Парламентское собрание Союза Беларуси и России

Постоянный Комитет Союзного государства

Оперативно-аналитический центр
при Президенте Республики Беларусь

Государственное предприятие «НИИ ТЗИ»

Полоцкий государственный университет

КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИИ

Материалы XXII научно-практической конференции

(Полоцк, 16–19 мая 2017 г.)

Новополоцк
2017

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)
К63

К63 **Комплексная защита информации :** материалы XXII науч.-практ. конф., Полоцк, 16–19 мая 2017 г. / Полоц. гос. ун-т ; отв. за вып. С. Н. Касанин. – Новополоцк : Полоц. гос. ун-т, 2017. – 282 с.
ISBN 978-985-531-564-4.

В сборнике представлены доклады ученых, специалистов, представителей ггосударственных органов и практических работников в области обеспечения информационной безопасности Союзного государства по широкому спектру научных напрвлений.

Адресуется исследователям, практическим работникам и широкому кругу читателей.

Тексты тезисов докладов, вошедших в настоящий сборник, представлены в авторской редакции.

УДК 004(470+476)(061.3)
ББК 32.81(4Беи+2)

ISBN 978-985-531-564-4

7. Девянин П.Н. Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Академия, 2005. С. 5.

8. Аккорд-АМДЗ // [Электронный ресурс] URL: http://www.accord.ru/amdz.html (дата обращения: 10.04.2017).

9. ПАК Аккорд-Win32(TSE) и ПАК Аккорд-Win64(TSE) [Электронный ресурс] URL: http://www.accord.ru/acwin32.html (дата обращения: 10.04.2017)

10.Мозолина Н. В. Контроль целостности виртуальной инфраструктуры и её конфигураций. // Комплексная защита информации. Материалы XXI Международной конференции. Смоленск 2016. С. 167–170.

11.Мозолина Н. В. Задание эталона при контроле целостности конфигурации виртуальной инфраструктуры // Новые Информационные Технологии и Системы. Сборник научных статей XII Международной научно-технической конференции г. Пенза. 2016 г. С. 219–225.

12.Мозолина Н. В. Выбор способа задания эталона при контроле целостности конфигурации виртуальной инфраструктуры // 59-я Всероссийская научная конференция МФТИ [Электронный ресурс]. URL: http://conf59.mipt.ru/static/prog.html (дата обращения: 16.01.2017).

13.Margheri A. et al. A rigorous framework for specification, analysis and enforcement of access control policies //arXiv preprint arXiv:1612.09339. – 2016.

ОБЗОР ПЕРСПЕКТИВНЫХ РЕШЕНИЙ ПО ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

С.П. ПАНАСЕНКО

ООО Фирма «АНКАД»

Фирма «АНКАД» основана в 1991 г. и известна как одна из ведущих компаний-производителей решений по обеспечению информационной безопасности. Основные направления деятельности компании включают в себя разработку, производство и поставку аппаратных и программных средств криптографической защиты информации, электронной подписи, защиты от несанкционированного доступа и разграничения доступа к компьютерным ресурсам, построения защищенных телекоммуникационных сетей и обеспечения безопасности персональных данных [1].

В качестве примеров продуктового ряда Фирмы можно привести:

семейство аппаратно-программных модулей доверенной загрузки (АПМДЗ) «КРИПТОН-ЗАМОК» (рис. 1);

компоненты защищенной архитектуры «тонкого клиента» «КРИПТОН-ТК»;

абонентские шифраторы серии «КРИПТОН».

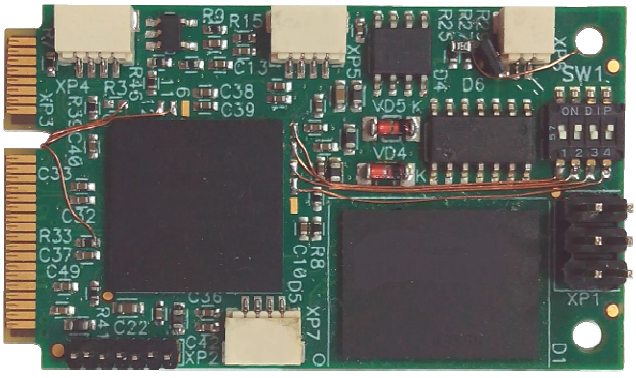

Рис. 1 – АПМДЗ «КРИПТОН-ЗАМОК/mini-E»

Поскольку разработка решений по обеспечению информационной безопасности, отвечающих современным требованиям, является достаточно наукоемким процессом, на Фирме «АНКАД» постоянно проводится научно-исследовательская работа. Данная деятельность охватывает не только направления, свойственные традиционным системам защиты информации, но и ряд смежных направлений.

