УДК 621.08

© Климов С.М.
Klimov S.

МОДЕЛЬ БЕСКОМПРОМАТНОГО АУДИТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СЕТИ СПУТНИКОВОЙ СВЯЗИ

THE AUDIT MODEL INFORMATION SAFETY SATELLITE COMMUNICATIONS NETWORK WITHOUT COMPROMISING

Аннотация. *В статье рассмотрена модель для осуществления бескомпроматного (скрытого) контроля реального уровня защищенности сети спутниковой связи на основе удаленного доступа к каналу связи через спутниковый модем и минимизации признаков сканирования уязвимых мест этой сети.*

Annotation. *The article discusses the model for the implementation of the without compromising (hidden) control of the real level of protection of the satellite communications network on the basis of remote access to the communication channel via satellite modem and minimize the signs of scanning vulnerabilities of the network.*

Ключевые слова. *Сеть, спутниковая связь, бескомпроматность, аудит, информационная безопасность, сканирование, уязвимое место.*

Key words. *Network, satellite communications, without compromising, audit, information security, scanning, vulnerability.*

Несмотря на жесткие требования руководящих документов ФСТЭК России (например, по защите от вторжений) и операторов связи к обеспечению информационной безопасности сетей спутниковой связи (ССС) при нарастании потенциальной опасности воздействия компьютерных атак и вредоносного кода на практике эти требования реализуются далеко не в полной мере.

Недостаточный уровень защищенности ССС обусловлен, прежде всего, опережающим ростом угроз информационной безопасности, отстающими от этих угроз темпами развития защищенных информационных технологий и человеческим фактором в ходе сопровождения средств защиты информации (СЗИ).

Особенностью ССС является тот факт, что тщательной защите, как правило, подвергается наземный проводной сегмент прикладной сети, использующей спутниковый канал обмена данными, а спутниковое оборудование и космическая радиолиния считается априори защищенной оператором связи.

Однако несанкционированный доступ к абонентам ССС через стандартное и легитимно приобретенное спутниковое оборудование вполне возможен.

Под СЗИ будем понимать комплекс средств, включающих средства защиты от несанкционированного доступа, встроенные средства защиты информации операционных систем и систем управления базами данных, антивирусные программы, межсетевые экраны, средства обнаружения компьютерных атак. Недостатком работы подобного комплекса СЗИ является несогласованная их работа в различных сегментах ССС и использование общедоступных протоколов передачи данных, что дает дополнительные возможности для нарушителя по проникновению в абонентскую сеть и осуществлению в них своих деструктивных действий.

Поэтому актуальным является аудит информационной безопасности ССС с использованием модели бескомпроматного проникновения инспектирующей стороны средствами контроля как в действующие системы, так и в макеты на испытательном стендовом полигоне, имитирующем основные функции ССС в условиях компьютерных атак.

Бескомпроматный контроль реального уровня защищенности ССС осуществляется в виде совокупности скрытых действий пассивного, активного сканирования и имитации компьютерных атак (генерации экстремальных нагрузок пакетами данных программами типа metasploit) через спутниковое оборудование на ССС.

Модель бескомпроматного аудита информационной безопасности ССС состоит из трех процессов:

1. Скрытого ведения сканирования уязвимых мест ССС.

Климов Сергей Михайлович – доктор технических наук, профессор, МГТУ им. Н.Э. Баумана, тел. (495)519-72-55.

Klimov Sergei – doctor of technical Sciences, Professor, MGTU. AD. Baumann, tel. (495)519-72-55.

2. Технологии имитации компьютерных атак на ССС.

3. Оценки возможности нарушения штатного функционирования (технологических циклов управления) ССС.

Под повышением бескомпроматности аудита информационной безопасности ССС понимается минимизация (снижение риска компрометации) обнаружения операторами и администраторами информационной безопасности признаков несанкционированных действий, обусловленных применением средств инструментального контроля.

Величина снижения риска определяется вероятностным образом на основе экспертных оценок по результатам испытаний макетов ССС на стенде (сегментов реальных сетей) и анализу системных журналов (log-файлов) средств обнаружения тестовых программ компьютерных атак и вредоносного кода. Значение вероятности обнаружения $P_{обн}$ признаков сканирования и компьютерных атак за время испытаний (проверки), равное 0, означает полную бескомпроматность экспериментальных исследований, а значение, равное 1, свидетельствует о полной компрометации действий инспектирующих.

