного самолета типа F-117A заявленная дальность обнаружения достигает 350 км. При использовании противником активных помех максимальная дальность обнаружения подобных целей заметно снижается. Утверждается, что путем модернизации передатчиков максимальная дальность обнаружения может быть увеличена.

Список использованных источников:

1. <https://topwar.ru/119178-radiolokacionnye-stancii-semeystva-vostok-3d-respublika-belarus.html>

РАДОЛОКАЦИОННАЯ СТАНЦИЯ «РОДНИК»

Стасько Н.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Хожевец О.А.

Аннотация. Преимущества и тактико-технические характеристики белорусской радиолокационной станции "РОДНИК".

РЛС «Родник» предназначается для использования в составе подвижных маловысотных радиолокационных групп (ПМРГ), в автоматизированных системах радиолокационной разведки воздушных целей и других системах для обнаружения, измерения координат и параметров движения воздушных (азимут, дальность, эшелон высоты полета, радиальная скорость) и наземных объектов (азимут, дальность, радиальная скорость), автоматического распознавания классов целей, автоматического сопровождения трасс целей в заданных зонах и выдачи радиолокационной информации потребителю по заданному протоколу.

Одно из предприятий системы Госкомвоенпрома продолжает активное развитие радиолокационных станций (РЛС) семейства «Родник», предназначенных для обнаружения маловысотных воздушных целей. В частности, в настоящее время идет выполнение опытно-конструкторской работы по созданию трехкоординатной радиолокационной станции X-диапазона для обнаружения маловысотных воздушных объектов «Родник-3D».

Перспективная разработка основывается на базе уже протестированной в ходе многочисленных испытаний и положительно зарекомендовавшей себя двухкоординатной РЛС «Родник».

Как двух-, так и трехкоординатные РЛС семейства «Родник» обеспечивают обнаружение, определение координат и параметров движения маловысотных воздушных объектов. Технологические решения, используемые при разработке РЛС этого семейства, позволяют обеспечить автоматическое распознавание классов целей и сопровождение их трасс в заданных зонах. Кроме того, РЛС семейства «Родник» имеют защиту от активных и пассивных помех.

Применение РЛС подобного класса приобретает особую актуальность с учетом тактики применения малоразмерных и маловысотных средств воздушного нападения, в частности, беспилотных летательных аппаратов (БПЛА), в вооруженных конфликтах последних лет.

Преимуществами РЛС семейства «Родник» является не только применение современных технологических решений, но также повышенная мобильность и живучесть за счет размещения аппаратуры РЛС на автомобильном шасси и минимального времени развертывания.

Кроме того, важным достоинством РЛС семейства «Родник» является возможность комплексирования со средствами радиоэлектронной борьбы с БПЛА, также производимыми предприятием, что позволяет расширить возможности их совместного использования для повышения эффективности обнаружения целей, включая БПЛА, выполняющие задания по заранее заданному маршруту без непосредственного управления оператором.

РЛС "Родник" может быть использована в комплексе со станциями радиоэлектронной борьбы (РЭБ) "Гроза-С", "Гроза-Р" и другими аналогичными средствами радиоэлектронной борьбы с малоразмерными маловысотными воздушными объектами (прежде всего, с беспилотными летательными аппаратами), в составе подвижных маловысотных радиолокационных групп, а также в автоматизированных радиолокационных системах разведки воздушных целей и других радиолокационных системах для обнаружения, измерения координат и параметров движения воздушных и наземных объектов, автоматического распознавания классов целей, автоматического сопровождения трасс целей в заданных зонах и выдачи радиолокационной информации по заданному протоколу.

Станцию можно смонтировать на унифицированной мобильной гидромеханической платформе, установленной на специальном колесном шасси прицепного типа, на любом средстве подвижности по требованию или на стационарной вышке (платформе).

При этом автоматизированное рабочее место РЛС "Родник" выносится на командный пункт, а обзор пространства, обнаружение целей, измерение координат и распознавание объектов осуществляется автоматически, без участия оператора. Изображение РЛС приведено на рисунке 1.

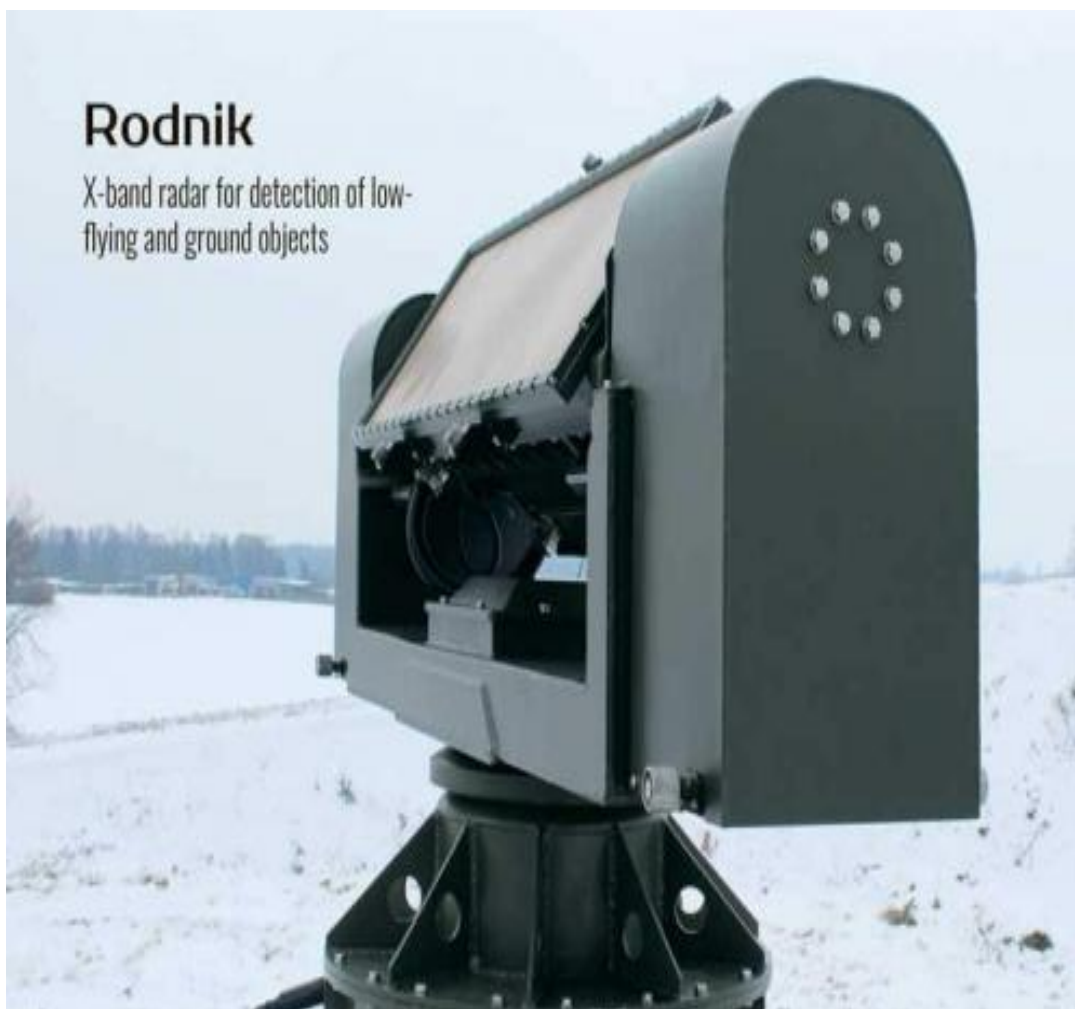


Рисунок 1 – РЛС «Родник»

Зона обзора пространства:

В РЛС предусмотрен обзор по азимуту в секторе 270 град. – механическое сканирование (два варианта скорости вращения антенны: 36 град./с и 72 град./с).

Зона обнаружения:

по азимуту в секторе, град. – 360;

по дальности, м – от 300 до 20000 (режим работы по БПЛА) и от 1500 до 50000 (режим работы по всем типам воздушных целей);

по углу места, град. – от 0 до 80;

по радиальной скорости, м/с – от 5 до 100 (режим работы по БПЛА) и от 5 до 1000 (режим работы по всем типам воздушных целей).

Дальности обнаружения целей РЛС обеспечивает дальности обнаружения с условными вероятностями правильного обнаружения 0,5 и ложной тревоги 10-5:

БПЛА планерного типа с эффективной отражающей поверхностью $\sigma_c = 1 \text{ м}^2$ на высоте 200 м – не менее 20 км (ограничивается инструментальной дальностью);

БПЛА планерного типа с эффективной отражающей поверхностью $\sigma_c = 0,01 \text{ м}^2$ на высоте 200 м – не менее 10 км;

БПЛА мультироторного типа с эффективной отражающей поверхностью $\sigma_c = 0,001 \text{ м}^2$ на высоте 200 м – не менее 6 км;

Крылатой ракеты с эффективной отражающей поверхностью $\sigma_c = 0,1 \text{ м}^2$ на высоте 200 м – не менее 17 км;

Истребителя с эффективной отражающей поверхностью $\sigma_c = 1 \text{ м}^2$ на высотах:

от 200 до 3000 м – не менее 25 км;

от 5000 до 8000 м – не менее 20 км;

Истребителя-бомбардировщика с эффективной отражающей поверхностью $\sigma_c =$ от 2,5 до 3 м² на высотах:

от 200 до 3000 м – не менее 45 км;

от 5000 до 10000 м – не менее 30 км;

Бомбардировщика с эффективной отражающей поверхностью $\sigma_c = 5 \text{ м}^2$ на высотах:

от 200 до 3000 м – не менее 50 км (ограничивается инструментальной дальностью);
от 5000 до 10000 м – не менее 40 км.

Определяемые координаты и параметры движения цели и точность их измерения:
среднеквадратические ошибки определения координат:

дальности, м – не более 50;

азимута, град. – не более 0,6 (значение может быть уточнено на этапе технического проектирования);

радиальной скорости – м/с – не более 0,1.

Разрешающая способность РЛС по измеряемым координатам и параметрам движения цели:

по дальности, м – не более 300;

по азимуту, град. – не более 3;

по радиальной скорости, м/с – не более 5.

Распознавание классов целей: РЛС должна обеспечивать распознавание пяти классов воздушных объектов («самолет», «вертолет», БПЛА мультироторного типа», «БПЛА планерного типа», «нераспознанный воздушный объект») и класса «наземная цель». Темп обновления информации,

с – не более 10.

Количество одновременно сопровождаемых трасс целей: в режиме работы по БПЛА – не менее 50; в режиме работы по всем типам воздушных целей – не менее 100.

РЛС является транспортируемой. Обнаружение и сопровождение целей производится в развернутом положении. Время развертывания (свертывания) РЛС из походного положения в боевое в любых климатических условиях, в любое время суток, мин. – не более 20; Время включения РЛС с проведением функционального контроля, мин – не более 10; Время перевода РЛС из дежурного режима в боевой, с - не более 10. Время непрерывной работы РЛС от внешней электросети, ч - не менее 24.

Семейство РЛС «Родник» - перспективный источник борьбы с беспилотниками.

Одно из предприятий системы Госкомвоенпрома продолжает активное развитие радиолокационных станций (РЛС) семейства «Родник», предназначенных для обнаружения маловысотных воздушных целей. В частности, в настоящее время идет выполнение опытно-конструкторской работы по созданию трехкоординатной радиолокационной станции X-диапазона для обнаружения маловысотных воздушных объектов «Родник-3D».

Перспективная разработка основывается на базе уже протестированной в ходе многочисленных испытаний и положительно зарекомендовавшей себя двухкоординатной РЛС «Родник».

Как двух-, так и трехкоординатные РЛС семейства «Родник» обеспечивают обнаружение, определение координат и параметров движения маловысотных воздушных объектов. Технологические решения, используемые при разработке РЛС этого семейства, позволяют обеспечить автоматическое распознавание классов целей и сопровождение их трасс в заданных зонах. Кроме того, РЛС семейства «Родник» имеют защиту от активных и пассивных помех.

Применение РЛС подобного класса приобретает особую актуальность с учетом тактики применения малоразмерных и маловысотных средств воздушного нападения, в частности, беспилотных летательных аппаратов (БПЛА), в вооруженных конфликтах последних лет.

Преимуществами РЛС семейства «Родник» является не только применение современных технологических решений, но также повышенная мобильность и живучесть за счет размещения аппаратуры РЛС на автомобильном шасси и минимального времени развертывания.

Кроме того, важным достоинством РЛС семейства «Родник» является возможность комплексирования со средствами радиоэлектронной борьбы с БПЛА, также производимыми предприятием, что позволяет расширить возможности их совместного использования для повышения эффективности обнаружения целей, включая БПЛА, выполняющие задания по заранее заданному маршруту без непосредственного управления оператором.

РЛС "Родник" может быть использована в комплексе со станциями радиоэлектронной борьбы (РЭБ) "Гроза-С", "Гроза-Р" и другими аналогичными средствами радиоэлектронной борьбы с малоразмерными маловысотными воздушными объектами (прежде всего, с беспилотными летательными аппаратами), в составе подвижных маловысотных радиолокационных групп, а также в автоматизированных радиолокационных системах разведки воздушных целей и других радиолокационных системах для обнаружения, измерения координат и параметров движения воздушных и наземных объектов, автоматического распознавания классов целей, автоматического сопровождения трасс целей в заданных зонах и выдачи радиолокационной информации по заданному протоколу.

Список использованных источников:

1. <https://www.bvpservice.by/node/217>

2. <https://www.belta.by/tech/view/v-belarusi-uspeshno-zavershilis-ispytaniya-radiolokatsionnoj-stantsii-rodnik-332769-2019/>

3. https://www.vpk.gov.by/news/comm_news/semeystvo-rls-rodnik-perspektivnyy-istochnik-borby-s-bespilotnikami.html

РАДИОЛОКАЦИОННАЯ СТАНЦИЯ «ПРОТИВНИК-ГЕ»

Сташкевич Н.В.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Петрукович М.С.

Аннотация. Преимущества и тактико-технические характеристики радиолокационной станции «Противник-ГЕ».

Средства радиолокационной разведки должны соответствовать требованиям воздушно-космических средств, при этом догоняя, либо находясь на несколько шагов впереди. Ко второй половине 1960-х годов войска ПВО ощутили острую необходимость в создании трехкоординатных РЛС, которые способны выдавать информацию для зенитно-ракетных войск и авиации в условиях массированного применения активных и пассивных помех. До этого радиотехнические войска ПВО оснащались достаточно громоздкими радиолокационными комплексами, состоящих из дальномеров и высотомеров. Они работали только по целеуказанию и обеспечивали выдачу информации по высоте со сравнительно невысоким темпом (порядка 3 целей в минуту).

На сегодняшний день, на вооружении стоит некоторое множество радиолокационных станций, которые великолепно справляются с обнаружением на больших дальностях и на маленьких высотах. Одной из них является РЛС «Противник-ГЕ».

Данный образец представляет собой высокоавтоматизированный комплекс воздушной разведки, использующий передовые достижения в области радиолокации, вычислительной техники и конструкторских решениях. Он относится к числу современных мобильных трехкоординатных локаторов боевого режима, с расширенной зоной обнаружения аэродинамических и баллистических целей с дальностью 10-400 километров высотой порядка 150-200 километров.

«Противник-ГЕ» предназначен для обнаружения воздушных целей, их сопровождения, выдачи трех координат (азимута, дальности, высоты), определения скорости, государственной принадлежности, типа и количества целей, на больших высотах и дальностях, с высокой интенсивностью в условиях применения противником помех.

За счет применения современных средств вычислительной техники данная радиолокационная станция справляется с этой задачей и является передовым образцом вооружения и превосходит по большинству показателей отечественные станции.

Например: вся аппаратура РЛС уместается на двух машинах-тягачах, что делает показатель мобильности значительно выше, чем у ее предшественников. Антенна уместается на одной транспортной единице, имея размеры 5,5х8,5 метров, скорости вращения 6 и 12 оборотов в минуту, что соответствует выдаче данных 10 и 5 секунд соответственно, что считается достаточным для работы по скоростным и высоколетящим целям. Благодаря фазированной антенной решетке – станция формирует диаграмму направленности 0-45°, а за счет боковых лепестков нового уровня автоматически обеспечивает высокую защищенность локатора от помех.



Рисунок 1 – Рабочее место оператора РЛС «Противник-ГЕ»

Преимущество высокой точности определения координат удалось добиться из-за применения аппаратуры цифровой пространственно-временной обработки сигнала. Устройства антенны формирует в своих 10 боках 20 одинаковых лучей. В случае отказа одного из блоков, в РЛС предусмотрена подстройка под состояние станции и уже не 20, а 18 лучей будут рассматривать цели в 45° воздушного пространства. При этом вся зона обзора воздушного пространства останется прежней, но незначительно ухудшатся показатели по точности, при этом продолжая работать в боевом режиме. Принцип построения антенны, позволяет проводить дальнейшую ее модернизацию в других диапазонах волн, тем самым улучшая ее характеристики.

В данной РЛС используется международный 23-х сантиметровый диапазон частот. В ней имеется вторичный локатор, обеспечивающий управление воздушным движением и большим количеством выдаваемой информации. Помимо наличия системы опознавания «свой-чужой», мы можем узнать уровень топлива, приметы сигнала бедствия и другие сообщения.

«Противник-ГЕ» способен определять радиальную скорость цели, что позволяет отсеять сложные цели. Всего локатор способен определить 150 воздушных объектов, которые могут являться самолетами пятого поколения. Самолеты, выполненные по технологии «стэлс», РЛС способна обнаружить на дальности 200 километров.

Время работы «на отказ» достигаем 600 часов, а время восстановления занимает около получаса. Расчет станции состоит из трех человек, что позволяет развернуть станцию всего за 40 минут. Данные показатели в разы превосходят показатели ранних РЛС.

Данная РЛС является унифицированной, что позволяет снизить затраты по ЗИП и ГСМ. Она может быть использована военно-воздушными силами, войсками противовоздушной обороны и сухопутными войсками.

Системам жизнеобеспечения было уделено должное внимание, для удобства работы были созданы системы обеспечения кислородом, освещения и температурного контроля.

Во время написания программного обеспечения, специалисты сделали все возможное, чтобы работа была максимально удобна, комфортна и приятна. Рабочая зона состоит из 6 полей, в которых находятся кнопки, отвечающие за включение определенного режима работы, инструменты для работы с индикатором обнаружения, а также для нахождения документации по аппаратуре данной станции.

На данном примере мы могли заметить, что прогресс не стоит на месте. Вооруженные силы стремятся к обновлению вооружения, которое способно быстро, своевременно, а главное качественно выполнять задачи, согласно своему предназначению, что позволит держать показатель боевой готовности на высоком уровне.



Рисунок 2 – Радиолокационная станция «Противник-ГЕ»

Список использованных источников:

1. https://structure.mil.ru/structure/forces/air/weapons/air_defense/more.htm?id=10393110@morfMilitaryModel.

РАДИОЛОКАЦИОННЫЙ КОМПЛЕКС ОБНАРУЖЕНИЯ МАЛОВЫСОТНЫХ ЦЕЛЕЙ «РОСА-РБ»

Язенков Г.В.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Маргель А.Б.

Аннотация. Преимущества и тактико-технические характеристики белорусской радиолокационного комплекса обнаружения маловысотных целей станции «Роса-РБ».

На сегодняшний день на вооружении РТВ стоит определенное количество радиолокационных станций и комплексов, которые хорошо справляются с обнаружением на больших дальностях и на маленьких высотах. Одной из них является РЛК «Роса-РБ».

Радиолокационный комплекс обнаружения маловысотных целей «Роса-РБ» предназначен для автоматического обнаружения и сопровождения маловысотных воздушных объектов, выдачи трассовой информации в автоматизированную систему управления.

Обеспечивает эффективное обнаружение воздушных объектов на предельно малых высотах с малой эффективной отражающей поверхностью; функционирует в автоматическом режиме без участия оператора; обладает высокой радиолокационной скрытностью и помехозащищенностью; функциональный контроль полностью автоматизирован; работает без выключения на перерыв не меньше месяца. По желанию Покупателя ТРЛК может комплектоваться аппаратурой АЗН-В.

Состав: от одной до пяти автономных автоматических радиолокационных станций обнаружения маловысотных целей (МРЛС); система дистанционного управления.

Основной элемент МРЛС - 16-канальное, интегрированное с антенной цифровое приемо-передающее устройство.



Рисунок 1 – Антенное устройство РЛК «Роса-РБ»

Достоинства МРЛК:

- обеспечивает эффективное обнаружение воздушных объектов на предельно малых высотах с малой эффективной отражающей поверхностью;
- функционирует в автоматическом режиме — без участия оператора;
- обладает высокой радиолокационной скрытностью и помехозащищенностью;
- функциональный контроль полностью автоматизирован;
- работает без выключения на перерыв не меньше месяца;
- отсутствие подвижных частей, за счет использования кольцевой твердотельной цифровой фазированной антенной решетки;
- использование цифрового синтеза зондирующего сигнала и цифровой обработки принятого сигнала.

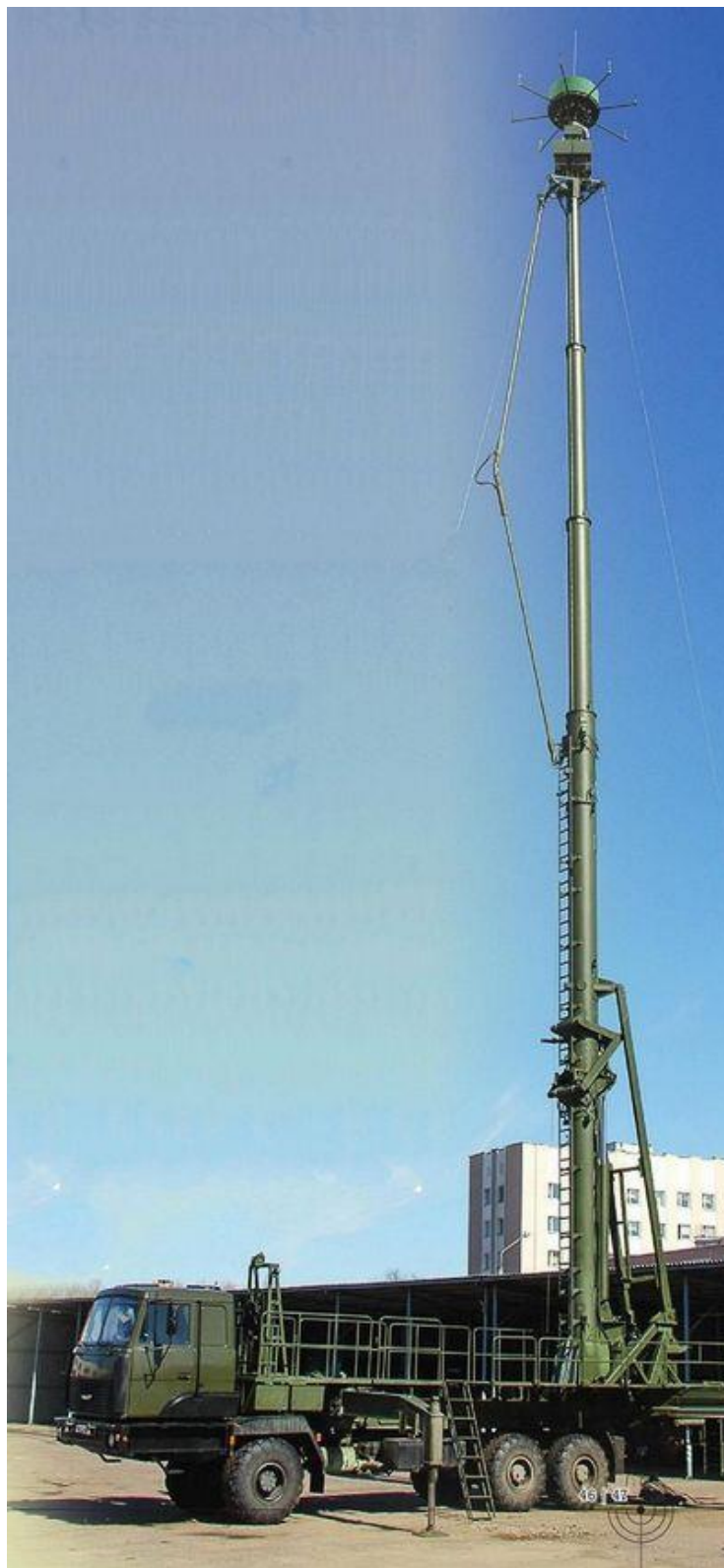


Рисунок 2 – Радиолокационный комплекс «Роса-РБ»

На данном примере мы смогли заметить, что прогресс движется вперёд. Вооруженные силы стремятся к обновлению вооружения, которое обязано своевременно, а главное качественно выполнять поставленные задачи, что позволит держать показатель боевой готовности на высоком уровне.

Список использованных источников:

1. Радиолокационный комплекс обнаружения маловысотных целей «РОСА-РБ» | bvps (bvpservice.by)

РОЛЬ ИСТОРИЧЕСКИХ ЗНАНИЙ В ФОРМИРОВАНИИ ВЗГЛЯДОВ НА ФОРМЫ И СПОСОБЫ ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ НА СОВРЕМЕННОМ ЭТАПЕ

Фирсов А.А., Бебех Д.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Комар Е.В. – канд. ист. наук, доц.

Аннотация. Рассмотрено понятие военной науки ее цели и составные части. Отражены цели и сущность военно-научного познания. Установлена роль военной истории в решении проблем современной военной науки.

На протяжении всей истории человечества неизменной составляющей его эволюции были войны. Они зачастую являлись инструментом зарождения государств и цивилизаций, а также их расцвета и падения. На всех этапах исторического развития человечество стремилось познать причины возникновения войн, их сущность, закономерности и принципы ведения военных действий. В государствах Древнего Востока, Древней Греции и Древнего Рима зародилась военная теория и появились первые труды, обобщившие опыт ведения войн. Военная мысль развивалась и совершенствовалась не одно столетие, что привело к оформлению военной науки как определенной системы практических и теоретических знаний, умений и навыков.

Военная наука занимается изучением войны, как сложного социально-политического явления, и представляет собой систему знаний о характере, законах войны, подготовке вооруженных сил и страны к войне и способах ее ведения [1]. Научное познание военной науки направлено на установление сущности и объективных закономерностей войны, описание, объяснение и предсказание процессов и явлений наблюдаемой действительности. Структурно, наряду с общей теорией и теорией военного искусства, военная наука включает и военную историю [2].

Военная история является базой военной науки. Доказательством этого является то, что развитие военной науки происходит, на основе обобщения исторического опыта, отражения в сознании человека явлений войны, условий и способов подготовки к ней, имея целью изучение войны, операции, боя, подготовки вооруженных сил и страны к ведению боевых действий в различных условиях обстановки, и осуществляется на основе военной практики и в целях ее совершенствования.

Проблема интенсификации военно-научных исследований крайне актуальна в современных условиях, в которых максимально обострено соперничество государств в политической, экономической, информационной и других сферах. Это, несомненно, ведет к нарастанию потенциала конфликтности, возникновению новых вызовов и угроз, которые при определенных обстоятельствах способны перейти в фазу вооруженного противостояния. Свидетельством этого являются события на Ближнем Востоке и в сопредельных с Республикой Беларусь государствах.

В 2023, 2024 гг. мы подошли к юбилейным датам военной истории – 80-й годовщине начала освобождения Беларуси от немецко-фашистских захватчиков и проведения Белорусской стратегической наступательной операции «Багратион» [3]. В связи с существующей вероятностью переноса боевых действий на территорию республики из пределов соседних государств, обращение к событиям 1943–1944 гг. видется крайне актуальным. Здесь важным является то, что это последний опыт ведения боевых действий на белорусской земле. Изучение событий того времени позволит рассмотреть положительные результаты, выявить ошибки, извлечь уроки и наметить пути дальнейшего развития белорусской армии в современных условиях.

В свете трансформации форм и способов ведения вооруженной борьбы, в настоящее время пристальное внимание обращается на тактику действий малочисленных групп, и здесь определенный опыт можно почерпнуть, изучая тактику боевых действий партизанских формирований.

Таким образом, изучение опыта ведения боевых действий Красной армии и партизанских формирований на территории Беларуси в годы Великой Отечественной войны, несомненно, имеет не только научно-познавательное, но и прикладное значение для Вооруженных Сил Республики Беларусь. Современные проблемы военной науки неразрывно связаны с ее историей, поскольку есть так называемые извечные вопросы (развитие средств, форм и способов ведения вооруженной борьбы), которые требуют решения, постоянного обновления и корректировки в свете эволюции общества и войн.

Список использованных источников:

1. Советская военная энциклопедия : [в 8 т.] / пред. гл. ред. комис. : А. А. Гречко. – М. : Воениздат, 1976–1980. – Т. 2. Вавилон – Гражданская. – 1976. – 640 с.
2. Военная наука в Республике Беларусь [Электронный ресурс]. – Режим доступа: https://www.mil.by/ru/forces/military_science/vn/. – Дата доступа: 27.03.2023.
3. Великая Отечественная война 1941–1945 годов : [в 12 т.] / ред. комис. : С. К. Шойгу (пред.) [и др.]. – М. : Кучково поле, 2011–2015. – Т. 1. Основные события войны. – 2011. – 848 с.

УДК 372.835.5

ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ ТАКТИКИ ОБЩЕВОЙСКОВОГО БОЯ

Семёнов М.И., Пинголь Д.И., курсант гр.230501

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Фомченко А.Л.

Аннотация: В статье подробно рассматривается вопрос о преимуществах использования инновационных технологий при изучении тактики общевойскового боя. Предоставлены аспекты, рассмотрены достижения при изучении тактики с использованием тех или иных технологий.

Ключевые слова. Инновация, тактика.

Введение инновационных технологий в содержание образовательного процесса включает в себя интеграцию различных предметных сфер с информатикой, что ведет к информатизации сознания военнослужащих и осмыслению ими процессов информатизации в тактике общевойскового боя (в его профессиональном аспекте). Существенное значение обладает осознание направленности хода процесса информатизации учебного заведения: изучения курсантами данных об информатике к применению компьютерных программных средств при изучении тактики, а затем к насыщению компонентами информатики структуры и содержания той или иной темы, реализация коренной перестройки всего учебного процесса на базе применения информационных технологий. Развитие компьютерных телекоммуникаций в образовании инициировало возникновение новых образовательных практик, что в свою очередь поспособствовало изменениям образовательной концепции в целом. Инновационные технологические процессы расширяют способности восприятия информации посредством органов чувств, применяя познавательную способность воображения, эмоциональное и эстетическое влияние, которые будут играть важнейшую составляющую при разработке учебных программ. С целью результативного применения технологий в образовании следует знать их свойства и функции, для того чтобы четко установить решения каких дидактических задач целесообразно (с точки зрения тактики) воспользоваться той или иной из них.

