УДК 004.415.2

РАЗРАБОТКА СИСТЕМЫ ОБЕСПЕЧЕНИЯ КОНТРОЛЯ ЛОКАЛЬНЫХ СРЕДСТВ ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ В ОРГАНИЗАЦИЯХ И ВОИНСКИХ ЧАСТЯХ ВООРУЖЕННЫХ СИЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

© 2023 А. А. Бойченко

Краснодарское высшее военное училище имени генерала армии С. М. Штеменко (Краснодар, Россия)

Для организации задач сбора, предварительного контроля, систематизации и нормализации данных контроля состояния безопасности информации на локальных средствах вычислительной техники организаций и воинских частей Вооруженных сил Российской Федерации предлагается автоматизированная система сбора информации о состоянии средств защиты информации, средств антивирусной защиты и операционных систем в целом. Предлагаемая система является двухкомпонентной, состоящей из локальной и сетевой подсистемы. В статье рассматривается функционал и общая структура локальной подсистемы.

Ключевые слова: угрозы безопасности информации, локальные средства вычислительной техники, контроль состояния безопасности информации, программные средства, автоматизированные системы военного назначения.

С начала XXI века роль вычислительной техники в повседневной жизни человека выросла в разы. С сейчас довольно трудно представить даже обыденные вещи без средств автоматизации и вычислительных модулей. Офис, бухгалтерия, передача как рабочих, так и официальных документов, обработка массивов текстовой, графической, видео и аудио информации – вот далеко не полный перечень сфер деятельности, в которых средства вычислительной техники плотно вошли в жизнь общества.

Вооруженные Силы не стали исключением. Безусловно со своей спецификой, но тем не менее плотно вычислительная техника вошла в жизнь Вооруженных Сил Российской Федерации.

Для примера: по статистике, полученной средствами контроля и мониторинга Министерства обороны Российской Федерации, количество хостов закрытого сегмента сети передачи данных с 2011 года по 2018 год увеличилось с 450-500 до более 9000, то есть примерно в 20 раз. В системе электронного документооборота на момент 2011 года эксплуатировалось 250 автоматизированных рабочих мест. В 2019 году их было уже более 4500. Программное изделие ресурсного обеспечения «Алушта» было введено в эксплуатацию в 2012 году. За 10 лет эксплуатации количество автоматизированных рабочих мест изделия увеличилось до 5500 (только введенных в домен Active Directory). При этом объём базы данных в настоящее время исчисляется десятками террабайт.

Такие объемы обрабатываемых данных являются крупной и достаточно соблазнительной целью для целенаправленных атак как в интересах иностранных разведок, так и частных и преступных организаций на территории Российской Федерации. Так, ежедневно на официальный сайт Минобороны России осуществляется около 1000 компьютерных атак. А если читать сканирование портов хоста официального сайта, указанная цифра вырастает в десятки раз. При этом нельзя сбрасывать со счетов проблему внутреннего нарушителя.

В таких условиях существенно возрастает проблема контроля состояния безопасности как автоматизированных систем военного назначения, так и отдельных средств вычислительной техники воинских частей. Не зря в настоящее время в состав каждого изделия, закупаемого Минобороны России, обрабатывающего информацию ограниченного распространения, включаются автома-

Бойченко Александр Александрович – Краснодарское высшее военное училище имени генерала армии С. М. Штеменко, слушатель магистратуры, e-mail: yesenin@bk.ru.

тизированные рабочие места администратора безопасности информации, равно как и средства контроля безопасности информации.

Проблема контроля состояния безопасности информации заключается в разрозненности различных сетей, изделий, наличии локальных средств вычислительной техники, что требует наличия большого количества высококвалифицированных специалистов в области безопасности информации. И если в сетях передачи данных данная проблема решается централизацией сбора и анализа событий, то с локальными автоматизированными рабочими местами и небольшими сетями, не подключенными к сетям передачи данных задачу контроля безопасности информации необходимо решать иначе.

При этом доля локальных средств вычислительной техники и локальных сетей, не имеющих выходов за пределы контролируемой зоны в большей части войсковых частей Вооруженных Сил Российской Федерации может достигать 90-95 %. Периодический контроль выездными проверками вышестоящих штабов ввиду редкой периодичности не может гарантировать оперативное получение, обработку, анализ, обобщение и передачу достоверной информации о состоянии безопасности информации на локальных средствах вычислительной техники войсковой части.

Таким образом необходимо предложить актуальный метод сбора информации о состоянии локальных автоматизированных рабочих мест.

Данный метод должен соответствовать ряду критериев:

- данные должны быть актуальными на всех этапах сбора, передачи, агрегации и анализа. В идеальном случае – указанные процессы должны проходить в режиме реального времени;
- процессы сбора, агрегации и анализа должны быть максимально автоматизированы;
- достоверность и неизменность полученной информации должны обеспечиваться на всех этапах жизненного цикла.

В данной работе предлагается для анализа состояния безопасности информации использовать систему контроля, состоящую из двух основных элементов (компонентов): сетевого и локального (рис. 1).

