УДК 621.263

Тарас Михайлович Дзюба
Вадим Вячеславович Вищун

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ ЖИВУЧЕСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ ОРГАНОВ ВОЕННОГО УПРАВЛЕНИЯ ПРИ ПРОВЕДЕНИИ КИБЕРАТАК

Постановка проблемы. Анализ последних исследований и публикаций

Использование информационно-управляющих систем для обеспечения процесса управления боевыми действиями подразделений и частей, создаваемой группировки войск, значительно повысят их боевой потенциал, а поэтому о необходимости и важности их использования и эффективного применения не может быть и речи.

В органах военного управления, в процессе управления, необходимо постоянно выполнять ряд важных задач, в режиме реального времени [1]:

проведение анализа большого массива информационных данных;

согласование и разработка планирующих документов и наполнение их блоками из различных баз данных и доверенных пользователей;

доведение управляющих команд и боевых документов;

обмен служебной информацией внутри и вне органа управления;

получение донесений и информации о состоянии управляемого объекта.

Процесс управления цикличен и имеет устоявшуюся классическую структуру, поэтому возникает необходимость повышения эффективности программных и технических средств обеспечения обменом, доставкой и обработкой информации, или так называемой функциональности информационно-управляющих систем.

Анализируя военные конфликты, которые произошли на протяжении последнего десятилетия можно сделать вывод, что в процессы управления включаются не только возможность в управлении подчиненным личным составом, но и необходимость управления автономными техническими средствами разведки, обеспечения, доставки, а также вооружением [2].

Предоставление таких полномочий на фоне значительного прироста эффективности боевого применения группировки войск, при потере контроля или ключевой информации в таких системах, приводит к катастрофическим последствиям и, в конце концов, к поражению.

Вероятность возникновения таких фактов, в ходе конфликтов, зависит не только от надежности программного и технического обеспечения таких систем. Усиление концентрации на новом домене противостояния, такого как киберпространство, привело к необходимости изучения возможных атак на информационно-управляющие системы и, как следствие планирование проведения в нём, защитных и атакующих действий.

Формулировка цели статьи. Изложение основного материала

Целью написания данной статьи является формирование основных подходов к обеспечению информационной живучести информационно-управляющих систем органов военного управления при проведении кибератак.

Перед решением данной проблемы надо определиться с тем, что единого средства по обеспечению безопасного функционирования – не существует.

На данный момент, ведущими учёными в области информационной безопасности, предложены следующие парадигмы по предотвращению критических процессов в информационно-управляющих системах [3]:

классическая парадигма защиты информации, основанная на контроле доступами;

парадигма эшелонированной, многоуровневой системы защиты информационных ресурсов и технологий (система круговой обороны);

сетецентрическая парадигма защиты информационных ресурсов;

парадигма кибербезопасности структурных ведомств и органов военного управления (переход от обеспечения информационной безопасности технологий к безопасности киберпространства организаций и пользователей).

Требования, предъявляемые к информационно-управляющим системам, для обеспечения процесса управления в интенсивном вооружённом конфликте очень высоки и, кроме функциональности таких

систем необходимо обеспечить и их информационную живучесть, в условиях воздействия атакующих действий противника на программную часть информационно-управляющих систем, или проще говоря, при проведении кибератак.

Под информационной живучестью информационно-управляющих систем органов военного управления при проведении кибератак, следует понимать состояние гарантированного предоставления заявленных характеристик функционирования и безопасности информационно-управляющих процессов, при сохранении возможности доступа к информации и к информационным ресурсам конечных пользователей, в условиях проведения атакующих действий на любые программные элементы информационно-управляющей системы.

Кибератакой на информационно-управляющие системы, будем считать, активные действия в киберпространстве программными средствами или пользователями сети, приводящие к нарушениям критериев безопасности и её нормального функционирования.

Информационная живучесть существующих информационно-управляющих систем органов военного управления обеспечивается комплексом мероприятий, реализующих защиту и устойчивость её функционирования [4].

Существуют различные программные продукты, которые в режиме реального времени проводят анализ атакующих действий и, соответственно противодействия для предотвращения проведения кибератак, а также восстанавливающие потерянную функциональность, после успешного их проведения.