Современные технологии дают возможность достигать:

- стимулирование познавательной работы;
- повышение эффективности учебного процесса;
- адаптирование учебного материала потребностям военнослужащих;
- роста профессионального мастерства.

Созданная форма рационального управления, а также технологический и информационный подходы к процессу преподавания были применены в работе с курсантами и могут быть базой с целью формирования вариативных путей оптимизации процесса обучения с применением инновационных технологий.

Но с возникновением новых средств борьбы невиданной мощности и дальнейшим формированием обычного вооружения гораздо сильно увеличились условия к эмоциональной подготовке и информатизации военных, к изучению ими орудия и военной техники, к непрерывному совершенствованию тактической выучки войск. Современный общевойсковой бой требует от участвующих в нем войск постоянного ведения разведывательных операций, опытного использования вооружения, техники, средств защиты и маскировки, значительной физической активности и организованности, абсолютного напряжения всех моральных и физических сил, непреклонной воли к победе, железной дисциплины и боевой сплоченности.

В рамках исследования научно-методического обеспечения программ тактики общевойскового боя с применением технологий обязаны быть рассмотрены следующие нюансы:

- анализ условий, определение, постановку цели обучения и утверждения её участниками процесса преподавания;
- предъявление учебного материала различными способами;
- выполнение обучающих и тренировочных действий и операций;
- качественная организация обратной связи, контроль и корректировка деятельности по усвоению материала;
- анализ и самоанализ, оценка результатов и др.

Применение компьютерных технологий обучения в условиях учебного процесса согласно программам подготовки офицеров запаса и офицеров с целью дальнейшей службы в Вооруженных Силах высших учебных заведений позволяет решать ряд задач:

1. повышение заинтересованности к исследуемой дисциплине;
2. увеличение объема информации по дисциплинам военной подготовки;
3. усовершенствование качества организации учебного процесса; использование индивидуального характера обучения;
4. формирование комплекса учебных пакетов, программ с целью концепций виртуальной подготовки военного специалиста.

Все вышеизложенное даст возможность сформировать личность будущего военного профессионала в условиях активного внедрения инновационных технологий в учебный процесс.

Положительные стороны использования новейших разработок и информационных технологий:

1. существенное сбережение ресурсов боевой аппаратуры на начальном этапе подготовки специалистов;
2. инновационные компьютерные технологии дают возможность максимально приблизиться к реальности, симитировать функционирование любой боевой техники;
3. дает возможность одновременно обучать неограниченное количество личного состава.

Тактика - это учение о бое. Она охватывает теорию и практику подготовки и ведения боевых действий подразделениями, частями и соединениями всех родов войск.

Тактика делится на общую тактику и тактику родов войск. Общая тактика рассматривает вопросы по организации и ведению общевойскового боя, а также определяет роль и место в нем каждого рода войск и специальных войск исходя из их тактико-технических свойств и возможностей. Тактика родов войск изучает боевые качества и возможности родов войск и определяет наиболее логические приемы и способы их действий как в общевойсковом бою, и при самостоятельных боевых действиях.

Вооружение и техника оказывают наиболее революционизирующее влияние на характер общевойскового боя и способы его ведения, на развитие тактики в целом. Как и каждая отдельная отрасль тактика должна включать мероприятия и задачи. Без тактической подготовки ни один из военнослужащих не может считать себя подготовленным к выполнению задачи по защите своего государства, страны.

Большое внимание при обучении уделяется исследованию закономерностей общевойскового боя. Только в бою возможно разгромить противника, лишить его возможности оказывать давление и овладеть его территорией. В процессе изучения тактики формируются аспекты на характер современной войны, на роль и предназначение видов и родов войск Вооруженных Сил Республики Беларусь. Обучающиеся усваивают основы теории общевойскового боя, овладевают умениями и навыками в организации и управлении подразделениями в бою.

В результате изучения тактики обучающиеся овладевают рациональными методами работы командира, познают искусство ведения боя. У них формируется такое важное качество, как творческое тактическое мышление, военно-профессиональная культура, вырабатываются умения проводить анализ, делать сравнения, сопоставлять и систематизировать факты, делать обобщения, выделять главное, существенное, формулировать выводы, обосновывать свои предложения, доказывать и отстаивать свое решение.

В дальнейшем эти качества совершенствуются и развиваются в процессе изучения других дисциплин. Данные умения и их реализация невозможны без процесса внедрения информационных и коммуникационных технологий в сферу военного образования. Разработанные компьютерные тестирующие и диагностирующие методики должны обеспечить систематический оперативный контроль и оценку уровня знаний обучающихся, повышение эффективности обучения.

Использование современных средств информационных технологий, таких как электронные версии занятий, электронные учебники, обучающие программы являются актуальными для современного профессионального военного образования. Все шире внедряются такие учебные технологии, как компьютер, цифровой проектор, интерактивная доска и т.д.

При ведении боя в современных условиях командир обязан предусмотреть все возможные варианты развития событий. Без тактики нет командира. Базой для развития технологий могут служить 3D карты местности, с помощью которых обучающийся сможет представить объемную картину местности, рассчитать необходимые показатели и т.п. Также существуют различные тактические симуляторы. В реальной обстановке без определенных знаний и навыков невозможно командовать личным составом.

В подготовке к реальным действиям может помочь симулятор, в котором обучающийся сможет отработать все необходимые навыки. Основными требованиями к инновационным технологиям должны быть просто и доступность использования, совместимость со многим

аппаратными и программными платформами и продуктами, независимо от их особенностей, возможность дальнейшего совершенствования данной программы или технологии.

Рассмотрим некоторые достижения в области изучения тактики общевойскового боя. Одним из примеров является то, что в 2016 году была представлена система «Виртуальное поле боя», предназначенная для планирования и отработки боевых действий.

Система предназначена для компьютерных имитаций военных действий на заданной территории. Поле боя VR отображает действия пользователя и 10 создаёт события в соответствии с заданными алгоритмами функционирования образцов военной техники. Описываемая система строится на основе цифровых карт, данных аэрофотосъемки, спутниковых снимков и фотографий. Виртуальное поле боя создаёт модели и сцены движения и стрельбы военнослужащих, информационно-командного обмена, военной техники и вооружения, в которой отображаются их реальные параметры: угол и скорость наведения, характеристики и возможности прицельных комплексов, характеристики боеприпасов. Адекватная оценка свойств местности позволяет принять верное решение при выборе направления военного удара, оперативного построения армии, а также организации взаимодействия между боевыми подразделениями.

Комбинируемая VR реализует принцип искусственной динамической среды, основанной на синтезе физической и виртуальной реальности. Активно используется для подготовки сухопутных войск. Суть технологии заключается в создании специфических искусственно созданных сцен VR и реального оборудования, снабженного специальными датчиками и сенсорами: шлем с 3D-дисплеем, переносным компьютером, сенсором положения тела, имитатор стрелкового оружия.

Один из примеров комбинируемой VR военного назначения является система Dismounted Soldier Training System (SDTS) Данная система представляет возможность визуализации участков местности и отработки ведения боя с различным оружием. Кроме того, система позволяет создавать внештатные ситуации: внезапное наступление врага, бой в одиночку и т.д.

Если говорить об использовании инновационных технологий на военном факультете в учреждении образования «Белорусский государственный университет информатики и радиоэлектроники», то использование все технических средств является неотъемлемой частью образовательного процесса.

В основу подготовки положены следующие компоненты и мероприятия:

1. учебная электронная литература, пособия и тестовые задания для обучения курсантов;
2. единая университетская сеть электронных общенаучных библиотек, банков и баз данных;
3. комплекс системотехнических сетевых решений, специального учебного интерактивного интерфейса и других средств, позволяющих использовать «Интернет» и формировать специальные сети, охватывающие вуз, так чтобы офицеры и курсанты могли эффективно совершенствоваться в профессиональном отношении;
4. комплекс директивных документов, в том числе отраженные в приказах и организационно-методических указаниях по организации боевой и оперативной подготовки, в планах боевой и оперативной подготовки войск;
5. разработка компьютерных моделей, симуляторов и тренажеров; применение результатов исследований в диссертациях, научно-исследовательских работах, изобретательской работе.

Основными видами учебных занятий, в которые входит использование технологий по тактике общевойскового боя, являются: лекции, семинарские, лабораторные, практические занятия, групповые упражнения и занятия, тактические (тактико-специальные) занятия и учения, командно-штабные тренировки, военно-научные конференции, контрольные работы (занятия), самостоятельная работа курсантов, консультации, практика, войсковая стажировка, выполнение курсовых работ (проектов), дипломных работ (проектов, задач).

Таким образом, можно утверждать, что задачи, стоящие перед повышением качества подготовки военных специалистов при изучении тактики общевойскового боя, решаются с применением новейших образовательных технологий в области военного образования. Но вместе с тем, все это не отрицает обмена передовым опытом. На сегодняшний день с их помощью можно облегчить подготовку солдат и обеспечить армию комплектом оснащения, повышающего её эффективность. По этой причине всё больше государств активно вводят технологии в программы военной подготовки.

Список используемых источников:

1. Инновационные технологии как средство оптимизации процесса обучения курсантов военного ВУЗа [Электронный ресурс], - 2013.
2. Основы современного общевойскового боя [Электронный ресурс]. – Режим доступа: <http://militera.lib.ru/science/tactic/02.html>
3. ОБЩАЯ ТАКТИКА: УЧЕБНОЕ ПОСОБИЕ Зарицкий В.Н., Харкевич Л.А. [Электронный ресурс]. – Режим доступа: <http://window.edu.ru/catalog/pdf2txt/730/56730/27309>

РОЛЬ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ ОБЩЕВОЙСКОВОГО БОЯ

Носко К.А., Николаев Е.А.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Соколов С.В.

За прошедшие тысячелетия тактика, как искусство боя, прошла большой и многосложный путь развития. Он складывался из определенных исторических ступеней - это военное искусство Древнего Востока (Индии, Китая, Египта, Вавилона), военное искусство Древней Греции и Древнего Рима; Средневековья; эпохи Возрождения; Нового времени; войн домашнего и машинного периодов; двух мировых и многочисленных локальных войн и вооруженных конфликтов второй половины двадцатого века. Поистине современная тактика олицетворяет собой мудрость веков. Выстраданный потом и кровью многих поколений боевой опыт, позволяет офицеру выбирать свои жизненные установки, вооружает ценностной ориентацией, пробуждает новаторский дух, конструктивное начало, учит видеть действительность через призму времени, помогает целеустремленно, с научных позиций решать проблемы современности.

Бой - основная форма тактических действий, представляет собой организованные и согласованные по цели, месту и времени удары, огонь и маневр соединений, частей и подразделений в целях уничтожения (разгрома) противника, отражения его ударов и выполнения других тактических задач в ограниченном районе в течение короткого времени.

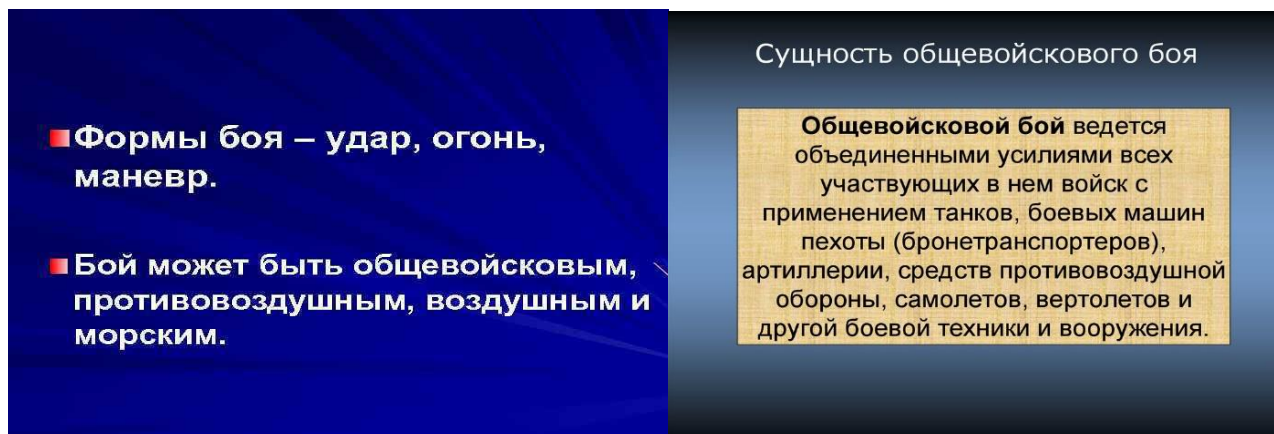


Рисунок - 1 Формы боя

Рисунок - 2 Сущность общевойскового боя

Сущность общевойскового боя состоит в нанесении огневого поражения противнику и уничтожению его в очагах обороны с последующим развитием успеха, главным образом, за счет ввода резервов в наступлении или в нанесении огневого поражения наступающему противнику в сочетании с прочным удержанием занимаемых позиций в обороне.

Современный общевойсковой бой характеризуется следующими чертами:

- решительностью;
- высокой маневренностью;
- напряженностью и скоротечностью;
- быстрыми и резкими изменениями обстановки и разнообразием применяемых способов его ведения;
- развертыванием боевых действий в быстром темпе на земле и в воздухе, на широком фронте, на большой глубине.

Основными принципами ведения современного общевойскового боя являются:

1. Постоянная высокая боевая готовность подразделений;
2. Высокая активность, решительность и непрерывность ведения боя;
3. Внезапность действий;
4. Постоянное и четкое взаимодействие, согласованное применение родов войск в бою;
5. Решительное сосредоточение основных усилий подразделений на главном направлении и в нужное время;
6. Сочетание огня с движением, широкое применение маневра подразделениями и огнем;

7. Учет и использование морального и психологического факторов в интересах выполнения поставленной задачи;
8. Всестороннее обеспечение боя;
9. Поддержание и своевременное восстановление боеспособности подразделений;
10. Твердое и непрерывное управление подразделениями; непреклонность в достижении намеченных целей, выполнении принятых решений и поставленных задач.

В обучении военнослужащих преимущественно реализуются ассоциативно-рефлекторные, информационные технологии, технологии поэтапного формирования умственных действий, которые ориентированы на условия осуществления военно-профессиональной деятельности, свойственные репродуктивному уровню обучения. Развивающие технологии проблемного, контекстного, заданного обучения курсантов и проблемно-деятельностные технологии, моделирующие различные аспекты непрерывно изменяющейся, саморазвивающейся военно-профессиональной деятельности, реализуются в основном спонтанно и не системно.

При изучении тактики общевойскового боя применяются различные методы проведения занятий у курсантов(студентов), например: лекции, семинары, групповые упражнения в классе и поле, тактические летучки и учения.

При чтении лекций достигается всестороннее освещение вопросов практической деятельности командира и штаба по организации и ведению боя и операции (уяснение задачи, оценка обстановки, выработка решения, постановка боевых задач, организация взаимодействия и всестороннего обеспечения боя и т. д.).

На тактических занятиях и учениях в еще большей степени возможно и даже необходимо применять приемы и способы развития творческого мышления. Однако следует помнить, что на учениях обучение усложняется, так как слушатели и курсанты действуют в одинаковых условиях (должностях).

Как показывает опыт, важное место в развитии творческого мышления занимают тактические летучки, которые могут проводиться на групповых упражнениях в поле. Их можно иметь одну-две на учебную задачу. Основной целью их является проверка и совершенствование теоретических знаний, практических навыков и умений.

Важный вид оперативно-тактической подготовки - групповые упражнения. Они могут быть классными и полевыми. Наиболее эффективными в развитии творческого мышления являются групповые упражнения в поле. Опыт показывает, что студенты и курсанты начинают творческую работу на тех занятиях, где возникает сложная и недостаточно ясная обстановка, т. е. когда создана проблемная ситуация, а вся их деятельность по организации и ведению операции и боя проходит строго ограничено по времени.

Главной целью инновационных технологий образования является подготовка человека к жизни в постоянно меняющемся мире. Сущность такого обучения состоит в ориентации учебного процесса на потенциальные возможности человека и их реализацию. Образование должно развивать механизмы инновационной деятельности, находить творческие способы решения жизненно важных проблем, способствовать превращению творчества в норму и форму существования человека.

Показателями нового качества образовательного процесса могут выступать следующие характеристики: новые знания, формирование основных компетенций у курсантов (студентов), повышение уровня их личностного развития; отсутствие отрицательных эффектов и последствий (перегрузки, утомление, ухудшение здоровья, психические расстройства, дефицит учебной мотивации и пр.); повышение профессиональной компетентности офицеров-педагогов и их отношения к работе; рост престижа образовательного учреждения, выражающийся в притоке обучаемых и преподавателей и др.



Рисунок 3 - Роль инновационных технологий в организации учебного процесса.

В свою очередь, происходящее внедрение новых образовательных технологий в образовательный процесс в вузах, затрагивает и подготовку военных специалистов на военных факультетах и кафедрах. Но при этом следует учитывать, что подготовка военного специалиста значительно отличается от подготовки гражданского специалиста, так как требует:

- всестороннюю личностную подготовку курсанта, как будущего офицера (гражданина, защитника Отечества, руководителя, организатора, воспитателя, общественного деятеля, носителя этнических ценностей и правовых норм);

- подготовку курсанта как профессионала, что требует качественного выполнения заданий в условиях определенной сложности при устойчивом сохранении работоспособности и оптимальных рабочих параметров в реальных экстремальных условиях службы в армии;

- воспитание курсанта, способного активно участвовать в интеграции Вооруженных Сил в экономическую, политическую, правовую и социальную систему общества;

- формирование моральной и психологической готовности к защите Отечества, Конституции и воинского долга;

- умение поддерживать воинскую дисциплину, обучать и воспитывать подчиненных.

Повышение качества подготовки военных специалистов на нашем военном факультете неразрывно связано с внедрением новых образовательных технологий, в основу которых положены следующие компоненты и мероприятия:

- учебная электронная литература, пособия и тестовые задания для обучения курсантов и студентов;

- единая университетская сеть электронных общенаучных библиотек, банков и баз данных;

- комплекс системотехнических сетевых решений, специального учебного интерактивного интерфейса и других средств, позволяющих использовать Интернет и формировать специальные сети;

- комплекс директивных документов, в том числе отраженные в приказах и организационно-методических указаниях по организации боевой и оперативной подготовки, в планах боевой и оперативной подготовки войск;

- разработка компьютерных моделей, симуляторов и тренажеров;

- применение результатов исследований в диссертациях, научно-исследовательских работах, изобретательской работе.

Работа по внедрению новых образовательных технологий в значительной степени активизирует и расширяет научную деятельность профессорско-преподавательского состава факультета.

Также военный руководитель обязан совершенствовать свои знания и педагогичность в ходе ведения занятий, с наклоном на развитие общего уровня культуры, с последующим появлением любви к военному делу.

Хочется отметить то, что методы проведения тактических занятий не стоят на месте и постоянно развиваются, повышаются требования к преподавателям данной учебной дисциплины, в ходе чего преподаватели более качественно могут передать свои знания и умения курсантам и студентам.

В целом, применение новых образовательных технологий обучения в условиях учебного процесса на кафедрах, при обучении курсантов и студентов, позволяет решать ряд таких важных задач как: повышение интереса к изучаемому предмету; увеличение объема информации по дисциплинам военной подготовки; улучшение качества организации учебного процесса; использование индивидуального характера обучения. создание комплекса учебных пакетов, программ для систем виртуальной подготовки военного специалиста. Таким образом, можно утверждать, что задачи, стоящие на военном факультете по повышению качества подготовки военных специалистов, решаются с применением новых образовательных технологий в области военного образования

В заключении хотелось бы добавить, что использование курсантами инновационных технологий в процессе обучения влечет за собой интенсификацию мышления, обеспечивает высокую активность учебно-познавательной (коммуникативной, творческой) деятельности, позитивное отношение курсантов к предмету усвоения, формирует готовность офицерских кадров к самостоятельным действиям в условиях новизны, помогает развитию внимания и способности его переключения на другие явления по мере необходимости.

Список использованных источников:

1. По материалам Специализированного образовательного портала: Военная литература [Электронный ресурс] <http://militera.lib.ru>.

2. Боевой устав сухопутных войск, часть III, Взвод, отделение, танк.

3. Тактика – искусство боя, учебник И.Н.Воробьев, Москва-2002.

4. По материалам Специализированного образовательного портала: Учебные материалы для студентов [Электронный ресурс] <https://studme.org>

ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ОБУЧЕНИЯ ПРИ ИЗУЧЕНИИ ТАКТИКИ ОБЩЕВОЙСКОВОГО БОЯ

Дубяга Е.В., Круглей В.В.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Бабич В.Н.

Аннотация. В данной статье были рассмотрены доступность, польза и перспектива применения инновационных технологий для изучения дисциплины «Тактика общевойскового боя» и в чем она заключается.

В системе образования за последнее время уделяется значительное внимание по улучшению, систематизации, а также оптимизации процессов получения теоретических знаний и практических навыков обучающимися в военных учебных заведениях таких как военная академия Республики Беларусь, военные факультеты, военные кафедры. На сегодняшний день обучение в системе высшего образования дает хорошие возможности для молодых специалистов, чтобы начать строить карьеру, имея за собой обширный багаж знаний и навыков, которые необходимы для их будущей профессиональной деятельности. Высококвалифицированные рабочие кадры и специалисты высшего звена на данный момент очень востребованы на бирже труда по самым разным направлениям.

Однако выпускники учебных заведений всех уровней во многом не обладают достаточной полнотой знаний ведения общевойскового боя ввиду отсутствия необходимого опыта, который они вынуждены приобретать уже в войсках. Должный профессионализм приобретается во время учений, армейских игр.

При изучении тактики ведения общевойскового боя необходимо приобрести умения такие как твердость в принятии решения, правильной оценки обстановки и общее ее виденье, понимание где, каким образом и чем выгоднее выполнять боевые задачи, тренировать выдержку и приобщаться к штабной культуре. При отсутствии должного воображения и знаний постигнуть искусство ведения общевойскового боя будет трудно. Именно поэтому роль инновационных технологий в войсках стремительно возрастает как для обучения командиров и их личного состава, так и для ведения ими боя. Инновационные технологии позволяют более качественно осуществлять подготовку специалистов, обеспечивают гибкость учебного процесса, что предоставляет возможность вносить в него коррективы в зависимости от объективно меняющихся требований, предъявляемых к специалисту.

Огромную пользу в развитии способностей и интеллектуального и творческого потенциала, слаженности, а также уверенности в действиях принесет применение новых информационных технологий в учебном процессе, которые должны быть направлены на:

- создание виртуальных тренажеров;
- создание обучающих (демонстрационных) программ;
- создание электронных учебных пособий;
- создание тестирующих программ;
- создание электронных учебно-методических комплексов;

Оценивать качество разработанных программ подготовки можно по двум группам критериев: по методической, по технологической. Технологическая дает возможность определить гибкость, простоту и доступность содержания учебного материала. Методическая оценивает комплексность данного материала, а также наличие стадий формирования компетенции: изложение, показ, закрепление и проверка полученных знаний, умений и навыков.

Разработку программ подготовки надлежит реализовывать, опираясь на научном подходе, учитывать непрерывно возрастающие требования к компетенции молодых специалистов, а также к оптимизации самого учебного процесса. В ходе составления программы обучения специалистов время отводится как для теоретических, так и для практических взаимосвязанных занятий, а также проводятся учения и тактико-специальные занятия. На теоретических занятиях дается самая актуальная информация, которую впоследствии отрабатывают на практических занятиях, а в ходе учений, кроме того, взаимодействие с другими подразделениями. Программа подготовки должна отвечать следующим критериям: присутствие структурно-логической связи и оптимальная последовательность в изучении учебных материалов в пределах тем занятий, придерживаться принципа комбинирования.

Оптимизация программы подготовки военных специалистов должна осуществляться, по как минимум трем направлениям: первое — непрерывное совершенствование содержания учебных

материалов, второе — разработка и внедрение новых форм и методов обучения, обеспечивающих возможность в кратчайшие сроки и с наименьшими затратами добиваться максимально высоких результатов по подготовке специалистов, третье — иметь качественный и простой подход к доведению учебного материала и передачи имеющегося опыта преподавателями обучаемым, знать и довести для обучаемых то, в чем заключается важность изучаемого предмета. Чем качественнее и доступнее преподаватели будут проводить свои занятия, тем лучше будет усваиваться учебный материал обучаемыми.

Оценить качество разработанных программ подготовки возможно по двум группам критериев: по методической и по технологической. Технологическая дает возможность определить гибкость, простоту и доступность содержания учебного материала. Методическая оценивает комплексность данного материала, а также наличие стадий формирования компетенции: изложение, показ, закрепление и контроль полученных знаний, умений и навыков.

Современные реалии требуют освоения обучения в сжатые сроки, чего трудно достичь без применения обучающих программ, созданных на основе передовых информационных технологий и научно-исследовательских работ. Они позволяют более наглядно и в доступной форме проводить обучение, объективно контролировать действия обучаемых, своевременно выявлять и устранять допускаемые ошибки. Другими словами, делать процесс обучения более эффективным.

В настоящее время в вооруженных силах стран СНГ используются следующие стрелковые тренажеры: «СКАТТ», «АРГОН», «РУБИН», «Тир», 1УЗЗ-Ижмаш.

Самыми эффективными в плане обучения стрельбе являются тренажеры «СКАТТ» и «РУБИН» (идентичный тренажеру «Сокол М1С»). В них предусмотрена визуализация действий обучаемого. Однако тренажер «СКАТТ» не предусматривает возможности использования панорамного изображения местности. Тренажер «РУБИН» и «Сокол М1С» предусматривают данную возможность.

В тренажерах используется 3D графика, что делает панорамное изображение очень реалистичным и динамичным. Но программа тренажера имеет всего 6 сценариев, не позволяет руководителю занятия самостоятельно изменять условия выполнения упражнения, отсутствует визуализация действий обучаемого, что делает использование данного тренажера в обучении стрельбе малоэффективным.

Тренажеры дают возможность обучать курсантов:

- 1) выполнению упражнений учебных стрельб;
- 2) правильности доклада в ходе их выполнения;
- 3) тренировать курсантов в правильности подачи команд командиром при управлении огнем подразделения.

Программное обеспечение позволяет выводить на экран различные виды местности любое время года и суток, при различных погодных условиях, видоизменять изображение целей: выводить их в виде мишеней, менять их окраску, имитируя маскировку.



Рисунок - 1 Панорамное изображение войскового стрельбища (отображение мишенной обстановки, команды целеуказания, доклада обучающегося)

В процессе изучения учебной дисциплины тактика, курсанты изучают подготовку и ведение всех видов боевых действий: наступления, обороны, встречного боя. История военных конфликтов говорит, что способы ведения боевых действий и используемых вооружений с каждым новым вооруженным конфликтом приобретает новые способы ведения боя, а также изменения и появления новых тактических способов.

Тактика - это одна из составных частей военного искусства, которая охватывает теорию и практику подготовки и ведения боя подразделениями, частями и соединениями видов Вооруженных Сил, родов войск и специальных войск.

Теория тактики направлена на исследование боя, разработки способов его подготовки и ведения. Практика тактики охватывает деятельность командиров (начальников), штабов и войск по подготовке и ведению боя.

Тактику подразделяют на общую тактику, тактику видов Вооруженных сил, тактику родов войск и тактику специальных войск. Эти подразделы охватывают вопросы боевого применения подразделений, частей и соединений Вооруженных Сил, родов войск и специальных войск как в общевойсковом бою, так и самостоятельно, исследования закономерностей боя, рекомендации по его подготовки и ведения, по повышению дальности и эффективности средств огневого поражения, по построению боевого порядка и организации управления и взаимодействия между подразделениями, частями и соединениями видов Вооруженных Сил.

В ходе боевой учебы тактическая подготовка является определяющей дисциплиной. Она - основа полевой выучки войск, занятии которой дают возможность выработать необходимые качества и навыки, способствующие победе в реальном бою. Для изучения тактики в войсках проводятся учения с приближенной к боевой обстановке по условиям, характеру тактических действий войск.

В ходе ее изучения применяются следующие средства наглядности:

- графические (карты, схемы, рисунки, чертежи, таблицы);
- экранные (кинофильмы, диафильмы, телевидение, диапозитивы, слайды);
- объемные (макеты местности, стенды); - имитационные (макеты, модели, очаги пожаров, зоны заражения и районы заграждений, имитация выстрелов и разрывов);
- натуральные (поучительная местность с характерным рельефом, ориентирами, препятствиями, заграждениями, оборудованными позициями; боевая техника, машины управления).

Тактическими действиями - это организованное применение сил и средств подразделений, частей и соединений при выполнении ими поставленных задач.

Основными видами тактических действий является оборона, наступление, марш и расположение на месте.

Основными формами тактических действий являются бой, удар и маневр.

Бой - основная форма тактических действий, направленный на достижение определенного конечного результата.

Современный бой войск является общевойсковым, представляет организованные и согласованные удары, маневры и огонь для уничтожения противника, отражения его ударов и выполнение других тактических задач в ограниченном районе в течении короткого времени. В нем применяются различные силы и средства, построенные в определенные боевые порядки, включающие различные подразделения и соединения видов и родов войск. Тесное и непрерывное взаимодействие разнородных сил и средств позволяет эффективно выполнять поставленные задачи, как результат достигается успех в победе над противником.

Для изучения тактики общевойскового боя курсантами применяются различные методические пособия, в том числе и электронные, тактические карты как бумажные так и интерактивные, осуществляется показ обучающих видеофильмов, а также осуществляется занятия на полигонах и учебных полях, на которых курсанты учатся правильно проводить рекогносцировку местности, оценивать обстановку и принимать решение, отдают боевые приказы, а также тренируются и сдают нормативы с целью более комплексного изучения данной дисциплины.

Использование электронных учебно-методических комплексов, виртуальных тренажеров, просмотр обучающих видеофильмов положительно сказывается как для уменьшения денежных затрат, так и для более наглядного представления дисциплины тактика. Использование интерактивных карт позволяет творчески подходить к обучению путем интерактивного взаимодействия. При просмотре обучающих видеофильмов обучаемый будет воспринимать информацию наглядно и на слух, что способствует лучшему ее усвоению.

В перспективе использование инновационных технологий окупится достаточно быстро, так как сократятся денежные расходы на топливо, боеприпасы, бумагу, чернила и тому подобное.

На данный момент инновационные технологии не заменят занятия в полях или на полигонах в полной мере, но зато позволят более комплексно изучать теоретическую базу различных дисциплин, а также помогут лучше оптимизировать учебный процесс и повысят его информативность и простоту усвоения учебного материала в целом.

Список использованных источников:

1. ТАКТИКА ЧАСТЬ 3 (ВЗВОД ОТДЕЛЕНИЕ ТАНК), ВАРЬ, МИНСК, 2011.

СИСТЕМНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Федоренко В.А.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Аннотация. В докладе рассмотрены основные аспекты комплексной системы защиты информации и системный подход объединяющий разнородные методы и средства противодействия различным видам угроз.

Важнейшим ресурсом современного общества является информация, проблема защиты которой весьма актуальна как для различных стран и организаций, особенно для вооруженных сил.

