Литература 1. J. Allen, A. Christle, W. Fithen et al. State of the Practice of Intrusion Detection Technologies.–Tehnical Report CMU/SEI-99-TR-028.–2000.–220 p. 2. J. Frank. Artificial Intelligence and Intrusion Detection: Current and Future Directions// Proceedings of 17th National Computer Security Conference.–1994. 3. О. Новіков, С. Кащенко. Розпізнавання сервісів TCP/IP за допомогою нейронних мереж// Збірник праць конференції "Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні"(Київ).–2000.–с. 222-226. 4. S. Axelsson. The Base-Rate Fallacy and its Implications for the Difficulty of Intrusion Detection// Proceedings of the 6th ACM Conference on Computer and Communications Security (Kent Ridge Digital Labs, Singapore).– 1999. 5. S. Kumar, E. Spafford. A Pattern Matching Model for Misuse Intrusion Detection// Proceedings of 17th National Computer Security Conference.–1994.–p. 11-21.

УДК 681.324

АНАЛИЗ ОБРАЗУЮЩИХ СРЕД ТИПОВЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

Игорь Яковив, Александр Черноног*

*Национальная академия СБ Украины, *Киевский военный институт управления и связи*

Анотація: **З загальної множини компьютерних систем виділена значна група, основною визначаючою характеристикою якої є обробка тільки файлів документів. Для цієї групи здійснений аналіз утворюючих середовищ компьютерних систем. Запропоновані підходи по утворенню комплексної системи захисту інформації для типових компьютерних систем.**

Summary: **From a common diversity of computer systems the significant group is selected, the main distinctive performance of which is the handling of document files only. For given group the analysis of forming mediums of computer systems is fulfilled. The approaches on the creation of the complex protection system of the information for standard computer systems are offered.**

Ключові слова: **Інформація, інформаційна безпека, комплексна система захисту інформації.**

I Введение

Из общего многообразия компьютерных систем (КС), для которых возникает необходимость построения комплексной системы защиты информации (КСЗИ), можно выделить довольно значительную группу, отличительными характеристиками которой являются:

- обработка только файлов документов;
- использование широко распространенных сетевых операционных систем (например, Windows NT, Windows 2000, Novell Net Ware, Unix и др.);
- применение для формирования документов хорошо зарекомендовавших себя прикладных программ (например, Microsof Word, Excel, Access, Corel Word Perfect и др.);
- сравнительно низкий уровень квалификации пользователей (достатоточный только для работы с перечисленными прикладными программами).

II Цели анализа образующих сред типовых компьютерных систем

Поскольку до сих пор только бумажные документы обладают юридической значимостью, то такие КС (далее – типовые КС) нашли широкое распространение в государственных учреждениях, общественных организациях и предприятиях различных форм собственности. В ближайшие годы ситуация, видимо, существенно не изменится.

Необходимость проведения анализа образующих сред типовых КС, обусловлена дальнейшим решением следующих задач:

1) разработать в рамках существующей нормативной базы единые подходы по защите информации, априорно учитывающие особенности типовых КС;
2) определить условия применения в КСЗИ штатных услуг сетевых операционных систем и в дальнейшем разработать соответствующие универсальные методики;
3) конкретизировать и сделать более доступными для практического применения в типовых КС ряд положений нормативных документов системы технической защиты информации;
4) показать возможности снижения затрат на некоторых стадиях жизненного цикла КСЗИ;
5) разработать методики сравнения эффективности КСЗИ различной структуры;
6) разработать структуру типовой подсистемы управления КСЗИ и ее математическую модель.

III Результаты анализа

В ходе проведения анализа образующих сред типовых компьютерных систем получены следующие результаты.

1. Информационная среда

1.1 Файлы документов по характеру использования подразделяются на:
- внешние (ФДВнш);
- внутренние (ФДВнт).

1.2 Как правило, ФДВнш формируются на основе одного или нескольких ФДВнт.

1.3 На основании ФДВнш формируются официальные бумажные исходящие документы, целостность и аутентичность которых обеспечивается традиционными методами (подпись, печать).