Нерешенной проблемой при обеспечении безопасного функционирования любой информационной системы, является необходимость создания комплексной системы контроля, которая должна учитывать стремительно растущее количество происходящих процессов, запущенных служб, программ, политик предоставления доступа к ресурсам и многих других.

За последнее десятилетие объёмы обрабатываемой информации в информационно-управляющих системах, увеличились в 40 раз [5], а количество служб, библиотек и ресурсов системы, необходимых для запуска одного приложения, также значительно возросли. На выполнение контроля стремительно растущего объёма информационных потоков необходимо выделять значительные ресурсы системы, что приводит к снижению её работоспособности, и как следствие, принятию решения по уменьшению количества контролируемых параметров.

Принятие решения по выбору варианта противодействия кибератакам, которые могут приводить к возможным критическим отклонениям необходимых показателей критериев безопасности, а также их нормального функционирования, ложится на плечи администраторов сетей и администраторов безопасности. В условиях боевых действий, где политики доступа и топология сетей будут динамически меняться, где необходимо осуществлять контроль значительного количества, как абонентов, так и параметров – эффективность такого контроля будет минимальна, а последствия – катастрофичны.

Факты проведения кибератак на закрытые системы подтверждают невозможность реализации «всеобъемлющего» контроля в многоуровневых сложных системах. Наличие человеческого фактора всегда будет угрозой обеспечения безопасного функционирования (соответствующих критериев безопасности), а предоставление полных прав программам безопасности – может привести к потере контроля, как над программами обеспечивающих безопасность, так и системой вообще. Именно сложность выбора стратегии обеспечения безопасного функционирования, как составляющую информационной живучести, движет авторами в решении данной проблемы.

Изучив психологию пользователей автоматизированных рабочих мест и, проанализировав прошедшие кибератаки в информационно-управляющих системах, можно сделать такие выводы [6-8]:

ограничение прав пользователя при выполнении своих функций, всегда будет вызывать желание расширения своих функциональных возможностей;

низкая эргономичность программного интерфейса, всегда будет приводить к желанию его замены или отказу в его использовании;

сложность в получении квалифицированной помощи, по возникающим проблемам функционирования автоматизированного рабочего места, всегда будет приводить к поиску альтернативных путей её решения;

низкая осведомлённость о происходящих информационных процессах, всегда будет приводить к несвоевременным противодействиям кибератакам.

Как видно из проведённого анализа, обеспечение информационной живучести напрямую зависит от действий каждого пользователя информационно-управляющей системы. При том, что программное обеспечение уже определено, при обеспечении системы защиты надо учитывать все выше перечисленные факты.

Следующим шагом к обеспечению информационной живучести является формирование базы данных по нормированию информационных потоков и процессов. Данный этап, является самым важным, ибо на основании этих данных будет формироваться стратегия предупреждения кибератак.

Для определения необходимого режима безопасности в дискретные моменты времени, введем понятие – сенсоры безопасности. Под

сенсорами безопасности будем считать показатели критериев безопасности, изменение которых будет вероятным при проведении определённого типа кибератаки. Сенсоры будут поделены на группы соответствующих требований – конфиденциальности, целостности, доступности и наблюдаемости. Порядок изменения данных сенсоров и интенсивность их изменения будут исходными данными при выборе стратегии противодействия кибератакам.

Как было сказано выше, предоставление максимальных полномочий соответствующим администраторам или программным средствам защиты, в процессе конечного выбора стратегии противодействия кибератакам и порядке функционирования системы опасно, по причине трансформации их, таким образом, в критический элемент всей информационно-управляющей системы. Для решения данной проблемы предлагается распределить возможность выбора варианта противодействия кибератакам конечным пользователям, в границах полученных полномочий.

Особенностью информационно-управляющих систем органов военного управления является их закрытость и ограничение вариативности программного обеспечения, поэтому при определении наиболее критических кибератак, проведен анализ аналогичных систем. Наиболее вероятной и критичной будет инсайдерская атака, маловероятной – DDoS-атака.