Это обусловлено тем, что дополнение традиционных методов защиты некоторыми из подсистем, основное назначение которых не относится к области защиты компьютерных данных, может дать в результате значительное усиление качества защиты. А более глубокая интеграция с ними иногда может оказаться крайне полезной и для подсистемы защиты, и для интегрируемой с ней подсистемы.

Рассмотрим некоторые из перспективных систем защиты, в т. ч. полученные путем подобной интеграции.

I. Автоматизированное распространение изменений по криптографически защищенному каналу.

Системы автоматизированного распространения изменений существуют достаточно давно. Наиболее частым примером таких систем можно считать широко используемые системы распространения и установки обновлений операционных систем и установленных в них приложений, драйверов устройств и т. п. Например, в операционных системах компании Microsoft таковыми являются система управления обновлениями Windows Update и более функциональная система развертывания и управления жизненным циклом операционных систем Windows Software Update Services.

Рассмотрим возможности по интеграции системы распространения изменений и системы криптографической защиты информации, включающей в себя следующие основные компоненты:

1. АПМДЗ, содержащий собственную доверенную операционную систему (ОС) и выполняющиеся в данной ОС программные модули:

модуль управления обновлениями операционной системы компьютера из доверенной ОС АПМДЗ;

модуль шифрования сетевого трафика, который опционально может быть заменен аппаратным проходным шифратором.

2. Сервер распространения изменений, содержащий задания на распространение изменений для всех компьютеров распределенной системы.

3. Автоматизированное рабочее место (АРМ) администрирования системы.

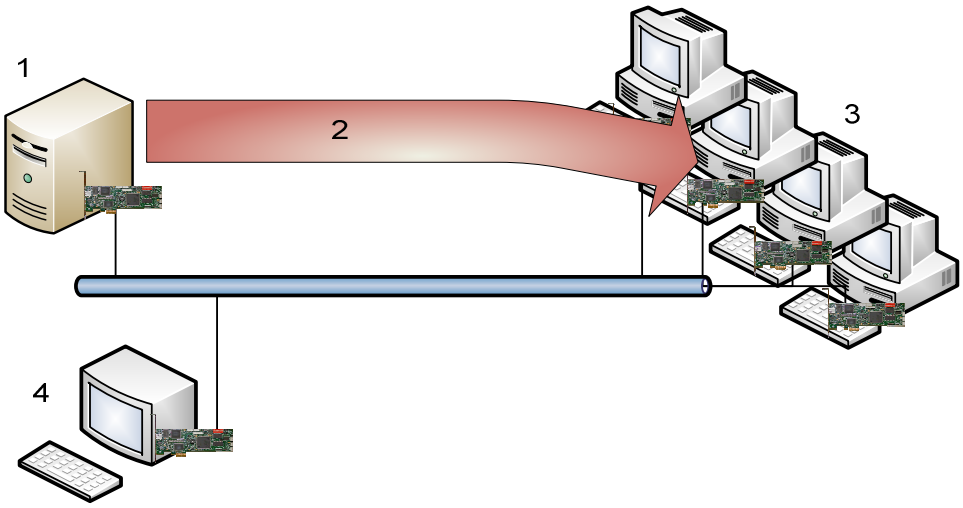

Рис. 2 – Схема системы защищенного распространения изменений

Схема такой системы автоматизированного распространения изменений приведена на рис. 2. Архитектура системы предполагает, что с сервера распространения изменений (1) выполняется распространение обновлений (2) на целевые компьютеры (3) под централизованным управлением АРМ администратора системы (4).