Вероятность $P_{обн}$ определяется статистическим методом по отношению количества выявленных фактов компьютерных атак $N_{выявл}$ к общему числу реализованных воздействий $N_{общ}$ за время имитационного моделирования действий нарушителя $T_{н}$.

Решения по соответствию средств аудита информационной безопасности ССС требуемому уровню бескомпроматности принимаются на основе значений вероятности таблицы.

ствий. Решения по двусторонним действиям в ходе экспериментальных исследований принимаются экспертным путем исходя из существующих моделей угроз и уязвимостей ССС, ограничений технологических циклов управления, имеющегося опыта. Ограничения на применение модели следующие:

1. Априорно достичь полной (гарантированной) бескомпроматности аудита информационной безопасности ССС не представляется возможным в реальной обстановке ввиду того, что объективно существуют факторы неопределенности реакции ССС на воздействия (сканирование и компьютерные атаки), порядка работы СЗИ и корректности работы самих средств аудита в этих условиях неопределенности.

2. Средства аудита подключаются с одним из штатных электронных адресов (IP-адресом) и логическим именем абонента ССС в соответствии с эталонной моделью взаимодействия открытых систем, как правило, реализованной в протоколах передачи данных TCP/IP.

3. Бескомпроматность применения средств аудита должна быть обеспечена на время непосредственного проведения инструментальной проверки. Сразу после завершения мероприятий эти средства должны быть отключены от ССС, а также удалены оставшиеся записи о воздействиях из системных файлов.

Общая схема модели бескомпроматного аудита информационной безопасности ССС приведена на рис 1.

Сущность схемы модели на рис. 1 заключается в том, что в ходе инспекции инструментальные средства аудита должны предотвращать возможные защитные

Шкала соответствия средств аудита информационной безопасности ССС требуемому уровню бескомпроматности

Вероятности обнаружения признаков применения средств аудита информационной безопасности ССС за заданное время	Значения вероятности	Уровни бескомпроматности
$P^{м}_{обн}$ (маловероятное событие)	0,1–0,3	Высокий уровень
$P^{н}_{обн}$ (вероятность низкая)	0,4–0,5	Средний уровень
$P^{в}_{обн}$ (событие вполне вероятно)	0,6–0,7	Низкий уровень
$P^{вв}_{обн}$ (вероятность события высокая)	0,8–0,9	Очень низкий уровень

Уровень риска компрометации средств аудита информационной безопасности прямо пропорционален значению вероятности обнаружения эксплуатирующим персоналом ССС признаков применения средств сканирования и компьютерных воздействий. Уровень бескомпроматности зависит от двусторонних действий: группы, производящей проверку защищенности ССС, и оперативности ответных действий операторов и администратора информационной безопасности по выявлению воздействия со стороны администратора информационной безопасности ССС и предусматривать функции контрмер по обеспечению бескомпроматности.

Источниками нарушения бескомпроматности аудита являются СЗИ ССС, собирающие сведения о характеристиках и демаскирующих признаках средств сканирования и имитации компьютерных атак. Возможности проверяемой стороны по противодействию воздействиям характеризуются рисками нарушения бескомпромат-

