УДК 621.391.28

Потапчик Н. Н.
ВА РБ, г. Минск
nikpotapchik89@gmail.com

СИСТЕМА ПРЕДУПРЕЖДЕНИЯ, ОБНАРУЖЕНИЯ И БЛОКИРОВАНИЯ ПРОГРАММНО-ТЕХНИЧЕСКИХ ВОЗДЕЙСТВИЙ ПРОТИВНИКА

Аннотация. В статье представлено обоснование необходимости включения системы предупреждения, обнаружения и блокирования (СПОБ) программно-технических воздействий (ПТВ) противника в состав телекоммуникационной подсистемы (ТП) системы управления специального назначения (СУ СН) в условиях ведения информационного противоборства (ИПб).

Определены основные функции, возлагаемые на СПОБ ПТВ противника, выполнение которых позволит повысить уровень интегрального свойства безопасности информационного обмена (ИО) в СУ СН. На основании реализуемых функций СПОБ предложен необходимый состав ее структурных элементов с детализацией выполняемых ими функций.

Ключевые слова: информационный обмен, интегральное свойство безопасности, программно-техническое воздействие, система предупреждения, обнаружения и блокирования, информационное противоборство.

Современный период развития вооруженных сил ведущих армий мира характеризуется постоянно возрастающей ролью управления [1]. Основным мероприятием организации управления при подготовке и в ходе ведения боевых действий (БД) является создание и развертывание СУ СН, представляющей собой совокупность органов управления (ОУ), размещаемых на пунктах управления, и информационной системы, обеспечивающей их нормальное функционирование и выполняющей задачи информационного обеспечения процесса управления. Удовлетворение потребностей ОУ в передаче заданного объема информации обеспечивается функционированием ТП СУ СН [1, 2].

Завоевание и удержание информационного превосходства является обязательным условием начала и ведения боевых БД [3, 4]. С этой целью военно-политическим блоком НАТО предусматривается ведение ИПб, основной задачей которого является нарушение функционирования систем управления различного назначения, дезорганизация управления войсками (силами) противника [3–5]. Для решения указанной задачи предусматривается активное применение информационно-технических воздействий (ИТВ) в виде ПТВ и электромагнитных воздействий (ЭВ), направленных на нарушение (блокирование) ИО в системах управления противоборствующей стороны; несанкционированное получение конфиденциальных сведений о замыслах предстоящих БД, составе, положении войск (сил), процессах управления подчиненными силами и средствами и другой информации о противнике; ввод ложной информации с целью введения в заблуждение или обмана [4, 6].

С учетом конфиденциальности передаваемой информации и наличия системы воздействия противника безопасность является одним из главных требований, предъявляемых СУ СН к ИО, как к процессу [2, 6].

В соответствии с разработанным сценарием воздействия комплекса дестабилизирующих факторов (ДФ) ИТВ противника, включающем в своем составе ПТВ в виде комплексных кибератак «Отказ в обслуживании, DDoS-атака» (ККА) и ЭВ в виде радиоэлектронного подавления (РЭП) преднамеренными радиоэлектронными помехами приемных устройств радиоэлектронных средств ТП произведена оценка интегрального свойства безопасности ИО в СУ СН [6].

Анализ полученных результатов оценки свидетельствует о том, что безопасность ИО не отвечает требуемому критериальному значению, убывает с ростом количества и глубины ДФ ИТВ противника и, в первую очередь, зависит от показателей стойкости ИО в элементах ТП к тому или иному ДФ, а также способности ИО к своевременному восстановлению [6].

Для решения выявленного противоречия между существующим и требуемым положением дел предлагается включение в состав ТП СУ СН СПОБ ПТВ противника. Функционирование СПОБ позволит снизить вероятность осуществления ПТВ, своевременно их обнаружить и блокировать до того, как они достигнут своей цели, что в совокупности позволит повысить интегральное свойство безопасности ИО при его прохождении в СУ СН.

Анализ интернет-ресурсов и литературных источников [3–5, 7–10], освещающих факты реализации ИТВ в различных странах мира показал, что в большинстве случаев для нарушения (блокирования) ИО в системах управления различного назначения использовались ПТВ в виде ККА, включающих в своем составе этапы ведения противником технической сетевой разведки (ТСР) и реализации распределенной кибератаки «Отказ в обслуживании, DDoS-атака», предпочтение применения которых вызвано высокой эффективностью, а также относительной простотой реализации и невысокой стоимостью осуществления [6].