1.4 ФДВнт формируются как промежуточный рабочий материал.

1.5 На печать, как правило, выводятся только ФДВнш.

1.6 Степень конфиденциальности определяется владельцем файла (т.е. пользователем, который его создал).

1.7 Существуют следующие виды файлов документов:
- текстовые (письма, отчеты и т. д.);
- табличные;
- диаграммы;
- схемы;
- комбинированные.

2. Технологическая среда

2.1 Автоматизированная система является организационно–технической системой, реализующей информационную технологию и объединяющая вычислительную сеть (ВС), физическую среду, персонал и обрабатываемую информацию [1]. В соответствии с [2] автоматизированные системы по совокупности характеристик (конфигурации аппаратных средств ВС и их физическому размещению, количеству пользователей и категорий пользователей) подразделяются на три класса, требования к функциональному составу комплекса средств защиты (КСЗ) которых существенно отличаются. Наибольший интерес в контексте поставленных задач представляют следующие автоматизированные системы:
- одно-машинный многопользовательский комплекс, на котором поочередно обрабатывается информация одной или нескольких категорий

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

конфиденциальности. Данный класс АС не присутствует в классификации нормативных документов;

- многомашинный многопользовательский комплекс, на котором одновременно обрабатывается информация одной или нескольких категорий конфиденциальности (например, локальная вычислительная сеть (ЛВС)).

2.2 Так как для обработки файлов документов применяется ограниченный, самодостаточный набор прикладных программ, то фактически исключается или становится крайне редкой необходимость экспорта в процессе эксплуатации дополнительных программ.

2.3 Широко распространенные сетевые операционные системы, как правило, обладают встроенными инструментами для обеспечения услуг:

- идентификации и аутентификации пользователей;
- административной конфиденциальности;
- доверительной конфиденциальности;
- распознавания, фиксирования и анализа действий и событий, связанных с политикой защиты от несанкционированного доступа.

3. Рабочая среда

3.1 Типовые КС, нуждающиеся в защите информации, как правило, располагаются или могут быть расположены в отдельном помещении (нескольких отдельных помещениях), для которого организационными и физическими мерами может быть реализован режим контролируемой зоны (т. е. исключается несанкционированное появление посторонних лиц).

3.2 Для локализованного на территории контролируемой зоны аппаратного комплекса по существующим детально разработанным методикам сравнительно просто можно обеспечить защиту информации от утечки по техническим каналам [3, 4].

4. Пользовательская среда

4.1 Как правило, подготовку документов с ограниченным доступом осуществляет только часть сотрудников организации (пользователи типовой КС).

4.2 Каждый документ авторизован, т. е. вероятность нарушения его конфиденциальности пользователем-владельцем значительно ниже угрозы, которую составляют остальные пользователи КС.

4.3 Пользователям КС достаточно предоставить только возможности запуска набора программ, реализующих заранее предусмотренные функции по обработке файлов документов.

4.4 Как правило уровень умений пользователей не превышает уровень, необходимый для формирования документов в типовой КС. Пользователей с иными способностями в ходе эксплуатации можно определить с помощью анализа действий и событий штатными средствами сетевой операционной системы.

Полученные результаты позволили разработать следующие подходы по созданию КСЗИ для типовых КС.

1. Локализовать аппаратный комплекс типовой КС границами контролируемой зоны, в пределах которой организационными, физическими и инженерно-техническими мерами выполнить следующее:
   - исключить несанкционированный доступ не пользователей к аппаратно-программным средствам;
   - обеспечить защиту информации от утечки по техническим каналам.

ISBN 966-622-022-9

2. Для устранения угроз применения программных закладок и внешнего несанкционированного воздействия не пользователями исключить физические условия реализации удаленного доступа.
3. Для устранения угроз воздействия компьютерных вирусов и применения несанкционированных программных средств организовать экспорт/импорт только через шлюз администратора.
4. Комплексным применением встроенных услуг операционных систем и организационных мер реализовать политику административной конфиденциальности, основными положениями которой могут быть следующие:

а) каждый пользователь для работы со своими файлами использует только свой авторизованный каталог;

б) в журнале учета работы отображаются основные этапы технологии подготовки распечатанного документа;

в) все значимые действия в электронных журналах соотносятся с журналами учета работы (ЖУР);

г) критичные действия пользователя оцениваются на предмет мотивации.