Интеграция системы автоматизированного распространения изменений с традиционными средствами защиты информации (СЗИ) позволяет обеспечить полностью доверенное распространение изменений. Полученная в результате система имеет следующие ключевые особенности:

1. Доверенная среда:

распространение изменений выполняется в операционной среде АПМДЗ;

отсутствуют возможности влияния на процесс доставки и установки изменений со стороны операционной системы и работающих в ней приложений;

гарантированное применение изменений – пользователь не может отказаться от установки назначенных для его компьютера изменений.

2. Криптографическая защита:

шифрование всех команд и данных;

защита целостности пакетов на распространение изменений;

взаимная аутентификация сторон.

3. Универсальность – наличие различных вариантов обновления, в частности, изменения могут включать в себя:

установку операционной системы штатными средствами установки;

принудительный запуск программ установки в целевой операционной системе;

модификацию объектов файловой системы и реестра, включая настройки операционной системы.

Описанная система автоматизированного распространения изменений по криптографически защищенному каналу может быть и далее усовершенствована. В частности, возможна дальнейшая интеграция системы со средствами защиты, например, с системами контроля и разграничения доступа (СКРД), работающими на уровне целевой операционной системы. В этом случае возможна также организация на эталонном компьютере автоматического сбора информации об изменениях средствами СКРД для автоматизированной подготовки заданий на распространение изменений.

В свою очередь, от комбинации с системой распространения изменений может выиграть и система защиты. В частности, контроль целостности операционной системы и программных модулей обычно выполняется АПМДЗ путем подсчета контрольных сумм (в роли которых чаще всего используются хэш-значения) основных модулей и их сравнения с эталонными. При обновлении операционной системы возникает последующая необходимость пересчета новых эталонных контрольных сумм уполномоченным лицом (например, администратором по безопасности). В случае применения описанной системы, поскольку изменения уже утверждены администратором и могут считаться доверенными, эталонные контрольные суммы могут быть пересчитаны автоматически, в процессе формирования изменений.

Таким образом, на базе комплексной системы распространения изменений с глубоко интегрированными средствами защиты можно построить замкнутую программную среду с автоматическим обновлением.

Описанная здесь комплексная система доверенного распространения изменений разработана Фирмой «АНКАД» на основе АПМДЗ «КРИПТОН-ЗАМОК» и существует в виде глубоко проработанного макета, доказывающего верность описанной выше концепции.

II. Использование компонентов систем контроля и управления доступом в классических системах защиты информации.

Рассмотрим следующее перспективное решение, которое объединяет возможности СЗИ, в частности, систем защиты от несанкционированного доступа, и систем контроля и управления физическим доступом персонала и/или посетителей в помещения с ограниченным доступом – СКУД.

СКУД и установленную на компьютере СЗИ можно воспринимать как два барьера, на которых выполняется контроль пользователя перед предоставлением ему доступа в защищаемое помещение и в информационную систему соответственно. Данные барьеры могут быть объединены, причем роль объединяющего элемента может играть ключевой носитель пользователя, единый для данных систем: СКУД и СЗИ. В качестве такого носителя может использоваться, например, криптографическая смарт-карта с дуальным интерфейсом: бесконтактным [2] для СКУД и контактным [3] для СЗИ.

С помощью такой смарт-карты можно организовать взаимодействие между двумя защитными барьерами с целью их согласованного функционирования. Взаимодействие может заключаться, например, в следующем (помимо выполнения основных функций систем защиты):

перед допуском пользователя в защищаемую компьютерную систему СЗИ анализирует, находится ли пользователь внутри данного помещения (в котором установлен компьютер с СЗИ) с точки зрения СКУД. Если нет, то СЗИ не предоставляет пользователю доступ.

и наоборот, при попытке выхода пользователя из помещения СКУД блокирует выход, если пользователь еще не закончил штатным образом работу с компьютером, защищенным СЗИ.

Согласованная работа барьеров защиты способствует повышению качества защиты и в результате позволяет, в частности, противодействовать некоторым сценариям атак на защищаемую систему. Описанная выше комбинация является одним из возможных путей усиления защиты компьютерной информации и защиты от несанкционированного доступа в контролируемые зоны за счет совместного использования СКУД и СЗИ.