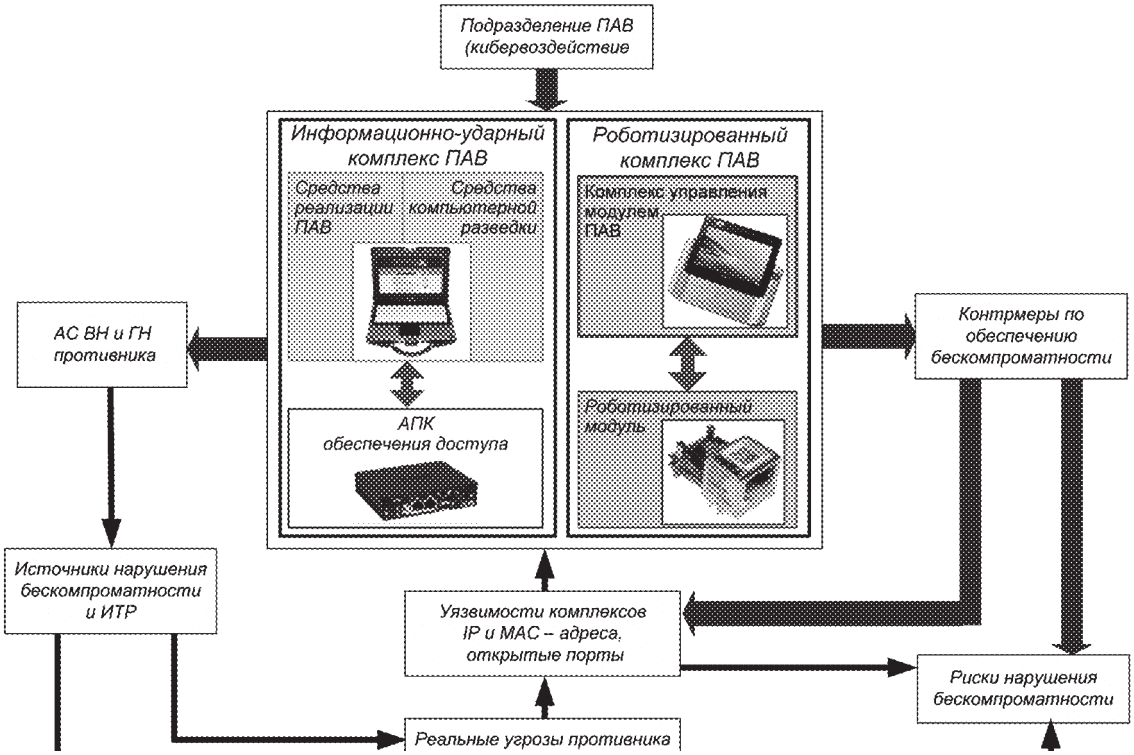

Рис. 1. Общая схема модели бескомпроматного аудита информационной безопасности ССС

ности аудита – значениями вероятностей (определяемыми экспертным путем) событий реализации угроз на выявленные уязвимые места средствами реализации компьютерных атак.

Контрмеры по повышению бескомпроматности средств аудита разрабатываются на основе настоящей модели и определяются вариантами организационно-технических мер, формируемых с учетом задач аудита, данных о технических характеристиках ССС и СЗИ, особенностей применения сегментов ССС в условиях компьютерных атак (времени и месте воздействий, привлекаемого компьютерного, коммуникационного и спутникового оборудования, назначения и принадлежности ССС).

Компроматными (демаскирующими) признаками средств аудита в ходе подготовки и реализации воздействий являются IP и MAC–адреса средств сканирования, реализации компьютерных атак и обеспечения доступа. Активные воздействия с направлением пакетов данных в сеть ССС должно производиться только с использованием IP и MAC–адресов его компьютерного и коммуникационного оборудования (от имени штатных абонентов сети), идентифицированных при сканировании.

Активные действия по бескомпроматности ИУК и РБК ПАВ обеспечиваются предотвращением нарушения функционирования комплексов, несанкционированного доступа к информации о них со стороны противника и минимизацией риска нанесения ущерба его информационным ресурсам (ИР).

Оперативность боевого применения ИУК и РБК ПАВ должна соответствовать его тактико-техническим характеристикам. Превышение необходимой длительности технологического цикла применения комплексов (времени компьютерной разведки и кибервоздействия) повышает возможности противника по вскрытию его параметров и местонахождения.

Кроме того, для минимизации компрометации ИУК и РБК ПАВ до начала их боевого применения должны быть произведены настройки для возможности оперативного изменения ПАВ по данным компьютерной разведки и автоматизированной коррекции сценария ПАВ в зависимости от действий противника.

С целью повышения оперативности применения средства РБК ПАВ должны быть настроены на автоматическое формирование и реализацию ПАВ (в том числе коррекцию параметров в зависимости от действий противника) на выявленные уязвимые места КВИТО.

Подразделение ПАВ должно принимать превентивные меры по предотвращению сбоев, отказов и аварийных ситуаций с ИУК и РБК ПАВ, нейтрализации несанкционированного применения, ошибок в установке и использовании программного обеспечения, вмешательства в информационно-вычислительные процессы.

В ходе планирования применения ИУК и РБК ПАВ должен также прогнозироваться ущерб противнику по количеству пораженных компьютеризированных элементов КВИТО ВН и ГН.

Схема обеспечения бескомпроматности аудита информационной безопасности ССС при проведении сканирования представлена на рис. 2.

Бескомпроматность должна быть обеспечена при осуществлении:

• сканирования вычислительных сетей ССС;

• анализа трафика в сети и определения значимых полей протоколов передачи данных;

• хранения информации о проведенной компьютерной разведке и результатов анализа сетевого трафика;

• представления информации о проведенной компьютерной разведке другим подразделениям.