Результаты проведенных исследований в области моделирования ИО со свойством стойкости в СУ СН и оценки интегрального свойства безопасности ИО в условиях ИТВ противника [2, 6], позволили сформулировать основные функции, возлагаемые на СПОБ ПТВ противника:

своевременное выявление и устранение уязвимостей в настройках и программном обеспечении (ПО) сетевых средств связи (ССС), входящих в состав аппаратных (станций) связи направлений связи (НС) ТП СУ СН;

мониторинг прохождения ИО в элементах ТП и оперативное его восстановление в результате воздействия ИТВ противника;

своевременное выявление ПТВ противника в виде ККА и их последующее блокирование.

На основе анализа функций СПОБ предлагается следующий состав ее структурных элементов:

подсистема предупреждения ПТВ противника;

подсистема обнаружения ПТВ противника;

подсистема блокирования ПТВ противника.

Декомпозиция возлагаемых на СПОБ функций позволила детализировать выполняемые функции ее подсистемами, реализация которых позволит обеспечить

прирост показателей стойкости ИО в ТП СУ СН и интегрального свойства безопасности в целом.

На подсистему предупреждения ПТВ противника возлагается выполнение следующих функций:

1. сбор и обработка сведений об топологии, принятой системе адресации и схеме маршрутизации ТП СУ СН, детальная инвентаризация всех ССС, входящих в состав аппаратных (станций) связи, используемых сетевых протоколах и сервисах, контроль появления новых ССС и их инвентаризация, а также сбор справочной информации:

1.1 об аппаратных (MAC) и сетевых (IP) адресах ССС, их текущих настройках и конфигурации, версий используемых операционных систем (ОС) и ПО;

1.2 о настройках сетевых интерфейсов, закреплении портов и правил межсетевого экранирования ССС;

1.3 об открытых TCP- и UDP- портах ССС, используемых сетевых протоколах и сервисах;

1.4 о характеристиках сетевого трафика ИО в ТП СУ СН (его пиковые, минимальные и средние значения);

1.5 об известных уязвимостях используемых сетевых протоколов и сервисов, ОС и ПО ССС аппаратных (станций) связи ТП;

2. сбор и обработка сведений об уязвимостях и недостатках в настройках ССС, их ОС и ПО, выполняющихся сетевых сервисах:

2.1 сбор данных о дате и времени проведения последнего сетевого сканирования элементов ТП СУ СН;

2.2 сбор данных о текущих версиях ПО и ОС ССС и их последних обновлениях;

2.3 формирование перечня выявленных уязвимостей и недостатков в настройках ССС, их ОС и ПО, выполняющихся сетевых сервисах;

2.4 статистическая и аналитическая обработка полученной информации;

2.5 своевременное обновление базы данных уязвимостей по средствам актуализации информации о них, содержащейся в различных классификаторах и базах данных уязвимостей;

3. формирование рекомендаций по минимизации угроз нарушения стойкости ИО в ТП СУ СН, содержащих перечень мер, направленных на устранение уязвимостей и недостатков;

4. генерация уведомлений о выявленных уязвимостях с целью своевременного принятия решения об их нейтрализации.

На подсистему обнаружения ПТВ противника возлагается выполнение следующих функций:

1. эффективное обнаружение ПТВ противника;

2. мониторинг прохождения ИО в средствах связи, аппаратных (станциях) связи, НС ТП с целью оперативного принятия решения на его восстановление;

3. анализ данных об ПТВ противника, полученных из разных источников, с целью констатации факта осуществления ККА и их идентификации;

4. сбор и обработка идентификационных данных об обнаруженных ПТВ противника с целью своевременного принятия решения реагирования на них и выбора наиболее эффективного способа их нейтрализации;

5. адаптация с целью обнаружения новых разновидностей ККА за счет своевременного обновления баз данных шаблонов (векторов) ККА.

На подсистему блокирования ПТВ противника возлагается выполнение следующих функций:

1. блокирование выявленных подсистемой обнаружения ККА до того, как они достигнут цели;

2. управление процессом реакции на ККА, вплоть до отмены блокирующих воздействий и возврата в исходное состояние;

3. оперативное восстановление ИО в ТП СУ СН в случае его нарушения (блокирования) в результате воздействия ИТВ противника;

4. сбор доказательной базы для проведения уголовных расследований о фактах проведения ПТВ противника.

К общесистемным требованиям СПОБ ПТВ противника относятся:

1. соответствие действующим принципам и сведение к минимуму влияния на функционирование ТП СУ СН;

2. максимальную автоматизацию процессов сбора, обработки, анализа и доведения до обслуживающего персонала информации об имеющихся уязвимостях в настройках и ПО ССС ТП, а также процессов принятия решения по выбору способа реагирования и активации необходимых для этого механизмов;

3. обеспечение собственной защиты элементов СПОБ от несанкционированного доступа к управляющей информации, блокирования ее функционирования и скрытности для ТСР противника;

4. минимизацию затрат на развертывание и функционирование СПОБ в составе ТП СУ СН;

5. обеспечение возможности гибкой настройки и модернизации СПОБ при изменении структуры и режимов функционирования ТП СУ СН, возникновении новых разновидностей ПТВ противника и способов их предупреждения, обнаружения и блокирования.