Обеспечение безопасности функционирования военной организации нашей страны требует привлечения всех имеющихся средств защиты во всех структурных подразделениях и на всех этапах технологического цикла обработки информации. Наибольший эффект может быть достигнут только в том случае, когда все используемые средства, методы и меры объединяются в единый целостный механизм – комплексную систему защиты информации (КСЗИ). При этом функционирование системы должно контролироваться, обновляться и дополняться в зависимости от изменения внешних и внутренних условий [1].

Защита информации требует к себе системного подхода, сущность которого состоит в создании защищенной среды обработки, хранения и передачи информации, объединяющей разнородные методы и средства противодействия угрозам: программно-технические, правовые, организационно-экономические.

В современных условиях КСЗИ также должна иметь несколько уровней защиты, перекрывающих друг друга [2]. Чтобы добраться до закрытой информации, злоумышленнику необходимо «взломать» все уровни.

На каждом рубеже угрозы нарушению безопасности должны быть обнаружены и по возможности ликвидированы, а в случае невозможности ликвидации, их распространению должны препятствовать последующие рубежи. При этом, чем сложнее защита каждого рубежа, тем больше времени потребуется злоумышленнику для его преодоления и тем вероятнее его обнаружение. Из этого следует, что защита каждого рубежа должна взаимно дополнять друг друга и эффективность всей системы защиты будет оцениваться как минимальное время, которое злоумышленник должен затратить на преодоление всех её рубежей. За это время (безопасное время) он должен быть обнаружен и обезврежен сотрудниками службы безопасности.

Количество и пространственное расположение зон и рубежей выбираются таким образом, чтобы обеспечить требуемый уровень безопасности защищаемой информации, как от внешних, так и внутренних злоумышленников. Чем более ценной является защищаемая информация, тем большим количеством рубежей и зон целесообразно окружать ее источник и тем сложнее злоумышленнику обеспечить разведывательный контакт с ее носителями.

В модели КСЗИ необходимо выделить следующие зоны (рубежи, барьеры) защиты: 1) территория, занимаемая организацией; 2) здание (здания) на территории, в котором расположены средства обработки информации; 3) помещения внутри здания, в которых расположены ресурсы автоматизированных систем и защищаемая информация; 4) линии (каналы) связи и источники питания, находящиеся как в пределах одного и того же здания, так и проходящие между различными зданиями на охраняемой территории и выходящие за пределы объекта; 5) аппаратные средства (терминалы пользователей, устройства ввода-вывода данных, центральные процессоры, аппаратные средства шифрования и дешифрования данных, внешние запоминающие устройства, устройства уничтожения информации, другое периферийное оборудование; 6) программные средства, в том числе операционная система и специальные программы, осуществляющие функции защиты и тестовый контроль механизма защиты в КСЗИ; 7) файлы и данные (включая бумажную информацию).

Для каждой из приведенных выше зон возможны четыре степени защиты информации: предотвращение, обнаружение, ограничение, восстановление [1].

На современном этапе необходимо совершенствовать способы борьбы с этим видом нарушений, которые должны носить системный характер, а также учитывать причины и условия их совершения. Все это обуславливает необходимость углубленного изучения принципов организации КСЗИ; способов анализа и оценки угроз безопасности информации; критериев и условий отнесения информации к защищаемой по видам тайн и степеням конфиденциальности и др.

Список использованных источников:

1. Гатчин Ю.А., Климова Е.В. Введение в комплексную защиту объектов информатизации: учебное пособие. – СПб: НИУ ИТМО, 2011 – 112 с.
2. Системный подход к защите информации [Электронный ресурс] – Режим доступа: <https://helpiks.org/7-90293.html>.

ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ ИЗУЧЕНИИ ТАКТИКИ ОБЩЕВОЙСКОВОГО БОЯ

Гаврилов Р.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Лялихов К.А.

Аннотация. Современный общевойсковой бой требует от участвующих в нем войск непрерывного ведения разведки, умелого применения вооружения, техники, средств защиты и маскировки, высокой подвижности и организованности, полного напряжения всех моральных и физических сил, непреклонной воли к победе, железной дисциплины и боевой сплоченности. С появлением новых средств борьбы невиданной мощности и дальнейшим развитием обычного вооружения неизмеримо повысились требования к физической закалке бойцов, к освоению ими оружия и боевой техники, к постоянному совершенствованию тактической выучки войск.

Одним из главных приоритетов и ценностей в нашей стране всегда считалось получение качественного образования. В настоящее время наблюдается широкий потенциал человеческих возможностей и желаний. Так, образование не стоит на месте, а модернизирует свои достижения, ориентируясь на личностный подход в процессе учебной деятельности. Инновационные технологии в образовании становятся вполне обыденной частью учебного процесса.

В образовании инновационные технологии – это новые способы и методы взаимодействия преподавателей и обучаемых, обеспечивающие эффективное достижение результата педагогической деятельности.

Инновационные технологии в образовании – это некий механизм, при помощи которого задействованы новые средства и способы образовательной системы, воплощаемые в реальном мире.

Что же такое сегодня «инновационное образование»? Это такое образование, которое способно к саморазвитию и которое создает условия для полноценного развития всех своих участников; отсюда главный тезис; инновационное образование - это развивающее и развивающееся образование.

Что же такое «инновационная образовательная технология»? Это комплекс из трех взаимосвязанных составляющих:

1. Современное содержание, которое передается обучающимся, предполагает не столько освоение предметных знаний, сколько развитие компетенций, адекватных современной бизнес-практике. Это содержание должно быть хорошо структурированным и представленным в виде мультимедийных учебных материалов, которые передаются с помощью современных средств коммуникации.

2. Современные методы обучения - активные методы формирования компетенций, основанные на взаимодействии обучающихся и их вовлечении в учебный процесс, а не только на пассивном восприятии материала.

3. Современная инфраструктура обучения, которая включает информационную, технологическую, организационную и коммуникационную составляющие, позволяющие эффективно использовать преимущества дистанционных форм обучения [1].

Организовывая занятия по «Тактике» необходимость учёта стиля учения позволяет осуществлять выбор программы индивидуального развития обучающегося в оптимальном для этого обучающегося режиме. Личностная ориентация образовательного процесса на основе учета стиля учения позволяет повысить мотивацию учащихся в условиях вариативности профессиональной подготовки будущих специалистов.

При организации как теоретических, так и практических занятий с курсантами необходимо стремиться к тому, чтобы тактическая обстановка на каждом занятии была максимально приближена к боевой действительности, создавалась без упрощения и шаблона, что способствовало выработке у курсантов познавательного интереса к занятиям тактикой, формированию самостоятельности и разумной инициативы, побуждало курсантов к активным действиям, максимальному использованию возможностей военной техники и вооружения.

С целью повышения эффективности занятий в результате проведения заседаний кафедры были предложены и реализованы на практике различные методические приемы активизации познавательной деятельности курсантов при изучении курса «Тактика». При организации учебных занятий, выборе форм и методов их проведения преподаватели опирались на статистические данные по стилям учения курсантов, полученные в результате наблюдений и проведения диагностических методик «Дихотомический тест», «Диагностический материал по определению доминирования вида восприятия».

Фундаментальные знания и умения, необходимые курсанту для глубокого изучения вопросов тылового обеспечения частей и подразделений в современном общевойсковом бою наиболее эффективно усваивались путем отработки учебно-методических и комплексных тактико-тыловых задач с использованием персональных компьютеров [2].

Практическая подготовка курсантов осуществлялись на основе: выявления общего уровня подготовленности курсантов к отработке каждой темы занятий; определения индивидуальных заданий курсантам с учетом уровня их подготовки накануне каждого занятия и стиля учения; осуществления индивидуального подхода к курсантам непосредственно на занятиях.

Учет стиля учения курсантов при проведении контроля реализовывался на основе возможности выбора формы зачета (беседа с обоснованием выполненного специально разработанного задания; собеседование по билетам, разработанным с практической направленностью; компьютерное тестирование). Такой выбор в наибольшей степени позволял выбрать курсантам форму контроля, более соответствующую его стилю учения [3].

При организации и руководстве самостоятельной работой курсантов, учитывающей их стили учения, осуществлялись: изучение и учет индивидуальных и социально-психологических особенностей курсантов, их учебных стилей; оказание помощи курсантам в овладении методами самостоятельной работы и в ее планировании на основе методики «обучение - закрепление - контроль»; разработка заданий на самостоятельную работу курсантов и методических рекомендаций по их выполнению; проведение групповых и индивидуальных консультаций; обеспечение самостоятельных занятий тренажерными комплексами, учебными приборами, другими техническими средствами обучения и учебными пособиями; контроль за ходом самостоятельной работы курсантов [4].

Виды общевойскового боя.

Основными видами общевойскового боя являются оборона и наступление. В начале войны оборона будет важнейшим и наиболее распространенным видом боя.

Оборона осуществляется преднамеренно или вынужденно с главной целью - остановить наступление противника, нанести ему потери и создать условия для перехода своих войск в наступление. Она будет широко применяться не только в начале, но и в ходе войны. Но одной обороной добиться победы невозможно. Оборона бывает позиционной и маневренной.

Изучение тактики общевойскового боя осуществляется по следующим методам при проведении занятий:

1. Лекционный метод в сочетании с показом (демонстрация) и рассказ-беседой. С целью ознакомить с понятиями боевого, предбоевого и походного порядками отделения и взвода, обеспечением их деятельности.

2. Лекционный метод с использованием наглядных пособий и технических средств обучения. С целью ознакомить с условиями, обеспечивающими успешное выполнение боевых задач войсками и подразделениями; воспитывать инициативу и самостоятельность в сложной обстановке.

3. Рассказ-беседа с практическим показом отдельных положений общей тактики на рельефном макете местности (ящике с песком, классной доске, плакатах, демонстрационных тактических схемах. С целью ознакомить с основами общей тактики и боевых действий вооруженных сил; добиться понимания основ общевойскового боя; на примерах боевого героизма советского народа прививать любовь к Родине и её Вооружённым Силам.

4. Рассказ-беседа (семинар) с применением наглядных пособий (показ) и технических средств обучения. С целью ознакомить с организацией, вооружением и тактикой действий определённых видов вооруженных сил, основными характеристиками их вооружения и боевой техники; воспитывать веру в победу над хорошо вооруженным противником.

5. Рассказ-беседа в ходе групповых упражнений. С целью ознакомить с основами управления отделением; научить обязанностям солдата в бою и привить навыки их выполнения.

6. Тактико-строевое занятие на местности. С целью изучить занимаемую огневую позицию, самоокапываться и маскировать место для стрельбы под огнём противника.

7. Практические занятия методом рассказ-беседы или, например, на местности с предварительным показом приёма метания гранат, которое проводится на учебном поле для тактических занятий или оборудованном учебном городке данного учебного заведения; подготовка учащихся сообщений, рефератов, научных работ; выполнение курсовых работ; самостоятельное изучение материала; выполнение тактических летучек; проведение практических занятий.

Заклучение. Формы и методы обучения следует применять творчески. Умелое их сочетание позволяет успешнее достигать поставленные цели, открывает широкие возможности для осуществления принципа единства и воспитания. Поэтому при планировании занятий по тактике руководитель для достижения поставленных целей должен правильно определить, какие применять формы и методы обучения, чтобы выработать у обучаемых необходимые навыки и умения при действиях в боевой обстановке, в какой последовательности проводить занятия, чтобы постепенно усложнять условия обучения, переходить от простого к более сложному.

Список использованных источников:

1. Войниленко Н.В. Совершенствование контрольно-оценочных процессов как фактор управления качеством начального общего образования. // Мир науки, культуры, образования. - № 4 (23) – 2010. – с.148-150
2. Загашев И.О., Заир-Бек С.И. Критическое мышление. Технология развития. СПб.: Альянс «Дельта». - 2003
3. Колоткин Ю.Н., Муштавинская И.В. Образовательные технологии и педагогическая рефлексия. СПб.: СПб ГУПМ. – 2002, 2003
4. Тактика : учебник [ув. МО РБ]. Кн. 3 : Взвод, отделение, танк / С. М. Абрамов [и др.]. - Минск : ВА РБ, 2012. - 602 с.

ЗАДАЧИ, ПРИЕМЫ И СПОСОБЫ ДЕЙСТВИЙ БОЕВЫХ ГРУПП В НАСТУПЛЕНИИ В ГОРОДЕ (ПО ОПЫТУ БОЕВЫХ ДЕЙСТВИЙ В ЛОКАЛЬНЫХ ВООРУЖЕННЫХ КОНФЛИКТАХ)

Шутко А.П.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Сименков Е.Л.

Аннотация. В данной статье были рассмотрены Задачи, приемы и способы действий боевых групп в наступлении в городе (по опыту боевых действий в локальных вооруженных конфликтах).

В войнах и вооруженных конфликтах последнего времени боевые действия ведутся, как правило, в городе (населенном пункте), и за город, в которых имеется большое количество каменных, железобетонных и кирпичных объектов, легко приспособляемых и переоборудуемых в оборонительные сооружения.

Обороняющиеся могут длительное время вести бой, неся минимальные потери и, одновременно, нанося жесткое поражение наступающим в живой силе и технике.

Исходя из опыта ведения боевых действий в городе возникает необходимость пристального изучения тактики подразделений в данных условиях, ее всестороннего анализа и последующего совершенствования. Эта проблема была и остается актуальной.

При ведении боя в городе (населенном пункте) встречается целый ряд трудностей. Прежде всего, в городе ограничен обзор и наблюдение, затруднен маневр техники и ведение огня. Вот почему бой в данных условиях требует огромного напряжения сил, решительных действий, железной выдержки, умения действовать оружием в любой ситуации и в любом положении, смелой и разумной инициативы.

Безусловно, основой основ является высокая профессиональная подготовка каждого солдата и, следовательно, индивидуальная тактика. Но только слаженные действия профессионалов в конечном итоге приведут к успеху, победе. Поэтому подробно проанализируем групповую тактику или по-другому – тактику «мелких» подразделений.

Задачи боевых групп в наступлении.

Взвод (отделение) в городе действует по боевым группам («двойкам», «тройкам», «четверкам») Имея надежную связь, четкое взаимодействие, поддерживая друг друга огнем и маневром, боевые группы при поддержке танков, БМП последовательно овладевают зданиями, оставляя в захваченных домах своих пулеметчиков, снайперов для прикрытия. Две группы, поддерживая друг друга огнем, достигнут большего и будут иметь меньше потерь, чем группа большого состава, без прикрытия и поддержки.

Командиру отделения может указываться:

- направление наступления;
- полоса выдвижения;
- рубеж перехода в атаку (или условный сигнал на переход в атаку);
- способ и объект атаки;
- направление продолжения наступления.

Старшему каждой боевой группы может указываться: направление наступления, полоса выдвижения, рубеж перехода в атаку (или условный сигнал на переход в атаку), способ атаки противника (с фронта, с выходом во фланг или в тыл, одновременно с соседней боевой группой или самостоятельно, с применением средств задымления или без них), объект атаки и направление продолжения наступления.

Старшие боевых групп определяют соответствующие задачи каждому солдату в ходе выдвижения к переднему краю противника (сближении с противником). Указанные задачи могут уточняться через каждые 50-100 м или ставиться заново (с учетом характера действий противника, потерь в личном составе, и т.д.).

Интервалы между военнослужащими боевой группы должны быть пять-шесть шагов.

Каждому военнослужащему, с учетом условий местности, на направлении действий группы указываются две-три огневых позиции, которые необходимо менять после нескольких коротких очередей.

Каждому военнослужащему боевой группы назначаются секторы стрельбы (основной и дополнительный), они должны перекрываться между военнослужащими, которые действуют рядом, не меньше чем на 10-15 градусов (170-250 тысячных), создавая зону сплошного огня [1].

Выдвижение на рубеж перехода в атаку совершается на дистанциях, которые обеспечивают визуальное наблюдение за действиями друг друга и взаимную поддержку огнем.

Атака противника совершается, как правило, под прикрытием дымов после максимально возможного сближения с ним (как с фронта, так и с выходом в один из флангов или тыл).

Перемещение на поле боя выполняется последовательно и бессистемно, с использованием условных сигналов (жестов) и команд.

Исходя из указанных требований, каждому "номеру" боевой группы определяются следующие задачи:

1. Задачи первого (в данном случае – стрелка):

- передвигаться на поле боя разными способами до указанного рубежа;
- вести разведку противника и местности на дальностях от 300 до 500 м;
- преодолевать минно-взрывные заграждения и препятствия;
- немедленно открывать неприцельный огонь разными способами в течении 2-3 секунд на глубину до 100 метров перед собой;
- оружие держать в готовности до немедленного применения – палец на спусковом крючке, куда глаза – туда и ствол.

2. Задачи второго и третьего:

- поддерживать перемещение первого стрелка ведением прицельного огня из-за укрытия по 3-5 секунд, на дальностях от 300 до 500 м с бессистемной сменой огневых позиций (выстрел – смена огневую позицию);
- вести разведку противника и местности на глубину от 500 до 700 м;

Старший группы управляет действиями боевой группы.

3. Задачи четвертого, пятого, шестого (вторая боевая группа):

- вести разведку противника и местности на глубину от 500 до 700 м;
- поддерживать прицельным огнем из-за укрытия по 3-5 секунд на дальностях до 500 м действия первой боевой группы (первого, второго и третьего номеров) с бессистемной сменой огневых позиций;
- выявлять и уничтожать бронированные цели противника на расстояниях от 300 до 500 м;

4. Задачи седьмого (механика-водитель, водителя - третья боевая группа):

- наблюдать за дорогой (местностью на маршруте движения) до 50 м и сигналами (условными жестами) командира отделения;
- выводить боевую машину на запланированные огневые позиции (укрытия) по команде;
- менять огневые позиции (укрытия) после каждой очереди пушки (пулемета).

5. Задачи восьмого (наводчика-оператора) - третья боевая группа:

- вести разведку противника и местности на дальностях до 2000 м;
- прикрывать прицельным огнем по 3-5 секунд, действия первых двух групп на дальностях от 600 до 1200 м [2].

При движении вдоль улицы в пешем порядке подразделения (боевые группы) одновременно продвигаются с обеих сторон, вдоль стен, бросками от укрытия к укрытию. Боковым зрением постоянно фиксировать возможные движения на чердаках, балконах, в окнах, а также быть в готовности укрыться за бетонным бордюром, сгоревшей машиной, в канаве, воронке и открыть ответный огонь или огонь на упреждение.

Когда подразделение (боевая группа) продвинулось вперед на 60–70 м, укрылось и открыло прицельный огонь, должна подтягиваться группа прикрытия (другая боевая группа). Огонь необходимо вести по целям, расположенным на противоположной стороне улицы, не забывая контролировать обстановку позади себя.

Группа прикрытия также не должна терять бдительности – противник может появиться с тылу.

Таким образом, действуя в населенном пункте, необходимо соблюдать следующие правила:

- «мотострелки» должны достоверно установить, идут ли справа и слева другие подразделения;
- строго соблюдать правило – никому не отставать и не вырываться вперед;
- не оставлять за собой непроверенные объекты. Очищенные от противника здания должны закрепляться специально назначенными подразделениями из состава вторых эшелонов.

Список использованных источников:

1. Специальные действия [Электронный ресурс]: учебник / С. М. Абрамов, И. А. Гордейчик, [и др.]. – Минск: ВА РБ, 2015. – электрон. опт. диск (CD-R).
2. Тактика. Специальные действия. Учебник/ Гордейчик И.А., Абрамов С.М. [и др.]: – Минск: ВА РБ, 2016.

ЭФФЕКТИВНОСТЬ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА НА БАЗЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УЧРЕЖДЕНИЯХ ВОЕННОГО ОБРАЗОВАНИЯ

Прокопенко В.А.

*«Белорусский государственный университет информатики и радиоэлектроники»,
Минск, Республика Беларусь*

Сименков Е.Л.

Аннотация: Эффективность применения информационных технологий в системе военного образования. Раскрываются положительные и отрицательные стороны применения информационных технологий. Учитываются особенности профессиональной компетенции преподавателя в вопросе эффективности образовательного процесса. Перечисляются различные средства информационных технологий, которые могут использоваться в процессе обучения.

Профессиональное военное образование, сосредоточенное на лидерстве, теории и практике управления, военной истории и оперативной доктрине, национальной оборонной политике, планировании и принятии решений, правовых обязанностях и профессиональной этике, является фундаментом Вооруженных Сил Республики Беларусь. Система военного образования должна быть прочной, надежной, отвечать требованиям времени и быть рассчитанной на дальнейшую перспективу.

Выпускники военных вузов должны быть готовы решать самые сложные задачи, для реализации которых необходимо разрабатывать эффективные образовательные программы, постоянно анализировать знания и умения, полученные в учебных заведениях.

Основываясь на это, нужно быть готовым вносить изменения в учебные программы, совершенствовать обучающие технологии, внедрять в учебный процесс положительный опыт нашей страны и зарубежных стран.

В связи с этим возникает необходимость расширения границ применения информационных технологий в системе военного образования, для того, чтобы обеспечить доступ курсантов к получению знаний, умений и первоначального профессионального опыта. Всё это создаёт предпосылки для повышения качества обучения и изменения характера образовательной деятельности, а также появлению современных технологий и инструментов, позволяющие преподавателю применять активные методы обучения.

В современных условиях развития информационных технологий во всех социально-экономических процессах является также неотъемлемой частью и в образовании военных специалистов. Стремительное развитие и широкое распространение глобальной компьютерной сети выявило актуальность и привело к необходимости внедрения информационно-коммуникационных технологий в сфере военного образования. Внедрение инновационных подходов, информационных систем и технологий в учебный процесс является важной составляющей подготовки военных специалистов (курсантов). Преподаватели также должны помнить, что они призваны донести до курсантов новейшие методы и формы работы, учитывая запросы современного общества для воспитания нового поколения профессионалов сегодня в соответствии с требуемыми стандартами. Для этого необходимо уделить должное внимание информационной составляющей при подготовке нового учебного материала, что позволит подать информацию для курсантов в более интересной, познавательной и близкой к реальности форме.

Информационные технологии позволяют моделировать реальные условия оперативно-боевой обстановки, дают возможность осуществлять тренировку не только в принятии необходимых управленческих решений, но и осуществлять профессиональную подготовку. Компьютерные средства обучения позволяют решить следующие задачи:

- обеспечить для каждого курсанта объём работы с изучаемым материалом и последовательность, состоящую в чередовании изучения теории, разбора примеров, отработки первоначальных профессиональных навыков, решения типовых компетентностно-ориентированных заданий;

- обеспечить возможность самоконтроля качества приобретённых знаний и умений;

- сократить время, необходимое для изучения материала.

Однако следует учитывать и тот факт, что чрезмерное применение компьютеров и компьютерных технологий в образовании также негативно может сказаться на развитии интуиции, мышления, неспособности к тщательному анализу и нехватки навыков межличностного общения. Наряду с этим существует также проблема отбора качественной и достоверной информации. Информационные технологии дают положительный результат только в случае, когда это использование даёт неоспоримый педагогический эффект.

Именно поэтому необходима разработка и реализация программ военного образования, основанных на системно-целостном подходе к организации учебного процесса.

По моему мнению, система подготовки военных специалистов, будет эффективной при условии соблюдения следующих организационных и педагогических требований:

- во-первых, в необходимости разработки стратегии специальной, профессиональной и информационной подготовки на основе системного подхода;

- во-вторых, информационные технологии будут всесторонне применяться в педагогическом процессе в комбинации трех взаимосвязанных компонентов - объектов обучения, инструментов для изучения военных дисциплин и новых технологий обучения;

- в-третьих, изучение предметов будет осуществляться непрерывно, поэтапно, последовательно в течение всего периода обучения с учетом принципов организации образовательно-информационной среды;

- в-четвертых, помимо общеобразовательных программ, в расписание необходимо будут включить прикладные темы, ориентированные на предметную область и профессиональную среду будущей деятельности военного специалиста;

- в-пятых, элементы информационных технологий, используемые в ходе обучения, будут соответствующим образом сочетаться с традиционной технологией и поддерживаться текущими техническими средствами.

Подбор и систематизация информационных технологий являются отдельным аспектом в повышении качества приобретения знаний курсантами. Большое значение для обучения является использование мультимедийного оборудования: мультимедийные проекторы, экраны для проекторов, ЖК-телевизоры, интерактивные электронные доски. Все эти средства информационных технологий оживляют обучение, делают его более понятным, интересным, образовательно эффективным и позволяет за минимальное время более четко представить учебный материал, разделить наиболее значимое от второстепенного и сосредоточить внимание курсантов на важных деталях изучаемого материала.

Современные педагогические нововведения связаны с использованием интерактивных методов обучения, при которых курсанты могут взаимодействовать, вести диалог, сотрудничать. Интерактивное обучение - это особая форма организации познавательной деятельности, имеющая конкретное, целевое назначение - создать комфортную среду обучения. Суть интерактивных технологий в том, что обучение происходит через взаимодействие всех обучаемых. Преподаватель выступает только в качестве организатора обучения, координатора учебных групп. Интерактивные технологии обучения являются наиболее подходящим подходом в образовательном процессе. Воспитательная работа осуществляется путем совмещения системы контроля фазы слушания и модульно-рейтинговой технологии обучения, обеспечивается не только направлением курсантов на профессионально-специальное обучение, но и отвечает принципам развития их творческих способностей и формирования навыков.

Использование современных информационных технологий в военном образовании позволяет увеличить объем запоминаемой информации и скорость ее обработки, улучшает качество самого учебного процесса, позволяет успешно «переваривать» огромное количество сложной и абстрактной информации в простой и понятной форме, повышает уровень интереса к учебе, познанию и тренировке; способствует росту профессиональной мотивации.

Многофункциональный, интегративный, непрерывный и многоуровневый характер профессиональной военной подготовки курсантов требует применения инновационных методов обучения: создание проектов, подготовка публичных выступлений, дискуссионное обсуждение профессионально важных проблем, обучение в сотрудничестве, создание проблемных ситуаций, подготовка профессионально направленных видеофильмов и презентаций и т. д.

Таким образом, внедрение новых технологий в образовательный процесс является объективным процессом, вектор которого определяется научно-техническим прогрессом, компьютеризацией и технологизацией общества, а также особенностями различных составляющих системы образования. Все компоненты методики обучения должны быть сосредоточены на том, чтобы сделать обучение максимально доступным и эффективным. Использование информационных и компьютерных технологий в обучении специальных дисциплин может значительно повысить уровень обучения курсантов и таким образом поднять уровень своих знаний. Информационные технологии - это универсальный инструмент, который при правильном использовании значительно помогает в обучении во всех областях.

Непрерывные темпы внедрения новых технологий, возобновление серьезной конкуренции великих держав - все это способствует ощущению того, что интеллектуальная ловкость и инновации имеют важное значение для обеспечения конкурентоспособности Вооруженных Сил Республики Беларусь в современное время.

Список использованных источников:

1. Совецание по вопросам развития системы военного образования [Электронный ресурс] – Режим доступа: <https://topwar.ru/36139-soveschaniye-po-voprosam-razvitiya-sistemy-voennogo-obrazovaniya.html>. – Дата доступа 25.03.2019.

2. Башкатов И. В. Информационные технологии в подготовке военных педагогов // Молодой ученый. – 2017. – №3.1. – С. 2-4. – URL [Электронный ресурс] – Режим доступа: <https://moluch.ru/archive/137/38209/> (дата обращения: 25.03.2019).

ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ВООРУЖЕННЫХ СИЛ. РАЗРАБОТКА И РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Хрипач Н.А.

*Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь*

Дудак М. Н. – магистр тех. Наук

Аннотация. Данный доклад посвящен обсуждению мер, которые необходимо реализовать для обеспечения защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности. Рассмотрение данной темы позволит определить основные проблемы и слабые места в системах безопасности войск связи, а также предложить рекомендации по усовершенствованию существующих механизмов защиты.

С развитием информационных технологий и сетевых технологий в последние годы угрозы безопасности в информационной сфере становятся все более серьезными. Войска связи Вооруженных Сил Республики Беларусь, как и любые другие организации, подвергаются угрозам кибербезопасности, которые могут иметь негативное влияние на их работу и деятельность.

Защита информационных ресурсов от кибератак и других угроз безопасности является одной из важнейших задач в области кибербезопасности. Критические объекты, такие как войска связи Вооруженных Сил Республики Беларусь, требуют особого внимания в вопросах обеспечения их кибербезопасности.

Задача обеспечения защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности является одной из ключевых проблем в области кибербезопасности [1].

Современные информационные технологии позволяют быстро и эффективно обрабатывать огромные объемы информации. Однако, это также открывает возможности для киберпреступников, которые могут использовать различные способы для получения несанкционированного доступа к информации, в том числе через войска связи.

Войска связи Вооруженных Сил Республики Беларусь имеют важное значение для обеспечения связи между военными и цивилизованными учреждениями, а также для связи между различными частями вооруженных сил. Поэтому, защита информационных ресурсов войск связи от кибератак и других угроз безопасности является ключевой задачей для обеспечения эффективности и безопасности их работы.

Основными угрозами для войск связи являются кибератаки, вирусы, трояны, фишинговые атаки, а также атаки на инфраструктуру связи. Кроме того, многие угрозы могут появиться изнутри организации, включая несанкционированный доступ к информации со стороны сотрудников и подрядчиков, несоблюдение правил безопасности, ошибки в процессе обработки информации и другие.

В настоящее время, во многих странах, включая Республику Беларусь, существует система защиты информационных ресурсов, которая включает в себя меры по предотвращению и обнаружению кибератак и других угроз. Однако, такие меры защиты не всегда эффективны и требуют дальнейшего совершенствования.

Одним из основных способов обеспечения защиты информационных ресурсов в войсках связи является использование современных технологий кибербезопасности, включая программное и аппаратное [2].

Кроме того, важным элементом защиты информационных ресурсов в войсках связи является разработка и внедрение соответствующих стандартов и правил использования информационных систем и сетей. Это включает в себя установку средств защиты, таких как антивирусные программы, межсетевые экраны и системы обнаружения вторжений, а также контроль доступа и аутентификацию пользователей.

Кроме того, не менее важным является регулярное обновление и модернизация информационных систем и сетей. Это позволяет улучшать их защиту и приспосабливать к новым видам угроз. Важно также обучать персонал военной связи использованию информационных систем и сетей, а также правилам информационной безопасности, чтобы минимизировать ошибки и уязвимости, возникающие из-за неопытности или небрежности пользователей.

Однако, защита информационных ресурсов в войсках связи является более сложной задачей, чем просто установка антивирусного программного обеспечения или межсетевого экрана. Во-первых, военная связь имеет свои специфические особенности, например, большой объем информации, передаваемой в режиме реального времени, и необходимость быстрого реагирования на изменения в боевой обстановке. Во-вторых, военная связь подвергается более высоким угрозам, чем другие

организации, так как она играет ключевую роль в обеспечении боеспособности Вооруженных Сил Республики Беларусь.

