УДК 004.9

ПРОБЛЕМЫ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ВУЗА: ИНФОРМАЦИОННЫЙ АСПЕКТ

Акперов Г.И.

Директор по маркетингу ЧОУ ВО ЮУ (ИУБиП)

e-mai: dpo@iubip.ru;

Акперова А.А.

e-mai: dpo@iubip.ru

Бочаров А.А.

Аннотация: В статье рассматриваются вопросы анализа комплексной безопасности организации на примере частного вуза Юга России. Оценивается эффективность обеспечения комплексной безопасности в условиях геополитической турбулентности и интенсификации информационных атак на ресурсы вуза. Даются рекомендации по выбору алгоритмов мониторинга безопасности и противостояния противникам и конкурентам.
Ключевые слова: разрушающие программные средства, функциональное программирование, хранение и обработка данных, вирусы и программные закладки

PROBLEMS OF INTEGRATED SECURITY OF HIGHER EDUCATIONAL INSTITUTIONS: INFORMATION ASPECT

Akperov G.I.

Akperova A.A.

Bocharov A.A.

Abstract: The article deals with the analysis of the complex security of an organization on the example of a private university in the South of Russia. The effectiveness of providing integrated security in the context of geopolitical turbulence and intensification of information attacks on university resources is evaluated. Recommendations are given on the choice of algorithms for monitoring security and confronting opponents and competitors.
Keywords: destructive software, functional programming, data storage and processing, viruses and software bookmarks.

Объективная необходимость защиты информации в современных автоматизированных системах управления обусловлена теми принципиальной значимости накоплениями и изменениями, которые

произошли в следующих направлениях: в развитии самой вычислительной техники и ее программного обеспечения; в концепциях организации и использования ресурсов вычислительной техники; в концепциях применения вычислительной техники в различных сферах общественной деятельности.

Основные изменения в развитии вычислительной техники и её программного обеспечения, которые произошли к настоящему времени и особенно затрагивающие область безопасности информации, могут быть охарактеризованы следующим образом: а) массовый выпуск персональных ЭВМ; б) расширение объемов ЗУ прямого доступа; в) резкое развитие общего программного обеспечения в направлении интеллектуализации, предназначенного для обеспечения программирования, организации вычислительного процесса, обеспечения функционирования технических средств и выполнения других функций; г) интенсивное развитие унифицированного системного ПО, предназначенного для организации и обеспечения функционирования информационно-вычислительных систем и сетей, включая и автоматизированную передачу данных по сетям; интенсивное развитие и повсеместное внедрение систем управления базами данных, предназначенных для централизованного накопления и хранения больших массивов данных, поиска и выдачи их пользователям или другим решаемым в системе задачам; ж) интенсивное развитие пакетов прикладных программ, что существенно облегчает разработку задач функциональной обработки информации.

Указанные изменения привели к резкому количественному и качественному росту угроз безопасности информации, среди которых особо следует выделить разрушающие программные средства (РПС). Известный [1] «экспоненциальный вирусный взрыв», начавшийся еще с конца 90-х годов., продолжает развиваться.

Особенность современной ситуации с РПС состоит даже не только в лавинообразном росте вирусов и появлении их генераторов, а в качественных изменениях РПС. Эти изменения можно выразить в следующих положениях:

функционирование большинства РПС приобретает целевой характер; практически любое программное средство содержит те или иные элементы РПС (например, функции нарушения целостности вычислительной системы: изменение распределения памяти системы, изменение файловой системы и т.п.)

В результате в вычислительных системах существенно снижается уровень безопасности программного обеспечения (ПО) по следующим основным причинам:

1. Персональная ЭВМ (РС) под управлением популярных операционных систем содержит не достаточно специальных средств защиты информации [2,3].

2. Стандартности РС, отсутствие в них уникальности, тем самым уменьшается время на исследование существующей в конкретной системе программной среды [4].

3. Широкое распространение в системах одних и тех же "популярных" прикладных программ, оказывающихся под угрозой из-за множества разработанных способов "атаки" на них, приобретение не лицензированных программных продуктов, бесконтрольный доступ и обмен информацией.

Поэтому использование РС требует срочного решения задач создания специальных средств защиты (ССЗ), адекватной оценки безопасности программных средств, функционирующих под управлением таких операционных систем. Причем среди множества приемов и методов защиты информации (организационные, технические, программные, программно-аппаратные, криптографические и т.д.) особо следует выделить программные в силу следующих причин [5]: простота тиражирования программных средств защиты на объекты заказчика и разработчика; простота технологии применения; применение программных методов не требует привлечения производства, при этом, возможно позволяя получить достаточный уровень безопасности данных.

Особое внимание в настоящее время следует уделять применению

программно-аппаратных средств защиты в сетях, учитывая переход производства на автоматизированную систему управления и интеллектуального применения на базе сети РС. Специалисты считают, что расширение масштабов практического применения компьютерных сетей сопровождается увеличением опасности преднамеренной дезорганизации их работы или использования их для преступных или разведывательных целей. В сетях наиболее необходимы специальные аппаратные и программные средства защиты, обеспечивающие постоянный контроль за работой сетевых устройств, кабельной системы и ПО, так называемые средства мониторинга.

