СТРУКТУРНАЯ ОСОБЕННОСТЬ ДОВЕДЕНИЯ СТАНДАРТОВ ДЛЯ ФОРМИРОВАНИЯ СИСТЕМЫ ИНФОРМАЦИОННОЙ ЗАЩИТЫ ПРЕДПРИЯТИЯ

STRUCTURAL FEATURE OF BRINGING STANDARDS TO THE FORMATION OF AN ENTERPRISE INFORMATION SECURITY SYSTEM

УДК 004

Козлов Никита Михайлович, студент, МГТУ им. Н.Э. Баумана

Россия, г.Москва

Kozlov Nikita Mikhailovich, student, MSTU N.E. Bauman

Russia, Moscow E-mail: ambientpower@gmail.com

Аннотация

Разработанные на данный момент информационные системы являются или чрезмерно массивными (по количеству охваченных функциональных областей и выполняемых функций) для внедрения и дорогими, несмотря на широкий охват функциональности кроме производственного планирования, или не в полной мере реализуют подходы планирования, которые бы привели к удовлетворению потребностей машиностроительных предприятий в планировании: в частности построение основного плана и составление оперативно-календарного расписания с опорой на основной план. Это позволяет сделать вывод о важности разработки инструмента планирования, который функционирует отдельно от массивных ERP-систем и при этом позволяет реализовывать различные подходы к планированию производства, учитывающие особенности конкретных машиностроительных предприятий.

S u m m a r y

Currently developed information systems are either too massive (in terms of the number of functional areas covered and functions performed) for implementation and expensive, despite the wide coverage of functionality other than production planning, or do not fully implement planning approaches that would lead to meeting the planning needs of machine-building enterprises: in particular, the construction of the main plan and the preparation of an operational calendar based on the main plan. This makes it possible to draw a conclusion about the importance of developing a planning tool that functions separately from massive ERP systems and at the same time allows you to implement various approaches to production planning that take into account the specifics of specific machine-building enterprises.

Ключевые слова: модель, облако, защита, структура, динамика.

Keywords: model, cloud, security, structure, and dynamics.

Одним из основных признаков развития современного общества является дальнейший рост зависимости от качества и надежности компьютеризированных ИС, применяемых в разнообразных отраслях человеческой деятельности. Соответствующее усиление стратегической направленности информационных ресурсов обусловливает необходимость повышения требований к уровню их информационной безопасности. Проблема обостряется тем, что особенности крупнейшей глобальной сети Интернет, с которой интегрировано большинство ИС, и использование общедоступного программного обеспечения приводят к значительным объемам случайных и непредвиденных негативных воздействий на указанные системы [5, с. 32]. Отметим, что Интернет-ориентация ИС рассматривается в ракурсе необходимости защиты ресурсов таких систем от кибератак в процессе реализации базовых технологических процессов получения, хранения, транспортировки, обработки и представления информации. При этом под понятием кибератак будем понимать реализацию в кибернетическом пространстве угроз безопасности его компонентов (а именно конфиденциальности, целостности и доступности) с учетом их уязвимостей. В то же время киберпространство – это

виртуальное пространство, полученный в результате взаимодействия пользователей, программного и аппаратного обеспечения, сетевых технологий для поддержки и управления процессами преобразования информации с целью обеспечения информационных потребностей общества [3, с. 702].

В общем случае под понятием информационная безопасность понимается состояние защищенности жизненно важных интересов человека, общества и государства, при котором предотвращается нанесение вреда через: неполноту, несвоевременность и недостоверность информации; негативное информационное влияние; негативные последствия применения информационных технологий; несанкционированное распространение, использование, нарушение целостности, конфиденциальности и доступности информации. В то же время под понятием безопасности информации (information security) понимают состояние информации, в котором обеспечивается сохранение определенных политикой безопасности свойств информации. При этом под понятием защиты информации в информационных системах понимают деятельность, которая направлена на обеспечение безопасности обрабатываемой в ИС информации и ИС в целом, и позволяет предотвратить или затруднить возможность реализации угроз, а также снизить величину потенциальных убытков в результате реализации угроз [2, с. 53].

С позиций причинения недостатков и деструктивных воздействий от информационной безопасности отделяют функциональную. При этом в определении функциональной безопасности акцент ставится на правильности функционирования и считается, что она в основном связана с нечаянно реализованными деструктивными факторами, ошибки носят случайный характер, а эталонное состояние объекта, отклонения от которого указывает на ошибку – известный. Однако сложность и многофакторность процессов функционирования ресурсов современных интернет-ориентированных ИС в большинстве случаев указывает на невозможность отдельного оценивания параметров функциональной и информационной безопасности.

Подтверждается вывод о нецелесообразности разделения параметров оценивания, где утверждается, что уровень функциональной безопасности

системного средства определяется тем, насколько адекватно соотносится набор механизмов защиты условиям конкретного использования, и тем, насколько корректно данные механизмы реализованы. При этом указывается, что как недостаточность механизмов защиты, так и некорректность их реализации определяют уязвимость системных средств. Раздела дестабилизирующих факторов на умышленные и случайные не предусмотрено. Кроме того, использовано определение информационная безопасность, которое включает в себя защиту информации от случайных или преднамеренных воздействий искусственного или естественного характера.