Таким образом, для обеспечения защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности необходимо использовать комплексный подход, который включает в себя как технические, так и организационные меры [3]. Это включает в себя не только установку антивирусного программного обеспечения и межсетевых экранов, но и разработку и внедрение соответствующих стандартов и правил использования информационных систем и сетей, а также обучение персонала военной связи.

Другой распространенной угрозой безопасности являются фишинговые атаки, которые часто используются для получения доступа к конфиденциальной информации. Фишинговые атаки могут быть выполнены путем отправки электронных писем, которые кажутся легитимными, но на самом деле являются поддельными и предназначены для получения доступа к информации, такой как логины, пароли или банковские данные. Чтобы защититься от фишинга, сотрудники войск связи должны быть обучены узнавать поддельные электронные письма и никогда не предоставлять личную информацию в ответ на такие письма.

С другой стороны, кибератаки могут быть проведены также с использованием вредоносных программ, таких как вирусы, трояны или черви. Эти программы могут проникнуть в информационную систему, чтобы украсть данные, вывести из строя систему или использовать ее в качестве платформы для других кибератак. Чтобы предотвратить атаки с использованием вредоносных программ, сотрудники войск связи должны использовать антивирусное программное обеспечение и обновлять его регулярно.

Помимо этого, войска связи могут стать жертвами кибершпионажа. Кибершпионы могут использовать различные методы, такие как перехват трафика, кража логинов и паролей, и другие, для получения доступа к конфиденциальной информации. Чтобы защититься от кибершпионажа, необходимо использовать шифрование данных, а также установить меры контроля доступа к конфиденциальной информации.

Одним из ключевых моментов в обеспечении безопасности информационных ресурсов является правильная организация процесса управления безопасностью. Войска связи должны иметь четкие процедуры и политики в отношении безопасности информации, которые должны строго соблюдаться всеми сотрудниками. Кроме того, необходимо проводить регулярную аудиторию информационных систем для выявления уязвимостей и устранения их вовремя.

Также важным моментом является контроль за доступом к информационным ресурсам военной связи. Военнослужащим следует выделять доступ к конкретным данным в соответствии с их должностными обязанностями и уровнем допуска. Это позволит уменьшить риски утечки конфиденциальной информации, а также предотвратить нежелательный доступ к данным со стороны третьих лиц.

Одним из наиболее эффективных способов защиты информационных ресурсов войск связи является использование специализированного программного обеспечения [4]. Такое ПО позволяет обнаруживать кибератаки и другие угрозы безопасности, блокировать подозрительный трафик, а также принимать меры по восстановлению работоспособности системы в случае атаки.

Но необходимо понимать, что технические средства не могут полностью защитить информационные ресурсы от кибератак. Поэтому решающим фактором становится обучение и профессиональная подготовка военнослужащих, ответственных за обеспечение безопасности информационных ресурсов. Только обученный персонал сможет быстро и эффективно реагировать на киберугрозы и предотвратить их негативные последствия.

Важно отметить, что задача обеспечения безопасности информационных ресурсов военной связи является многоплановой и требует комплексного подхода. Для достижения максимальной эффективности необходимо сочетать технические и организационные меры, включая контроль за доступом к информационным ресурсам, обучение и профессиональную подготовку военнослужащих, а также использование специализированного программного обеспечения.

Таким образом, обеспечение защиты информационных ресурсов в войсках связи Вооруженных Сил Республики Беларусь от кибератак и других угроз безопасности является важной задачей, требующей постоянного внимания и усилий. Необходимо развивать средства защиты информационных ресурсов и повышать квалификацию

Список использованных источников:

1. А. А. Минаев, А. А. Колесников, В. М. Гершман. Обеспечение безопасности информационных систем вооруженных сил. Материалы VII Международной научно-технической конференции "Информационная безопасность и защита информации", 2016.
2. М. М. Левин. Информационная безопасность в военном строительстве. Электронное научное издание "Вестник Южно-Уральского государственного университета", 2015.
3. И. А. Смирнов, В. Г. Кравцов. Комплексный подход к защите информации в военных организациях. Материалы конференции "Информационная безопасность в телекоммуникационных системах", 2017.
4. А. С. Поляков. Информационная безопасность в вооруженных силах. Материалы конференции "Актуальные проблемы информационной безопасности в современном мире", 2018.

ИНТЕГРАЦИЯ НОВЫХ ТЕХНОЛОГИЙ И ИННОВАЦИОННЫХ РЕШЕНИЙ В СИСТЕМЫ СВЯЗИ И УПРАВЛЕНИЯ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Хрипач Н.А.

*Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь*

Дудак М. Н. – магистр тех. наук

Аннотация. Целью доклада является рассмотрение возможностей интеграции новых технологий и инновационных решений в системы связи и управления в войсках связи Вооруженных Сил Республики Беларусь. Наша задача - рассказать о преимуществах такой интеграции и предоставить конкретные примеры внедрения этих технологий и решений.

Обзор существующих систем связи и управления в войсках связи Вооруженных Сил Республики Беларусь

Для начала необходимо рассмотреть текущие системы связи и управления в войсках связи Вооруженных Сил Республики Беларусь.

В настоящее время используются различные средства связи, такие как радио-, радиорелейные-, тропосферные и спутниковые станции, сети связи, средства передачи данных и т.д. Управление производится через КНП, которые обеспечивают координацию и контроль действий военных связистов.

Однако, текущие системы связи и управления имеют ряд недостатков:

1. Ограниченная пропускная способность: Старые системы связи могут иметь ограниченную пропускную способность, что может привести к задержкам в передаче данных, нестабильности соединений и другим проблемам, которые могут негативно повлиять на командование и контроль военных операций.

2. Необходимость частой замены оборудования: Технологии быстро меняются, и оборудование, которое было современным несколько лет назад, может уже устареть и не соответствовать требованиям современных задач и операций. Это может привести к необходимости частой замены оборудования, что требует дополнительных затрат на обучение персонала и закупку новых средств связи.

3. Сложность интеграции новых технологий и решений: Интеграция новых технологий и решений может быть сложной и требовать дополнительных затрат на обучение персонала и настройку систем. Более того, в некоторых случаях новые технологии и решения могут не совместимы с существующим оборудованием и системами, что может потребовать замены большого количества компонентов [1].

Одним из дополнительных недостатков является отсутствие гибкости системы, что затрудняет быстрое и эффективное реагирование на изменяющиеся требования и ситуации.

Например, в случае возникновения кризисной ситуации, когда необходимо быстро передавать большие объемы данных и координировать действия разных подразделений, текущая система связи и управления может оказаться недостаточно эффективной.

Также следует отметить, что текущие системы связи и управления требуют высокой степени квалификации и опыта от военных связистов, что может быть проблематично при наборе новых кадров и подготовке кадров в кратчайшие сроки.

Все эти недостатки могут приводить к задержкам, ошибкам и неправильной координации действий, что в свою очередь может негативно сказываться на результативности операций и безопасности войск.

Новые технологии и инновационные решения в системах связи и управления

Существуют многообещающие новые технологии и инновационные решения, которые могут быть интегрированы в системы связи и управления в войсках связи Вооруженных Сил Республики Беларусь. Например, это могут быть технологии, основанные на искусственном интеллекте, которые позволяют анализировать и обрабатывать большие объемы данных, предоставляя более точную информацию о положении и действиях врага.

Для анализа данных в Вооруженных Силах часто используются методы машинного обучения и искусственного интеллекта. Например, анализ изображений с помощью компьютерного зрения может помочь идентифицировать объекты и распознавать лица на видеозаписях, а анализ данных сонаров и радаров может помочь обнаруживать и классифицировать объекты в морских и воздушных пространствах.

Одним из примеров применения анализа данных в Вооруженных Силах является создание системы управления боевыми действиями [2]. Такая система включает в себя анализ данных с

различных источников, включая данные разведки и наблюдения, и предоставляет информацию командирам о текущей ситуации на поле боя. Это позволяет быстро принимать решения и адаптировать тактику, чтобы достичь успеха в боевых действиях.

Кроме того, анализ данных в Вооруженных Силах может использоваться для мониторинга и предотвращения кибератак, определения вероятных угроз и прогнозирования будущих событий [3].

Например, анализ социальных медиа-данных может помочь предотвратить насилие или террористические акты, а анализ трафика данных может помочь обнаружить кибератаки на информационную инфраструктуру Вооруженных Сил.

В целом, анализ данных является важной составляющей военных операций и обеспечивает Вооруженным Силам возможность получать ценную информацию из больших объемов данных, что позволяет принимать более обоснованные и эффективные решения.

Также можно использовать технологии блокчейн. Примеры использования технологии блокчейн: Управление запасами. Военные организации должны иметь доступ к ресурсам и запасам, необходимым для выполнения своих задач. Блокчейн-технологии могут помочь упростить и оптимизировать управление запасами, улучшив прозрачность и контроль над цепочкой поставок. Технология может помочь обеспечить прозрачность и эффективность процесса закупки, отслеживания, распределения и учета запасов.

Финансовые транзакции. Блокчейн-технологии могут использоваться для обеспечения безопасности и прозрачности финансовых транзакций в Вооруженных Силах. Технология может обеспечить точность, прозрачность и быстроту обработки финансовых операций, позволяя улучшить управление бюджетом и снизить возможность мошенничества и коррупции.

Обеспечение безопасности и целостности данных. Вооруженные силы могут использовать блокчейн-технологии для защиты данных и обеспечения их целостности. Технология может помочь защитить конфиденциальность данных, предотвратить несанкционированный доступ и манипуляции с данными.

Контроль доступа. Блокчейн-технологии могут использоваться для управления доступом к различным системам и ресурсам в Вооруженных Силах. Технология может помочь обеспечить безопасность и контроль доступа к конфиденциальной информации, установив точную и автоматизированную систему авторизации и идентификации пользователей.

Кроме того, новые технологии и решения в области связи могут быть основаны на волоконно-оптических линиях связи, которые имеют высокую скорость передачи данных и обеспечивают стабильную связь на больших расстояниях. Также можно использовать беспилотные летательные аппараты, которые обеспечивают более широкий охват связи и управления в труднодоступных местах.

Примеры интеграции новых технологий и инновационных решений в системы связи и управления

Примером является использование искусственного интеллекта для обработки больших объемов данных и анализа информации о положении и действиях врага [4]. Это позволяет военным связистам получать более точную и полную информацию о противнике, что помогает принимать более обоснованные решения.

Также можно использовать беспилотные летательные аппараты для обеспечения связи и управления на труднодоступных территориях. Это позволяет получать информацию о состоянии территории и действиях врага без необходимости высылать туда людей.

Важным примером инновационного решения является использование технологии блокчейн для обеспечения безопасности передачи данных и управления доступом к ним. Это позволяет защитить данные от несанкционированного доступа и внесения изменений, что крайне важно в военных операциях.

В целом, интеграция новых технологий и инновационных решений в системы связи и управления в войсках связи Вооруженных Сил Республики Беларусь может значительно повысить эффективность их деятельности и обеспечить более быстрый и точный обмен информацией на поле боя.

Список использованной литературы:

1. Соколов, Д. А. Инновационные технологии в системах связи и управления в войсках связи, Электронный журнал "Наука и техника в XXI веке". – 2019. – № 1. – С. 25-30.
2. Бабич, А. В. Разработка и исследование системы управления средствами связи на основе инновационных технологий, Материалы научно-технической конференции "Системы связи и управления в информационном обществе". – 2017. – С. 45-49.
3. Шатский, А. А. Особенности интеграции инновационных решений в системы связи и управления в войсках связи, Сборник научных трудов "Современные проблемы радиотехники, телекоммуникаций и связи". – 2016. – Вып. 15. – С. 135-138.
4. Кузьмич, И. П. Интеграция новых технологий в системы связи и управления в войсках связи Вооруженных Сил Республики Беларусь, Научно-технический вестник Беларуси. – 2018. – № 3. – С. 51-56.

ОПТИМИЗАЦИЯ СТРУКТУРЫ И ФУНКЦИОНИРОВАНИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И УСЛУГ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ В КОНТЕКСТЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЧЕСКИХ ТРЕНДОВ

Хрипач Н.А.

*Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь*

Дудак М. Н. – магистр тех. наук

Аннотация. Этот текст обсуждает возможности оптимизации структуры и функционирования инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь в контексте современных технологических трендов. В тексте рассматриваются основные технологические тренды, такие как облачные технологии, Интернет вещей (IoT), большие данные (Big Data) и искусственный интеллект (AI), а также предлагаются меры для оптимизации работы инфокоммуникационных систем и услуг. Оптимизация может включать внедрение новых технологий, обучение персонала, оптимизацию процессов работы и повышение безопасности. В целом, перспективы развития инфокоммуникационных систем и услуг в Вооруженных Силах Республики Беларусь в контексте современных технологических трендов очень благоприятны.

В современном мире информационные технологии играют важную роль во всех сферах деятельности, включая военную. В Вооруженных Силах Республики Беларусь также существует необходимость в использовании современных технологий в области связи и информационных систем.

В данном докладе мы рассмотрим возможности оптимизации структуры и функционирования инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь в контексте современных технологических трендов.

В настоящее время наблюдается быстрое развитие технологий, связанных с обработкой, хранением и передачей информации [1].

В сфере военной связи и информационных систем существует несколько основных технологических трендов:

1. Облачные технологии - это технология, позволяющая обрабатывать и хранить данные на удаленных серверах. Облачные технологии позволяют сократить расходы на оборудование и программное обеспечение, а также увеличить гибкость и масштабируемость системы.

2. Интернет вещей (IoT) - это технология, позволяющая управлять устройствами и получать данные с них через Интернет. В военной сфере IoT может использоваться для управления беспилотными летательными аппаратами, танками и другими военными машинами.

3. Большие данные (Big Data) - это технология, позволяющая анализировать и обрабатывать большие объемы данных. В военной сфере большие данные могут использоваться для прогнозирования событий, анализа действий противника и принятия решений на основе большого количества данных.

Искусственный интеллект (AI) - это технология, позволяющая компьютерам анализировать данные и делать выводы на основе обучения и опыта. В военной сфере искусственный интеллект может использоваться для анализа данных, прогнозирования событий и управления боевыми системами.

Для эффективного использования современных технологий в сфере военной связи и информационных систем необходимо оптимизировать структуру инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь [2].

Оптимизация может включать следующие меры:

- внедрение облачных технологий для улучшения гибкости и масштабируемости системы связи;

- внедрение облачных технологий в Вооруженные Силы Республики Беларусь может быть применено в различных сферах, таких как управление, хранение и обработка информации, а также коммуникации.

Одним из примеров применения облачных технологий в военной сфере может быть использование облачных хранилищ для хранения и обработки больших объемов данных, таких как изображения и видео, полученные с беспилотных летательных аппаратов или других военных систем. Это позволит ускорить процесс обработки данных и повысить их точность и качество.

Также военные коммуникационные системы могут использовать облачные технологии для повышения масштабируемости и гибкости системы, а также снижения затрат на оборудование и программное обеспечение.

Например, военные коммуникационные системы могут использовать облачные платформы для создания и управления виртуальными машинами, которые могут использоваться для различных целей, включая передачу данных и обмен информацией.

Для внедрения облачных технологий в военной сфере могут использоваться различные методы, включая разработку собственных облачных решений.

Использование IoT для управления беспилотными летательными аппаратами, танками и другими военными машинами.

Применение технологии Big Data для анализа и обработки больших объемов данных, в том числе для прогнозирования событий и анализа действий противника.

Внедрение искусственного интеллекта для улучшения анализа данных, прогнозирования событий и управления боевыми системами.

Также необходимо обеспечить защиту информации, передаваемой по системам связи, в том числе с помощью средств шифрования и контроля доступа к данным.

Для оптимизации работы систем связи и услуг необходимо изучить их текущее состояние и выявить возможные проблемы и узкие места. Это позволит разработать план мероприятий по оптимизации работы систем связи и услуг, который включает в себя следующие шаги:

Внедрение новых технологий и обновление существующего оборудования может включать в себя:

- установку нового оборудования для передачи и обработки данных;
- переход на облачные технологии;
- улучшение программного обеспечения и т.д. [3].

Обучение персонала.

Оптимизация функционирования инфокоммуникационных систем также может зависеть от уровня знаний и навыков персонала, использующего эти системы. Регулярное обучение может помочь повысить квалификацию персонала и улучшить производительность систем.

Оптимизация процессов работы.

Повышение эффективности работы инфокоммуникационных систем может быть достигнуто путем оптимизации процессов и процедур работы. Это может включать в себя улучшение процессов мониторинга и управления системами, улучшение процессов поддержки и обслуживания пользователей и т.д.

Повышение безопасности.

Одним из главных требований к военным информационным системам является высокий уровень безопасности. Оптимизация функционирования инфокоммуникационных систем может включать в себя внедрение дополнительных мер защиты и повышение уровня безопасности систем.

Мониторинг и анализ производительности систем.

Регулярный мониторинг и анализ производительности систем может помочь выявить проблемы и недостатки, которые могут приводить к снижению производительности систем. На основе этого анализа можно разработать меры по оптимизации функционирования инфокоммуникационных систем и услуг.

Результаты и выводы данного исследования показывают, что внедрение современных информационных технологий и облачных вычислений в военную инфраструктуру Вооруженных Сил Республики Беларусь является важным шагом в обеспечении эффективности и надежности функционирования систем связи и передачи данных.

Оптимизация работы инфокоммуникационных систем и услуг является необходимым условием для эффективной работы военных частей и повышения общей безопасности. Для достижения этой цели, необходимо использовать современные методы оптимизации, такие как автоматизация, мониторинг и анализ производительности, управление ресурсами, сокращение времени доступа и др.

В целом, перспективы развития инфокоммуникационных систем и услуг в Вооруженных Силах Республики Беларусь в контексте современных технологических трендов очень благоприятны [4].

Внедрение новых технологий позволит повысить эффективность работы военных частей, улучшить связь и передачу данных, а также обеспечить более высокий уровень безопасности и защиты важных данных.

Список использованных источников:

1. Ковалева, Е. А. (2018). Актуальные проблемы и перспективы развития информационных и коммуникационных технологий в Вооруженных Силах Республики Беларусь, Молодой ученый, №5 (184), с. 40-43.
2. Информационно-аналитический центр при Президенте Республики Беларусь. (2017). Анализ современных технологий и обеспечения информационной безопасности в военных организациях. Минск: ИАЦ.
3. Клименок, В. А. (2016). Инфокоммуникационные технологии в современных условиях, Научные труды БГТУ, №2, с. 114-118.
4. Белоус, В. М., & Богданович, В. С. (2019). Проблемы и перспективы развития инфокоммуникационных систем в войсках связи Вооруженных Сил Республики Беларусь, Военная мысль, №4, с. 58-66.

ОСОБЕННОСТИ АДАПТАЦИИ ВОЕННОСЛУЖАЩИХ К УСЛОВИЯМ БОЕВЫХ ДЕЙСТВИЙ В ПЕРИОД БОЕВОГО СЛАЖИВАНИЯ

Лейбук Е.В.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Вербицкий Г.И.

Аннотация. В данной статье рассмотрены актуальные вопросы психологической адаптации военнослужащих к условиям боевых действий с учетом отсутствия боевого опыта.

Трудности адаптации и эмоциональный стресс в боевых условиях становятся большой проблемой для военнослужащих.

Опыт боевых действий вооруженных конфликтов последнего десятилетия, в том числе опыт боевых действий в Украине показывает неослабевающую актуальность этих вопросов и важность их для успешных тактических результатов в бою.

Необходимость психологической подготовки военнослужащего к предстоящим боевым действиям была и остается одной из ключевых обязанностей офицеров тактического звена наряду с боевой подготовкой, подготовкой вооружения, военной и специальной техники или материально-техническим обеспечением в мирное время. Рассмотренный вариант предлагается для проведения скорейшей адаптации военнослужащих в период боевого слагивания как для военнообязанных (призванных из запаса) так и для военнослужащих срочной военной службы [1].

Коммуникативные возможности как способ адаптации. Для успешной адаптации конкретного военнослужащего также весьма значимо то, как к нему относятся окружающие. Положительное отношение окружающих способствует адаптации, а отрицательное, напротив, затрудняет протекание адаптационных процессов.

Психологическая саморегуляция - это осознанное целенаправленное динамическое изменение отдельных психофизиологических функций и психического состояния в целом посредством специально организованной психической активности [2].

Комплекс методов:

- нервно-мышечная релаксация;
- дыхательные техники;
- концентрация;
- аутотренинг;
- медитация;
- кинезиологическая гимнастика;
- индивидуальный навыковый тренинг;
- групповые психологические тренинги и др. [2].

Психологическая полоса препятствий как средство успешной адаптации военнослужащих к факторам боевой обстановки в период боевого слагивания.

Психологическая полоса препятствий - комплекс профессионально значимых препятствий (учебных позиций), расположенных в 3-5 м друг от друга и преодолеваемых военнослужащими в едином упражнении.

Цель – создать психический образ, а это то, что человек увидел, услышал, пережил. Полоса может располагаться на участке территории, реже в учебных помещениях или спортивном зале [3].

Имитацией разрушений, «погибших» животных и людей (муляжи), в затрудненных условиях - в сумерках, в темноте (плохо просвечивающая повязка на глазах), при сильном ветре, дожде, снеге, гололеде, при контрастах света и темноты.

Таким образом, процесс адаптации к условиям боевой обстановки затрагивает все аспекты функционирования человека. При этом, успех адаптации во многом зависит от особенности личности военнослужащего, его коммуникативных возможностей, а также условий, способствующих приобретению опыта восприятия и переживания факторов современного боя.

Следовательно, в обязанности каждого офицера при формировании у подчиненных тех личностных качеств, которые обеспечивают успешность адаптации в самых разнообразных, в том числе и экстремальных, условиях.

Список использованных источников:

1. Березин Б.Ф. Психическая и психофизиологическая адаптация человека. JL, 2018. - 375 с.
2. Маклаков А.Г. Военная психология: Учебник для вузов. — СПб: Питер. — 2007. — 583 с.
3. Караяни А.Г. Полоса психологической подготовки. За и против.— Москва : Юрайт, 2022. - 593 с.

ПРАКТИКО-ОРИЕНТИРОВАННОЕ ОБУЧЕНИЕ – ВАЖНЕЙШЕЕ УСЛОВИЕ ПОДГОТОВКИ ВОЕННЫХ СПЕЦИАЛИСТОВ

Дудкин А.Е.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Мартыненко В.О.

Боевые действия в Украине сейчас изучают специалисты всех стран, т.к. там на практике проверяются концепции и доктрины ведения боевых действий, разработанные в разных странах для их уточнения и коррекции. Впервые за последние несколько десятков лет произошел военный конфликт между двумя современными технологически сопоставимыми вооруженными силами с применением всего арсенала обычных средств поражения, искусственного интеллекта, использованием информационного пространства над полем боя, массовых боев в городских условиях.

За всем этим стоит человеческий фактор, его качественные, особенно морально-психологические характеристики.

В настоящее время к военным специалистам предъявляются следующие требования: профессиональная компетентность, морально-психологическая готовность и устойчивость к профессиональным трудностям, в том числе на поле боя, дисциплинированность и др. Современное образование, не теряя своей фундаментальности, приобретает новое, практико-ориентированное содержание, цель которого, развитие у обучаемых профессиональных компетенций практической работы и понимания, где их применить на практике.

В отличие от традиционного образования, ориентированного на усвоение знаний, практико-ориентированное обучение направлено на приобретение опыта практической деятельности, который выступает как готовность обучаемых к определенным действиям на основе имеющихся знаний, умений и навыков. Приобретение общих знаний будущей профессии требуется для качественного исполнения в будущем должностных обязанностей.

Результаты различных исследований показывают, что в среднем, только 25% военнослужащих осознанно используют полученные в результате обучения знания в реальных условиях, что указывает на необходимость формирования конкретных, стандартных и стандартизуемых навыков и умений.

Чем ближе учебно-боевая подготовка будет приближена к реальным условиям предстоящей практической деятельности обучаемых, тем ближе мотивы, цели, действия, операции у будущих военных специалистов будут приближены к тем, которые требуются для успешного выполнения ими своих функциональных обязанностей и решения повседневных задач.

По этой причине в процессе учебной подготовки целесообразно увеличивать массив практико-ориентированного обучения.

Подходы к практико-ориентированному обучению можно разделить по следующим направлениям:

1. Доведение во время обучения в ВУЗе базовых профессиональных умений и навыков по профилю подготовки до уровня классного специалиста. В воинские части должны направляться уже обученные и подготовленные к управлению подразделениями, обслуживанию (работе) боевой и иной техники, применению стрелкового и иного вооружения специалисты.

2. Внедрение современных профессионально-ориентированных технологий обучения, нацеленных на формирование умений и навыков (получения опыта) по будущей специальности, таких как интерактивных, цифровых, виртуальных и др.

3. Подготовка учебно-тренировочной базы, ее оснащение. Наиболее эффективными считаются макетирование поля предстоящего боя, моделирование (имитация) действий противника в реальных пространственно-временных параметрах, моделирование боевых событий с использованием тренажеров и компьютерных систем, психологические полосы препятствий и т.п.

4. Формирование в процессе обучения личности будущих офицеров, как военных руководителей, которые должны соответствовать духовно-нравственным, деловым, профессиональным и другим необходимым качествам.

Подобные методы подготовки у нас в настоящее время не применяются, но их внедрение в практику процесса учебной деятельности не требует особых компетенций и научных разработок. Зато позволит с значительно повысить эффективность процесса обучения, придать ему практически ориентированную направленность.

РАЗВИТИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ ВОЕННОГО НАЗНАЧЕНИЯ

Митько Е.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Масейчик Е.А.

Аннотация. Данная статья рассматривает возможности применения облачных технологий для хранения и обработки информации военного назначения.

Современная военная техника становится все более сложной и информатизированной, что в свою очередь требует увеличения объемов и качества обработки информации. Для решения этих задач военные используют облачные технологии.

Облачные технологии позволяют хранить и обрабатывать большие объемы данных, а также предоставлять доступ к этим данным из разных мест и устройств. Это особенно важно для военных операций, когда необходимо быстро получать доступ к информации из разных частей вооруженных сил.

Одним из основных преимуществ облачных технологий является возможность создания единой информационной среды. Облачные решения позволяют интегрировать различные информационные системы и создавать единую информационную базу, что повышает эффективность работы и обеспечивает более быстрый и точный обмен информацией между подразделениями [1].

Кроме общих преимуществ облачных технологий, существуют и некоторые специфические возможности, которые эти технологии могут предоставить для военной сферы. Например, использование облачных технологий может улучшить управление логистикой и снабжением, что особенно важно для проведения длительных операций вдали от баз.

Также облачные технологии могут быть использованы для обработки и хранения данных с различных источников, таких как дроны, камеры видеонаблюдения, датчики и т.д. Это может помочь военным получать более полную и точную картину обстановки на поле боя.

Еще одним преимуществом облачных технологий является возможность использования распределенных вычислений. Это означает, что различные вычислительные ресурсы могут быть объединены в единую сеть, что позволяет выполнять более сложные вычисления и задачи. Кроме того, облачные технологии обладают высокой степенью гибкости. В случае изменения задач и потребностей в обработке информации, можно быстро изменить настройки и параметры облачной системы, что обеспечивает быстрое реагирование на изменения в ситуации на поле боя [2].

Еще одним важным аспектом развития облачных технологий для военной сферы является возможность использования искусственного интеллекта (ИИ). Современные системы ИИ могут быстро анализировать большие объемы данных и выдавать наиболее значимые результаты, что позволяет военным принимать более обоснованные решения. К примеру, анализ видео- или аудиозаписей с помощью ИИ может помочь идентифицировать угрозы и опасности на поле боя [2].

Необходимо отметить, что использование облачных технологий для военных нужд может значительно сократить затраты на развитие и поддержание инфраструктуры. Вместо того чтобы иметь множество различных серверов и хранилищ данных, военные могут использовать единую облачную платформу, которая может быть настроена для выполнения различных задач и функций.

Однако использование облачных технологий в военной сфере также сопряжено с определенными рисками. Одним из основных рисков является возможность кибератак на информационные системы, использующие облачные технологии. Чтобы предотвратить такие атаки, необходимо использовать высокие стандарты защиты данных и систем безопасности.

Несмотря на эти ограничения, облачные технологии продолжают развиваться и улучшаться, предоставляя все больше возможностей для военной сферы. Развитие этих технологий позволяет военным получать более точную и оперативную информацию, улучшать качество принимаемых решений и повышать эффективность военных операций.

В заключение можно сказать, что развитие облачных технологий является важным направлением развития военной информационной технологии. Это позволяет улучшить качество и скорость обработки информации, создать единую информационную среду и повысить эффективность военных операций. Однако для использования облачных технологий в военной сфере необходимы высокие стандарты защиты данных и систем безопасности.

Список использованных источников:

1. Исследование "Облачные технологии в системах защиты информации государственных структур" от Института инновационных технологий и телекоммуникаций.
2. Статья "Cloud Computing and the Military" в журнале *Defense Acquisition Research Journal*.

КИБЕРБЕЗОПАСНОСТЬ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Остапчук Ю.М.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Масейчик Е.А.

Аннотация. В докладе рассмотрены перспективы и преимущества использования мобильных технологий в военных операциях, а также выделены основные проблемы и уязвимости, связанные с их использованием.

Современные войска связи Республики Беларусь используют компьютерные сети и Интернет для передачи и обработки информации. Это делает их уязвимыми для кибератак и других угроз. Поэтому необходимо создание мощной системы кибербезопасности, которая будет обеспечивать защиту от взлома и хакерских атак [1].

Для обеспечения кибербезопасности в Вооруженных Силах Республики Беларусь необходима система, которая будет включать в себя несколько ключевых элементов. Например, для обеспечения конфиденциальности передаваемых сообщений и данных необходимо использовать криптографические методы и технологии.

Криптография - это наука о методах защиты информации от несанкционированного доступа, использования и изменения. Системы шифрования данных и коммуникаций должны быть построены на основе новейших алгоритмов и стандартов, обеспечивающих надежность и безопасность передачи информации [2].

Для защиты от взлома и хакерских атак необходимо использовать средства защиты информации, такие как брандмауэры, антивирусы, антишпионы и другие.

Брандмауэры используются для блокирования несанкционированных соединений и передачи информации, антивирусы обнаруживают и блокируют вирусы, антишпионы - для защиты от шпионского ПО.

Еще один элемент системы кибербезопасности - это контроль и управление доступом к информации. Для этого необходимо использовать системы аутентификации и авторизации, позволяющие определить, кто имеет доступ к каким данным и какие действия могут выполнять.

Одним из самых важных элементов системы кибербезопасности является обучение и подготовка персонала, который будет работать с системами связи и защиты информации. Специалисты должны иметь не только технические знания и навыки, но и понимание основных принципов кибербезопасности.

Для эффективной работы системы кибербезопасности Вооруженных Сил Республики Беларусь, необходимо также учитывать множество факторов, таких как персональные данные, защита облачных систем хранения данных, а также обеспечение безопасности мобильных устройств и приложений [2].