Указанные рекомендуемые подходы по созданию КСЗИ для типовых КС могут быть реализованы с помощью политики безопасности, которая является совокупностью правил, ограничений, рекомендаций, инструкций и т. д., регламентирующих порядок обработки информации [1].

Ниже представлен один из вариантов политики безопасности для типовой КС. Этот вариант разрабатывался для следующих условий функционирования:

1) используются штатные для сетевой операционной системы механизмы защиты от несанкционированного доступа к папкам и файлам;

2) выполняется однозначная идентификация и аутентификация пользователей;

3) штатными средствами администратором обеспечивается аудит действий пользователей;

4) информация в КС хранится только на жестких дисках. Дисководы гибких носителей информации заблокированы.

В рамках указанных условий политика безопасности может быть реализована с помощью следующего набора правил и ограничений.

1. Работа пользователя на персональном компьютере (ПК) начинается с регистрации в журнале учета работы (ЖУР), который выполнен как бумажный носитель. В журнале регистрируется фамилия и время начала работы.
2. Пользователь интерактивно регистрируется на ПК путем ввода своего идентификатора и проходит аутентификацию при вводе своего пароля.
3. Каждый пользователь для работы имеет свою папку, которая хранится на жестком диске ПК пользователя или же на выделенном сервере. Доступ к папкам других пользователей запрещен. Пользователь выполняет действия с файлами документов только в пределах отведенной ему папки.
4. При создании файла документа пользователь регистрирует в ЖУРе время его создания и объем.
5. Для печати документов используется выделенный сервер, на котором обеспечена возможность аудита печати. Распечатка документов пользователем производится на учтенных листах. Свои действия по печати пользователь также фиксирует в ЖУРе.
6. При необходимости установку дополнительных приложений и программ производит только администратор или уполномоченное им лицо.

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.

7. Сохранение при необходимости файлов документов пользователя на учтенную гибкую дискету производит администратор. Импорт данных с носителей информации в интересах пользователя производится также администратором после предварительной проверки этих носителей.
8. Штатными средствами сетевых операционных систем организуется контроль за всеми действиями пользователей путем отображения их в электронном журнале аудита. Пользователю доступ к журналу аудита блокируется.
9. Попытки пользователя нарушить правила разграничения доступа (обращения к папкам и файлам, к которым ему доступ запрещен) фиксируются в журнале аудита.
10. Администратор периодически анализирует журнал аудита и сравнивает приведенные в нем данные с данными машинного журнала. На основании сравнения администратор регулярно оценивает действия пользователей.

IV Выводы

Проведенный анализ образующих сред широко распространенных автоматизированных систем для обработки файлов документов, разработанные рекомендации по созданию комплексной системы защиты информации для таких систем и приведенный вариант политики безопасности позволяют:

- выработать единый комплексный подход по защите информации, априорно учитывающий особенности обработки файлов документов с помощью распространенного операционного и прикладного программного обеспечения;
- определить возможности и порядок применения в КСЗИ штатных услуг сетевых операционных систем по защите и аудиту;
- конкретизировать и сделать более доступными для практического применения в типовых КС ряд положений нормативных документов системы технической защиты информации;
- разработать структуру типовой подсистемы управления КСЗИ, ее математическую модель и методики сравнения эффективности КСЗИ различной структуры;
- удешевить создание и эксплуатацию системы защиты информации для рассматриваемых КС.