Схема обеспечения бескомпроматности аудита при имитации компьютерных атак на ССС представлена на рис. 3.

Бескомпроматность должна обеспечиваться при реализации кибервоздействий на компьютерное и коммуникационное оборудование КВИТО.

Бескомпроматно должны быть реализованы следующие кибервоздействия на КВИТО:

• подмена абонентов сети;

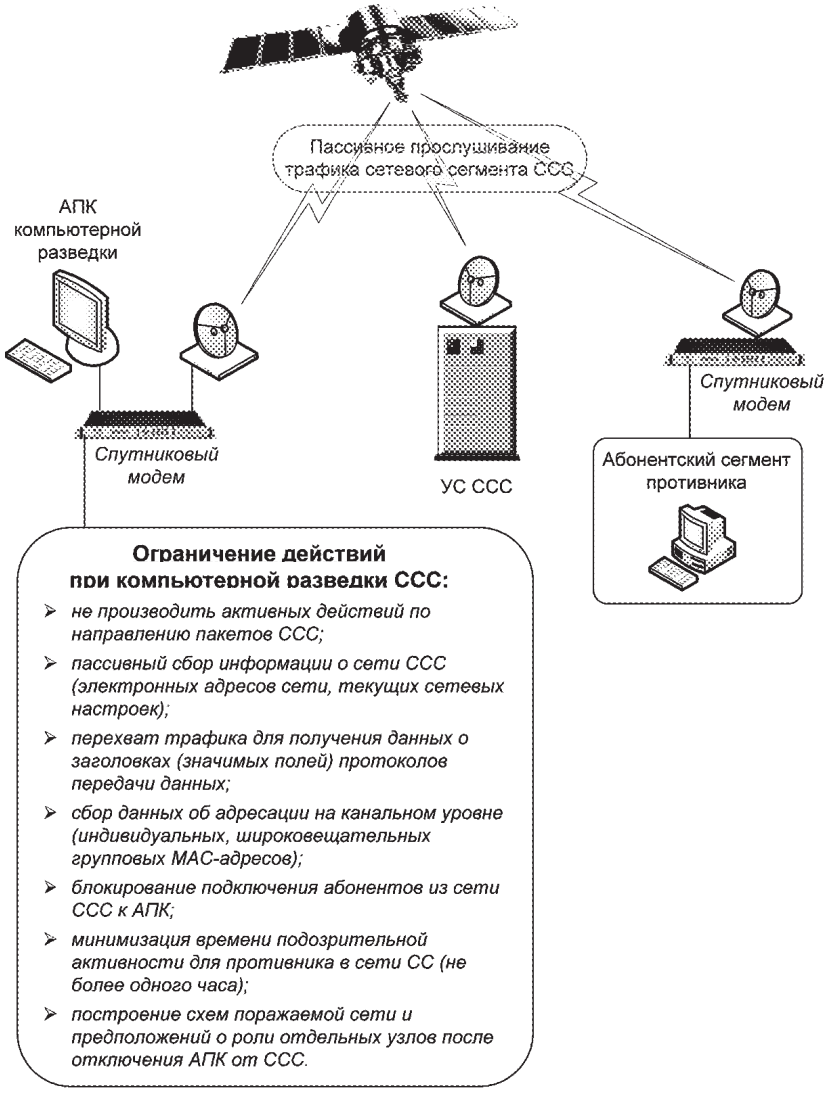

Рис. 2. Схема обеспечения бескомпроматности аудита информационной безопасности ССС при проведении сканирования

• нарушение функционирования;

• «отказ в обслуживании» абонентам в выдаче информации;

• логический разрыв соединений между абонентами;

• искажение инструментальных настроек и данных администрирования;

• функциональное поражение;

• перегрузка сетей спамом информации;

• программы коммуникационного оборудования наземного сегмента ССС.

