УДК 681.3

КОМПЛЕКСНЫЙ ПОДХОД К ОБЕСПЕЧЕНИЮ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

© 2022 Я. Е. Львович, Ю. П. Преображенский

Воронежский государственный технический университет (Воронеж, Россия)
Воронежский институт высоких технологий (Воронеж, Россия)

Рассматриваются возможности применения комплексного подхода для обеспечения информационной безопасности в распределенных информационных системах. Указаны общие требования по архитектуре, связанной с системой защиты информации. Приведены компоненты комплексной защиты информации. Показаны составляющие, которые могут быть выделены в комплексной защите информации.

Ключевые слова: информационная безопасность, защита информации, информационная система.

Целостный и достаточный набор средств защиты в организации рассматривается в виде комплексной системы защиты информации. Он позволяет бороться с актуальными угрозами, происходит его интегрирование в защищаемую систему [1, 2].

Обеспечение безопасности распределенных информационных систем и трудности, связанные с их управлением определяются сложностью формирования таких систем. Развивается централизованное управление по всей распределенной системе, реализуется управление подразделениями, направленное на приложения и серверы. Существует управление, направленное на локальную сеть и выход в Интернет, а также на пользователей. Данные уровни управления могут рассматриваться в виде объектов угроз с точки зрения информационной безопасности организации. Защита по каждому уровню управления распределенными информационными системами должна входить в систему информационной безопасности [3, 4].

Необходимо чтобы в ходе разработок учитывались общие требования, связанных с архитектурой комплексной системы защиты информации (КСЗИ):

- важно обеспечить информационную безопасность по всем уровням защиты и по всем стадиям жизненного цикла информационных систем;
- распределенная и многоуровневая структура должна быть в архитектуре КСЗИ;
- решения, которые образуют КСЗИ, должны выбираться с учетом масштабируемости и модульного принципа построения;
- внедрение мер безопасности должно осуществляться в рамках всей инфраструктуры (а не только на критичных ресурсах);
- должна быть интеграция КСЗИ информационной системы со встроенными средствами защиты информации прикладных систем, операционных систем и сервисов [5, 6].

Средства защиты информации (СЗИ) – совокупность инженерно-технических, электронных, электрических, оптических и прочих устройств, приборов и технических систем, а также других элементов, применяемых для обеспечения защиты информации, в том числе предупреждения утечки данных [7, 8].

СЗИ можно разделить на универсальные и специализированные (по области применения), на частные и комплексные (по совокупности решаемых задач), на встроенные в системные средства и добавочные (по способу построения). В зависимости от способа реализации средства защиты информации делят на следующие группы.

1) Технические (аппаратные) средства - различные по типу устройства (механические, электромеханические, электронные и другие), которые аппаратными средствами решают задачи защиты информации. Они либо препятствуют физическому проникно-

Львович Яков Евсеевич – Воронежский государственный технический университет, доктор техн. наук, профессор, e-mail: office@vivt.ru.
Преображенский Юрий Петрович – Воронежский институт высоких технологий, канд. техн. наук, профессор, e-mail:petrovich@vivt.ru.

вению, либо, если проникновение все же состоялось, доступу к информации [9, 10], в том числе с помощью ее маскировки.

2) Программные средства, которые включают программы для идентификации пользователей, контроля доступа, шифрования информации, удаления остаточной (рабочей) информации типа временных файлов, тестового контроля системы защиты и др.

3) Смешанные аппаратно-программные средства, которые реализуют те же функции, что аппаратные и программные средства в отдельности, и имеют промежуточные свойства [11, 12].

4) Организационные средства, которые складываются из организационно-технических мер (подготовка помещений с компьютерами, прокладка кабельной системы с учетом требований ограничения доступа к ней и др.) и организационно-правовых мероприятий (национальные законодательные документы и правила работы, устанавливаемые руководством конкретного предприятия).

Таблица

Компоненты комплексной системы защиты информации

№	Подсистема КСЗИ	Характеристика подсистемы КСЗИ
1	Подсистема управления КСЗИ	предназначена для управления процессами защиты информации на основе законодательства и регламентации правил и порядка доступа к защищаемой информации и контроля процессов КСЗИ
2	Подсистема защиты от физического НСД	Необходима для того, чтобы контролировать пребывание на территории и объектах защиты персонала организации и предотвращения неконтролируемого пребывания посторонних лиц, для извещения о случаях несанкционированного доступа
3	Подсистема анализа, управления рисками, контроля защищенности ИС	предназначена для снижение внешних и внутренних угроз информационной безопасности в распределенных сетях, опасности принятия ошибочного решения и уменьшение возможных негативных последствий нежелательного развития событий
4	Подсистема идентификации и аутентификации	предназначена для проведения процедур аутентификации/ идентификации сетевых сущностей, входящих в состав распределенной ИС
5	Подсистема фильтрации и межсетевого экранирования	предназначена для реализации фильтрации открытого и зашифрованного IP-трафика, фиксации его во внутренних журналах, фильтрации пакетов служебных протоколов, регистрации и учета запрашиваемых сервисов прикладного уровня
6	Подсистема защиты от вредоносных программ	предназначена для защиты распределенных ИС от несанкционированного воздействия с применением компьютерных вирусов и других видов вредоносных программ