Только одного мониторинга явно недостаточно. Требуются средства борьбы с компьютерными вирусами. Конечно, вирусы не могут просто так появиться на компьютере. Когда "незараженный" компьютер полностью изолирован от внешнего мира, вирус не может попасть в такой компьютер. Но такой вариант практически невозможен.

Современная антивирусная программа должна "отслеживать" обычные, полиморфные и "невидимые" вирусы, занимать малый объем, производить сканирование в режиме реального времени и восстанавливать зараженное ПО. В настоящее время практически не существует универсальной, эффективной и надежной антивирусной программы.

В рамках решения этой задачи может быть перспективным создание программно-аппаратных средств защиты (ПАСЗ) для противодействия скрытым информационным объектам (СИО) в ПО. Ущерб от воздействия таких объектов в несколько раз превышает последствия проникновения вирусов. Кроме того, они представляют собой не только "внешнюю", но и "внутреннюю" угрозу компьютерной системе, которая, например, проявляется из-за растущего использования накопителей информации на внешних носителях. С этой стороны опасно внедрение СИО в ПО, поставляемое на таких устройствах.

Воздействие СИО может произойти и на сами ПАСЗ информации, «поскольку обращение к аппаратным средствам происходит, как правило,

через некоторую промежуточную программу управления»[6]. Поэтому ко всем вышеперечисленным действиям добавляется самоконтроль целостности ПАСЗ. Он должен осуществляться с использованием программ или вшитых в ПЗУ, или обладающих свойством противодействия их исследованию, т.е. скрытие алгоритма своего функционирования.

Таким образом, к основным объективным и субъективным факторам, определяющим в основном возрастание степени риска нанесения ущерба, и требованиям в области уровня безопасности автоматизированных систем управления в целом в настоящее время можно отнести следующие [7]: недостаточная законодательная и нормативно-правовая база в области информационной безопасности; информационных систем, создаваемых на базе импортных технологий, технических и программных продуктов; отсутствие взаимосвязанного пакета основополагающих документов, определяющих стратегию безопасности и необходимость защиты создающих основу механизмов или процессов, снижающих риск нанесения ущерба и достижения необходимого уровня безопасности (концепция, модели угроз, модели обеспечения, количественные и качественные показатели уровня безопасности); [8,9] возрастание уязвимости автоматизированных систем управления критического назначения; недостаточный уровень информационного обеспечения, современной нормативной базы.

Библиографический список

1. Akperov, I.G. Soft models of management in terms of digital transformation / I.G. Akperov, G.I. Akperov, T.V. Alekseichik [et al.]. – Rostov-on-Don: PEI HE SU (IMBL), 2019. – 188 p.
2. Алекперов И.Д. Информационная безопасность и защита информации в цифровой экономике: элементы теории и тестовые задания / И.Д. Алекперов, В.В. Храмов, А.А. Горбачева, Д.П. Фомичев. – Ростов-на-Дону: Южный университет (ИУБиП), 2020. – 114 с.
3. Храмов, В.В. Агрегирование информации как проблема личностной самоорганизации // Российский психологический журнал. – 2007. – Т. 4. – № 4. – С. 9-21.
4. Чернышев, Ю.О. Особенности агрегирования качественных признаков опорных ориентиров в системах технического зрения / Ю.О. Чернышев, В.В. Храмов // Известия ТРТУ. – 2001. – № 3(21). – С. 55.
5. Храмов, В.В. Защита информации в вычислительных системах : учебное пособие для вузов / В.В. Храмов, В.В. Садовов, А.Н. Трубников, О.К. Губарев. – Москва: Пущинский научный центр Российской академии наук, 2002. – 192 с.

6. Akperov, G. I. Using soft computing methods for the functional benchmarking of an intelligent workplace in an educational establishment / G.I. Akperov, V.V. Khramov, A. A. Gorbacheva // Advances in Intelligent Systems and Computing (см. в книгах). – 2020. – Vol. 1095 AISC. – P. 54-60. – DOI 10.1007/978-3-030-35249-3_6.

7. Sakharova L.V., Stryukov M.B., Alekseichik T.V., Chuvenkov A.F., Akperov I.G. Application of fuzzy set theory in agro-meteorological models for yield estimation based on statistics // Procedia Computer Science. – 2017. – С. 820-829.

8. Akperov I.G., Khramov V.V. Development of instruments of fuzzy identification of extended objects based on the results of satellite monitoring // Advances in Intelligent Systems and Computing (см. в книгах). – 2019. – Т. 896. – С. 325-332.

9. Храмов, В.В. Оценка качества подготовки специалистов в условиях современного образовательного процесса / В.В. Храмов // Интеллектуальные ресурсы – региональному развитию. – 2014. – № 1. – С. 125-130.

10. Храмов, В.В. Моделирование на ЭВМ: пособие для курсового и дипломного проектирования / В.В. Храмов. – Москва: Министерство обороны РФ, 1992. – 98 с.

11. Перспективы и возможности формирования системы экспертно-аналитического сопровождения международной деятельности российских университетов / А.А. Акишина, И.В. Антипина, А.И. Богуш [и др.]. – Москва: Издательский Центр РИОР, 2020. – 295 с. – DOI 10.29039/02044-9.