Используемые в СКУД технологии радиочастотной идентификации (RFID – Radio-frequency identification) могут использоваться для решения и других задач по обеспечению информационной безопасности, например [4]:

1. Контроль местонахождения каких-либо материальных объектов, в частности, флэш-носителей. Контролируемые носители могут быть оснащены RFID-метками. Поскольку RFID-метки могут быть достаточно легко экранированы, контроль местонахождения носителей можно организовать по следующему принципу: в конкретный момент времени (за исключением заранее заданных таймаутов) носитель должен находиться в зоне действия одного из предопределенных RFID-ридеров, то есть, например, на рабочем месте пользователя или на складе с ответственным хранением.

2. Контроль попыток вскрытия корпусов компьютеров, который может быть осуществлен с помощью RFID-метки, находящейся внутри корпуса и экранируемой им в закрытом виде.

Комплексная схема использования технологий RFID в системах защиты компьютерной информации приведена на рис. 3.

Пример комплексной системы защиты, схема которой приведена на рис. 3, предполагает, что существует защищаемое рабочее помещение (1), склад (2) и выделенное помещение для администрирования системы (3). Описанные выше подсистемы

защиты могут быть объединены и управляться с единого сервера управления (4), который, в свою очередь, администрируется с помощью выделенного АРМ администратора системы (5).

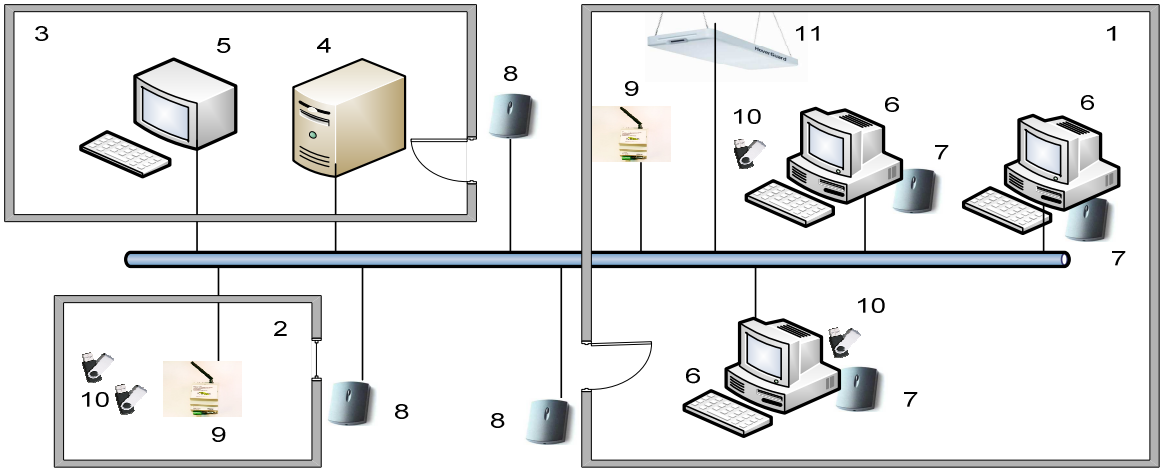

Рис. 3 – Схема комплексной системы защиты на основе RFID

При этом компьютеры (6), находящиеся в рабочем помещении, оснащаются считывателями (7) обеспечивающими интеграцию СКУД и СЗИ по описанному выше принципу. Все помещения оснащаются считывателями (8) системы контроля доступа, рабочее помещение и склад – считывателями (9), обеспечивающими контроль носителей (10). Рабочее помещение, кроме того, оснащается считывателем (11), отслеживающим попытки несанкционированного вскрытия корпусов компьютеров.

Отметим, что централизованное администрирование комплексной системы с единого рабочего места (АРМ администратора) дает также широкие возможности для мониторинга состояния системы и ее компонентов и отслеживания в режиме реального времени событий, относящихся к компонентам системы и защищаемым объектам.