Инсайдерская атака – тип кибератаки, при котором нарушение функционирования информационно-управляющей системы, а также критериев безопасности, происходит в результате разрешённых действий пользователя системы.

Так, при проведении инсайдерской кибератаки, об изменении показателей сенсоров безопасности

на определенном автоматизированном рабочем месте, уведомляется не только ответственный администратор (программа), но и пользователь, который непосредственно участвует в сеансе с инсайдером, а также пользователи, заранее определённые, соседние по расположению или подчинению. Такой подход в обеспечении информационной живучести убирает критичность каждого элемента информационно-управляющей системы и повышает динамичность обеспечения защищенности системы от кибератак.

Система обеспечения информационной живучести, на каждом автоматизированном рабочем месте информационно-управляющей системы, может быть представлена следующей функциональной схемой на рис.1.

При обеспечении информационной живучести, контроль функционирования проводится по двум направлениям: контроль над информационными процессами и контроль над информационными потоками. Процесс контроля информационных процессов начинается с анализа их активности. После этого, проводится определение показателей сенсоров безопасности при каждом запущенном процессе, в соответствии с возможностью нарушения критериев безопасности из существующей базы данных.

Помеченный таким образом активный процесс, проходит проверку на соответствие установленному требованию безопасности, при несоответствии – процесс блокируется. При успешном прохождении проверки, проводится анализ процессов на наличие атакующих действий в режиме реального времени. При обнаружении нарушений, одним из блоков обеспечения безопасности функционирования (анализа аномалий, анализа связности, база данных кибератак), – процесс блокируется и, выдаётся извещение соответствующему администратору процессов.

В процессе контроля информационных потоков вначале проводится анализ активных соединений, затем, сравниваются IP-адреса пользователей с базой данных доверенных IP-адресов, при несоответствии – закрытие сеанса. При определении сеанса как доверенного – проводится проверка служебной информации передаваемых пакетов и их содержимого, в соответствии с требованиями безопасности и грифом секретности пользователя, участвующего в сеансе, который является наивысшим. Затем, проводится проверка содержимого на наличие вредоносного кода и допустимого контента. При нарушении любого из показателей – закрытие сессии, с уведомлением администратора сеанса.

Выводы

Таким образом, обеспечение информационной живучести необходимо проводить с учётом парадигмы обеспечения кибербезопасности всей информационно-управляющей системы.

Ограничение прав управления и контроля информационными процессами, администраторам безопасности или программным средствам безопасности, приведет к уменьшению критичности информационно-управляющей системы. Рассредоточение возможности выполнения таких действий на автоматизированных рабочих местах, с предоставлением контроля определенным пользователям, приведет к динамичному осуществлению защиты таких систем от любого типа кибератак.

При проектировании информационно-управляющих систем, необходимо учитывать не только защищённость программных продуктов и их функциональную устойчивость, но и их эргономичность, простоту и завершённость при использовании, что, в конце концов, уменьшит вероятность появления инсайдерских кибератак.