В ходе нарушения штатного функционирования КВИТО ВН и ГН должно быть предусмотрено скрытое преодоление средств защиты информации от несанкци-

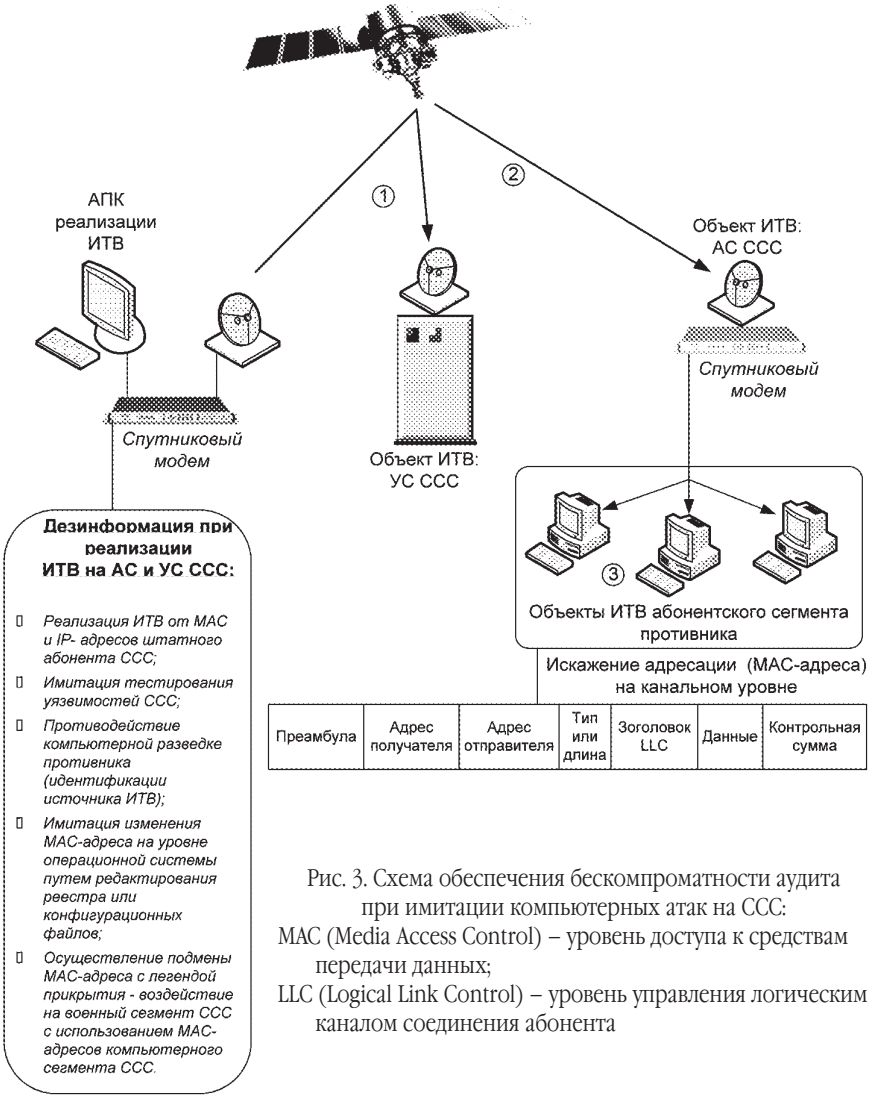

Рис. 3. Схема обеспечения бескомпроматности аудита при имитации компьютерных атак на ССС:
MAC (Media Access Control) – уровень доступа к средствам передачи данных;
LLC (Logical Link Control) – уровень управления логическим каналом соединения абонента

онированного доступа.

При использовании ИУК и РБК ПАВ должно быть обеспечено:

• незаметное для операторов (администратора) КВИТО подключение и обеспечение доступа в сегменты вычислительных сетей;

• бескомпроматное воздействие на компьютерное и коммуникационное оборудование (скрытие параметров электронных адресов источника воздействия).

Защита от раскрытия сведений об ИУК и РБК ПАВ со стороны КВИТО ВН и ГН должна обеспечиваться на основе защиты информации комплексов от несанкционированного доступа путем выполнения требований руководящих документов ФСТЭК России:

• по защите информации автоматизированных систем от несанкционированного доступа – класс 2 А;

• по защите информации средств вычислительной техники от несанкционированного доступа – не ниже 4-го класса;

• по показателям защищенности межсетевых экранов, используемых в составе комплексов – не ниже 3-го класса.

Схема обеспечения бескомпроматности аудита при оценке возможности нарушения штатного функционирования ССС приведена на рис. 4.

Основой обеспечения бескомпроматности ИУК и РБК ПАВ при нарушении штатного функционирования КВИТО ВН и ГН являются авторизованный доступ операторов комплекса (субъектам, которым предоставлены права доступа) и единый диспетчер доступа для внутренних и внешних абонентов, осуществляющий контроль параметров их электронных адресов.