При работе с облачными системами хранения данных, необходимо использовать меры защиты, такие как многофакторная аутентификация, шифрование данных и аудит действий. Также необходимо строго контролировать доступ к информации в облачных системах, предоставляя его только необходимому количеству пользователей с минимальными правами доступа.

При использовании мобильных устройств, таких как смартфоны и планшеты, необходимо использовать средства защиты информации, такие как антивирусы, антишпионы, брандмауэры и VPN-сервисы. Также необходимо обеспечивать регулярное обновление операционной системы и установленных приложений для минимизации рисков уязвимостей и уязвимых мест [2].

Для обучения и повышения квалификации специалистов в области кибербезопасности, Вооруженные Силы Республики Беларусь могут использовать различные методы, такие как обучение в учебных центрах, симуляторах и компьютерных тренажерах. Также возможно привлечение экспертов в области кибербезопасности для проведения тренингов и мастер-классов.

В целом, система кибербезопасности Вооруженных Сил Республики Беларусь должна обеспечивать надежную защиту от кибератак и других угроз, которые могут возникнуть при использовании информационно-коммуникационных систем и услуг.

Важно понимать, что создание и поддержание такой системы требует постоянного мониторинга и обновления технологий и методов защиты, а также обучения и подготовки специалистов в области кибербезопасности.

Список использованных источников:

1. *Электронный ресурс министерства обороны РБ.*
2. *Электронный ресурс министерства связи и информатизации Республики Беларусь*

ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Готин Н.А.

*Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь*

Федоренко В.А.

Аннотация. Рассматриваются проблемы реализации в перспективе единого инфокоммуникационного пространства Вооруженных Сил Республики Беларусь. Приводится перечень перспективных информационных и телекоммуникационных технологий, практическое применение которых должно обеспечить реализацию ЕИКП с требуемой функциональностью.

В современных условиях роль системы связи при управлении группировками войск (сил) на театре военных действий (далее ГВ(С) на ТВД) существенно возрастает. Этот тезис сегодня приобретает особую значимость, так как именно система связи, выполняя задачи обеспечения информационного обмена в системе управления, должна быстро реагировать на изменения обстановки, динамично изменять свою структуру, совершенствовать способы построения и режимы работы.

Достигнуть этого возможно только путем создания эффективной системы управления ГВ(С) на ТВД, функционирующей в едином информационном пространстве (ЕИП), способной в реальном масштабе времени обрабатывать информацию, вырабатывать информационные воздействия и доводить приказы и команды до боевых платформ.

Инновационность системы связи неразрывно связана с технической составляющей современных Вооруженных Сил и может быть определена следующими признаками:

- интенсивная сменяемость поколений техники связи и автоматизации, быстрое внедрение принципиально новых, нетрадиционных технологий в образцы средств связи;
- опережение любой армии мира в комплексах технических средств связи на поколение;
- нахождение в войсках не более двух поколений однотипных комплексов технических средств связи;
- разработка новых перспективных способов организации связи и построения системы связи [1].

В обобщенном виде эволюция технологий может иллюстрироваться данными, приведенными в таблице 1.

Таблица 1 – Перечень представительных технологий и эволюция их развития

Технологии	XX век	2000-2015 г.г.	2016 г. и далее
Телекоммуникационные	ISDN. Internet	Internet. Корпоративные сети. NGN. IMS. 4G (мобильные) Web 2.0	Широкополосные конвергентные сети. Самоорганизующиеся сети.
Информационные	Системы «клиент-сервер». Распределенные вычисления. Распределенные БД	Сервисноориентированные архитектуры. Системы поддержки принятия решений. Системы управления знаниями. Многоагентные локальные системы	Системы управления знаниями. Многоагентные глобальные системы. Интеллектуальные агенты реального времени
Поддержки эксплуатационных процессов	TMN. TMF	NGOSS. Системы поддержки принятия решений	Интеллектуальные системы поддержки эксплуатационных процессов.
Формализация знаний о проблемной области	Спецификации. Языки визуального моделирования	Языки визуального моделирования. Онтологии отдельных проблемных областей	Универсальные онтологии для Глобального инфокоммуникационного пространства

Таким образом, развитие и применение информационных и телекоммуникационных технологий в долгосрочной перспективе коренным образом изменит структуру и принципы построения системы связи ГВ(С) на ТВД и потребует перестроения организационных структур соединений и воинских частей связи. Эти процессы будут направлены в первую очередь на обеспечение управления ГВ (С) на ТВД при подготовке и ведении военных действий в едином информационном пространстве. Реализация инновационных подходов в построении систем связи позволит уже в ближайшее время подойти к решению проблемы создания единого информационного пространства.

Список использованной источников:

1. Буренок. В.М. К инновационной армии. – Воздушно-космическая оборона, 2009. – № 3. – С. 16-25.

ВЗАИМОДЕЙСТВИЕ ВОЕННЫХ И ГРАЖДАНСКИХ ИНФРАСТРУКТУР СВЯЗИ В УСЛОВИЯХ ВОЕННЫХ ДЕЙСТВИЙ

Кириллюк Н.Н.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Федоренко В.А.

Аннотация. Данная научная работа посвящена вопросам взаимодействия военных и гражданских инфраструктур связи в условиях военных действий. Рассматривается актуальность проблемы и ее влияние на эффективность ведения военных действий. Анализируются особенности взаимодействия между военными и гражданскими инфраструктурами связи, а также предлагаются практические рекомендации по улучшению данного взаимодействия. Особое внимание уделено вопросам безопасности и защиты информации в условиях военных действий. Результаты исследования могут быть использованы в практической деятельности при разработке и внедрении новых подходов к взаимодействию военных и гражданских инфраструктур связи в условиях военных действий.

Военные действия могут приводить к разрушению гражданской инфраструктуры связи, что затрудняет обмен информацией между военными и гражданскими службами. Однако, в то же время, военные инфраструктуры связи могут быть использованы гражданскими службами в целях обеспечения связи в зоне военных действий [1].

В настоящее время существует несколько подходов к взаимодействию военных и гражданских инфраструктур связи. Например, один из подходов состоит в использовании так называемых "военных операторов связи". Это специалисты, которые обладают знаниями и навыками в области связи и работают на военных объектах. Они могут быть задействованы в качестве консультантов гражданских служб при возникновении проблем с связью в зоне военных действий [1].

Кроме того, существуют специальные комплексы связи, которые могут использоваться как военными, так и гражданскими службами в случае необходимости. Эти комплексы обеспечивают высокую степень защищенности информации и могут использоваться для организации связи на крупных объектах, таких как аэропорты или вокзалы [2].

Важным аспектом взаимодействия военных и гражданских инфраструктур связи является обучение персонала гражданских служб правилам использования военных инфраструктур связи. Это позволит ускорить процесс взаимодействия и уменьшить количество ошибок при использовании этих инфраструктур [2].

В заключение, можно сказать, что взаимодействие военных и гражданских инфраструктур связи является важным аспектом военных действий. Для обеспечения эффективного взаимодействия необходимо создание специальных команд, использование новых технологий и оборудования, а также обучение персонала гражданских служб правилам использования военных инфраструктур связи [3].

Для улучшения взаимодействия военных и гражданских инфраструктур связи также необходимо обеспечить эффективное управление данным процессом. В частности, следует разработать механизмы координации и согласования действий между военными и гражданскими службами, а также обеспечить своевременный обмен информацией и ресурсами. Кроме того, необходимо учитывать особенности местности и ситуации в зоне военных действий при выборе той или иной формы взаимодействия между военными и гражданскими инфраструктурами связи. Все эти меры позволят обеспечить эффективное и безопасное взаимодействие между военными и гражданскими службами в условиях военных действий [3].

Однако, важно понимать, что взаимодействие военных и гражданских инфраструктур связи является сложным и многогранным процессом, который требует совместных усилий со стороны всех заинтересованных структур и организаций. В этом контексте, необходимо развивать межведомственное взаимодействие и взаимодействие с промышленными предприятиями, которые способны обеспечить необходимое оборудование и технологии для создания инфраструктур связи в зонах военных действий. Кроме того, важно проводить совместные учения и тренировки для совершенствования навыков и умений по организации взаимодействия между военными и гражданскими службами связи в условиях реальных угроз и рисков [4].

Список использованных источников:

1. Казанцева Е. В. Информационная безопасность в условиях взаимодействия военных и гражданских инфраструктур связи // Материалы конференции "Современные информационные технологии и информационная безопасность". - Москва: Издательство МГТУ им. Н. Э. Баумана, 2021. - С. 99-103.
2. Кравченко В. Н., Беляева Е. Н. Взаимодействие военных и гражданских инфраструктур связи в условиях военных действий // Материалы конференции "Информационные технологии и защита информации". - Москва: Издательство МГТУ им. Н. Э. Баумана, 2018. - С. 158-162.
3. Бабаков А. В., Жуковский В. С. Взаимодействие военных и гражданских служб связи в условиях локальных вооруженных конфликтов // Материалы конференции "Современные информационные технологии и IT-образование". - Краснодар: Издательство ЮФУ, 201
4. Хабибуллин А. Р., Габдуллин Р. З. Технические средства связи в военной деятельности // Сборник научных трудов "Современные проблемы техники и технологии". - Казань: КГТУ, 2019. - С. 127-130.

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ ВОЙСК СВЯЗИ ВС РБ

Листванович А.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Федоренко В.А.

Аннотация. В статье рассматриваются преимущества искусственного интеллекта и машинного обучения при разработке инфокоммуникационных систем для войск связи ВС РБ, включая обработку естественного языка, компьютерное зрение, прогнозную аналитику и оптимизацию сети, подчеркивается их потенциальное влияние на повышение эффективности связи, ситуационной осведомленности и производительности сети в военных операциях.

Инфокоммуникационные системы имеют решающее значение для войск связи, поскольку они обеспечивают эффективную и безопасную связь в ходе различных боевых действиях. В связи с быстрым развитием новых технологий, таких как искусственный интеллект (ИИ) и машинное обучение (МО), для войск связи важно понимать их влияние на информационно-коммуникационные системы и то, как их можно использовать для улучшения управления в ходе боевых действий [1].

В наши дни искусственный интеллект предлагает быстрые решения для большинства повседневных задач. На рисунке 1 можно заметить, что рост интереса к решениям такого типа прослеживается ежегодно.

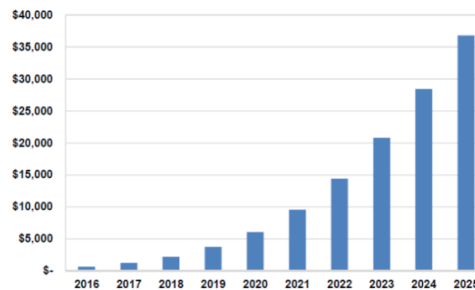


Рисунок 1 – Оценка рынка искусственного интеллекта в миллионах долларов

ИИ и МО имеют множество преимуществ для связи в разработке инфокоммуникационных систем. Например, обработка естественного языка (NLP) может использоваться для разработки чат-ботов и виртуальных помощников, которые могут обеспечивать перевод в режиме реального времени, что позволяет более эффективно и результативно общаться с союзниками и партнерами из разных стран.

Компьютерное зрение также может быть использовано при разработке систем наблюдения, которые имеют решающее значение в военных операциях [2]. Эта технология может позволить выявлять потенциальные угрозы и повышать ситуационную осведомленность, тем самым повышая безопасность и защищенность войск.

Прогнозная аналитика – еще одно применение ИИ и МО, которое может быть полезно для связи. Анализируя большие объемы данных, предиктивная аналитика может помочь предсказать потенциальные проблемы и определить области для улучшения в системах связи, обеспечивая более эффективную и действенную связь в операциях.

ИИ и МО также можно использовать для оптимизации производительности сети. Эта технология может анализировать сетевой трафик и настраивать сетевые ресурсы, обеспечивая более надежную и эффективную связь в операциях даже в сложных условиях.

В заключение, ИИ и МО имеют многочисленные преимущества для связи в разработке инфокоммуникационных систем. Эти технологии могут повысить эффективность связи, улучшить ситуационную осведомленность и повысить производительность сети, что позволит повысить эффективность военных операций. Поскольку ИИ и МО продолжают развиваться, важно, чтобы войска связи изучили их потенциальные приложения и последствия для разработки инфокоммуникационных систем.

Список использованных источников:

1. Олссон, Э.С., Хеделин, П., и Мондал, С. Роль искусственного интеллекта в военной связи: Журнал оборонной науки, 2019, 166с.
2. Искусственный интеллект и машинное обучение: возможности и проблемы в коммуникационных сетях. [Электронный ресурс] / Альянс отраслевых решений для телекоммуникаций (ATIS). – 2018 – Режим доступа: <https://www.atis.org/technologies/artificial-intelligence-ai/ai-and-machine-learning-opportunities-and-challenges-in-communication-networks/> – Дата доступа: 30.03.2023.

РАЗВИТИЕ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ВОЕННЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ТЕХНОЛОГИЙ

Новицкий И.Р.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Федоренко В.А.

Аннотация: В работе рассматривается роль и возможности использования облачных технологий в военном образовании. Облачные технологии являются инструментом современной образовательной среды, позволяющим повысить эффективность образовательного процесса, создать персонализированные образовательные траектории, проводить онлайн-тестирование и контроль знаний. Также описываются успешные примеры использования облачных технологий в образовательной среде военных учебных заведений в Республике Беларусь и других странах. Работа включает анализ облачных образовательных платформ, перспективы и проблемы использования облачных технологий в будущем, а также оценку эффективности их использования в военном образовании.

Современные технологии позволяют внедрять в процесс обучения военнослужащих связи новые методы и средства, которые значительно повышают эффективность обучения и позволяют увеличить уровень подготовки солдат и офицеров. Одним из таких инновационных подходов является интеграция виртуальных и расширенных реальностей в процесс обучения военных связистов. Эти технологии позволяют создавать более реалистичные ситуации и условия, которые помогают военнослужащим лучше подготовиться к выполнению своих обязанностей на практике. Благодаря этому, интеграция виртуальных и расширенных реальностей в процесс обучения становится все более актуальной для военных связистов, которые должны быть готовы к выполнению сложных задач в любых условиях.

Интеграция облачных технологий в процесс обучения военных специалистов будет являться инновационным подходом, повышающий эффективность обучения военнослужащих. В то же время облачные технологии предоставляют инструменты для создания современной образовательной среды в военных учебных заведениях. Роль облачных технологий в повышении эффективности обучения, возможности их использования для создания персонализированных образовательных траекторий, контроля знаний обучающихся, реализации системы электронного документооборота, проведения онлайн-тестирования и обеспечения информационной безопасности являются важными темами для исследования в области военного образования. Разработка облачных сервисов для проведения дистанционных лекций и семинаров, развитие системы онлайн-тестирования и использование облачных платформ для проведения военных симуляций и тренировок также важны для развития военного образования в будущем.

Одним из основных преимуществ облачных технологий в образовании является возможность получения доступа к информации и ресурсам из любой точки мира при помощи интернета. Это позволяет обучаемым изучать материалы и выполнять задания даже во время нахождения военной службы в другом регионе или стране. Другим преимуществом облачных технологий является более высокий уровень безопасности и защиты данных, поскольку данные хранятся в виртуальном хранилище, а не на локальных устройствах. Кроме того, облачные технологии могут поддерживать совместные проекты и совместную работу между обучающимися и преподавателями. Это позволяет создавать возможности для коммуникации и сотрудничества между обучающимися и улучшает качество образования. Для того чтобы использовать облачные технологии в обучении, необходимо настроить соответствующую инфраструктуру, включая организацию доступа к высокоскоростному интернету и серверам, которые будут обеспечивать хранение и обработку данных.

Помимо преимуществ, использование облачных технологий в обучении военных специалистов также имеет некоторые недостатки. Первым недостатком является зависимость от доступности интернета и стабильности сетевой связи. Если интернет-соединение недоступно или низкого качества, то обучающиеся могут столкнуться с проблемами доступа к необходимым ресурсам. Вторым недостатком является возможность утечки конфиденциальных данных. Хранение информации в облаке может представлять определенный риск, поскольку она может быть доступна не только обучающемуся, но и третьим лицам. Третьим недостатком является ограниченный доступ к учебным материалам и ресурсам во время оффлайн-режима. В случае отсутствия доступа к Интернету обучающиеся не смогут получить доступ к своим учебным материалам и ресурсам. Четвертым недостатком является высокий уровень стоимости облачных технологий. Настройка и поддержка инфраструктуры для использования облачных технологий может быть дорогой.

В целом, использование облачных технологий в военных учебных заведениях имеет огромный потенциал, а также имеет свои недостатки, которые необходимо учитывать перед их внедрением. Но при правильном подходе использование облачных технологий может оказаться эффективным инструментом в обучении и подготовке военных специалистов.

1. Облачные технологии как инструмент современной образовательной среды в военных учебных заведениях.
2. Роль облачных технологий в повышении эффективности образовательного процесса в военных учебных заведениях.
3. Возможности облачных технологий в создании персонализированных образовательных траекторий для обучающихся в военных учебных заведениях.
4. Облачные технологии как инструмент содействия в процессе обучения военных специалистов в Вооруженных Силах Республики Беларусь.
5. Опыт использования облачных технологий в образовательном процессе военных учебных заведений в других странах.
6. Примеры успешной реализации облачных технологий в образовательном процессе военных учебных заведений в Республике Беларусь.
7. Использование облачных технологий в создании системы электронного документооборота в военных учебных заведениях.
8. Возможности использования облачных технологий для проведения онлайн-тестирования и контроля знаний обучающихся в военных учебных заведениях.
9. Проблемы, связанные с использованием облачных технологий в образовательном процессе военных учебных заведений.
10. Облачные технологии и проблемы информационной безопасности в военных учебных заведениях.
11. Влияние облачных технологий на профессиональную подготовку военных специалистов в Вооруженных Силах Республики Беларусь.
12. Роль облачных технологий в повышении качества образования в военных учебных заведениях.
13. Развитие системы онлайн-тестирования с помощью облачных технологий для оценки знаний.
14. Реализация облачной платформы для проведения военных симуляций и тренировок в военных учебных заведениях.
15. Использование облачных сервисов для обеспечения безопасности информации и данных в военных учебных заведениях.
16. Перспективы использования и развития облачных технологий в военном образовании в будущем.
17. Примеры успешной реализации облачных технологий в образовательной среде военных учебных заведений.
18. Оценка эффективности использования облачных технологий в образовательном процессе военных учебных заведений и планы на будущее.
19. Возможности облачных сервисов для проведения дистанционных лекций и семинаров.

В заключение, можно отметить, что современные технологии, включая облачные, позволяют существенно увеличить эффективность и качество обучения военнослужащих, что в свою очередь приведет к повышению уровня подготовки и доведению до максимально возможного уровня профессиональных навыков. Внедрение виртуальных и расширенных реальностей в процесс обучения военных связистов также играет важную роль в подготовке к выполнению сложных задач в реальных условиях. Однако, следует учитывать и проблемы, возникающие в процессе использования облачных технологий, такие, как информационная безопасность. Несмотря на это, перспективы использования облачных технологий в военном образовании кажутся очень обнадеживающими. Развитие и дальнейшее совершенствование облачных технологий должно быть нацелено на максимальное повышение качества подготовки военнослужащих и эффективности военного образования в целом.

Список использованных источников:

1. *Облачные технологии и образовательный процесс в высшей школе: методические рекомендации / Под ред. В.Н. Хохлова, И.Е. Баранцевой, М.В. Беляева. - Москва: МЦФЭР, 2016. - 187 с.*
2. *Абакумова, И.В., Букин, В.Н. Использование облачных технологий в военном образовании // Инновационные технологии в образовании. - 2018. - Т. 1, № 28. - С. 24-27.*
3. *Ханнанов, Р.И., Романов, М.А. Особенности применения облачных технологий в военном образовании // Наука, техника и образование. - 2019. - Т. 7, № 6. - С. 15-18.*
4. *Винокурова, Т.А., Беляков, А.В. Применение облачных технологий в образовательном процессе военного вуза // Информационные технологии в науке, образовании и производстве. - 2019. - Т. 17, № 1. - С. 14-19.*
5. *Куркин, А.А., Смулевич, А.Б. Облачные технологии в высшем военном образовании: перспективы и проблемы // Вестник Военной академии Республики Беларусь. - 2020. - № 3 (79). - С. 145-150.*
6. *Сатимов, А.С., Лугин, А.Г. Особенности использования облачных технологий в военных учебных заведениях // Военно-технический вестник. - 2020. - Т. 6, № 3. - С. 58-63.*
7. *Куркин, А.А., Смулевич, А.Б. Облачные технологии в высшем военном образовании: опыт, проблемы, перспективы // Научно-технический вестник информационных технологий, механики и оптики. - 2021. - Т. 21, № 1. - С. 157-162.*

АКТУАЛЬНЫЕ ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ

Пеляк Г.В.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь)*

Федоренко В.А.

Современный мир, где технологии продолжают развиваться, не обходится без различных видов угроз, направленных на нарушение безопасности информации. В настоящее время, киберпреступники и хакеры развивают свои методы преступной деятельности пропорционально совершенствованию технических инструментов, используемых для борьбы с ними. Руководствуясь этим принципом, потенциальные противники стремятся нарушить кибербезопасность военных информационных систем, чтобы добиться стратегической выгоды в конкурентной среде.

В связи с этим, кибербезопасность является одной из главных проблем в развитии инфокоммуникационных систем военного назначения. Недостаточная защищенность военных информационных систем может привести к слежке, краже конфиденциальной информации, а также к различным другим видам кибератак, которые могут повлечь за собой серьезные последствия, вплоть до потерь национальной безопасности. Поэтому, актуальность решения проблемы кибербезопасности находится на переднем плане при развитии военных информационных систем и услуг для защиты страны от потенциальных киберугроз.

Кибернетика (от греч. *kybernetiké* – искусство управления), наука об управлении, связи и переработке информации. Основной объект исследования – так называемые «кибернетические системы», рассматриваемые абстрактно, вне зависимости от их материальной природы. Кибернетика разрабатывает общие принципы создания систем управления и систем для автоматизации умственного труда. Таким образом, ключевым элементом кибернетических систем является именно информация. Очевидно, что границы области применения терминов с использованием части слова «кибер» лежат именно в информационной и управленческой сферах. Можно сказать, что объектом кибернетики являются все управляемые информационные системы.

«Атака» – это стремительное наступательное движение войск, быстрое и решительное наступление или стремительное нападение на неприятеля, действия, направленные против кого-нибудь или для достижения какой-нибудь цели.

В руководящих документах армии США существует термин – компьютерная сетевая атака (Computer Network Attack) – действия по нарушению, подавлению, уничтожению информации или воспрещению пользоваться информацией, находящейся в компьютерах и компьютерных сетях, или против самих компьютеров и компьютерных сетей. Этот термин не синонимичен термину «кибератака», так как означает действия именно в сети, а не в киберпространстве и скорее всего является ее слагаемым.

Таким образом, кибератака – форма враждебных (противоправных) действий в киберпространстве; действия, направленные против кибернетических систем, информационных ресурсов или информационной инфраструктуры для достижения какой-либо цели и осуществляемые при помощи специальных программно-аппаратных средств и приемов (способов) воздействия.

Защита военных информационных систем от кибератак – это комплексная задача, которая требует использования различных ключевых принципов и подходов. Основные технологические требования к новым системам информационной безопасности (ИБ) включают следующие аспекты: открытость, масштабируемость, гибкость, надежность и слежение за безопасностью.

В целом, новые системы ИБ должны быть интегрированными, настраиваемыми и автоматизированными, чтобы улучшить эффективность их работы и максимально защитить военные системы Республики Беларусь от кибератак и утечек информации.

Защита военных информационных и инфокоммуникационных систем от кибератак является одним из важнейших аспектов безопасности национальной обороны. Киберугрозы имеют свойство постоянно эволюционировать, для обхода защитных мер и технических решений. Поэтому, актуальность защиты военных информационных систем от кибератак только возрастает с каждым годом и с развитием технологий.

Список использованных источников:

1. По материалам Специализированного образовательного портала: *MilitaryArticle* [Электронный ресурс] <https://militaryarticle.ru/>.
2. Искусственный интеллект ChatGPT4.

ИНТЕГРАЦИЯ ВИРТУАЛЬНЫХ И РАСШИРЕННЫХ РЕАЛЬНОСТЕЙ В ПРОЦЕСС ОБУЧЕНИЯ В ВОЙСКАХ СВЯЗИ

Плешко А.А.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Федоренко В.А.

Аннотация. Обзорная статья рассматривает преимущества использования виртуальных и расширенных реальностей в военном обучении, в частности, в войсках связи.

Современные технологии, такие как виртуальная и расширенная реальности, с каждым годом становятся все более популярными и доступными. В этой работе будет рассмотрен их потенциал в обучении военным специальностям, в частности в области связи. Одной из главных целей обучения является повышение эффективности и качества подготовки, а использование виртуальных и расширенных реальностей может быть важным инструментом в достижении этой цели. В данной работе мы рассмотрим несколько тезисов, подтверждающих возможности виртуальной и расширенной реальности в обучении военным специальностям.

1. Интеграция виртуальных и расширенных реальностей в обучение может помочь улучшить восприятие материала и увеличить уровень участия студентов.

2. Виртуальные и расширенные реальности могут быть использованы для симуляции сложных ситуаций, которые могут возникнуть в реальном мире.

3. Виртуальные и расширенные реальности могут помочь учащимся лучше понимать сложные процессы и технологии в войсках связи.

4. Использование виртуальных и расширенных реальностей в обучении может сократить время, необходимое для тренировок и обучения новым навыкам.

5. Виртуальные и расширенные реальности могут быть использованы для тренировки виртуальных командных центров и командного взаимодействия.

6. Виртуальные и расширенные реальности могут помочь учащимся лучше понимать важность точности и своевременности передачи информации.

7. Использование виртуальных и расширенных реальностей может помочь обучающимся лучше понимать, как оборудование и технологии влияют на качество связи.

8. Повышение мотивации и заинтересованности обучающихся в военных областях благодаря реалистичным симуляциям, доступным в виртуальной и расширенной реальности.

9. Возможность индивидуализации обучения в виртуальной и расширенной реальности для удовлетворения потребностей каждого обучающегося.

10. Применение виртуальных и расширенных реальностей для обучения в ситуациях, которые слишком опасны или сложны для реальных тренировок.

11. Уменьшение затрат на обучение за счет использования виртуальной и расширенной реальности вместо реальных объектов и устройств.

12. Возможность обучения на больших расстояниях благодаря возможности виртуального присутствия и интерактивного общения.

13. Возможность обучения виртуальным и расширенным реальностям на разных языках и для разных культур, что может быть особенно полезным для военных, работающих в международных операциях.

Использование виртуальных и расширенных реальностей в обучении войскам связи имеет большой потенциал для улучшения эффективности обучения и тренировок. Они могут помочь учащимся лучше понимать сложные процессы, технологии и процедуры, а также повысить их мотивацию и заинтересованность в военных областях.

Кроме того, использование виртуальных и расширенных реальностей может значительно снизить затраты на обучение, позволяя симулировать ситуации, которые слишком опасны или сложны для реальных тренировок, а также обучать на больших расстояниях благодаря возможности виртуального присутствия и интерактивного общения.

Наконец, виртуальные и расширенные реальности могут быть использованы для обучения на разных языках и для разных культур, что может быть особенно полезным для военных, работающих в международных операциях. В целом, применение виртуальных и расширенных реальностей в обучении войскам связи является перспективным направлением развития образования в этой области.

Список использованных источников:

1. Yu, T., Lu, S. J., & Liu, C. (2021). Augmented reality technology in education: A systematic review and future research directions. *Educational Research Review*, 32, 100365.
2. Dunn, J., & McDaniel, R. (2019). Augmented reality in education and training. *TechTrends*, 63(2), 171-177.

РАЗВИТИЕ МОБИЛЬНЫХ КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЙСКАХ СВЯЗИ РБ

Шкляр Ф.И.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Федоренко В.А.

Аннотация. В докладе рассмотрены перспективы и преимущества использования мобильных технологий в военных операциях, а также выделены основные проблемы и уязвимости, связанные с их использованием.

Войска связи являются самостоятельными специальными войсками, входят в состав военной организации государства и выступают как средство обеспечения его вооруженной защиты.

Тенденции изменения содержания вооруженной борьбы, опыт локальных войн и вооруженных конфликтов последнего десятилетия свидетельствуют, что требования к современной системе связи существенно повысились:

- автоматизация работы должностных лиц значительно увеличила объемы передаваемых сообщений и сократила время их обработки для получения достоверной информации, необходимой для принятия решений;

- быстрое изменение обстановки требует ведения информационного обмена в реальном масштабе времени;

- высокая подвижность объектов и субъектов управления в боевом пространстве обязывает устанавливать связь абонентам преимущественно в движении и с коротких остановок [1].

Проводя плановые мероприятия по переходу на современную технику связи, войска связи становятся более компактными и мобильными, при этом боевые возможности воинских частей и подразделений связи увеличились на порядок. Для продолжения совершенствования войск связи проводятся мероприятия по разработке и внедрению мобильных средств связи.

В настоящее время мобильные технологии стали неотъемлемой частью жизни людей, а также сферы бизнеса и государственного управления. В войсках связи РБ также активно используются мобильные технологии для обеспечения связи и передачи данных в режиме реального времени.

Одним из примеров использования мобильных технологий в войсках связи РБ является создание специализированных приложений для мобильных устройств, которые позволяют быстро и эффективно передавать информацию между подразделениями, координировать действия военнослужащих и контролировать выполнение задач.

Одной из перспективных технологий для военных коммуникаций является внедрение сети 5G, которая обеспечивает высокоскоростную передачу данных, низкую задержку и повышенную стабильность соединения. 5G может также использоваться для управления беспилотными авиационными системами, которые применяются для разведки, мониторинга и охраны территории.

Развитие мобильных коммуникационных технологий связано с использованием различных типов устройств, таких как планшеты, ноутбуки, смарт-часы, умные очки и др. Данные устройства повышают мобильность и удобство использования программного обеспечения, а также могут применяться для сбора и анализа данных, а также для более эффективного управления операциями.

При создании приложений для мобильных средств передачи информации, необходимо учитывать специфику военных операций и создавать мобильные приложения, которые могут быть использованы в различных ситуациях. Например, мобильные приложения для навигации, обмена сообщениями и мониторинга состояния оборудования и оружия могут значительно повысить эффективность военных операций.

Развитие мобильных коммуникационных технологий играет важную роль в укреплении обороноспособности и повышении эффективности военных операций. Однако, следует помнить о важности защиты передаваемой информации и необходимости использования современных технологий защиты связи и данных. Для обеспечения безопасности передаваемой информации, особенно при использовании открытых сетей связи используются различные технологии шифрования и защиты данных, такие как виртуальные частные сети (VPN) и двухфакторная аутентификация.