Вместе с тем, в зарубежных публикациях, посвященных оценке безопасности информационных технологий, содержатся требования к функциональным требованиям безопасности. Поэтому, несмотря на некоторую неоднозначность современной терминологии, можно считать, что процедура оценивания ПБ ИС сводится к определению величин параметров безопасности, что свидетельствуют о наличие/отсутствие кибератак. При этом под понятием множества параметров безопасности будем понимать множество параметров, отражающих состояние безопасности объектов защиты ИС. В общем случае множество ПБ интерент-ориентированных ИС формируются на основе анализа:

– параметры входных и выходных сетевых соединений по разнообразным протоколам;

– код потенциально опасного программного кода, который передается в ИС;

– параметров, отражающих функционирование системного и прикладного программного обеспечения ИС;

– функциональные параметры аппаратного обеспечения ИС;

– параметры, характеризующие содержание информации, передаваемой в ИС.

Источником статистических данных для формирования такого множества ПБ являются: системные журналы операционных систем рабочих станций и серверов ИС, базы данных средств защиты информации (сетевых экранов, антивирусов,

систем защиты от спама, DLP-систем), а также базы данных параметров кибератак (КДД-99) [1, с. 37].

Проведем декомпозицию проблемы оценивания ПБ Интернет-ориентированных ИС для распознавания кибератак. Отметим, что акцент ставится на ИС общего назначения, которые в основном используются в сферах организационного управления, промышленности и экономике. Согласно [4, с. 59], характерными свойствами Интернет-ориентированных ИС являются:

– поддержка типовых интернет-сервисов (веб-сайта, электронной почты),

– сложность описания (достаточно большое количество функций, процессов, элементов данных и сложные взаимосвязи между ними);

– применимо разнородность методов и моделей, использованных при построении ее компонентов;

– наличие совокупности тесно взаимодействующих компонентов (подсистем), имеющих свои локальные задачи и цели функционирования (например, традиционных приложений, связанных с обработкой транзакций и решением регламентных задач, и приложений аналитической обработки (поддержки принятия решений), использующих нерегламентированные запросы к данным большого объема;

– функционирование в неоднородной среде на нескольких аппаратнопрограммных платформах;

– необходимость постоянной интеграции в ИС существующего и вновь созданного программного обеспечения;

– использование программного обеспечения, созданного разобщенными и разнородными группами разработчиков с разным уровнем квалификации и традициями использования тех или иных инструментальных средств;

– использование программного обеспечения, которое во многих случаях не имеет официальной поддержки и несет в себе потенциальную угрозу безопасности за счет ошибок, и люков, которые могут проявляться только в определенных условиях эксплуатации;

– широко используется в архитектуре программного обеспечения распределенных объектов;

– сложности администрирования как в штатных условиях эксплуатации, так и при модификации программного обеспечения;

– формирование управленческих рекомендаций на основе обработки больших объемов разнородной информации;

– необходимость постоянной актуализации информационных ресурсов;

– интегрируемость с другими интернет-ориентированными ИС, часть из которых несут в себе потенциальные угрозы как преднамеренного, так и непреднамеренного характера;

– тесное взаимодействие с внешней интернет-средой, которое включает в себя большое количество информационно-программных деструктивных средств;

– стандартизация и унификация процедур взаимодействия между различными функциональными блоками ИС;

– интеллектуализация процедур обработки данных, что значительно усложняет оценивание управляющих сигналов ИС;

– адаптируемость к пользователям с различной квалификацией, что значительно уменьшает эффективность защиты от деструктивных воздействий;

– взаимодействием с удаленными пользователями;

– но децентрализованность управления как системой защиты, так и всей ИС в целом, что во многих случаях определяет опоздание и уменьшение эффективности управленческих воздействий.

Литература

1. Витомский Е. В., Сомов Д. Н. Методы защиты локальной беспроводной сети, направленные на обеспечение временной скрытности сигналов и структуры информационного взаимодействия // Вопросы радиоэлектроники. – 2020. – № 3. – С. 35-40.

2. Жалнова Э. М. Информационные системы сферы социальной защиты населения регионов России (обзор) // Энигма. – 2020. – № 21-3. – С. 50-54.
3. Магомедов Ш. Г. Анализ защиты компьютерных сетей и приложений информационных процессов учреждений здравоохранения // Cloud of Science. – 2020. – Т. 7. – № 3. – С. 685-704.
4. Немовленко А.Е., Макарова А. В., Будко Е. А. Проблема защиты информационного потока в «internet» // Символ науки. – 2020. – № 5. – С. 58-59.
5. Семёнов Д.А., Чичикин Г.Я. Защита информационных активов // Academy. – 2020. – № 6 (57). – С. 31-33.

Literature

1. Vitomsky E.V., Somov D.N. Methods of protecting a local wireless network aimed at providing temporary secrecy of signals and the structure of information interaction // Questions of Radioelectronics. - 2020. - No. 3. - S. 35-40.
2. Zhalnova E. M. Information systems of the sphere of social protection of the population of the regions of Russia (review) // Enigma. - 2020. - No. 21-3. - S. 50-54.
3. Magomedov Sh. G. Analysis of protection of computer networks and applications of information processes of healthcare institutions // Cloud of Science. - 2020. - T. 7. - No. 3. - S. 685-704.
4. Nemovlenko AE, Makarova A. V., Budko E. A. The problem of protecting the information flow in the “internet” // Symbol of science. - 2020. - No. 5. - S. 58-59.
5. Semenov D.A., Chichikin G.Ya. Protecting Information Assets // Academy. - 2020. - No. 6 (57). - S. 31-33.