Фирмой «АНКАД» разработан макет комплексной системы, реализующий описанные выше возможности в соответствии с приведенной схемой. Макет снабжен полнофункциональной подсистемой мониторинга, отображающей события, относящиеся к субъектам и объектам системы на интерактивной карте контролируемой территории. Макет основан, в частности, на применении АПМДЗ «КРИПТОН-ЗАМОК» и системы разграничения доступа «КРИПТОН-ЩИТ» в качестве СЗИ на стороне компьютера.

III. Защищенная система видеонаблюдения.

Распределенные системы видеонаблюдения обладают рядом проблем в части защиты информации:

видеотрафик, передаваемый в открытом виде, может быть перехвачен, что особенно актуально для видеокамер с беспроводным интерфейсом;

аналогичным образом может быть навязан ложный видеотрафик;

в ряде случаев не решаются вопросы защиты видеоданных в серверных компонентах систем видеонаблюдения – при обработке видеоинформации и при ее хранении.

Таким образом, необходимо оснащение систем видеонаблюдения средствами обеспечения целостности и конфиденциальности видеоданных при их передаче и средствами защиты данных от несанкционированного доступа и модификации в дальнейшем. Получившаяся в результате интеграции с СЗИ защищенная система видеонаблюдения представлена на рис. 4.

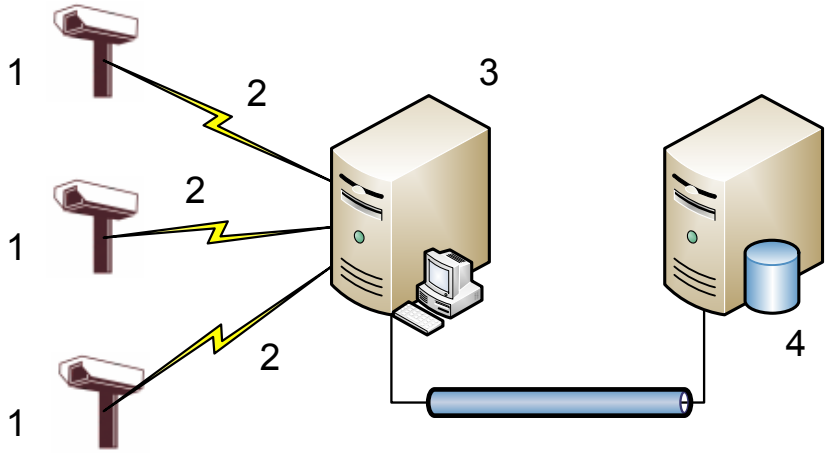

Рис. 4 – Схема защищенной системы видеонаблюдения

В данной системе используются беспроводные IP-видеокамеры (1), которые по защищенным каналам (2) соединяются с сервером обработки и мониторинга (3), который, в свою очередь, соединен по локальной сети с сервером баз данных (4), хранящим полученную видеоинформацию.

Защита видеотрафика организована в виде VPN-туннелей, построенных на основе отечественных криптографических стандартов, в частности, [5]. Серверная часть системы защищается от несанкционированного доступа с помощью АПМДЗ «КРИПТОН-ЗАМОК» и системы разграничения доступа «КРИПТОН-ЩИТ». Таким образом, достигаются следующие ключевые особенности системы:

обеспечение конфиденциальности и контроля целостности передаваемого видеопотока;

обеспечение защиты доступа к серверам и обрабатываемым и/или хранящимся на них данным.

IV. Средства защиты информации для беспилотных летательных аппаратов.

В последние годы всеобщий интерес к беспилотным летательным аппаратам (БПЛА) заставляет разработчиков обращать все большее внимание на развитие технологий БПЛА. В частности, в посвященном развитию технологий и инфраструктуры БПЛА плане мероприятий «Аэронет» [6] предполагается, что развитие данных технологий и инфраструктуры их использования приведет к активному применению БПЛА для выполнения работ и услуг в рамках удовлетворения различных, постоянно возрастающих, потребностей экономики. По приведенным в дорожной карте «Аэронет» оценкам над территорией Российской Федерации к 2035 г. постоянно могут находиться порядка 100 000 БПЛА.