Для обеспечения всех требований связи, важно обучать военнослужащих использованию современных мобильных технологий и приложений, повышать осведомленность военнослужащих в области кибербезопасности и защиты данных, проводить регулярную аудиторскую проверку систем связи и обновление программного обеспечения для устранения уязвимостей, и повышения уровня защиты. Это поможет уменьшить риски нарушения конфиденциальности и целостности информации.

Список использованных источников:

1. Военный информационный портал Министерства обороны Республики Беларусь [Электронный ресурс] - Режим доступа: <https://www.mil.by/ru/forces/special/us/history/>

ЦИФРОВОЙ ФОРМАТ ОБУЧЕНИЯ: ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ

Кругляк А.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Тутков Е.В.

Аннотация. В данном тезисе описано применение цифровых технологий в образовании.

В последние годы, образование постепенно переходит к цифровой педагогике. Использование цифровых технологий в образовании открывает новые возможности для учебного процесса и повышает качество образования. Мы рассмотрим инновационные технологии и новые возможности, которые они предоставляют в образовании.

Одним из главных преимуществ цифровой педагогики является её доступность. Современные технологии позволяют создавать интерактивные учебные материалы, включать в них графику, анимацию, видео, звук и другие средства, которые позволяют лучше понимать учебный материал. Также, использование цифровых учебных материалов позволяет сократить затраты на печать и распространение учебных пособий, что позволяет сэкономить деньги и время.

Вторым преимуществом цифровой педагогики является её мобильность. Современные устройства, такие как смартфоны и планшеты, позволяют получать доступ к учебным материалам и выполнять задания в любом месте и в любое время. Это позволяет улучшить эффективность обучения и снизить затраты на образование.

Одним из наиболее инновационных технологий в цифровой педагогике является виртуальная реальность. Виртуальная реальность позволяет создавать имитацию реального мира и дает возможность погружения в виртуальную среду. Виртуальная реальность может быть использована в обучении, чтобы создать более эффективную и интерактивную среду для обучения. Она может быть использована для создания тренажеров для медицинского обучения, для обучения пилотов и многих других профессиональных навыков.

Еще одной инновационной технологией в цифровой педагогике являются онлайн-курсы. Онлайн-курсы позволяют студентам получать образование в любое удобное для них время и из любой точки мира. Это позволяет сократить затраты на образование и увеличить доступность образования для людей, которые не могут посещать учебные заведения из-за местоположения или других обстоятельств [1].

Другим примером инновационных технологий являются адаптивные учебные платформы. Адаптивные платформы позволяют студентам получать индивидуализированное образование, анализируя их знания и прогресс, и предоставляя им учебные материалы и задания, которые лучше соответствуют их уровню знаний.

Несмотря на все преимущества цифровой педагогики, ее использование также имеет свои недостатки. Некоторые студенты могут испытывать затруднения с использованием технологий, что может привести к ухудшению учебных результатов. Также, цифровые технологии могут не всегда заменить общение в реальном мире и могут привести к уменьшению личной связи и эмоциональной связи между преподавателями и студентами [2].

В целом, цифровая педагогика - это перспективный подход к образованию, который позволяет расширить доступность образования, улучшить качество обучения и создать более эффективные и инновационные методы обучения. Для успешного применения цифровой педагогики необходимо разработать и реализовать комплексную стратегию, которая учитывает потребности студентов и преподавателей и использует наиболее эффективные технологии [3].

Чтобы применить на практике предложенные решения, необходимо обеспечить доступность и обучение цифровым технологиям для преподавателей и студентов, разработать и реализовать эффективные учебные материалы и использовать социальные сети и коллаборативные платформы для общения и сотрудничества между студентами. Также, необходимо проводить регулярную оценку эффективности цифровых технологий, чтобы корректировать и улучшать методы обучения.

В целом, переход к цифровой педагогике может быть сложным процессом, но он является необходимым и перспективным для развития современного образования. Инновационные технологии позволяют расширить границы обучения и создать более интересные и эффективные методы обучения, что способствует повышению уровня знаний и навыков студентов.

Список использованной источников:

- 1 Siemens, G. (2005). *Connectivism: A Learning Theory for the Digital Age*. *International Journal of Instructional Technology and Distance Learning*, 2(1), 3-10.
- 2 Johnson, L., Adams, S., Estrada, V., Freeman, A., & Hall, C. (2016). *NMC/CoSN Horizon Report: 2016 K-12 Edition*. Austin, Texas: The New Media Consortium.
- 3 Oblinger, D. G., & Oblinger, J. L. (2005). *Educating the Net Generation*. EDUCAUSE.

ПЕРЕХОД К ЦИФРОВОЙ ПЕДАГОГИКЕ: ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ И НОВЫЕ ВОЗМОЖНОСТИ В ОБРАЗОВАНИИ

Николаев Е.А., Хаткевич Д.Н.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Тарайкович В.А.

Аннотация. В данном тезисе рассказывается о важнейших аспектах в образовании при использовании инновационных технологий.

В настоящее время невозможно представить современное образование без использования цифровых технологий. Современная педагогика постоянно развивается и адаптируется к новым реалиям, внося изменения в учебный процесс.

Переход к цифровой педагогике - это новая эра в образовании, которая открывает новые возможности для обучения и развития студентов. В данном эссе рассмотрим, какие инновационные технологии могут использоваться в образовательном процессе, и как их можно применить на практике.

Одним из ключевых преимуществ цифровой педагогике является возможность переносить образовательный процесс в онлайн-режим [1].

Дистанционное обучение может проводиться через специальные платформы, которые позволяют общаться с преподавателем и другими студентами, а также получать доступ к учебным материалам. Это удобно как для преподавателей, так и для студентов, так как дает возможность получать знания в любом месте и в любое время.

Еще одной инновационной технологией является использование интерактивных досок. Интерактивные доски - это доски, которые подключаются к компьютеру и позволяют управлять компьютером с помощью ручки. Они позволяют показывать презентации, записывать заметки и комментарии, а также проводить интерактивные занятия.

Также в образовательном процессе могут использоваться электронные учебники. Они позволяют преподавателям и студентам легко получать доступ к учебным материалам, а также выполнять задания и тестирование.

Однако, необходимо помнить, что использование цифровых технологий в образовании требует не только умения работать с компьютером, но и компетентности в области информационной безопасности. Важно научить студентов основам кибербезопасности, чтобы они могли защитить свои данные и персональную информацию в цифровой среде.

Для успешного использования инновационных технологий в образовательном процессе необходимо уметь их правильно интегрировать в образовательный процесс. При выборе технологий необходимо учитывать цели и задачи учебного курса, уровень подготовки студентов и доступность технологий. Также важно проводить оценку эффективности использования цифровых технологий в образовательном процессе, чтобы внести коррективы в случае необходимости.

Одним из ключевых моментов при переходе к цифровой педагогике является обеспечение качественной технической поддержки и безопасности данных. Необходимо разработать эффективные системы защиты информации и обучить студентов и преподавателей правильной работе с технологиями.

Применение цифровой педагогике в образовательном процессе имеет множество преимуществ. Она позволяет сократить затраты на обучение и упростить доступ к учебным материалам, повышает мотивацию студентов и стимулирует их активное участие в учебном процессе. Также использование цифровых технологий позволяет преподавателям более эффективно контролировать процесс обучения и оценки знаний студентов.

Однако, помимо преимуществ, использование цифровых технологий в образовании также имеет некоторые ограничения и проблемы. Например, не все студенты могут иметь доступ к высокоскоростному интернету или иметь возможность работать с цифровыми технологиями. Также возможны технические проблемы, такие как неполадки в компьютерной технике или проблемы с программным обеспечением.

В целом, переход к цифровой педагогике открывает новые возможности для образования, однако требует грамотного подхода к выбору и интеграции цифровых технологий в образовательный процесс, а также обучения студентов безопасному использованию цифровых средств.

В будущем, использование цифровых технологий в образовании будет становиться все более широко распространенным, и для успешной адаптации к новым реалиям, необходимо постоянно совершенствовать и адаптировать подходы и методы обучения.

Список использованной источников:

1 Prensky, M. (2010). Teaching digital natives: Partnering for real learning. Corwin Press.

ПРИМЕНЕНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Ахапкина А.М.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Способ С.П. – магистр техн. наук

Аннотация. В данном тезисе описано применение интеллектуальных инфокоммуникационных систем и сетей в войсках связи, так и в Вооруженных силах Республики Беларусь в целом. Написано плюсы и минусы их применения для войск связи и для различных сфер жизни. Дано предположение о перспективах развития данных систем как в войсках, так и в целом для Вооруженных сил.

Современная военная деятельность немыслима без использования передовых технологий. Одной из таких технологий являются интеллектуальные инфокоммуникационные системы и сети. Эти системы и сети значительно упрощают процессы связи и передачи информации в войсках связи Вооруженных Сил Республики Беларусь. В данной статье рассматривается применение и перспективы развития интеллектуальных инфокоммуникационных систем и сетей в войсках связи Республики Беларусь.

Интеллектуальные инфокоммуникационные системы и сети - это передовые технологии связи, которые позволяют автоматизировать процессы передачи, хранения и обработки информации. Они могут включать в себя различные виды оборудования, такие как компьютеры, маршрутизаторы, сетевые принтеры, а также программное обеспечение для управления и контроля сети. Интеллектуальные инфокоммуникационные системы и сети могут использоваться для обмена информацией между различными подразделениями вооруженных сил, для управления военными операциями и для связи с командованием.

Интеллектуальные инфокоммуникационные системы и сети применяются во многих областях вооруженных сил. Например, они используются для передачи информации о местоположении военных объектов и для обмена данными между командами в реальном времени. Также они могут использоваться для мониторинга техники и оружия, чтобы оптимизировать их использование и обслуживание. Во войсках связи интеллектуальные инфокоммуникационные системы и сети используются для обеспечения связи между различными подразделениями, а также для передачи сигналов связи на дальние расстояния.

Одним из примеров интеллектуальной инфокоммуникационной системы, применяемая в Вооруженных силах, является система "Автоматизированная система управления средствами связи войск (АСУ ССВ)", которая предназначена для управления всей системой связи в войсках, включая управление средствами связи и мониторинг состояния сети. Эта система позволяет быстро реагировать на изменения в сети и устранять неполадки, а также планировать и координировать работу средств связи в соответствии с задачами, стоящими перед войсками.

Другим примером является система "Средства передачи данных и голосовой информации" (СПДГИ), которая обеспечивает передачу голосовой и данных информации в режиме реального времени. СПДГИ позволяет быстро передавать информацию между различными военными подразделениями, что повышает эффективность управления войсками и оперативную связь между ними.

Результаты применения этих систем в армии Беларуси показывают, что они значительно повышают эффективность командования и управления войсками, снижают время реакции на изменения в боевой обстановке и улучшают качество связи между военными подразделениями. Кроме того, использование интеллектуальных инфокоммуникационных систем и сетей способствует более эффективному использованию ресурсов и повышению оперативности принятия решений.

Плюсы использования интеллектуальных инфокоммуникационных систем и сетей в войсках связи Вооруженных Сил Республики Беларусь:

1. Ускорение процессов связи и передачи информации.
2. Улучшение управления военными операциями.
3. Повышение эффективности взаимодействия между различными подразделениями.
4. Улучшение качества обучения и подготовки военных специалистов.

Минусы использования интеллектуальных инфокоммуникационных систем и сетей в войсках связи Вооруженных Сил Республики Беларусь:

1. Возможность нарушения конфиденциальности передаваемой информации.
2. Риск недоступности системы в случае аварий и сбоев.
3. Высокие затраты на разработку, внедрение и обслуживание системы.

Применение интеллектуальных инфокоммуникационных систем и сетей в войсках связи Вооруженных Сил Республики Беларусь уже доказало свою эффективность. Они помогли ускорить процессы связи и передачи информации, улучшить управление военными операциями и повысить эффективность взаимодействия между различными подразделениями. Кроме того, интеллектуальные инфокоммуникационные системы и сети могут использоваться для улучшения качества обучения и подготовки военных специалистов.

Перспективы применения интеллектуальных инфокоммуникационных систем и сетей в войсках связи Республики Беларусь связаны с их постоянным развитием и улучшением. Например, можно ожидать использование более современных технологий и оборудования, таких как искусственный интеллект, виртуальная и дополненная реальность. Также можно ожидать улучшения безопасности и защиты передаваемой информации.

Интеллектуальные инфокоммуникационные системы и сети не только нашли свое применение в вооруженных силах, но и имеют перспективы использования в современном обществе. Они могут применяться в различных сферах деятельности, включая бизнес, науку, медицину, транспорт и др.

В бизнесе интеллектуальные системы могут помочь оптимизировать производственные процессы, увеличить производительность и улучшить качество продукции, а также снизить затраты на производство. В науке интеллектуальные системы могут применяться для анализа больших объемов данных, моделирования сложных процессов и разработки новых материалов.

В медицине интеллектуальные системы могут использоваться для анализа медицинских данных, диагностики и прогнозирования заболеваний, а также для управления медицинскими учреждениями и оптимизации процессов лечения.

В транспорте интеллектуальные системы могут помочь снизить количество аварий на дорогах, повысить безопасность движения, улучшить транспортную доступность и сократить время в пути.

Таким образом, интеллектуальные инфокоммуникационные системы и сети имеют огромный потенциал для применения в различных сферах деятельности и могут значительно улучшить качество жизни людей.

В заключение можно отметить, что интеллектуальные инфокоммуникационные системы и сети являются неотъемлемой частью военной деятельности в наше время. Их применение в войсках связи Вооруженных Сил Республики Беларусь имеет множество преимуществ, таких как ускорение процессов связи, улучшение взаимодействия между подразделениями и повышение эффективности военных операций.

Однако, стоит учитывать и некоторые недостатки, такие как возможность нарушения конфиденциальности передаваемой информации. Несмотря на это, развитие и применение интеллектуальных инфокоммуникационных систем и сетей в войсках связи Республики Беларусь будет продолжаться в будущем, что позволит совершенствовать систему связи и повышать эффективность боевых действий.

Кроме того, важно отметить, что использование интеллектуальных инфокоммуникационных систем и сетей может существенно улучшить контроль за информацией и защитить военные данные от несанкционированного доступа не только в войсках связи, но и в системе управления Вооруженных Сил.

Однако, введение новых технологий требует соответствующей подготовки и обучения военных специалистов, что может быть дополнительным финансовым и временным затратами для вооруженных сил.

Важно также учитывать потенциальные угрозы кибербезопасности, которые могут привести к сбоям в работе систем и сетей. В связи с этим необходимо принимать меры по защите интеллектуальных инфокоммуникационных систем и сетей, включая усиление кибербезопасности, а также проведение регулярных проверок и тестирований.

В целом, применение интеллектуальных инфокоммуникационных систем и сетей в войсках связи Вооруженных Сил Республики Беларусь имеет большие перспективы, но требует комплексного подхода и соответствующих мер по обеспечению кибербезопасности и подготовки военных специалистов.

Список использованных источников:

1. Волков А.Н., *Исследование и разработка методов построения интеллектуальных инфокоммуникационных сетей* // диссертация, 2021
2. Кайсина Т.В., *Проблемы безопасности интеллектуальных инфокоммуникационных систем промышленного назначения* // автореферат, 2013.
3. Саломатина Е.В., *Разработка моделей телекоммуникационных информационно-управленческих сетей и методов их эффективного использования* // диссертация, 2019.
4. Косик Т.С., *Разработка модели автоматизированного построения интеллектуальных информационных систем по результатам анализа топологии сети* // диссертация, 2017.
5. Кулик С.М., *Эффективное применение интеллектуальных инфокоммуникационных сетей на объектах промышленного назначения* // автореферат, 2019.
6. Аванесова Н.Б., *Расчет рисков эффективного использования интеллектуальных инфокоммуникационных систем и сетей в бизнес-аналитике* // диссертация, 2017.

АСПЕКТЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ

Готченя Д.Г.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Сасновский А.А.

Аннотация. Инфокоммуникационные системы и услуги в войсках связи Вооруженных Сил Республики Беларусь. Их развитие и пути совершенствования.

Развития инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь является приоритетной. В свете быстро меняющихся технологий и вызовов, стоящих перед нашей армией, это является одним из самых важных направлений развития.

Для эффективного управления войсками, необходима быстрая и безопасная передача информации. Это важно для координации действий между подразделениями на поле боя.

В настоящее время мы столкнулись с тем, что наши высокоскоростные каналы связи не всегда обеспечивают необходимую пропускную способность для передачи растущих потоков информации

в реальном времени. Для того, чтобы решить эту проблему, необходимо продолжать работу по увеличению пропускной способности каналов связи.

В рамках этой работы важно уделить внимание следующим аспектам:

1. Развитию оптических сетей связи: Оптические сети связи позволяют обеспечить высокую скорость передачи данных на большие расстояния. Разработка и внедрение оптических сетей связи является приоритетной задачей [1].

2. Применению новых технологий: Современные технологии многоволнового разделения, позволяют обеспечить передачу большого количества данных в одном канале связи. Эти технологии позволяют увеличить скорости передачи данных в сетях связи [2].

3. Разработке новых сетевых решений: Необходимо постоянно развивать новые сетевые решения, которые позволят обеспечить быстрый и безопасный обмен информацией. Для этого важно следить за развитием технологий и разрабатывать новые решения, которые будут отвечать нашим потребностям.

Армии иностранных государств постоянно инвестируют в развитие своих инфокоммуникационных систем. Например, американские вооруженные силы интенсивно разрабатывают свою инфраструктуру связи, используя новые технологии, такие как облачные вычисления и сенсорную сеть, которые позволяют им быстро обмениваться информацией и оперативно реагировать на изменения в боевой обстановке.

Великобритания активно развивает свои инфокоммуникационные системы и услуги, путем внедрения новых технологий в области цифрового радио, которые позволяют обмениваться зашифрованной информацией в режиме реального времени.

Наши Вооруженные Силы также должны развиваться в этом направлении. Важно инвестировать в новые технологии, такие как 5G сети и системы искусственного интеллекта, которые позволят быстро обмениваться информацией и улучшить управление на поле боя.

Кроме того, хотелось бы обратить внимание на конкретные разработки, которые могут быть полезными нашим Вооруженным Силам. Например, одной из таких разработок является система коммуникации на основе лазеров [3], которая может обеспечить быструю передачу данных на большие расстояния без необходимости использования кабелей или радиосвязи. Это может быть особенно полезно в условиях многоэтажной застройки или в горных районах.

Другой пример — это разработка системы распознавания лиц, которая может помочь в идентификации вражеских солдат или террористов на поле боя. Эта технология может использоваться в сочетании с дронами или камерами видеонаблюдения для обеспечения безопасности и улучшения действий наших войск.

В заключение хотелось бы подчеркнуть, что развитие инфокоммуникационных систем и услуг является важнейшим направлением в развитии Вооруженных Сил.

Мы должны инвестировать в новые технологии, обучать наш персонал и разрабатывать конкретные решения, которые помогут эффективно действовать на поле боя.

Список использованных источников:

1. Волоконно-оптические линии связи [электронный ресурс] - 2022.- режим доступа <https://skomplekt.com/solution/vols.htm/>. Дата доступа: 28.03.2023.

2. Технология WDM [электронный ресурс] - 2022. - режим доступа https://componentltd.ru/technical_information/articles/tehnologiya-wdm/ Дата доступа: 28.03.2023.

3. Лазерная связь - еще один способ беспроводной связи [электронный ресурс] - 2022.- режим доступа https://skomplekt.com/articles/laser_con.htm/. Дата доступа: 28.03.2023.

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ

Кабаков В.П.

*Белорусский государственный университет информатики и радиоэлектроники,
г. Минск, Республика Беларусь*

Гусаков П.Б.

Аннотация. Рассмотрены основные принципы защиты данных в сетях, включая аутентификацию, шифрование и контроль доступа. Представлены существующие методы обеспечения безопасности передачи данных в военных сетях, включая системы защиты информации на различных уровнях, средства шифрования, сетевые фильтры и прочие методы.

В настоящее время проблема ведения военных действий в едином информационном пространстве приобретает особую актуальность, поскольку при реализации сетецентрического принципа управления войсками (силами) информация играет ключевую роль в обеспечении анализа ситуации в реальном масштабе времени и принятия обоснованного решения. С помощью информационных и телекоммуникационных технологий можно мгновенно собрать, обработать и распространить информацию (или дезинформацию) в любой точке зоны ответственности группировки войск (сил).

Современные сети связи стали неотъемлемой частью военных операций и обороны. Военные сети обрабатывают огромные объемы информации, включая секретную, конфиденциальную и критически важную информацию, требующую надежной защиты от несанкционированного доступа, взлома или утечки.

Безопасность сети, в свою очередь, имеет несколько аспектов и уровней. Физическая безопасность охватывает защиту линий и узлов сети (например, защиту маршрутизаторов различными средствами управления доступом). В целом же уровень сетевой безопасности решает вопросы защиты связей между двумя узлами. Цель сетевой безопасности в беспроводной сети состоит в том, чтобы обеспечить такую же степень безопасности, как и в проводной сети. Как правило, безопасность сети включает установление подлинности абонента (его идентификацию) и шифрование (кодирование). Кроме того, протоколы безопасности сети должны обеспечить защиту от преднамеренного изменения ее структуры или нарушения управления сетью.

Обеспечение безопасности передачи данных в сетях военного назначения является одним из наиболее актуальных и важных вопросов в области военной техники и обороны. Несанкционированный доступ к секретной информации может привести к серьезным последствиям для национальной безопасности, а также может нанести значительный ущерб военным операциям и оперативной работе [1].

Данная работа посвящена анализу и разработке эффективных методов обеспечения безопасности передачи данных в сетях военного назначения. В работе рассмотрены основные принципы защиты данных в сетях, включая аутентификацию, шифрование и контроль доступа. Также представлены существующие методы обеспечения безопасности передачи данных в военных сетях, включая системы защиты информации на различных уровнях, средства шифрования, сетевые фильтры и прочие методы.

Кроме того, данная работа содержит анализ современных угроз безопасности в сетях военного назначения и рекомендации по их предотвращению. В целом, цель данной работы - разработать эффективные методы обеспечения безопасности передачи данных в сетях военного назначения для обеспечения защиты национальных интересов и безопасности страны.

Основная часть данной работы посвящена анализу и разработке эффективных методов обеспечения безопасности передачи данных в сетях военного назначения. В этой части рассмотрены основные принципы защиты данных в сетях, включая аутентификацию, шифрование и контроль доступа, а также представлены существующие методы обеспечения безопасности передачи данных в военных сетях, включая системы защиты информации на различных уровнях, средства шифрования, сетевые фильтры и прочие методы. Кроме того, данная работа содержит анализ современных угроз безопасности в сетях военного назначения и рекомендации по их предотвращению.

Принципы защиты данных в сетях военного назначения.

Аутентификация – это процесс проверки подлинности пользователя или устройства, путем проверки учетных данных, таких как имя пользователя и пароль. Аутентификация помогает предотвратить несанкционированный доступ к сети и защитить конфиденциальную информацию.

Шифрование - это процесс преобразования понятной информации в нечитаемую форму, чтобы предотвратить ее прослушивание или вмешательство со стороны злоумышленников. Существует множество алгоритмов шифрования, таких как AES, RSA и другие, которые используются для защиты данных военных сетей.

Контроль доступа – это процесс ограничения доступа к определенным ресурсам или информации только для авторизованных пользователей. Этот процесс включает идентификацию пользователей и устройств, определение прав доступа и мониторинг доступа к ресурсам.

Методы обеспечения безопасности передачи данных в сетях военного назначения.

Системы защиты информации на различных уровнях - это системы, которые обеспечивают защиту информации на различных уровнях сети, включая уровни приложения, сети и транспортного уровня. Каждый уровень имеет свои собственные механизмы защиты, которые помогают защитить информацию от несанкционированного доступа и вмешательства.

Средства шифрования – это программное и аппаратное обеспечение, которое используется для защиты данных в военных сетях. Шифрование может происходить на разных уровнях, включая уровень приложения, уровень сети и уровень транспорта. Некоторые из наиболее распространенных алгоритмов шифрования, используемых в военных сетях, включают AES, RSA, Diffie-Hellman и другие.

Сетевые фильтры – это программное обеспечение, которое используется для фильтрации трафика в сети и блокировки нежелательного трафика. Сетевые фильтры могут использоваться для блокировки вредоносного программного обеспечения и других угроз безопасности, а также для предотвращения атак на сеть [2].

Угрозы безопасности в сетях военного назначения.

Существует множество угроз безопасности, которые могут повлиять на военные сети, включая атаки на периметр сети, вредоносное программное обеспечение, атаки на приложения и другие. Атаки на периметр сети могут включать в себя попытки проникновения в сеть через незащищенные узлы, уязвимые точки входа и другие уязвимости в сети. Вредоносное программное обеспечение может использоваться для получения доступа к конфиденциальной информации, блокировки доступа к ресурсам и других угроз.

Рекомендации по предотвращению угроз безопасности в сетях военного назначения.

Для предотвращения угроз безопасности в сетях военного назначения необходимо использовать комплексный подход, который включает в себя использование средств аутентификации, шифрования и контроля доступа, а также обновление систем и программного обеспечения для предотвращения уязвимостей. Также рекомендуется использовать многофакторную аутентификацию и применять меры по защите от вредоносного программного обеспечения, такие как установка антивирусных программ и регулярное обновление программного обеспечения. Кроме того, необходимо обучать пользователей безопасности и проводить регулярные проверки на предмет обнаружения уязвимостей и атак в сети [3].

Таким образом, обеспечение безопасности передачи данных в сетях военного назначения является критически важным вопросом, который требует комплексного подхода и постоянного совершенствования. Использование современных методов шифрования и сетевых фильтров является необходимым условием для защиты конфиденциальной информации в военных сетях. Однако, угрозы безопасности постоянно меняются и развиваются, поэтому необходимо постоянно обновлять системы и программное обеспечение, а также проводить регулярные проверки на предмет обнаружения уязвимостей и атак в сети.

Безопасность сетей военного назначения играет критически важную роль в защите национальных интересов и безопасности страны. Поэтому необходимо уделять особое внимание разработке и реализации мер по обеспечению безопасности передачи данных в военных сетях. Только комплексный и постоянно совершенствующийся подход к обеспечению безопасности может обеспечить эффективную защиту конфиденциальной информации в сетях военного назначения.

В заключении можно сказать, что обеспечение безопасности передачи данных в сетях военного назначения является критически важным вопросом для национальной безопасности и защиты конфиденциальной информации. Необходимо использовать современные методы шифрования и сетевые фильтры для защиты данных военных сетей, а также постоянно обновлять системы и программное обеспечение, а также проводить регулярные проверки на предмет обнаружения уязвимостей и атак в сети.

Поддержание безопасности сетей военного назначения является сложным и постоянным процессом, который требует комплексного подхода и постоянного совершенствования. Только такой подход может обеспечить эффективную защиту конфиденциальной информации и национальной безопасности.

Список использованных источников:

1. Информационная безопасность вооруженных сил РФ [Электронный ресурс]. – 2020. – Режим доступа <https://searchinform.ru/resheniya/otraslevye-resheniya/informatsionnaya-bezopasnost-vooruzhennykh-sil-ru/>. – Дата доступа :28.03.2023.

2. Разработка предложений по повышению защищенности информации в локальной вычислительной сети военного назначения от несанкционированного доступа [Электронный ресурс]. – 2020. – Режим доступа : https://knowledge.allbest.ru/programming/3c0b65635a3bd78b5c43a88421306d27_0.html– Дата доступа :28.03.2023.

3. Использование хеш-функции для защиты информации в локальных вычислительных сетях военного назначения [Электронный ресурс]. – 2020. – Режим доступа : <https://cyberleninka.ru/article/n/ispolzovanie-hesh-funktsii-dlya-zaschity-informatsii-v-lokalnyh-vychislitelnyh-setyah-voennogo-naznacheniya>– Дата доступа :28.03.2023.

НАСТОЯЩЕЕ И БУДУЩЕЕ РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Пинголь А.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Федоренко В.А.

Аннотация. Данная работа рассматривает основные аспекты развития ИКТ в Вооруженных Силах. Называет особенности будущих изменений и нововведений, которые затронут каждую сторону данной технологии.

В инновационной экономике, основанной на знаниях, важной задачей является оценка уровня развития информационно-коммуникационных технологий (ИКТ) как в мире, так и в отдельном государстве. Информационно-коммуникационные технологии – это двигатель научно-технического прогресса, поэтому для развития передового оборонного комплекса эта технология очень необходима.

В настоящее время информационно-коммуникационные технологии используются практически во всех сферах жизни, в том числе и в оборонной. Современные реалии мировых военных конфликтов и столкновений показывают, что успешное решение задач, стоящих перед Вооруженными Силами, во многом определяется уровнем информационного и аналитического обеспечения их деятельности. Систематическое накопление и оперативное использование достоверной информации, характеризующей оперативную обстановку, ее своевременный анализ - одно из важнейших условий успешного функционирования армий как в мирное, так и военное время [1].

В целом в Вооруженных Силах Республике Беларусь в автоматизированном режиме с помощью ЭВМ обрабатывались задачи самого различного уровня с количеством обрабатываемых запросов примерно одного миллиона в год. Повышается качество управления процессами использования информационно-коммуникационных технологий. Доля затрат на закупку программного обеспечения и услуги системной интеграции в структуре бюджетных расходов на использование информационно-коммуникационных технологий в деятельности Вооруженных Сил увеличивается, что в целом отражает развитие функциональных возможностей и повышение сложности используемых в деятельности систем и ресурсов [2].

На современном этапе главными задачами информационного обеспечения деятельности служб и подразделений Вооруженных Сил Республики Беларусь следует определить:

- создание единого информационного пространства в рамках Республики Беларусь, обеспечивающего оперативное представление информации сотрудникам всех подразделений;
- в соответствии с основными положениями Концепции национальной безопасности Республики Беларусь – обеспечение необходимого уровня безопасности информационных систем и ресурсов, их целостности и конфиденциальности, основанных на применении единых требований защиты информации от несанкционированного доступа или изменения [3];
- применение криптографических средств защиты информации является обязательным для информационных систем и ресурсов, содержащих сведения, составляющие служебную и государственную тайну [3];
- централизацию и объединение конкурсов на поставку однотипной продукции для нужд подразделений Вооруженных Сил, в том числе типового аппаратного, а также программного обеспечения, имеющего соответствующие лицензии, осуществляющегося в целях экономии бюджетных средств и повышения эффективности бюджетных расходов [4];
- улучшение материально-технического обеспечения;
- информирование в Вооруженных Силах о передовом опыте и инновациях в сфере информационно-коммуникационных технологий.

Перед информационно-коммуникационными технологиями в Вооруженных Силах впереди еще долгая история развития и обширные перспективы. Этот то путь развития, на который стоит уделять наиболее пристальное внимание. В будущем именно акцент на ИКТ, позволит содержать оборонную силу нашей Республики Беларусь на самом высоком уровне.