Рисунок 1. Структурная схема системы

Локальный компонент предназначен для непосредственного сбора данных с локального автоматизированного рабочего места, первичного анализа и формирования массива данных в формате JSON.

Собираемые им данные основываются в первую очередь на основных угрозах безопасности информации [1].

В ходе анализа банка данных угроз Федеральной службы по техническому и экспортному контролю (ФСТЭК) России было выявлено шестьдесят три угрозы различных типов, однако все они так или иначе сводятся к основным тринадцати угрозам безопасности информации (УБИ):

УБИ.067: Угроза неправомерного ознакомления с защищаемой информацией;

УБИ.071: Угроза несанкционированного восстановления удалённой защищаемой информации;

УБИ.088: Угроза несанкционированного копирования защищаемой информации;

УБИ.091: Угроза несанкционированного удаления защищаемой информации;

УБИ.115: Угроза перехвата вводимой и выводимой на периферийные устройства информации;

УБИ.124: Угроза подделки записей журнала регистрации событий;

УБИ.143: Угроза программного выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.156: Угроза утраты носителей информации;

УБИ.157: Угроза физического выведения из строя средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.160: Угроза хищения средств хранения, обработки и (или) ввода/вывода/передачи информации;

УБИ.179: Угроза несанкционированной модификации защищаемой информации;

УБИ.203: Угроза утечки информации с неподключенных к сети Интернет компьютеров;

УБИ.205: Угроза нарушения работы компьютера и блокирования доступа к его данным из-за некорректной работы установленных на нем средств защиты.

Анализ проводился в соответствии с Методикой оценки угроз безопасности информации ФСТЭК России [2].

Учитывая, что согласно национальному стандарту Российской Федерации ГОСТ Р 50922-2006 [3] «безопасность информации [данных]: Состояние защищенности информации [данных], при котором обеспечены ее [их] конфиденциальность, доступность и целостность», угрозы и направления контроля (собираемые данные) будут выглядеть в соответствии с таблицей:

Свойство информации	**Угрозы**	**Направления контроля**
Конфиденциальность	УБИ.067	Контроль функционирования системы разграничения доступа, средств защиты информации и антивирусной защиты. Выявление фактов подключения неразрешенных носителей информации.
	УБИ.071	
	УБИ.088	
	УБИ.115	
	УБИ.203	Мониторинг подключения устройств, реализующих технологии беспроводного доступа. Выявление фактов выхода пользователей в сети общего пользования.
Целостность и доступность	УБИ.091	Контроль функционирования системы разграничения доступа, средств защиты информации и антивирусной защиты.
	УБИ.143	
	УБИ.179	
	УБИ.205	
Все свойства	УБИ.156	Контроль аппаратного состава средств хранения информации и средства вычислительной техники в целом.
	УБИ.157	
	УБИ.160	
Скрытие фактов воздействия	УБИ.124	Контроль функционирования системы разграничения доступа, средств защиты информации и антивирусной защиты

Дополнительно для установления персональной ответственности за события безопасности требуется идентификация пользователей, ответственных за работу на средстве вычислительной техники и ответственных за защиту информации, которые имеют разный уровень доступа и, соответственно, разный уровень возможного влияния на состояние средства вычислительной техники, включая как возможность искажения данных, представляемых сборщиком, так и возможность скрытия средства вычислительной техники в целом (в случае если данные со средства умышленно не будут собираться и проверки проводиться не будут).

Таким образом, локальный компонент системы контроля локальных средств вычислительной техники состоит из трех подсистем: сборщика, преобразователя и метки.

Сборщик является основным элементом локального компонента системы. Именно он осуществляет сбор информации о средстве вычислительной техники, который проводится как в интерактивном, так и в автоматическом режиме. Пример отчёта приведён на рисунке 2.