Литература: 1. Нормативный документ системы технической защиты «Общие положения по защите информации в компьютерных системах от несанкционированного доступа» от 28. 04. 1999 г. // НД ТЗИ 1.1 – 002 – 99. 2. Нормативный документ системы технической защиты «Классификация автоматизированных систем и стандартные функциональные профили защищенности обрабатываемой информации от несанкционированного доступа» от 28. 04. 1999 г. // НД ТЗИ 2.5 – 005 – 99. 3. Нормативный документ системы технической защиты информации «Тимчасові рекомендації з технічного захисту інформації від витоку каналами побічних електромагнітних випромінювань і наводок» от 09. 06. 95 г. // ТР ТЗІ-ПЕМВН-95. 4. Нормативно-технический документ Гостехкомиссии СССР «Нормы эффективности защиты АСУ и ЭВМ от утечки информации за счет побочных электромагнитных излучений и наводок» от 26 . 09. 77 г. // Документ действительный в Украине на основании постановления Верховної Ради України № 1545-12 от 12. 09. 91 р. "Про порядок тимчасової дії на території України окремих актів законодавства Союзу РСР".

УДК 519.25

УРОВНЕВЫЙ АНАЛИЗ ИНФОРМАЦИИ В СИСТЕМЕ ОЦЕНКИ ЕЕ ЦЕЛОСТНОСТИ И ДОСТОВЕРНОСТИ

Александр Манухин, Татьяна Ковальчук*, Вадим Томчук
*Военный институт НТУУ "КПИ",*НИЦ "ТЕЗИС" НТУУ "КПИ"*

Анотація: **Розглядається проблема аналізу цілісності та достовірності інформації, що транслюється, на бінарному та логічному рівнях в контексті комплексних систем її захисту.**

Summary: **Considering problem of analysis safe and authentic information, what transmitting in the binary and logically levels, in a context complex protection systems of the information.**

Ключові слова: **Системи цілісності та достовірності інформації, коректуючі коди, електронний цифровий підпис, інформаційний конфлікт.**

Введение

После поля и вещества информация представляет собой третий вид существования материи. Жизненный цикл ее трансформаций предполагает, что информация добывается, обрабатывается, хранится, охраняется, используется, транслируется, расхищается и уничтожается. В зависимости от условий она может выступать сырьем, продуктом, товаром и, как следствие, превращаться в деньги. Следовательно, информация, имеющая определенные стоимость (важность), цену и значение может представлять интерес для определенных потребителей – юридических и физических лиц во всех сферах общественной деятельности (субъекты исследования). В свою очередь это означает, что если объект не выдается добровольно и безвозмездно, если он не продается по приемлемой цене, то всегда будет иметь место стремление к его хищению. Таким образом, применение информационных технологий, требующих в определенных случаях сохранения конфиденциальности содержания объекта, обуславливает внедрение комплексной системы защиты информации (КСЗИ), что включает в себя способы контроля целостности и достоверности информационных потоков (СЦДИ).

Следует различать два уровня существования объекта – структурный и логический. Первый служит его материальной основой в виде лексико-грамматических языковых структур, второй – носитель интерпретирующей составляющей события у субъекта. Назовем первый уровень низким, второй – высоким и рассмотрим механизмы естественного (или искусственного) воздействия на объект с точки зрения его целостности и достоверности.

II Низкий уровень трансляции объекта

Материальной основой структурного уровня объекта M является его бинарное представление 2^n-возможными кодовыми комбинациями, $M \Rightarrow V$. Ошибки трансляции для данного уровня возникают из-за врожденных или приобретенных дефектов носителя объекта, качества каналов связи, неисправностей электронного и электромеханического оборудования. Наиболее реальный способ обеспечения достоверности объекта – применение корректирующих кодов, служащих для обнаружения и коррекции ошибок.

В настоящее время разработано сравнительно большое количество корректирующих кодов, основанных на различных разделах математики: теории групп, коммутативной алгебры, теории конечных полей. Возможности обнаружения и коррекции ошибок повышаются при увеличении избыточности кода, однако, одновременно усложняются алгоритмы кодирования и декодирования. Для обеспечения высокой достоверности трансляции объекта при относительно простой технике кодирования и декодирования

ISBN 966-622-022-9
Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні, вип. 2, 2001 р.