Программный диспетчер доступа выполняет следующие функции:

• контроль прав доступа оператора к конкретному средству,

• авторизацию или блокирование доступа оператора к средству,

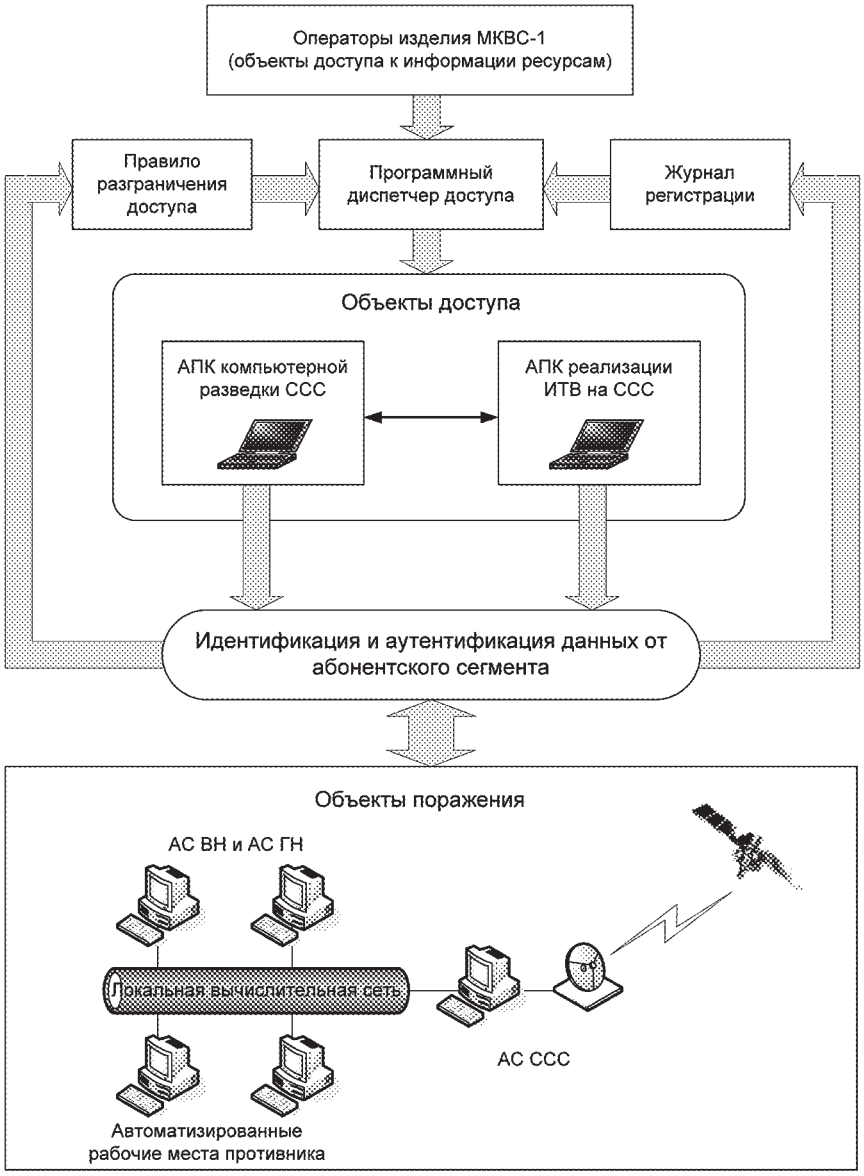

Рис. 4. Схема обеспечения бескомпроматности при оценке возможности нарушения штатного функционирования ССС

• регистрацию фактов санкционированного и несанкционированного доступа в электронном журнале регистрации,

• мониторинг и блокирование операций из сегментов КВИТО ВН и ГН по доступу к информационным ресурсам ИУК и РБК ПАВ.

Для защиты информации в ИУК и РБК ПАВ от внешнего и внутреннего нарушителя должны использоваться только мандатные (полномочные) механизмы защиты информации и управления доступом на основе идентификации и аутентификации операторов подразделения. Мандатные механизмы защиты информации предусматривают такую настройку программного обеспечения комплексов, при которой не допускается хранение и передача паролей абонентов в открытом виде, а также организуется систематическая смена паролей операторов (ежемесячно в рамках технического обслуживания). Внесение изменений информации о правах доступа операторов комплексов (субъектов доступа) к объектам (средствам ИУК и РБК ПАВ) допускается только командиру подразделения (администратору информационной безопасности комплексов) на этапе подготовки и планирования информационной операции (акции).

Материал поступил в редакцию 19. 04. 2013 г.