В ряде случаев средства защиты информационных систем делят по 2 группам: физические и логические. Первые из них будут создавать препятствия для нарушителей на путях к защищаемым данным. В качестве примера, можно указать территорию, на которой располагаются объекты. Они будут выполнять функции охраны территории и зданий, охраны внутренних помещений, охраны оборудования и наблюдения за ним, контроля доступа в защищаемые зоны, нейтрализации излучений и наводок, создания препятствий визуальному наблюдению и подслушиванию, противопожарной защиты, блокировки действий нарушителя и т. п.

Регулирование доступа на территорию и в помещения может осуществляться с помощью специальных замков и датчиков, а также идентифицирующих устройств. Применяются экранирование и зашумляющие генераторы излучений для защиты от перехвата электромагнитного излучения. К логическим средствам защиты информации от угроз информационной безопасности и несанкционированный доступ (НСД) относят аппаратные, программные и криптографические средства. В составе комплексной системы защиты информации на предприятии можно выделить компоненты, описанные в таблице. В составе КСЗИ могут быть также выделены следующие подсистемы: по обеспечению целостности, по обнаружению вторжений, криптографической защиты; защиты персональных данных в системе от утечки за счет побочных

электромагнитных излучений и наводок (ПЭМИН), а также другие подсистемы комплексной системной защиты.

Вывод. В работе приведены основные шаги по формированию комплексной защиты информации.

СПИСОК ИСТОЧНИКОВ

1. Mironov V. V. Situation-oriented databases: processing office documents / V. V. Mironov, A. S. Gusarenko, N. I. Yusupova // Modeling, Optimization and Information Technology. – 2022. – Т. 10. – № 2 (37).

2. Zhuravleva K. I. Human resource management and extracting information about research activity in the field / K. I. Zhuravleva, O. N. Smetanina, N. I. Yusupova // Modeling, Optimization and Information Technology. – 2022. – Т. 10. – № 2 (37).

3. Гвоздев В. Е. Поддержка управления функциональной безопасностью аппаратно-программных комплексов на основе системных архетипов / В. Е. Гвоздев, О. Я. Бежаева, М. Б. Гузаиров, В. И. Васильев // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 2 (37).

4. Васильев В. И. Анализ и управление рисками информационной безопасности асу тп на основе когнитивного моделирования / В. И. Васильев, А. М. Вульфин, А. Д. Кириллова // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 2 (37).

5. Ковалев И. В. Анализ тестовых задач мультиверсионного формирования отказоустойчивых программных систем / И. В. Ковалев, Д. И. Ковалев, Н. Д. Амбросенко, Д. В. Боровинский // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 2 (37).

6. Рындин Н. А. Компонентная оптимизация развивающейся цифровой среды управления в организационных системах / Н. А. Рындин // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – № 2 (37).

7. Преображенский А. П. Построение многокритериальной модели работы предприятия / А. П. Преображенский, О. Н. Чоповров // Наука Красноярья. – 2017. – Т. 6. – № 3-4. – С. 183-188.

8. Мэн Ц. Анализ методов классификации информации в интернете при решении задач информационного поиска / Ц. Мэн // Моделирование, оптимизация и информационные технологии. – 2016. – № 2 (13). – С. 19.

9. Преображенский Ю. П. Некоторые проблемы автоматизации процессов / Ю. П. Преображенский // Техника и технологии: пути инновационного развития. Сборник научных трудов 8-й Международной научно-практической конференции. Юго-Западный государственный университет. – 2019. – С. 62-64.

10. Филипова В. Н. О применении информационных технологий в туристической сфере / В. Н. Филипова // Успехи современного естествознания. – 2012. – № 6. – С. 112-113.

11. Львович И. Я. Применение методологического анализа в исследовании безопасности / И. Я. Львович, А. А. Воронов // Информация и безопасность. – 2011. –Т. 14. – № 3. – С. 469-470.

12. Преображенский Ю. П. О возможностях роста эффективности функционирования современных компаний / Ю. П. Преображенский // Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципального управления. Материалы XIII международной научно-практической конференции. Под редакцией Ю. В. Вертаковой. – 2018. – С. 215-218.

INTEGRATED APPROACH TO INFORMATION SECURITY OF DISTRIBUTED INFORMATION SYSTEMS

© 2022 Ya. E. Lvovich, Yu. P. Preobrazhensky

Voronezh State Technical University (Voronezh, Russia)
Voronezh Institute of High Technologies (Voronezh, Russia)

Possibilities of using an integrated approach to maintain information security in distributed information systems are considered. The general requirements for the architecture associated with the information security system are indicated. The components of complex information protection are given. The components that can be distinguished in the complex information protection are given.

Keywords: information security, information protection, information system.