Интернет-журнал «Науковедение» ISSN 2223-5167 http://naukovedenie.ru/

Том 9, №3 (2017) http://naukovedenie.ru/vol9-3.php

URL статьи: http://naukovedenie.ru/PDF/24TVN317.pdf

Статья опубликована 27.05.2017

Ссылка для цитирования этой статьи:
Варлатая С.К., Гончаренко А.С. Формирование системы защиты информации и взаимодействие информационных подразделений при создании автоматизированной системы // Интернет-журнал «НАУКОВЕДЕНИЕ» Том 9, №3 (2017) http://naukovedenie.ru/PDF/24TVN317.pdf (доступ свободный). Загл. с экрана. Яз. рус., англ.

УДК 004

Варлатая Светлана Климентьевна
ФГАОУ ВО «Дальневосточный федеральный университет», Россия, Владивосток[1]
Руководитель направления «Информационная безопасность»
Кандидат технических наук, профессор
E-mail: sk-varl@yandex.ru

Гончаренко Алексей Сергеевич[2]
ФГАОУ ВО «Дальневосточный федеральный университет», Россия, Владивосток
Студент направления «Информационная безопасность»
E-mail: Goncharenko.as@students.dvfu.ru

Формирование системы защиты информации и взаимодействие информационных подразделений при создании автоматизированной системы

Аннотация. В наше время, когда информационные технологии максимально развиты и интегрированы в жизнь каждого человека в любой из сфер его жизнедеятельности, когда ни одно предприятие не обходится без хотя бы одной собственной автоматизированной системы, большую роль играет защита обрабатываемых, передаваемых и хранящихся данных. Создание систем защиты информации, служащих для обеспечения безопасности автоматизированных систем различного назначения (управление, проектирование, обработка и т.п.) зачастую становится достаточно проблематичной в плане полноты исполнения и обеспечения защиты информации, что является одной из важнейших проблем в сфере информационной безопасности, возникающей в следствии недостаточного количества теоретического и практического материала. Для пресечения возможности совершения ошибки при формировании системы можно использовать описанный материал, раскрывающий процесс создания типичной и усредненной автоматизированной системы на таких стадиях, как проектирование, разработка, реализация, испытания, ввод в эксплуатацию и сопровождение. В данной статье изложен уточненный порядок проведения необходимых мероприятий, связанный с созданием автоматизированной системы с точки зрения специалиста защиты информации, принимающего на себя роль как исполнителя, так и наблюдателя, подкрепленный теоретическими знаниями и практическим опытом.

[1] 690922, г. Владивосток, о. Русский, кампус ДВФУ, нп Аякс, 10

[2] https://vk.com/id123991df273

Вклад авторов. Гончаренко Алексей Сергеевич - автор осуществил написание статьи, изложил имеющийся опыт и наработки, проанализировал и интерпретировал использованную литературу. Варлатая Светлана Климентьевна - автор оказывал участие в написании статьи, предоставлял необходимые материалы и литературу, консультировал в вопросах теоретической составляющей статьи, одобрил окончательную версию статьи перед её подачей для публикации.

Ключевые слова: информационная безопасность; информационные технологии; автоматизированная система; проектирование; создание; документация

Введение

В наше время широкой распространенности информационных технологий одной из проблем создания автоматизированных систем является сильно преувеличенная уникальность близких по отрасли специалистов. При рассмотрении вопросов проектирования, разработки, испытания и внедрения автоматизированной системы полная ответственность зачастую складывается на едином круге специалистов, отвечающих одновременно за всё. В конечном итоге, всё сводится к недопустимым упрощениям в таких специфичных и узких сферах, как обеспечение информационной безопасности.

Использование необходимых и дополнительных средств защиты создает некоторые затруднения при работе и обслуживании автоматизированной системы, требует высоких материальных, физических и системных ресурсов, знаний и опыта [8]. Поэтому специалисты, заинтересованные в своевременном выполнении проекта и достижении минимального порога качества, не видят должного стимула для полноценной его доработки.

Подспорьем к этому служит и процедура приема работы, которая чаще всего сводится к проведению подготовленных заранее испытаний и слепому подписанию приема-сдачи, что также влечет за собой определенную цепь проблем, состоящую в последующем сопровождении регулирующих органов и исправлении вышедших из стоя компонентов системы или модернизации.

Для упрощения организации работы между отделами администрирования, проектирования и информационной безопасности существует максимально конкретизированный порядок взаимодействия подразделений на различных стадиях создания автоматизированных систем. Существует шесть основных стадий [3], которые могут дополняться в зависимости от требований Заказчика, типа системы и ситуации в целом [12]:

- Проектирование;
- Разработка;
- Реализация;
- Испытания;
- Ввод в эксплуатацию;
- Сопровождение.

На практике для упрощения организационной составляющей работы подразделений некоторые стадии совмещают в силу непосредственной близости их реализации.