Список использованных источников:

1. Борзенкова, Т.А. Анализ развития отрасли ИКТ в Беларуси/ Т.А. Борзенкова, Н.С. Баранова// 52-я науч. конф. аспирантов, магистрантов и студентов, Минск, 25-30 апреля 2016 г. / Белорус. гос. ун-т информатики и радиоэлектроники. Минск, 2016. – С. 87–88.
2. Информационное общество в Республике Беларусь: стат. сборник / Национальный статистический комитет Республики Беларусь, 2017. – 109 с.
3. Концепция национальной безопасности Республики Беларусь : Указ Президента Респ. Беларусь от 9 ноября 2010 г., № 575 // Консультант Плюс : Беларусь. Технология 3000 [Электронный ресурс] / ООО «ЮрСпектр», Нац. Центр правовой информ. Респ. Беларусь. - Минск, 2015.
4. М. Ибрагим //Веснік сувязі, 2016. – №1. –С. 11– 14.

ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ГЕОПРОСТРАНСТВЕННЫХ ТЕХНОЛОГИЙ В ВОЕННОЙ СВЯЗИ

Рудаковский В.С.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Федоренко В.А.

Аннотация. Доклад представляет обзор современных тенденций в применении геопространственных технологий в военной связи. В докладе рассмотрены перспективы использования геопространственных данных в таких областях, как разведка, мониторинг и навигация, а также проанализированы вызовы и риски, связанные с использованием таких технологий в военных операциях.

Современные геопространственные технологии позволяют получать и анализировать геоданные с высокой точностью и в режиме реального времени. Эти технологии могут быть применены в различных областях, включая военную связь. Они могут обеспечить военным командам точное представление о местоположении сил и средств, а также о географических особенностях территории.

Одним из примеров применения геопространственных технологий в военной связи является использование системы GPS для навигации и контроля местоположения боевых единиц. Это позволяет военным командам точно определять местоположение своих сил и средств и контролировать передвижение противника. Кроме того, геопространственные технологии могут быть использованы для создания электронных карт, которые могут быть полезны при планировании и проведении военных операций.

Однако, применение геопространственных технологий в военной связи также сталкивается с некоторыми вызовами. Во-первых, необходимо обеспечить надежную защиту данных, которые собираются и обрабатываются с помощью этих технологий. Во-вторых, необходимо обеспечить высокую точность и надежность систем геопозиционирования, чтобы военные команды могли полагаться на эти системы при принятии решений. В-третьих, необходимо обучать военных специалистов работе с геопространственными технологиями и разрабатывать новые методы и стратегии использования этих технологий в военной связи [1].

Ключевыми преимуществами использования геопространственных технологий в военной связи являются следующие особенности:

1. Увеличение эффективности операций: благодаря геопространственным технологиям военные могут получать точную информацию о местоположении объектов и персонала, что позволяет быстро и точно реагировать на изменения в боевой обстановке.

2. Улучшение навигации: геопространственные технологии позволяют военным определять свое местоположение с высокой точностью, а также планировать маршруты перемещения с учетом географических и климатических условий.

3. Разведка: использование геопространственных технологий позволяет быстро и точно собирать информацию о местоположении объектов, а также получать данные о рельефе местности и климатических условиях, что особенно важно в условиях боевых действий.

4. Управление операциями: геопространственные технологии позволяют в режиме реального времени контролировать положение своих сил и противника, что помогает оптимизировать управление операциями и принимать более эффективные решения.

Одним из наиболее перспективных направлений использования геопространственных технологий в военной связи является разработка и внедрение интеллектуальных систем управления боевыми действиями. Эти системы используются для анализа и обработки данных о местоположении в реальном времени, а также для принятия решений на основе анализа данных [2].

Также следует отметить, что геопространственные технологии могут быть использованы для поддержки военно-медицинских операций. Например, системы геолокации могут использоваться для быстрого нахождения раненых в боевых условиях, а также для определения места высадки медицинских эвакуационных вертолетов.

В заключение, геопространственные технологии предоставляют множество возможностей для улучшения военной связи и управления боевыми действиями. Однако необходимо учитывать риски и вызовы, связанные с их использованием, и разрабатывать соответствующие меры для обеспечения безопасности и конфиденциальности военной информации.

Список использованных источников:

1. Данко Л.В., Запольский В.В., Шустов А.А. *Геоинформационные технологии в задачах военного применения*. М.: МГТУ им. Н.Э. Баумана, 2014. – 103с.

2. Liao, J. (2019) *Research on the Application of Geospatial Information Technology in Military Training // International Conference on Artificial Intelligence, Big Data and Computing (ICABDC) C.195-199.*

ВОЗМОЖНЫЕ НАПРАВЛЕНИЯ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И УСЛУГ В ВОЙСКАХ СВЯЗИ

Седеневский А.М.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Божко Р.А.

Аннотация. Информационно-коммуникационные технологии являются неотъемлемой частью современной военной связи. Беларусь, как и многие другие страны, активно развивает свои информационно-коммуникационные системы и услуги в военных коммуникациях, чтобы улучшить эффективность и надежность своих вооруженных сил.

В условиях современных боевых действий войска связи занимают особое место. Своевременная передача информации является ключевым фактором успеха операции. Современный прогресс в области технологий связи и информационных технологий (ИТ) открывает новые возможности для совершенствования инфокоммуникационных систем и услуг в вооруженных силах. Республика Беларусь активно работает над повышением эффективности своих вооруженных сил путем внедрения современных технологий связи и ИТ. Основными направлениями развития инфокоммуникационных систем и услуг в военной связи являются:

1. Усиление мер по защите информации [1]. В связи с увеличением количества кибератак и угроз информационной безопасности, необходимо усилить меры по защите информации в вооруженных силах Республики Беларусь. Это включает в себя не только использование современных криптографических алгоритмов и механизмов, но и обучение персонала правилам безопасного обращения с информацией.

2. Использование облачных технологий. Облачные технологии могут значительно улучшить работу военных связистов, позволяя им получать доступ к необходимой информации и ресурсам из любой точки мира. В этом случае, необходимо обеспечить надежную защиту облачной инфраструктуры от киберугроз и несанкционированного доступа.

3. Развитие системы управления данными [2]. В связи с ростом объема и сложности информации, необходимо развивать систему управления данными, которая позволит эффективно хранить, обрабатывать и передавать информацию военным связистам. Это включает в себя использование современных баз данных, аналитических инструментов и механизмов обработки больших данных.

4. Создание единой информационной среды [3]. Различные системы связи, используемые в Вооруженных Силах, должны быть интегрированы в единую информационную среду, обеспечивающую своевременную передачу и обработку информации. Важно также создание единой базы данных, обеспечивающей хранение и обработку данных различных систем связи.

5. Улучшение качества обучения военных связистов. Для успешного функционирования инфокоммуникационных систем и услуг в вооруженных силах Республики Беларусь, необходимо иметь высококвалифицированных и подготовленных военных связистов. Поэтому, необходимо улучшать качество и доступность обучения военных связистов, в том числе использовать современные образовательные технологии.

6. Внедрение новых технологий и инноваций [4]. Развитие инфокоммуникационных систем и услуг в вооруженных силах Республики Беларусь требует внедрения новых технологий и инноваций. Это может включать в себя использование искусственного интеллекта, блокчейна и других технологий для повышения эффективности и надежности систем связи и обработки информации.

7. Развитие систем видеонаблюдения и видеоконференций. Системы видеонаблюдения и видеоконференций являются важными средствами обеспечения безопасности и эффективной коммуникации в вооруженных силах. Развитие этих систем и использование современных технологий позволит улучшить мониторинг и контроль за ситуацией на территории, а также обеспечить более эффективную коммуникацию между военнослужащими.

Таким образом в свете быстро меняющихся технологий и новых задач, стоящих перед вооруженными силами, важно постоянно развивать инфокоммуникационные системы и услуги в войсках связи.

Список использованных источников:

1. Тарасевич А. И. Информационные технологии в системе обеспечения безопасности Республики Беларусь. Минск: БГТУ, 2018. 192 с
2. Баранов О. Н., Баранова Т. В. Многофункциональные информационные системы связи. М.: Издательский дом "Спутник+", 2015. 232 с.
3. Левченко А.М. Создание единой информационной среды Вооруженных Сил Республики Беларусь // Информационно-коммуникационные технологии в науке, управлении, социальной сфере и медицине (ИКТНУС-2019): сб. науч. тр. Междунар. науч.-практ. конф., 19-20 дек. 2019 г. – Минск: Академия управления при Президенте Республики Беларусь, 2019. – С. 99-102.
4. Долгов А.С., Долгов С.А. Информационная безопасность: проблемы и решения. – Минск: БГУИР, 2016. – 176 с.

ВЛИЯНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ НА ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС

Куцуленко И.И.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Будиков Ю.Н.

Аннотация. В данном тезисе рассказывается о влиянии инновационных технологий на образовательный процесс.

С развитием технологий и доступностью информации в интернете, образовательные учреждения сталкиваются с необходимостью адаптировать свои методы обучения и использовать новые технологии в учебном процессе. Инновационные технологии в образовании включают в себя различные средства и методы, такие как интерактивные доски, онлайн-курсы, вебинары, мультимедийные презентации, электронные учебники, компьютерные программы и многие другие. [1] В данном материале мы рассмотрим влияние инновационных технологий на образовательный процесс в университете.

Интерактивные доски

Одной из наиболее важных инновационных технологий в образовании являются интерактивные доски. Эти доски позволяют преподавателям проводить уроки в интерактивном формате, используя различные приложения и программы, и демонстрировать информацию на большом экране. Интерактивные доски также позволяют студентам активно участвовать в уроке, задавать вопросы и вносить свои идеи. В результате, образовательный процесс становится более интересным и захватывающим, а студенты более активно участвуют в уроке.

Онлайн-курсы и вебинары

Другой важной инновационной технологией являются онлайн-курсы и вебинары. Эти технологии позволяют студентам получать знания и навыки в удобное для них время, не выходя из дома. Онлайн-курсы также позволяют студентам проходить курсы по своему темпу и повторять материал при необходимости. Вебинары также позволяют студентам участвовать в уроках, не находясь в аудитории, а также задавать вопросы и обсуждать темы с преподавателем и другими студентами. [2]

Электронные учебники и компьютерные программы

Инновационные технологии также включают в себя электронные учебники и компьютерные программы. Эти технологии позволяют студентам получать доступ к информации и материалам в электронном формате, что удобно и экономит время. Электронные учебники и компьютерные программы также позволяют студентам более глубоко изучать темы и технологии, благодаря более широкому доступу к информации и возможности использовать интерактивные модели и симуляции.

Мультимедийные презентации

Еще одной важной инновационной технологией в образовании являются мультимедийные презентации. Эти презентации позволяют преподавателям демонстрировать информацию в различных форматах, включая видео, аудио, графику и другие элементы. Мультимедийные презентации помогают ученикам лучше понимать и запоминать материал, а также делают уроки более интересными и привлекательными.

Интерактивные учебные программы

Интерактивные учебные программы являются еще одним примером инновационных технологий в образовании. Эти программы позволяют студентам изучать темы в интерактивном формате, используя различные элементы, такие как визуализации, симуляции и тесты. Интерактивные учебные программы помогают студентам лучше понимать материал и повышать свой уровень знаний и навыков. [3]

Инновационные технологии в образовании играют важную роль в улучшении качества образовательного процесса. Они позволяют учителям и студентам использовать новые методы обучения и получать доступ к информации и материалам в более удобном и интерактивном формате. В итоге, инновационные технологии помогают повышать эффективность образовательного процесса и улучшать уровень образования в целом.

Список использованных источников:

- 1 Prensky, M. (2010). *Teaching digital natives: Partnering for real learning*. Corwin Press.
- 2 "Disrupting Class: How Disruptive Innovation Will Change the Way the World Learns" by Clayton Christensen, Michael B. Horn, and Curtis W. Johnson
- 3 "Teaching in a Digital Age: Guidelines for Designing Teaching and Learning" by Tony Bates

ИННОВАЦИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ: БУДУЩЕЕ ОБРАЗОВАНИЯ

Нусин Н.А

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Вершило Д.Н.

Аннотация. В данном тезисе рассказывается об инновационных технологиях в образовательном процессе.

Инновации в образовательном процессе - это процесс внедрения новых технологий и методов в обучение. Такие изменения помогают создать более эффективную систему образования, а также развивают учеников и образовательные учреждения. В настоящее время происходит быстрый технологический прогресс, который вносит существенные изменения в образовательный процесс. Изучение инноваций в образовательном процессе имеет большое значение для будущего образования.

Существует множество причин, почему инновации в образовании являются важными.

Во-первых, они могут улучшить качество обучения. Новые технологии позволяют создавать интерактивные учебные материалы и использовать новые методы обучения. [1]

Во-вторых, инновации могут повысить доступность образования. Они могут предоставить возможность обучения всем желающим, включая тех, кто живет в отдаленных районах или не может посещать учебные заведения в силу физических ограничений.

В-третьих, инновации могут помочь учащимся развивать навыки, которые могут быть важными для их будущей карьеры. Например, использование новых технологий и методов может помочь студентам развить компьютерные навыки, коммуникативные и социальные умения.

Одним из примеров инноваций в образовании является использование онлайн-курсов. Они позволяют учащимся изучать темы в своем собственном темпе и в любое удобное для них время. Это особенно важно для тех, кто имеет ограниченное время или не может посещать учебные заведения. Онлайн-курсы также могут быть доступными для большого количества людей, что помогает повысить доступность образования. [2]

Еще одним примером инновации в образовании является использование виртуальной реальности в учебном процессе. Эта технология может помочь студентам погрузиться в окружающую среду и получить более глубокое понимание материала.

Например, использование виртуальной реальности может помочь студентам изучать географию и историю, позволяя им путешествовать во времени и пространстве, посещать места и события, которые им не доступны в реальной жизни. [3]

Также, машинное обучение и искусственный интеллект могут помочь в создании более персонализированной системы образования. Алгоритмы могут анализировать данные обучающихся, учитывать их особенности и создавать индивидуальную программу обучения для каждого студента.

Однако, необходимо учитывать, что инновации в образовании могут иметь как положительные, так и отрицательные последствия. Внедрение новых технологий может потребовать значительных финансовых и временных затрат, а также может привести к нежелательным последствиям, таким как недостаток контроля качества обучения и уменьшение социальной интеракции между студентами.

Поэтому, при внедрении инноваций в образовательный процесс необходимо учитывать все возможные последствия и сбалансировать их с потенциальными преимуществами. Однако, несмотря на все риски и сложности, инновации в образовании будут продолжать играть важную роль в развитии образования в будущем. Будущее образования зависит от того, насколько успешно мы сможем внедрять новые технологии и методы в обучение, а также от того, как мы сможем справляться с возникающими проблемами и вызовами. [4]

Кроме того, в будущем образование будет всё более глобализированным и международным. Развитие интернет-технологий и возможность обучения онлайн уже сейчас позволяют студентам получать образование в любой точке мира. В будущем это станет ещё более доступным и распространенным, что создаст возможность для студентов учиться в разных культурных и образовательных средах и расширять свой кругозор.

Список использованных источников:

- 1 Prensky, M. (2010). *Teaching digital natives: Partnering for real learning*. Corwin Press.
- 2 "Disrupting Class: How Disruptive Innovation Will Change the Way the World Learns" by Clayton Christensen, Michael B. Horn, and Curtis W. Johnson
- 3 "Teaching in a Digital Age: Guidelines for Designing Teaching and Learning" by Tony Bates
- 4 "Learning and Education in Developing Countries: Research and Policy for the Post-2015 UN Development Goals" edited by Samer Al-Samarrai and Pauline Rose

СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В СФЕРЕ ОБРАЗОВАНИЯ: ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ И НОВЫЕ ПОДХОДЫ

Иванов Е.А., Мурашко Д.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Коношенко А.В.

Аннотация. В данном тезисе рассказывается о тенденциях в образовательном процессе, касающихся применения инноваций и новых подходов в образовании и учебных учреждениях.

Сегодняшний мир стремительно меняется, и важно, чтобы наша система образования была способна адаптироваться к этим изменениям и обеспечивать нашим студентам знания и навыки, которые им будут необходимы для успешной карьеры и жизни в целом. Инновации могут играть важную роль в этом процессе, предоставляя новые методы обучения и новые инструменты для обучения.

Инновации в образовательном процессе – это ключевой фактор в улучшении качества образования и подготовки будущих лидеров. В современном мире, где технологии развиваются с невероятной скоростью, образовательные учреждения должны использовать все возможности, чтобы обеспечить студентам максимально эффективное обучение. Однако, на пути к инновациям могут возникнуть многие препятствия.

Важным решением внедрения инноваций в образовательный процесс может стать создание современной и гибкой инфраструктуры. Это может включать в себя установку современного оборудования, включая компьютеры и другие электронные устройства, а также создание цифровых платформ и систем для обучения онлайн.

Одним из примеров инноваций в образовании являются онлайн-курсы и массовые открытые онлайн-курсы (МООС). Эти курсы предоставляют студентам возможность изучать новые темы и приобретать новые знания в удобное для них время, а также позволяют учителям расширить свою аудиторию и достичь студентов, которые могут находиться далеко от них географически. МООС также обеспечивают доступ к материалам ведущих университетов и экспертов в различных областях знаний.

Другим примером инноваций в образовании является использование искусственного интеллекта (ИИ) и машинного обучения для обучения и адаптации к индивидуальным потребностям студентов. Эти технологии позволяют учителям и студентам получать обратную связь и анализировать данные об успеваемости студентов, чтобы улучшить процесс обучения и удовлетворить потребности каждого студента.

Также существует возможность использования виртуальной реальности (VR) и дополненной реальности (AR) для обучения. Эти технологии могут помочь студентам более глубоко понимать материал, используя визуальные и пространственные примеры. Это может быть особенно полезно для студентов, изучающих научные и технические дисциплины, так как это может помочь им визуализировать и понять сложные концепции.

Инновации также могут помочь сократить расходы на образование, например, путем использования электронных учебников и материалов, а также перехода на электронные формы тестирования и оценки. Это может сократить затраты на печать и распределение материалов и снизить затраты на обслуживание технического оборудования для тестирования. [1]

Кроме того, инновации могут помочь сделать образование более доступным для людей с ограниченными возможностями. Технологии, такие как специальные программы и устройства, помогающие людям с нарушениями слуха, зрения и моторных навыков, могут сделать образование более инклюзивным и помочь этим людям получить качественное образование.

Наконец, инновации могут помочь сделать образование более интерактивным и захватывающим. Использование игровых элементов, таких как геймификация, может помочь студентам лучше усваивать материал и стимулировать их интерес к учебному процессу. [2]

В заключение, инновации имеют большой потенциал для улучшения образовательного процесса. Онлайн-курсы и МООС, искусственный интеллект, виртуальная и дополненная реальность, электронные учебники и игровые элементы могут помочь сделать образование более эффективным, доступным и интерактивным для всех студентов. Я надеюсь, что мы будем продолжать искать и использовать инновации в нашем образовательном процессе, чтобы обеспечить нашим студентам лучшие возможности для достижения своих целей и успехов в жизни.

Список использованных источников:

1 "Disrupting Class: How Disruptive Innovation Will Change the Way the World Learns" by Clayton Christensen, Michael B. Horn, and Curtis W. Johnson

2 "Learning and Education in Developing Countries: Research and Policy for the Post-2015 UN Development Goals" edited by Samer Al-Samarrai and Pauline Rose

ОСНОВНЫЕ ВИДЫ БОЕВОГО ОБЕСПЕЧЕНИЯ

Мурашко Д.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минска, Республики Беларусь

Тимошенко В.В.

Аннотация: В статье рассмотрены виды боевого обеспечения. Их характеристики и применения в боевых действиях.

В вооружённых силах каждого государства существует свой перечень обеспечения боевых действий, которых следует относить к боевому обеспечению. К примеру, в Вооружённых силах СССР таковых было шесть видов.

Боевое обеспечение — комплекс мероприятий, осуществляемый в войсках, которые планируются и осуществляются во всех видах операций для создания благоприятных условий для применения своих войск и военной техники, а также снижения эффективности применения войск и вооружения противника. Является составной частью обеспечения военных действий [1].

Основным способом ведения боя с применением только обычного оружия является последовательный разгром группировок войск противника. Ведя боевые действия, войска применяют различные тактические приемы и всевозможные их сочетания, которые разделяют на виды боя по основным, наиболее существенным признакам.

Разведка является комплексом мер по добыче разведывательных данных необходимых для эффективного применения своих войск, средств поражения и радиоэлектронного подавления. По задачам, решаемым разведывательными органами, разведка подразделяется на три уровня.

Маскировка является комплексом мероприятий и действий, служащих для обмана противника, скрытие от него состава, положения, состояния своих войск (сил), замысла предстоящих действий. Целью маскировки служит обеспечение внезапности действий и повышения живучести своих войск (сил). Маскировка должна осуществляться непрерывно, убедительно для противника, быть разнообразной и активной.

Инженерное обеспечение является комплексом мероприятий для создания необходимых условий для своевременного и скрытного развёртывания войск, проведения ими манёвра, перегруппировок и выполнения поставленных боевых задач, для повышения защиты и устойчивости войск (сил) и объектов от всех средств.

Радиационная, химическая и биологическая защита является комплексом мер по снижению потерь войск и выполнения ими поставленных задач при действиях в условиях радиационного, химического и биологического заражения, применения высокоточного и других видов оружия.

Радиоэлектронная борьба ведётся в целях дезорганизации управления войсками противника, снижения эффективности применения его оружия, боевой техники и технических средств разведки, а также для повышения устойчивости работы систем и средств управления собственными войсками и оружием. Мероприятия в радиоэлектронной борьбе проводятся в сочетании с уничтожением радиоэлектронных станций противника.

Топогеодезическое обеспечение проводится в целях подготовки и своевременного доведения до штабов войск топогеодезических данных, необходимых для изучения и оценки местности при подготовке и ведении операции, а также для эффективного применения оружия и боевой техники. Основной задачей топогеодезического обеспечения является составление топографических карт местности.

Навигационное обеспечение проводится в целях своевременного определения местоположения, направления и скорости перемещения мобильных объектов и войск для более эффективного планирования и ведения операции и применения вооружения, и военной техники [2].

Управление тылом является составной частью управления войсками. Оно осуществляется командиром лично, а также через штаб, заместителей по тылу и по технической части, начальников родов войск, специальных войск и служб. Эти должностные лица организуют работу тыла на основе решения и указаний командира, а также распоряжений соответствующих начальников вышестоящего звена по вопросам тылового обеспечения. При подготовке боя или других действий войск задачи по тыловому обеспечению в зависимости от обстановки доводятся до исполнителей приказами или распоряжениями по тылу, в ходе боя - короткими распоряжениями, отдаваемыми подчиненным преимущественно по техническим средствам связи или при личном общении.

Список использованных источников:

1. Виды общевойскового боя [Электронный ресурс]- Режим доступа: <https://studfile.net/preview/9056733/page:3/>. Дата доступа: - 30.03.2023;
2. Боевое обеспечение [Электронный ресурс]- Режим доступа: <http://militera.lib.ru/science/tactic/04.html>. Дата доступа: - 29.03.2023.

ИННОВАЦИИ В ОБЕСПЕЧЕНИИ ВОЕННОЙ СВЯЗИ В ВООРУЖЕННЫХ СИЛАХ РЕСПУБЛИКИ БЕЛАРУСЬ

Лапаревич Д.Ю.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Масейчик Е.А.

Аннотация. Данный тезис посвящен проблемам обеспечения военной связи в Вооруженных Силах Республики Беларусь и возможностям внедрения инновационных технологий для улучшения ее эффективности. В работе рассмотрены существующие проблемы в области военной связи и необходимость развития инновационных технологий для повышения безопасности государства и эффективности военных операций. Описаны перспективы внедрения квантовых, оптических и технологий искусственного интеллекта в обеспечении военной связи, а также необходимость развития научно-технического потенциала и обеспечения квалифицированным персоналом. Аннотация данного тезиса подчеркивает важность внедрения инновационных технологий в обеспечении военной связи в Вооруженных Силах Республики Беларусь для повышения эффективности военных операций и обеспечения безопасности государства.

1. Актуальность проблемы обеспечения военной связи в Вооруженных Силах Республики Беларусь

В условиях современных военных конфликтов обеспечение связи является одним из основных элементов обеспечения национальной безопасности. Ведение боевых действий требует постоянной связи между командованием, отдельными подразделениями и солдатами на поле боя. Недостаток связи может привести к серьезным последствиям, таким как потеря контроля над войсками, невозможность оперативного реагирования на изменение обстановки, а также угроза жизни и здоровью солдат. В связи с этим, обеспечение надежной и эффективной военной связи является одним из приоритетных направлений развития военной техники и технологий [1].

В Беларуси существует система военной связи, которая включает в себя радиотехнические средства, компьютерные сети и другие технические средства связи. Однако, для обеспечения надежности и эффективности связи в условиях современных военных конфликтов необходимо постоянное развитие.

2. Инновации в обеспечении военной связи в Вооруженных Силах Республики Беларусь

2.1. Использование квантовых технологий в военной связи

Одной из новейших и наиболее перспективных технологий в обеспечении военной связи являются квантовые технологии. Квантовые технологии позволяют защитить передаваемую информацию от несанкционированного доступа и подслушивания. В настоящее время в Республике Беларусь ведутся работы по созданию системы квантовой связи для обеспечения надежной военной связи [2].

2.2. Использование искусственного интеллекта для автоматизации процессов связи

В современных военных конфликтах важно оперативно реагировать на изменение обстановки и принимать решения на основе анализа больших объемов информации. Для решения этой задачи можно использовать искусственный интеллект, который позволяет обрабатывать большие объемы данных и принимать решения на основе анализа этих данных. В Республике Беларусь также проводятся работы по созданию системы искусственного интеллекта для автоматизации процессов связи [3].

2.3. Использование средств связи на основе оптических технологий

Средства связи на основе оптических технологий обеспечивают высокую скорость передачи данных и надежность связи. В Республике Беларусь в настоящее время проводятся работы по созданию системы военной связи на основе оптических технологий [4].

В заключении можно отметить, что внедрение инновационных технологий в обеспечении военной связи является важным направлением развития Вооруженных Сил Республики Беларусь. Однако, для успешной реализации проектов необходимо обеспечить квалифицированный персонал, адекватное финансирование и научно-технический потенциал. Только в этом случае можно говорить о положительных результатах в области обеспечения военной связи в Вооруженных Силах Республики Беларусь.

Список использованных источников:

1. Концепция развития инфокоммуникационной системы в Вооруженных Силах Республики Беларусь до 2025 года [Электронный ресурс]. Режим доступа: https://www.ncpi.by/ru/news/ncekr_razrabotala_koncepciyu_razvitiya – Дата доступа: 17.02.2023 г.
2. Информационные технологии в Вооруженных Силах Республики Беларусь [Текст] / В.Н. Сидорович, И.И. Звырков, С.В. Лисовский. - Минск: БГТУ, 2018. - 157 с.
3. Центр информационных технологий при Министерстве обороны Республики Беларусь [Электронный ресурс]. — Режим доступа: <https://www.mil.by/ru/itcenter/> — Дата доступа: 21.02.2023 г.
4. Инновационный проект "Развитие инфокоммуникационной системы в Вооруженных Силах Республики Беларусь" [Электронный ресурс]. — Режим доступа: https://www.bsuir.by/m/12_100136_1_52244.html — Дата доступа: 21.02.2023 г.

ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ ВООРУЖЕННЫХ СИЛ

Гудков А.С.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Балденко А.А.

Аннотация. Рассматривается применение машинного обучения и искусственного интеллекта в инфокоммуникационных системах вооруженных сил, описываются преимущества применения данных технологий, а также представлены конкретные примеры их использования в военных коммуникациях.

Инфокоммуникационные системы и услуги играют важную роль в связи и управлении вооруженными силами любого государства. Они позволяют командирам получать информацию в режиме реального времени, а также контролировать и управлять действиями войск, независимо от локации. Однако, чтобы опережать противника на несколько шагов вперед, необходимо быстро обрабатывать и анализировать огромные объемы данных. На сегодняшний день наука и технологии развиваются с невероятной скоростью и такие вещи как машинное обучение (далее - МО) и искусственный интеллект (далее - ИИ) могут существенно помочь в решении этих задач.

Искусственный интеллект (англ. Artificial Intelligence) – это комплексные компьютерные программы, способные выполнять задачи, которые раньше были доступны только для людей. Эти задачи могут включать в себя распознавание речи, обработку естественного языка, обучение, решение проблем и др. Машинное обучение (англ. Machine Learning) – это подраздел ИИ, который позволяет компьютерным системам учиться на основе данных и алгоритмов, следовательно, система может самостоятельно находить закономерности и шаблоны в данных.

Одним из примеров применения МО и ИИ в инфокоммуникационных системах вооруженных сил является анализ данных разведки. Современные системы разведки включают в себя датчики и сенсоры, которые собирают данные с различных источников, таких как дроны, спутники, беспилотные летательные аппараты и другие средства разведки. МО и ИИ могут помочь анализировать эти данные и выявлять шаблоны и закономерности, которые могут указывать на присутствие вражеских сил или потенциальных угроз.

Еще один пример применения МО и ИИ в инфокоммуникационных системах вооруженных сил – это системы управления беспилотными летательными аппаратами (БПЛА). БПЛА используются для разведки, наблюдения и ударных действий. Однако, управление большим количеством БПЛА требует больших усилий и ресурсов. МО и ИИ позволяет улучшить управление БПЛА, в том числе автоматическую навигацию и обнаружение целей.

Кроме того, машинное обучение и ИИ могут помочь повысить кибербезопасность вооруженных сил. Кибератаки на инфраструктуру и информационные системы стали все более распространенными и сложными, и военные системы не являются исключением. Применение МО и ИИ в кибербезопасности может помочь автоматически обнаруживать и анализировать кибератаки, а также разрабатывать эффективные методы защиты и предотвращения будущих атак.

Автоматическое управление сетью – следующий аспект, который можно оптимизировать. Военные коммуникации требуют надежной и безопасной сети связи, способной работать в самых различных условиях. МО и ИИ могут помочь создать умную и адаптивную сеть, способную самостоятельно анализировать состояние своих компонентов, прогнозировать возможные сбои и принимать меры для их предотвращения. Это поможет значительно повысить эффективность военных коммуникаций и сократить время на восстановление работоспособности сети.

Создание экспертных систем – также важная задача, которую можно решить с помощью МО и ИИ. Экспертные системы – это системы, использующие знания экспертов в определенной области для решения сложных задач.

В заключение, следует сказать, что машинное обучение и искусственный интеллект имеют огромный потенциал для инфокоммуникационных систем и услуг в ВС РБ. Они могут помочь решить многие задачи, которые ранее были невозможны для человека. Однако, важно помнить, что использование этих технологий требует специальных знаний и навыков, а также строгого соблюдения правил безопасности.

