УДК 681.3

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМ

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

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

Обсуждаются проблемы обеспечения информационной безопасности распределенных информационных систем. Проведена классификация угроз информационной безопасности. Показаны особенности задачи, связанной с реализацией информационной безопасности. Продемонстрированы особенности комплексной защиты информации. Отмечаются особенности информационной безопасности в распределенных информационных системах.

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

В настоящее время человечество переживает процесс перехода к качественно новому этапу развития, известному как «информационное общество». В процесс формирования единого информационно-коммуникационного поля вовлечены практически все субъекты информационных отношений: от частных лиц до межгосударственных образований.

Новые информационные технологии, глобальная компьютеризация, масштабное использование информационно-вычислительных сетей, облачных вычислений и общего информационного контента породили новые источники угроз для всей информационной среды, в которой существует и развивается современное общество [1, 2]. Происходит изменение экономических и социальных сторон жизни общества вследствие стремительного развития информационных технологий, масштабного применения информационных систем. Информационные системы выступают одним из системообразующих факторов современного социума, и влияние информационной безопасности и на все стороны жизнедеятельности людей с течением времени будет только возрастать [3, 4].

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.

В связи со всё возрастающей ролью информации в жизни современного общества задачи информационной безопасности занимают особое место и требуют к себе привлечения все большего внимания.

Современные информационные системы уже немыслимы без использования средств защиты информации и создания комплексной системы информационной безопасности [5, 6].

Практика разработки современных информационных систем показывает, что большинство из них носит распределенный характер. Анализ показывает, что распределенную информационную систему (ИС) можно рассматривать в виде информационной системы, ресурсы которой могут находиться на физически различных, связанных коммуникационными линиями (сетью), серверах, при этом сохраняется логическая целостность информации. Поддержка единообразного доступа к системе будет обеспечиваться через любую точку входа (единые пользовательские интерфейсы).

К распределенным информационным системам относят компьютерные сети (КС).

Наряду с компьютерными сетями к распределенным ИС также относят и мультипроцессорные компьютеры и многомашинные комплексы [7, 8]. Разнородность, гетерогенность компонент распределенных информационных систем, сложность их построения, открытость протоколов обмена данными, огромное количество включаемых

в сети абонентов создают проблемы обеспечения информационной безопасности, контроля за состоянием сетей. Постановка задачи обеспечения информационной безопасности в наши дни приобретает ряд особенностей:

- защита информации становится все более актуальной для массы объектов (больших и малых, государственной и негосударственной принадлежности);

- резко расширяется разнообразие подлежащей защите информации (государственная, промышленная, коммерческая, персональная и т. п.);

- на первый план выходит проблема комплексной защиты информации.

Успешное осуществление указанных мероприятий возможно только при наличии научно-методологических основ комплексной защиты информации, под которыми понимается совокупность подходов, принципов и методов (научных и технических направлений), которые требуются для исследования и анализа проблемы комплексной защиты.

Главной целью создания комплексной системы защиты информации (КСЗИ) является обеспечение максимальной эффективности защиты с помощью одновременного использования необходимых методов, ресурсов и средств, которые исключают несанкционированный доступ к защищаемым данным и обеспечивают физическую сохранность носителей в системе [9, 10].

Обеспечение безопасности информации в распределенных системах предполагает создание препятствий для попыток несанкционированного доступа к данным, хищениям или модификациям передаваемых данных по сети. При этом важным является сохранение таких свойств информации, как:

1) доступность – свойство информации, ее способность обеспечивать своевременный и беспрепятственный доступ пользователей к нужным данным;

2) целостность – существование информации в неизменном виде;

3) конфиденциальность – необходимость введения ограничений на доступ к информации ограниченному кругу пользователей.

Чтобы в полной мере оценить возможный реальный ущерб от потери или порчи информации распределенной системы или переданных данных по каналам связи, необходимо рассмотреть угрозы информационной безопасности для разработки адекватных мер их предотвращения.

Угроза информационной безопасности – это совокупность условий и факторов, создающих опасность нарушения информационной безопасности. Угрозы информационной безопасности можно классифицировать по следующим признакам:

1) По цели реализации угроз:

- нарушения целостности информации;

- нарушения конфиденциальности информации;

- нарушения (частичные или полные) работоспособности ИС и ее компонент.

2) По принципу воздействия на объекты угрозы ИС могут реализовываться:

- с применением доступа субъектов системы (пользователей, процессов) к объектам ИС (каналу связи, файлам данных и т. д.);

- с применением скрытых каналов (пути передачи информации, позволяющие обмениваться информацией двум процессам способами, нарушающими системную политику безопасности).

3) По способу воздействий на объекты атаки (при их активном воздействии) могут иметь место:

- непосредственные воздействия на объекты атаки, например, доступ к наборам данных, программам, каналу связи и проч., используя ошибки;

- воздействие на систему разрешений (включая захват привилегий). Несанкционированные действия при этом выполняются относительно прав на объект, а сам же доступ к объекту потом осуществляется законным образом.

4) Относительно объекта атаки классификация угроз предполагает, что воздействиям угроз могут подвергаться компоненты АИС автоматизированная информационная система:

- автоматизированная информационная система в целом;

- определенные объекты системы - программы или данные в оперативной памяти, на внешних носителях, внешние и внутренние устройства системы (дисководы, флешнакопители, маршрутизаторы и проч.);

- субъекты системы, то есть процессы и подпроцессы при участии пользователей;

- каналы передачи данных, то есть пакеты данных, которые передаются по каналу связи, а также сами каналы.

Вывод. Обеспечение комплексной информационной безопасности в распределенных автоматизированных системах требует классификации информационных угроз, средств атак, учет целей злоумышленников.

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. Львович А. И. Алгоритмизация процесса визуально-экспертного моделирования при оптимизации управления развитием организационных систем с использованием мониторинговой информации / А. И. Львович, А. П. Преображенский. // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. – №1 (36). – [Электронный ресурс]: https://moitvivt.ru/ru/journal/article?id=1154 (дата обращения 10.09.2022)

7. Мельникова Т. В. Моделирование обработки больших массивов данных в распределенных информационно-телекоммуникационных системах / Т. В. Мельникова, М. В. Питолин, Ю. П. Преображенский // Моделирование, оптимизация и информационные технологии. – 2022. – Т. 10. №1 (36). – [Электронный ресурс]: https://moitvivt.ru/journal/article?id=1117 (дата обращения: 10.09.2022).

8. 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).

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

10. 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.

11. 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.

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

13. 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.

14. Преображенский Ю. П. О возможностях роста эффективности функционирования современных компаний / Ю. П. Преображенский // Актуальные проблемы развития хозяйствующих субъектов, территорий и систем регионального и муниципаль-

ного управления. Материалы XIII международной научно-практической конференции. Под редакцией Ю. В. Вертаковой. – 2018. – С. 215-218.

THE PROBLEMS OF PROVIDING 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)

The problems of ensuring information security of distributed information systems are discussed. A classification of information security threats has been carried out. The features of the task associated with the implementation of information security are shown. The features of integrated information protection are demonstrated. The features of information security in distributed information systems are noted.

Keywords: information security, information protection, information system.