Стадия проектирования и разработки

В начале построения любой автоматизированной системы первоочередной задачей является проектирование и разработка будущей системы. Специалисты отдела

информационной безопасности совместно с сотрудниками других связанных с данной задачей отделов и представителями Заказчика должны участвовать в разработке спецификаций, технического задания и технического проекта как сторона, определяющая требования защищенности системы.

Основываясь на рассмотрении категорий пользователей автоматизированной системы, обрабатываемых сведения, способов их хранения и многих других особенностях проектируемой системы обработки данных, а также учитывая требования Политики информационной безопасности компании и других организационных документов, сотрудники отдела информационной безопасности проводят анализ рисков и задают требования обеспечению безопасности ресурсов проектируемой системы [4; 6; 9].

Принятые отделом защиты информации меры должны быть согласованы с руководством отдела защиты информации и включены в проектную документацию как специальный раздел.

Помимо вышеизложенного, задействованные сотрудники отдела защиты информации принимают непосредственное участие при выборе программно-технических средств, которые планируют использовать в разрабатываемой системе.

Для подведения итогов стадии проектирования и разработки специалисты отдела информационной безопасности, отдела администрирования и отдела проектирования должны обсудить все возникшие вопросы и прийти к единому мнению относительно конфигурации коммуникационных связей в области соответствия требованиям информационной безопасности, которые формируются в соответствии с анализом потребностей системы при выполнении назначенных ей задач и категориями обрабатываемых данных. Всё это выполняется с учётом реальных возможностей выполнения требований с помощью организационных мер, программных и программно-технических средств.

Стадия реализации и испытаний

На данной стадии производится соответственная техническому заданию и техническому проекту реализация автоматизированной системы. Сотрудники задействованных отделов организации производят установку технической составляющей системы, разрабатывают программное обеспечение, создают структуру базы данных, осуществляют конфигурацию компонентов системы в соответствии с заявленными требованиями на своей территории для имитации подготовленных сценариев, основанных на реальных ситуациях. Реализация автоматизированной системы завершается подтверждением разработки проектной документации (руководство по установке, настройке и эксплуатации; шаблон базы данных; реестр программных продуктов; методические указания к испытанию системы и т.д.) [5].

Для организации испытательных мероприятий сотрудники отделов информационной безопасности, администрирования и разработки совместно со специалистами соответствующих сторон Заказчика участвуют в пробных запусках реализованной системы, в ходе прохождения которых происходит демонстрация работоспособности и функциональности, проверка работы автоматизированной системы в непредвиденных и критических ситуациях, а также соответствие системы установленным требования по обеспечению защищенности информации. По итогу между сторонами Заказчика и Исполнителя подписывается акты, описывающие результаты испытаний.

Стадия ввода в эксплуатацию

Данная стадия является завершающей в рамках подготовки системы к полноценной работе и подтверждает ожидаемый на стадии проектирования результат. Специалистами отдела

защиты информации и отдела администрирования производится окончательная разработка организационно-распорядительной документации, необходимой для регламентации эксплуатационных отношений между системой и её операторами, формуляров, инструкций, оказывающих вспомогательную функцию для обслуживающего персонала Заказчика в случае возникновения внештатных проблем в работе системы, а также подача необходимой документации в регулирующие органы в зависимости от характера системы [2].

Проведение работ по развертыванию системы на стороне Заказчика специалистами отдела администрирования или отдела автоматизации контролируется специалистами отдела информационной безопасности, которые следят за правильностью выполнения развертывания и настраивают дополнительные средства защиты в соответствии с требованиями, описанными в проектной документации и других регулирующих документах. Пользователи эксплуатируют систему, руководствуясь созданными на предыдущей стадии рекомендациями, правилами и регламентами, в ходе чего фиксируются возникающие ошибки и недоработки, которые обязаны устранить сотрудники Исполнителя в соответствии со своими полномочиями [10].

Специалисты отдела безопасности информации совместно с сотрудниками отдела безопасности Заказчика участвуют в разработке специальных требований по обеспечению безопасности информации в должностных инструкциях для пользователей автоматизированной системы.

После ряда доработок и условного подтверждения соответствия системы ранее предъявленным требованиям сторона Заказчика официально подтверждает успешный ввод в эксплуатацию автоматизированной системы путем передачи протокола о вводе автоматизированной системы в эксплуатацию.

Стадия сопровождения

На стадии сопровождения системы ответственными за эксплуатацию системы администраторами безопасности и администрирования производится доработка модели доступа пользователей и дополнительная настройка средств защиты в соответствии с нуждами и полномочиями пользователей.

Внесение любых изменений, модификаций, осуществление ремонта и обновлений программной или программно-технической составляющей системы осуществляется специалистами технической поддержки и администрирования, которые должны быть утверждены и согласованы с отделом защиты информации по заявкам, подтвержденным руководством отдела информационной безопасности в соответствии с имеющейся инструкцией, регулирующей какие-либо внешние манипуляции, несущие потенциальную угрозу целостности системы, её работоспособности или подвергающие опасности данные, обрабатываемые в системе [11].