Подобный масштаб использования подразумевает крайне интенсивный обмен информацией между БПЛА и наземными службами, а также между собой в рамках выполнения единых задач с помощью самоорганизующихся групп беспилотных летательных аппаратов.

Для обеспечения безопасности применения БПЛА, включая обеспечение невозможности несанкционированного перехвата управления БПЛА и их применения в различных противоправных целях (от вмешательства в частную жизнь граждан до проведения террористических актов с использованием беспилотных летательных аппаратов), необходимо предъявление жестких требований к защите каналов информационного обмена БПЛА и разработка систем в соответствии с предъявленными требованиями.

На рис. 5 приведена схема взаимодействия БПЛА.

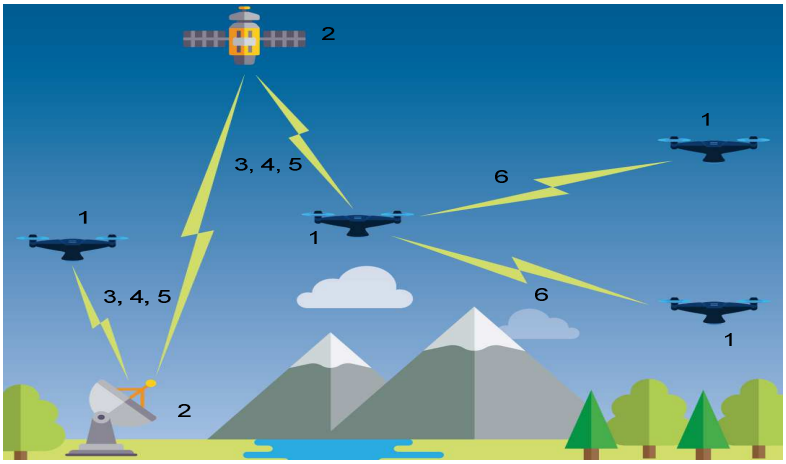

Рис. 5 – Схема взаимодействия БПЛА

Видно, что необходимо обеспечение защиты (включая аутентификацию сторон, контроль целостности и, в ряде случаев, обеспечение конфиденциальности данных) следующих составляющих информационного обмена между БПЛА (1) и управляющей инфраструктурой (2):

команд управления БПЛА со стороны инфраструктуры (3);

данных мониторинга состояния БПЛА и телеметрической информации (4);

полезной информации, передаваемой со стороны БПЛА (5);

данных, передаваемых в рамках взаимодействия БПЛА между собой (6).

В настоящее время Фирмой «АНКАД» ведется разработка системы защиты, обеспечивающей безопасный информационный обмен между БПЛА и наземной инфраструктурой для ряда моделей БПЛА гражданского назначения.

В качестве заключения сформулируем основной вывод доклада: оснащение традиционных систем защиты информации дополнительными подсистемами из смежных областей информационных технологий в ряде случаев может не только усилить защиту, но и вывести ее на качественно новый уровень, что было проиллюстрировано приведенными выше примерами.

Список литературы

1. Доверенные средства защиты информации. // Материалы сайта ООО Фирма «АНКАД» – http://www.ancud.ru.

2. ГОСТ Р ИСО/МЭК 14443-1 – 2004. Карты идентификационные. Карты на интегральных схемах бесконтактные. Карты с индуктивной связью близкого действия. Часть 1. Физические характеристики. – М.: Госстандарт России.

3. ГОСТ Р ИСО/МЭК 7816-1 – 2010. Карты идентификационные. Карты на интегральных схемах с контактами. Часть 1. Физические характеристики. – М.: Стандартинформ, 2011.

4. Панасенко С. П., Сырчин В. К. Перспективные комбинированные решения по защите информации. // Сборник трудов XXV Всероссийской конференции «Информатизация и информационная безопасность правоохранительных органов». – М.: Академия управления МВД России, 2016 – с. 295-299.

5. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования. – М.: Государственный комитет СССР по стандартам, 1989.

6. План мероприятий («дорожная карта») «Аэронет» Национальной технологической инициативы. // http://www.rvc.ru.