Сущность полученного научного результата заключается в обосновании необходимости включения в состав ТП СУ СН СПОБ ПТВ противника, что позволит повысить уровень интегрального свойства безопасности ИО в условиях ИТВ, проводимых противоборствующими сторонами с целью завоевания и удержания ИП. Предложен состав структурных элементов СПОБ и сформулированы выполняемые ими функции.

Полученный научный результат имеет важное методологическое значение для выбора конкретных средств и мер защиты, позволяющих реализовать все представленные функции СПОБ ПТВ противника, а также определить их количество, местоположение и взаимосвязь при функционировании в составе ТП СУ СН.

Список использованных источников и литературы

1. Боговик, А. В., Игнатов, В. В. Эффективность систем военной связи и методы ее оценки. – СПб. : ВАС, 2006. – 184 с.

2. Пылинский, М. В., Потапчик, Н. Н. Многоуровневая логико-вероятностная модель информационного обмена в системе управления специального назначения // Сб. науч. статей Воен. акад. Респ. Беларусь. – 2024. – № 46. – С. 42–52.

3. Бедрицкий, А. В. Информационная война: концепции и их реализации в США / под ред. Е. М. Кожина. – М. : РИСИ, 2018. – 187 с.

4. Макаренко, С. И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века : моногр. – СПб. : Наукоемкие технологии, 2017. – 546 с.
5. Макаренко, С. И. Модели системы связи в условиях преднамеренных дестабилизирующих воздействий и ведения разведки : моногр. – СПб. : Наукоемкие технологии, 2020. – 337 с.
6. Потапчик, Н. Н. Методический подход к оценке стойкости информационного обмена в условиях информационно-технического воздействия противника // Вестн. Воен. акад. Респ. Беларусь – 2024. – № 3 (84). – С. 36–50.
7. Обзор первого квартала 2024: отчет о DDoS-атаках от компании StormWall [Электронный ресурс]. – Режим доступа : https://stormwall.pro/otchet-o-ddos-atakah-2024-perviy-kvartal/. – Дата доступа : 24.01.2025.
8. В Совбезе рассказали о создании системы противодействия опасным DDoS-атакам [Электронный ресурс]. – Режим доступа: https://ria.ru/20240305/ddos-1931151155.html/. – Дата доступа : 25.01.2025.
9. В Куркой области наблюдаются перебои с мобильной связью и интернетом [Электронный ресурс]. – Режим доступа : https://vedomosti.ru/technology/ news/2024/08/09/1054950-na-blyudayutsya-pereboi.html/. – Дата доступа : 28.01.2025.
10. Давыдов, А. Е., Максимов, Р. В., Савицкий, О. К. Защита и безопасность ведомственных интегрированных инфокоммуникационных систем. – М. : Воентелеком, 2015. – 520 с.

УДК 681.5

к.т.н., доцент Михнёнок Е. И.
к.т.н., доцент Сахарук Д. А.
Сергеенко А. В.
УО «ВА РБ», г. Минск
andrew-sergeenko@mail.ru

ТРЕБОВАНИЯ К СОВРЕМЕННЫМ УСТРОЙСТВАМ ПЕРЕДАЧИ ДАННЫХ ТАКТИЧЕСКОГО УРОВНЯ

Аннотация. В статье проведен краткий анализ организации системы связи и передачи данных на тактическом уровне в ходе проведения специальной военной операции Вооруженных сил Российской Федерации на Украине. Определены основные требования предъявляемые к перспективным устройствам передачи данных, применяемым на тактическом уровне.

Ключевые слова: средства связи, передача данных, тактический уровень.

Проводимая Вооруженными силами Российской Федерации специальная военная операция (СВО) на Украине подтвердила тезис о необходимости повышения устойчивости системы связи и передачи данных при организации и ведении боевых действий, особенно на тактическом уровне. Анализ реализованной системы связи и передачи данных, позволил выделить ряд вопросов, требующих решения для успешного ведения современного общевойскового боя:

- укомплектованность индивидуальными средствами связи в пехотных подразделениях. На начало СВО только в специальных подразделениях индивидуальные средства связи имелись у каждого военнослужащего, в обычных механизированных подразделениях такие средства связи появлялись у командиров начиная от командира отделения. Современные условия ведения общевойскового боя требуют наличия индивидуальны средств связи у каждого бойца;