Список использованных источников:

1. Дмитриук, А. М. Основы организации связи : учеб.-метод. пособие / А. М. Дмитриук, С. Н. Касанин, Р. А. Градусов, И. В. Антоненко – Минск : БГУИР, 2012. – 150 с.
2. Artificial intelligence and machine learning / Vinod Chandra S. S., Anand Hareendran S. // PHI Learning, – 2014. – 449 P.

АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И УСЛУГ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ

Мазур-Грабовский Е.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Балденко А.А.

Аннотация. В данной работе рассматриваются актуальные вопросы развития, а также описываются основные направления модернизации инфокоммуникационных систем и услуг в войсках связи.

Информационные технологии военной связи играют существенную роль в обеспечении национальной безопасности и успешного выполнения боевых задач. Современные военные конфликты все больше направлены на воздействие на инфраструктуру коммуникаций противника, а также на использование средств информационной войны. В связи с этим, актуальным становится вопрос развития инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь. Основными направлениями развития инфокоммуникационных систем и услуг в военной связи являются:

1. Усиление информационной безопасности систем связи [1]. Для этого необходимо внедрение современных средств защиты информации, таких как шифрование, цифровая подпись, межсетевые экраны и прочие. Кроме того, важным является повышение уровня кибербезопасности и защита от кибератак, которые могут нанести значительный ущерб военной связи.

2. Развитие многофункциональных инфокоммуникационных систем [2]. Системы связи должны обеспечивать передачу не только голосовой информации, но и данных, видео, геоданных, а также обеспечивать возможность удаленного управления вооруженными формированиями. Важным направлением является развитие систем связи, обеспечивающих совместную работу войск различных видов войск.

3. Создание единой информационной среды [3]. Различные системы связи, используемые в Вооруженных Силах, должны быть интегрированы в единую информационную среду, обеспечивающую своевременную передачу и обработку информации. Важно также создание единой базы данных, обеспечивающей хранение и обработку данных различных систем связи.

4. Развитие мобильных инфокоммуникационных систем [4]. Важным направлением является создание мобильных систем связи, обеспечивающих возможность быстрой и надежной связи на различных уровнях управления войсками в любых условиях. Кроме того, важно развитие систем, обеспечивающих связь с подвижными объектами, такими как беспилотные летательные аппараты.

5. Развитие средств радиоэлектронной борьбы [5]. В связи с увеличением числа электронных систем боевой техники противника, актуальным становится вопрос развития средств радиоэлектронной борьбы.

6. Управление и мониторинг состояния систем связи [6]. Важным аспектом развития инфокоммуникационных систем и услуг является создание систем управления и мониторинга их состояния. Это позволит оперативно реагировать на сбои и устранять их, а также проводить анализ использования систем связи.

Таким образом, развитие инфокоммуникационных систем и услуг в войсках связи Вооруженных Сил Республики Беларусь является актуальным вопросом национальной безопасности и обеспечения успешного выполнения боевых задач. Необходимо усиление информационной безопасности, развитие многофункциональных систем связи, развитие мобильных систем связи, средств радиоэлектронной борьбы, а также управление и мониторинг состояния систем связи.

Список использованных источников:

1. Козлов А. А., Козлов С. А. Информационная безопасность. СПб.: Питер, 2016. 319 с.
2. Баранов О. Н., Баранова Т. В. Многофункциональные информационные системы связи. М.: Издательский дом "Спутник+", 2015. 232 с.
3. Тарасевич А. И. Информационные технологии в системе обеспечения безопасности Республики Беларусь. Минск: БГТУ, 2018. 192 с.
4. Долгов А.С., Долгов С.А. Информационная безопасность: проблемы и решения. – Минск: БГУИР, 2016. – 176 с.
5. Михайлова И.В. Развитие многофункциональных инфокоммуникационных систем в войсках связи // Научный журнал КубГАУ. – 2018. – № 144(10). – С. 1099-1112.
6. Левченко А.М. Создание единой информационной среды Вооруженных Сил Республики Беларусь // Информационно-коммуникационные технологии в науке, управлении, социальной сфере и медицине (ИКТНУС-2019): сб. науч. тр. Междунар. науч.-практ. конф., 19-20 дек. 2019 г. – Минск: Академия управления при Президенте Республики Беларусь, 2019. – С. 99-102.

ПРОГРАММНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ СВЯЗИ

Хорошавин В.Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Балденко А.А.

Аннотация. В работе представлен обзор одного из современных алгоритмов шифрования, на основе которого возможно строить сети связи с повышенным уровнем безопасности без использования специализированной аппаратуры.

Войска связи в рамках Вооруженных Сил являются неотъемлемым звеном, обеспечивающим функциональное взаимодействие всех существующих родов войск. Исторический опыт ведения боевых действий показывает, что выполнение задач по предназначению невозможно в отсутствие качественной связи не только между командирами и подчинёнными, но и между взаимодействующими подразделениями в том числе. Совершенствование системы связи Вооруженных Сил ведется одновременно по нескольким приоритетным направлениям. Это перевод стационарной системы связи на цифровые способы передачи и обработки информации, модернизация имеющихся на вооружении подвижных комплексов связи для повышения их качественных показателей, разработка и внедрение современных средств и комплексов связи в различных звеньях управления, создание унифицированной автоматизированной системы управления связью на всех уровнях военного управления, обеспечение информационной безопасности системы связи [1].

Поскольку цифровизация является одним из приоритетных направлений в списке, приведённом выше, предлагается внедрить в процесс организации сетей связи открытый алгоритм шифрования RSA, с помощью которого представляется возможным без использования сложных и специализированных средств обеспечение безопасного зашифрованного обмена сообщениями. RSA является достаточно удобным и безопасным алгоритмом для применения в военных системах коммуникации. Это связано с тем, что он является асимметричным, т.е. для шифрования и расшифрования используются разные ключи. При его использовании создаётся пара ключей (закрытый и открытый). Закрытый ключ хранится у одного корреспондента и используется для расшифровки сообщений, а открытый распространяется свободно и используется для шифрования сообщений. Он является достаточно устойчивым к прямому взлому, т.к. требует подбора больших псевдослучайных чисел, что часто невыполнимо в разумные сроки по времени. К известным уязвимостям рассматриваемого алгоритма относятся атаки типа “Человек посередине”, когда у злоумышленника есть возможность подделывать входящие сообщения посредством выдачи себя за нашего корреспондента. Частным случаем такой ситуации может быть физический доступ к передающему устройству корреспондента. Также возможно возникновение проблем, связанное с неаккуратным выбором исходных параметров для генерации ключей. Хотя последний случай может быть несущественен в определённых ситуациях, как, например, в каналах с низкой продолжительностью существования или при скорой потере актуальности сообщения (т.е. при его расшифровании сообщение не будет иметь никакой ценности). Более подробно с деталями и доказательствами безопасности алгоритма можно ознакомиться в работах [2, 3].

Далее рассмотрим на примере то, как возможно использовать описанный алгоритм для создания сети связи. Для простоты моделирования рассмотрим проводную сеть с иерархической топологией. Выбранный пример не означает, что решение не может быть распространено и на сети с другими средами распространения сигнала или топологиями. В нашем случае нужно будет обеспечить настройку и функционирование алгоритма на каждом из участков в сети. Т.е. для каждой пары узлов связи, непосредственно общающихся между собой, необходимо сгенерировать пару ключей. Причем очевидно, что для передачи сообщений с нижестоящих пунктов управления на вышестоящий достаточно будет сгенерировать только одну пару ключей. После этого необходимо со своими соседями обменяться открытыми ключами, что позволит начать использовать передачу зашифрованных сообщений. При задействовании схожей системы в рамках радиосети может получиться ухудшиться безопасность в случаях с широко вещанием, т.к. в таком случае необходимо будет распространить закрытый ключ нескольким корреспондентам. При работе в радиосети возможно использование данного алгоритма. Для этого потребуется организовать отдельные направления или подсети, в которых и будут общаться конкретные корреспонденты.

Список использованных источников:

1. Войска связи: современное состояние и перспективы развития [Электронный ресурс]. — Режим доступа: https://www.mil.by/special/ru/news/press_center/press_releases/8439. — Дата доступа: 30.03.2023.
2. Asjad Sirajuddin. *The RSA Algorithm*. — University of South-Eastern Norway, Campus Kongsberg, 2019. — 23 p.
3. Michael J. Wiener. *Cryptanalysis of Short RSA Secret Exponents*. — Ottawa, Canada, 1989. — 14 p.

ПРИМЕНЕНИЕ СРЕДСТВ РЭБ В ОБЩЕВОЙСКОВОМ БОЮ

Ахапкина А.М., Можейко В.Д.

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Ларев В.В.

Аннотация. В данном тезисе описана актуальность и необходимость применения средств РЭБ в современных военных конфликтах. Дано описание возможностей российских средств и эффективность их применения против БЛА в вооруженных конфликтах. Сделаны выводы о возможностях имеющихся на вооружении белорусских комплексов РЭБ.

Каждый конфликт, будь то масштабный или локальный, имеет свои уникальные особенности, связанные с причинами возникновения, географическими условиями, социально-политической обстановкой, уровнем технического развития и составом участников. Опыт, полученный противоборствующими сторонами конфликтов, является ценным материалом для анализа и обобщения.

Быстрое развитие технологий и компьютеризация военного дела приводят к созданию новых средств поражения и подразделений с новыми возможностями. Это требует постоянного совершенствования или создания новых форм и методов противодействия.

Активное и результативное применение боевых беспилотных летательных аппаратов в Сирийской Арабской Республике и Ливии, затем в Нагорном Карабахе, а сегодня на Украине неопровержимо свидетельствует о том, что БЛА в военных конфликтах стали неотъемлемым и эффективным средством как разведки, так и боевого применения. Причем количество беспилотников, принимающих участие в вооруженных конфликтах, постоянно увеличивается, а их номенклатура расширяется от совсем миниатюрных до высокотехнологичных комплексов размером в несколько метров. [2]

Сегодня значение невидимого оружия в современной войне постоянно растет, наряду с ударными группировками мотострелков, боевой авиации и артиллерии активно, в круглосуточном режиме действуют подразделения радиоборьбы. Работа подразделений РЭБ включает в себя целый спектр мероприятий по радиоэлектронному подавлению противника, противодействию вражеской разведке, а также по защите собственных систем управления оружием и войсками. Применение средств РЭБ позволяет ослабить или полностью уничтожить возможности противника в области электронной борьбы, что повышает шансы на успех в боевых действиях. Комплексы радиоэлектронной борьбы позволяют обнаруживать и подавлять все виды воздушных целей, даже на предельно малых высотах, технологически недоступных радарам зенитных ракетных систем. Средства РЭБ не заменяют, а уплотняют систему ПВО, действуют в интеграции с зенитными средствами поражения. Особую актуальность приобрела задача противодействия БЛА в части радиоэлектронного подавления каналов управления, передачи данных, а также навигационной аппаратуры. [3]

Практически все беспилотные летательные аппараты страдают от проблемы зависимости от устойчивости радиоканалов, через которые передаются команды, телеметрия и видеосигналы. Подавление этих каналов может привести к неисполнению задач. Поэтому комплексы радиоэлектронной борьбы являются эффективным, гибким и удобным средством борьбы с беспилотными летательными аппаратами.

В ходе специальной операции на Украине российские средства радиоэлектронной борьбы решают ряд важнейших задач, результаты некоторые уже известны - например, благодаря РЭБ померкла слава турецких дронов Bayraktar.

Только приводя данные из иностранных открытых источников (СМИ) в ходе проведения специальной военной операции вооруженными силами Российской Федерации на Украине, российские войска активно используют различные комплексы радиоэлектронной борьбы, начиная с начала операции. Они применяются как полноразмерные комплексы на автомобильном шасси, так и переносные или везомые системы, как в зоне боевых действий, так и в тылу.

Особенно эффективно используются мобильные системы радиоэлектронной борьбы, такие как «Красуха-4С», предназначенная в первую очередь для обнаружения и подавления больших радаров, например, на самолётах дальнего радиолокационного обнаружения и управления. С её помощью могут блокироваться не только связь в украинских войсках, но также сигналы сообщения с беспилотниками, на которые пытается делать ставку Украина. Во многом именно благодаря этой станции, как можно понять из официальных данных, было уничтожено несколько сотен зенитных ракет и беспилотных летательных аппаратов вооружённых сил Украины (ВСУ).

Её официально заявленная максимальная дальность поражения наземных и воздушных целей составляет от 150 до 300 километров в любом направлении в зависимости от различных факторов окружающей среды. По данным производителя – концерна «Радиоэлектронные технологии», система помех «Красухи-4С» может излучать достаточно мощные лучи радиочастотной

энергии, чтобы физически повредить чувствительные электронные системы определённых целей. Как опасаются иностранные эксперты, они могут ослепить различного рода пилотируемые и беспилотные летательные аппараты, действующие из безопасного воздушного пространства НАТО.

Показывает свою эффективность в условиях СВО комплекс РЭБ дальнего действия "Мурманск БН", работающий по КВ-диапазону (от 3 МГц до 30 МГц). Он создаёт в эфире помехи, оглушая и ослепляя средства вражеской разведки, подавляет датчики так называемого интеллектуального оружия. Он ведёт радиоразведку, осуществляет перехват сигналов, делая беспомощными самолёты-шпионы противника. Свои боевые задачи выполняет на дальности до пяти тысяч километров. [2]

Впервые использовали новую разработку российской оборонной промышленности — ружье радиоэлектронной борьбы ЛПД-801. Это вооружение успешно применили против малоразмерных беспилотных летательных аппаратов, используемых ВСУ.

С помощью воздействия электронного импульса ЛПД-801 способен выводить из строя малоразмерные беспилотники на дальности до 1-1,5 км. Максимальная мощность излучения, которое воздействует на электронную аппаратуру БЛА — около 10 Вт. Изделие работает в трёх диапазонах рабочих частот: первый — 2400–2483 МГц, второй — 5725–5925 МГц, третий — 1575–1602 МГц. Это позволяет направленно глушить каналы управления и навигационный сигнал беспилотников. В том числе блокировать сигналы Wi-Fi, Bluetooth, спутниковых систем GPS, Galileo, ГЛОНАСС и пресекать несанкционированную передачу данных. Может работать в ручном и автоматическом режимах. Аппарат выполнен в компоновке обычного магазинного карабина, где антенна выглядит, как ствол, а на месте магазина - сменный аккумулятор (работает около 60 минут), масса ружья составляет 3,5 кг (сопоставимо с массой АК-74). [3]

В Вооруженных Силах нашей страны рэбовцы на особом счету — без них не обходятся ни одни учения. В течение последних двух десятков лет система РЭБ Вооруженных Сил Республики Беларусь находится в постоянном развитии. Совершенствуется организационно-штатная структура воинских частей РЭБ, на вооружение планомерно поступает новая специальная техника. Благодаря тесному сотрудничеству с предприятиями белорусской промышленности Беларусь получила на вооружение более полутора десятков принципиально новых образцов специальной техники РЭБ, по своим характеристикам не уступающих зарубежным аналогам.

На данный момент в Республике Беларусь основными системами РЭБ являются: бортовой комплекс обороны «Талисман» и изделия семейства «Гроза». Первые предназначены для авиации, действие которых основано на разрушении работы моноимпульсной пеленгации, что приводит к срыву наведения зенитной или авиационной управляемой ракеты. Изделия семейства «Гроза», начиная от радиоэлектронного ружья «Гроза-Р2», способны не только блокировать каналы управления беспилотником, но и полностью подавлять его бортовые навигационные приемники, разрывая тем самым связь дрона с оператором и дезориентируя БЛА в пространстве, и заканчивая новейшей мобильной системой защиты объектов – «Гроза-З1». Эти системы обеспечивают ведение разведки, идентификацию угрозы и своевременную постановку силовых или интеллектуальных дезинформирующих помех.

Кроме того, среди новейших комплексов РЭБ, поступивших на вооружение - две станции помех Р-934УМ2, предназначенные для поиска, обнаружения, пеленгования источников радиоизлучения и линий связи и их радиоподавления, а также мобильный комплекс радиомониторинга, который предназначен для выполнения мероприятий радиоэлектронной защиты подразделений. Новая техника РЭБ весьма эффективна, в том числе, в борьбе со средствами воздушного нападения противника. Вдобавок, успешно освоены аппаратно-программные комплексы «Сфера», предназначенные для обнаружения, пеленгования и подавления каналов управления и навигации беспилотных летательных аппаратов коммерческого назначения типа мультикоптер посредством постановки помех в диапазонах частот каналов управления и навигации беспилотных летательных аппаратов. [1]

Таким образом в современных условиях, когда информационные технологии развиваются с невероятной скоростью, использование средств РЭБ является крайне необходимым для обеспечения эффективности действий войск общевойсковом бою. Без применения средств РЭБ, военные действия становятся крайне уязвимыми к радиоэлектронному воздействию противника, что может привести к серьезным потерям и поражениям на поле боя. Средства РЭБ могут помочь получить ценную информацию о противнике и его действиях, что повышает эффективность планирования и проведения боевых действий. Отсутствие такой информации может привести к серьезным ошибкам в принятии решений, что может повлечь за собой крупные потери.

Список использованных источников:

1. Давыдов Д.С., *Комплексы радиоэлектронной борьбы: история в прошлом и применение в настоящем* // реферат, 2021 год
2. Кайсина Т.В., *Применение средств радиоэлектронной борьбы в бою: невидимая схватка в эфире* // автореферат, 2018 год.
3. Саломатин Е.В., *Эффективность применения комплексов радиоэлектронной борьбы против БПЛА в современных вооруженных конфликтах* // реферат, 2022.
4. Василевский Т.С., *«Приоритетное значение»: на что способны войска РЭБ в современных условия* // статья, 2022 год.

ОГЛАВЛЕНИЕ

1. МЕТОДИКА КАЛИБРОВКИ ВОЛЬТМЕТРА ЦИФРОВОГО УНИВЕРСАЛЬНОГО В7-65/2	
(Белоус А.Ю., научный руководитель – Дмитренко А.А.).....	3
2. СИСТЕМА БОРЬБЫ С БПЛА «ГРОЗА-Р»	
(Босак Д.И., научный руководитель – Лавринчик Н.Н.).....	6
3. ПРОБЛЕМАТИКА БОРЬБЫ с БПЛА	
(Бутевич П.А., научный руководитель – Назаров Д.Г.).....	8
4. БЕСПИЛОТНЫЕ ЛЕТАТЕЛЬНЫЕ АППАРАТЫ РЕСПУБЛИКИ БЕЛАРУСЬ	
(Войтович Б.А., научный руководитель – Хожевец О.А.).....	10
5. МЕТОДИКА КАЛИБРОВКИ НИЗКОЧАСТОТНОГО ГЕНЕРАТОРА	
(Гладков А.Ю., научный руководитель – Дмитренко А.А.).....	13
6. РАЗВИТИЕ РЭТ ВВС И ВОЙСК ПВО	
(Крижик В.А., научный руководитель – Маргель А.Б.).....	16
7. РАЗВИТИЕ РЭТ ВВС И ВОЙСК ПВО	
(Некрасов Н.С., научный руководитель – Беккеров Д.Э.).....	18
8. ТРАССОВЫЙ РАДИОЛОКАЦИОННЫЙ КОМПЛЕКС «СОПКА-2»	
(Никулин Н.С., научный руководитель – Лавринчик Н.Н.).....	20
9. МЕТОДИКА КАЛИБРОВКИ ОСЦИЛЛОГРАФА УНИВЕРСАЛЬНОГО	
(Парахневич А. В., научный руководитель – Дмитренко А.А.).....	23
10. ТРЕХКООРДИНАТНАЯ РАДИОЛОКАЦИОННАЯ СТАНЦИЯ «ВОСТОК 3Д»	
(Салей Ф.Н., научный руководитель – Назаров Д.Г.).....	25
11. РАДОЛОКАЦИОННАЯ СТАНЦИЯ «РОДНИК»	
(Стасько Н.А., научный руководитель – Хожевец О.А.).....	27
12. РАДИОЛОКАЦИОННАЯ СТАНЦИЯ «ПРОТИВНИК-ГЕ»	
(Сташкевич Н.В., научный руководитель – Петрукович М.С.).....	30
13. РАДИОЛОКАЦИОННЫЙ КОМПЛЕКС ОБНАРУЖЕНИЯ МАЛОВЫСОТНЫХ ЦЕЛЕЙ «РОСА-РБ»	
(Язенков Г.В., научный руководитель – Маргель А.Б.).....	32
14. РОЛЬ ИСТОРИЧЕСКИХ ЗНАНИЙ В ФОРМИРОВАНИИ ВЗГЛЯДОВ НА ФОРМЫ И СПОСОБЫ ВЕДЕНИЯ БОЕВЫХ ДЕЙСТВИЙ НА СОВРЕМЕННОМ ЭТАПЕ	
(Фирсов А.А., Бебех Д.И., научный руководитель – Комар Е.В.).....	34
15. ПРЕИМУЩЕСТВА ИСПОЛЬЗОВАНИЯ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ ТАКТИКИ ОБЩЕВОЙСКОВОГО БОЯ	
(Семёнов М.И., Пинголь Д.И., научный руководитель – Фомченко А.Л.).....	35
16. РОЛЬ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ ОБЩЕВОЙСКОВОГО БОЯ	
(Носко К.А., Николаев Е.А., научный руководитель – Соколов С.В.).....	38
17. ИСПОЛЬЗОВАНИЕ СОВРЕМЕННЫХ МЕТОДОВ ОБУЧЕНИЯ ПРИ ИЗУЧЕНИИ ТАКТИКИ ОБЩЕВОЙСКОВОГО БОЯ	
(Дубяга Е.В., Круглей В.В., научный руководитель – Бабич В.Н.).....	41
18. СИСТЕМНЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В ОРГАНИЗАЦИЯХ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ	
(Федоренко В.А.).....	44
19. ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ ПРИ ИЗУЧЕНИИ ТАКТИКИ ОБЩЕВОЙСКОВОГО БОЯ	
(Гаврилов Р.Ю., научный руководитель – Лялихов К.А.).....	45
20. ЗАДАЧИ, ПРИЕМЫ И СПОСОБЫ ДЕЙСТВИЙ БОЕВЫХ ГРУПП В НАСТУПЛЕНИИ В ГОРОДЕ (ПО ОПЫТУ БОЕВЫХ ДЕЙСТВИЙ В ЛОКАЛЬНЫХ ВООРУЖЕННЫХ КОНФЛИКТАХ)	
(Шутко А.П., научный руководитель – Сименков Л.Л.).....	47

21. ЭФФЕКТИВНОСТЬ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА НА БАЗЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ В УЧРЕЖДЕНИЯХ ВОЕННОГО ОБРАЗОВАНИЯ	
(Прокопенко В.А., научный руководитель – Сименков Л.Л.).....	49
22. ОБЕСПЕЧЕНИЕ ЗАЩИТЫ ИНФОРМАЦИОННЫХ РЕСУРСОВ ВООРУЖЕННЫХ СИЛ. РАЗРАБОТКА И РЕАЛИЗАЦИЯ КОМПЛЕКСНОЙ СТРАТЕГИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ	
(Хрипач Н.А., научный руководитель – Дудак М. Н.).....	51
23. ИНТЕГРАЦИЯ НОВЫХ ТЕХНОЛОГИЙ И ИННОВАЦИОННЫХ РЕШЕНИЙ В СИСТЕМЫ СВЯЗИ И УПРАВЛЕНИЯ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ	
(Хрипач Н.А., научный руководитель – Дудак М. Н.).....	53
24. ОПТИМИЗАЦИЯ СТРУКТУРЫ И ФУНКЦИОНИРОВАНИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И УСЛУГ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ В КОНТЕКСТЕ СОВРЕМЕННЫХ ТЕХНОЛОГИЧЕСКИХ ТРЕНДОВ	
(Хрипач Н.А., научный руководитель – Дудак М. Н.).....	55
25. ОСОБЕННОСТИ АДАПТАЦИИ ВОЕННОСЛУЖАЩИХ К УСЛОВИЯМ БОЕВЫХ ДЕЙСТВИЙ В ПЕРИОД БОЕВОГО СЛАЖИВАНИЯ	
(Лейбук Е.В., научный руководитель – Вербицкий Г.И.).....	57
26. ПРАКТИКО-ОРИЕНТИРОВАННОЕ ОБУЧЕНИЕ – ВАЖНЕЙШЕЕ УСЛОВИЕ ПОДГОТОВКИ ВОЕННЫХ СПЕЦИАЛИСТОВ	
(Дудкин А.Е., научный руководитель – Мартыненко В.О.).....	58
27. РАЗВИТИЕ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ХРАНЕНИЯ И ОБРАБОТКИ ИНФОРМАЦИИ ВОЕННОГО НАЗНАЧЕНИЯ	
(Митько Е.А., научный руководитель – Масейчик Е.А.).....	59
28. КИБЕРБЕЗОПАСНОСТЬ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ	
(Остапчук Ю.М., научный руководитель – Масейчик Е.А.).....	60
29. ТЕНДЕНЦИИ РАЗВИТИЯ СОВРЕМЕННЫХ ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ	
(Готин Н.А., научный руководитель – Федоренко В.А.).....	61
30. ВЗАИМОДЕЙСТВИЕ ВОЕННЫХ И ГРАЖДАНСКИХ ИНФРАСТРУКТУР СВЯЗИ В УСЛОВИЯХ ВОЕННЫХ ДЕЙСТВИЙ	
(Кириллюк Н.Н., научный руководитель – Федоренко В.А.).....	62
31. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ И МАШИННОЕ ОБУЧЕНИЕ В ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ ВОЙСК СВЯЗИ ВС РБ	
(Листванович А.А., научный руководитель – Федоренко В.А.).....	63
32. РАЗВИТИЕ ОБРАЗОВАТЕЛЬНОЙ СРЕДЫ ВОЕННЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ С ИСПОЛЬЗОВАНИЕМ ОБЛАЧНЫХ ТЕХНОЛОГИЙ	
(Новицкий И.Р., научный руководитель – Федоренко В.А.).....	64
33. АКТУАЛЬНЫЕ ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ ВОЕННОГО НАЗНАЧЕНИЯ	
(Пиляк Г.В., научный руководитель – Федоренко В.А.).....	66
34. ИНТЕГРАЦИЯ ВИРТУАЛЬНЫХ И РАСШИРЕННЫХ РЕАЛЬНОСТЕЙ В ПРОЦЕСС ОБУЧЕНИЯ В ВОЙСКАХ СВЯЗИ	
(Плешко А.А., научный руководитель – Федоренко В.А.).....	67
35. РАЗВИТИЕ МОБИЛЬНЫХ КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ В ВОЙСКАХ СВЯЗИ РБ	
(Шкляр Ф.И., научный руководитель – Федоренко В.А.).....	68

36. ЦИФРОВОЙ ФОРМАТ ОБУЧЕНИЯ: ПЕРСПЕКТИВНЫЕ ТЕХНОЛОГИИ (Кругляк А.Д., научный руководитель – Титков Е.В.).....	69
37. ПЕРЕХОД К ЦИФРОВОЙ ПЕДАГОГИКЕ: ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ И НОВЫЕ ВОЗМОЖНОСТИ В ОБРАЗОВАНИИ (Николаев Е.А., Хаткевич Д.Н., научный руководитель – Тарайкович В.А.).....	70
38. ПРИМЕНЕНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ ИНТЕЛЛЕКТУАЛЬНЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И СЕТЕЙ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ (Ахапкина А.М., научный руководитель – Способ С.П.).....	71
39. АСПЕКТЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ (Готченя Д.Г., научный руководитель – Сасновский А.А.).....	73
40. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПЕРЕДАЧИ ДАННЫХ В СЕТЯХ ВОЕННОГО НАЗНАЧЕНИЯ (Кабачков В.П., научный руководитель – Гусаков П.Б.).....	74
41. НАСТОЯЩЕЕ И БУДУЩЕЕ РАЗВИТИЯ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ (Пинголь А.И., научный руководитель – Федоренко В.А.).....	76
42. ПЕРСПЕКТИВЫ ИСПОЛЬЗОВАНИЯ ГЕОПРОСТРАНСТВЕННЫХ ТЕХНОЛОГИЙ В ВОЕННОЙ СВЯЗИ (Рудаковский В.С., научный руководитель – Федоренко В.А.).....	77
43. АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И УСЛУГ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ (Седеневский А.М., научный руководитель – Божко Р.А.).....	78
44. ВЛИЯНИЕ ИННОВАЦИОННЫХ ТЕХНОЛОГИЙ НА ОБРАЗОВАТЕЛЬНЫЙ ПРОЦЕСС (Куцуленко И.И., научный руководитель – Будиков Ю.Н.).....	79
45. ИННОВАЦИИ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ: БУДУЩЕЕ ОБРАЗОВАНИЯ (Нусин Н.А., научный руководитель – Вершило Д.Н.).....	80
46. СОВРЕМЕННЫЕ ТЕНДЕНЦИИ В СФЕРЕ ОБРАЗОВАНИЯ: ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ И НОВЫЕ ПОДХОДЫ (Иванов Е.А., Мурашко Д.Ю., научный руководитель – Коношенко А.В.).....	81
47. ОСНОВНЫЕ ВИДЫ БОЕВОГО ОБЕСПЕЧЕНИЯ (Мурашко Д.Ю., научный руководитель – Тимошенко В.В.).....	82
48. ИННОВАЦИИ В ОБЕСПЕЧЕНИИ ВОЕННОЙ СВЯЗИ В ВООРУЖЕННЫХ СИЛАХ РЕСПУБЛИКИ БЕЛАРУСЬ (Лапаревич Д.Ю., научный руководитель – Масейчик Е.А.).....	83
49. ПРИМЕНЕНИЕ МАШИННОГО ОБУЧЕНИЯ И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В СОВРЕМЕННЫХ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМАХ ВООРУЖЕННЫХ СИЛ (Гудков А.С., научный руководитель – Балденко А.А.).....	84
50. АКТУАЛЬНЫЕ ВОПРОСЫ РАЗВИТИЯ ИНФОКОММУНИКАЦИОННЫХ СИСТЕМ И УСЛУГ В ВОЙСКАХ СВЯЗИ ВООРУЖЕННЫХ СИЛ РЕСПУБЛИКИ БЕЛАРУСЬ (Мазур-Грабовский Е.Д., научный руководитель – Балденко А.А.).....	85
51. ПРОГРАММНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОЙ СВЯЗИ (Хорошавин В.Д., научный руководитель – Балденко А.А.).....	86
52. ПРИМЕНЕНИЕ СРЕДСТВ РЭБ В ОБЩЕВОЙСКОВОМ БОЮ (Ахапкина А.М., Можейко В.Д., научный руководитель – Ларев В.В.).....	87

Научное издание

Материалы докладов 59-й научной конференции
аспирантов, магистрантов и студентов

**ИННОВАЦИОННЫЕ ТЕХНОЛОГИИ
В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ**
(Минск, 17–21 апреля 2023 года)

В авторской редакции

*Ответственный за выпуск Л.Л.Утин
Компьютерная верстка С.В.Романовский*