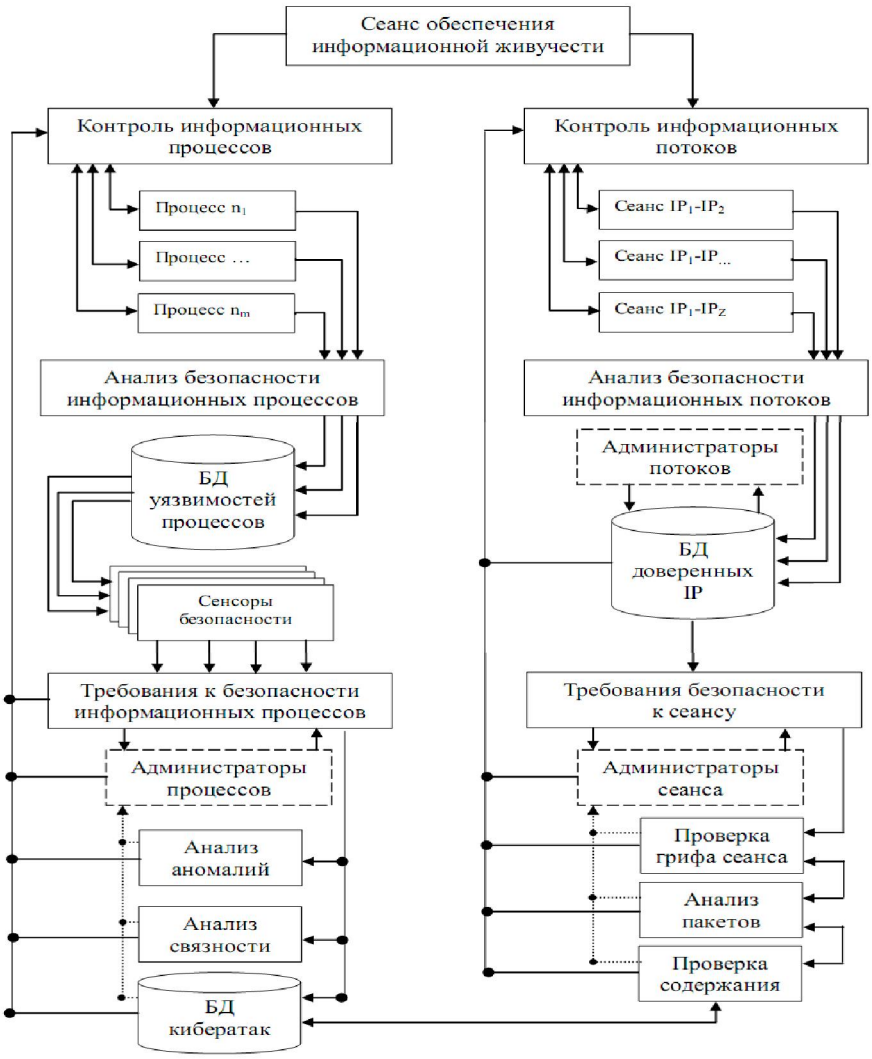

Рис.1 Функциональная схема системы обеспечения информационной живучести

Литература

1. Застосування інформаційних технологій в роботі органів управління. – Частина 2: Підручник. К.: Вид. НАОУ, 2006. – 308 с. **2. Kaspersky Lab** provides its insights on Stuxnet worm, режим доступу – http://www.kaspersky.com/news?id = 207576183$. **3. Рекомендация** МСЭ-Т X.1205. Безопасность электросвязи. Обзор кибербезопасности. – Женева, 2009. – 55 с. **4. Климов С.М.** Проблемы создания компьютерных стратегических игр для оценки защищенности критически важных информационных сегментов. – ЗАО «ЭКА». **5. Каргаполов Ю.** Есть ли предел у мечты? режим доступу – http://itstrateg.net/story/est-li-predel-u-mechty.

6. Информационная безопасность государства в военной сфере: науч.-метод. издание / Н.Н. Биченок, Т.М. Дзюба, А.А. Рось, В.В. Витковский, В.В. Вищун – К.: НУОУ, 2012 р. – 264 с. **7. Шаньгин В.Ф.** Защита компьютерной информации. Эффективные методы и средства / В.Ф. Шаньгин. – М.: ДМК Пресс, 2008. – 544 с. **8. Кононович В. Г.** Технічна експлуатація систем захисту інформації телекомунікаційних мереж загального користування. Частина 3. Архітектура безпеки Концепція захисту інформації : [навч. посібник для вузів, затверджено Міністерством транспорту та зв'язку України] / Кононович В. Г. ОНАЗ. – Одеса, 2009. – 194 с.

Викладені результати досліджень щодо порядку забезпечення інформаційної живучості інформаційно-управляючих систем органів військового управління при здійсненні кібератак, представлена функціональна схема системи забезпечення інформаційної живучості інформаційно-управляючих систем від впливу кібератак.

Ключові слова: інформаційно-управляючі системи органів військового управління, інформаційна живучість, кібератаки.

The results of researches are expounded in relation to the order of military management staff information management systems informative vitality providing during cyberattacks, the functional diagram of military management staff information management systems informative vitality providing system during cyberattacks realization is presented.

Key words: military management staff information management systems, informative vitality, cyberattacks.