В случае возникновения чрезвычайных ситуаций специалисты отделов технической поддержки и администрирования обязаны опираться на руководство (план) по обеспечению непрерывной работы и восстановления, подготовленного специалистами администрирования, проектирования и защиты информации стороны Исполнителя [7].

Сотрудники отделов информационной безопасности, администрирования и технической поддержки стороны Исполнителя обязаны провести инструктаж и обучение всех конечных пользователей с целью обеспечения использования системы в соответствии с инструкцией во избежание нарушений, поломок, утечек информации и несанкционированного доступа.

Специалистами отделов информационной безопасности, администрирования и технической поддержки стороны Исполнителя, либо стороны Заказчика, в соответствии с

дополнительным соглашением ведется непрерывный контроль за соблюдением правил функционирования, эксплуатации и настроек системы, в том числе настроек безопасности.

Заключение

Таким образом, в создании автоматизированной системы огромную роль играет непосредственное участие специалистов защиты информации с момента начала проектирования вплоть до вывода её из эксплуатации. Они не только принимают решения, которые, возможно, в дальнейшем могут повлиять на статус защищенности системы и всех внутренних данных, но и принимают участие в решении таких вопросов, как срок службы системы, гибкость и комфортность эксплуатации. Помимо интересов Заказчика, которые удовлетворяют специалисты информационной безопасности, должны быть соблюдены требования законодательства и регулирующих органов федерального уровня.

ЛИТЕРАТУРА

1. Безопасность Информационных Технологий (Курс БТ01): учебное пособие - 3-е изд. - М.: Учебный Центр «Информзащита», 2012. - 377 с.
2. Варлатая С.К. Алгоритм создания и введения в эксплуатацию информационных систем персональных данных / С.К. Варлатая, А.В. Белев, С.В. Ширяев // Доклады ТУСУРа - 2011. - №2. - с. 255-257.
3. Гагарина Л.Г., Киселев Д.В., Федотова Е.Л. Разработка и эксплуатация автоматизированных информационных систем: учебное пособие / Л.Г. Гагарина // М.: ИД «Форум» - ИНФРА-М, 2010. - 324 с.
4. Гришина Н.В. Организация комплексной системы защиты информации. - М.: Гелиос АРВ, 2012. - 256 с.
5. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия / Санкт-Петербург: БХВ-Петербург, 2013. - 747 с.
6. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности: Учебное пособие для вузов. - 2-е изд., испр. - М.: Горячая линия-Телеком, 2014. - 130 с.
7. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации / под ред. А.С. Маркова. - М.: Радио и связь, 2012. 192 с.
8. Поликарпов А.А. Подходы к созданию комплексной системы защиты информации с применением менеджмента информационной безопасности // Труды международного симпозиума «Надежность и качество». - 2015. - с. 75-75.
9. Тарасюк М.В. Защищенные информационные технологии. Проектирование и применение / М.В. Тарасюк - М.: Издательство Солон-пресс - 2011. - 192 с.
10. Цирлов В.Л. Основы информационной безопасности автоматизированных систем: краткий курс. - М.: Феникс, 2008. - 173 с.
11. Шаханова М.В. Современные технологии информационной безопасности: Учебно-методический комплекс. - ДВФУ. - 2013. - 180 с.
12. Руководящий документ Гостехкомиссии РФ. «Автоматизированные системы. Защита информации от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». - М.: ГТК РФ, 1992.

Varlataya Svetlana Kliment'evna
Far Eastern federal university, Russia, Vladivostok
E-mail: sk-varl@yandex.ru

Goncharenko Alexey Sergeevich
Far Eastern federal university, Russia, Vladivostok
E-mail: Goncharenko.as@students.dvfu.ru

Formation of information protection system and interaction between information departments in the creation of automated system

Abstract. Nowadays, when information technologies are maximally developed and integrated into the life of every person in any sphere of his life activity, when no enterprise manages without at least one of his own automated systems, the protection of processed, transmitted and stored data plays an important role. The creation of information security systems that serve to ensure the security of automated systems for various purposes (management, design, processing, etc.) often becomes problematic in terms of completeness and protection of information, which is one of the most important problems in the field of information security arising In consequence of a lack of theoretical and practical material. To curb the possibility of making a mistake in the formation of the system, you can use the material described, which discloses the process of creating a typical and average automated system at such stages as design, development, implementation, testing, commissioning and maintenance. This article outlines the precise procedure for carrying out the necessary measures related to the creation of an automated system from the point of view of an information security specialist who assumes the role of both the performer and the observer, supported by theoretical knowledge and practical experience.

Keywords: information security; information technologies; automated system; engineering; creation; documentation