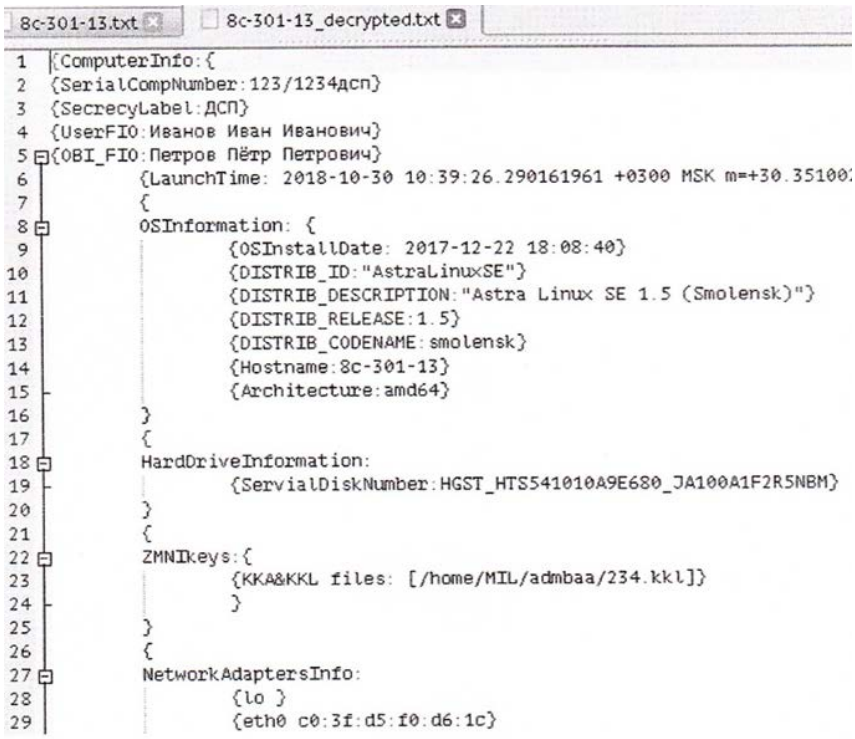

Рисунок 2. Пример отчета сборщика (элемент)

Учитывая тот факт, что локальные автоматизированные рабочие места могут функционировать как на базе Linux, так и на базе Windows и быть как 32-х, так и 64-х разрядными, должно быть несколько версий программного обеспечения (ПО) для разных систем, но с единым функционалом, перечнем собираемых данных и выходным форматом.

Собираются следующие данные:

1. В интерактивном режиме:

1.1. Воинское звание и ФИО пользователя, закрепленного за рабочим местом;

1.2. Воинское звание и ФИО ответственного за защиту информации;

1.3. Учётный номер жесткого магнитного диска;

1.4. Категорию конфиденциальности (гриф секретности) обрабатываемой информации.

2. В автоматическом режиме:

2.1. Имя автоматизированного рабочего места;

2.2. Имя текущего пользователя;

2.3. Имена всех пользователей автоматизированного рабочего места;

2.4. Серийный номер жесткого магнитного диска;

2.5. Перечень установленного программного обеспечения;

2.6. Статус установки критических обновлений;

2.7. Дата установки операционной системы;

2.8. Статус установки и основные и настройки средств защиты информации;

2.9. Статус установки, основные настройки и дату обновления баз вирусных сигнатур средства антивирусной защиты;

2.10. Перечень и даты подключений USB-устройств;

2.11. История браузера каждого пользователя

2.12. При наличии остаточных файлов предыдущей операционной системы (Windows.old) поиск указанных данных проводится и в файлах предыдущей версии ОС.

С целью защиты полученного отчета от модификации предлагается использовать алгоритмы асимметричного преобразования, включенные в отдельный элемент локального компонента – **преобразователя**.

Данный элемент преобразует отчёт по алгоритмам шифрования с открытым ключом, что позволит избежать модификации отчёта должностными лицами, ответственными за организацию защиты информации на местах.

И, наконец, последним элементом локального компонента является специальная **метка**, включающая в себя информацию о дате и времени запуска проверки, серийном номере жесткого магнитного диска, имени автоматизированного рабочего места, дате установки операционной системы и преобразованная тем же методом, что и отчёт. Метка остаётся на локальном средстве вычислительной техники и проверяется при проведении периодической проверки выездной комиссией.

Полученный отчёт в преобразованном виде загружается в закрытый сегмент сети передачи данных Минобороны на сервер, обеспечивающий функционирование сетевого компонента. Сервер представляет собой web-сервер с базой данных, который проводит обратное преобразование загружаемых отчетов, считывание данных отчетов, сформированных в формате JSON и распределение информации по полям таблиц базы данных.

Таким образом, применение системы контроля состояния защиты информации указанного типа позволит осуществлять проверки локальных средств вычислительной техники без проведения выездных проверок, тем самым увеличив периодичность мероприятий контроля защищённости информации без увеличения расходов на работу выездных комиссий.

При этом, использование указанной в статье системы не исключает проведения проверок состояния защиты информации выездными комиссиями. Более того, данные методы контроля лишь дополняют друг друга, так как сам факт применения системы контроля локальных средств вычислительной техники в воинской части возможно установить только в ходе проверки выездной комиссией

СПИСОК ИСТОЧНИКОВ

1. Банк данных угроз безопасности информации Федеральной службы по техническому и экспортному контролю России. https://bdu.fstec.ru/threat.

2. Методический документ. Методика оценки угроз безопасности информации. Утвержден ФСТЭК России 5 февраля 2021 г.

3. Национальный стандарт Российской Федерации ГОСТ Р 50922 2006. Введён в действие 1 февраля 2008 г.

DEVELOPMENT LOCAL COMPUTER FACILITIES CONROL SYSTEM IN ORGANIZATIONS AND MILITARY UNITS OF RUSSIAN FEDERATION ARMED FORCES

© 2023 A. A. Boychenko

Krasnodar Higher Military School named after Army General S. M. Shtemenko (Krasnodar, Russia)

To organize the tasks of collecting, preliminary control, systematization and normalization of information security control data on local computer facilities of organizations and military units of the Armed Forces of the Russian Federation, an automated a system for collecting information about the status of information protection tools, anti-virus protection tools and operating systems in general is proposed. The proposed system is a two-component one, consisting of a local and a network subsystem. The article discusses the functionality and general structure of the local subsystem.

Keywords: information security threats, local computer facilities, information security state control, software tools, military automated systems.