УДК 004.056.5 Вестник УрФО № 3(49) / 2023, с. 61–67

Никитенко А.В., Бойков С.Ю.

DOI: 10.14529/secur230306

ЭТАПЫ ПРОВЕДЕНИЯ РАБОТ ПО ПРОЕКТИРОВАНИЮ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

В статье описываются этапы проведения работ по проектированию систем защиты информации. По результатам анализа нормативно-правовых актов в области защиты информации выделены такие этапы как: выявление и анализ информационных активов; формирование требований к защите информации; определение мер для нейтрализации угроз; создание системы защиты информации. Даны краткое описание каждого этапа и составляющих подэтапов, а также рекомендации по их реализации. Апробация реализации этих этапов проведена при подготовке студентами бакалавриата курсовых и выпускных квалификационных работ по проектированию систем защиты информации. Все такие работы были успешно защищены.

Ключевые слова: *система защиты информации, проектирование, нейтрализация угроз.*

Nikitenko A.V., Boykov S. Yu.

STAGES OF WORK ON THE DESIGN OF THE INFORMATION SECURITY SYSTEM

The article describes the stages of preparation of the works on the design of information security systems. Based on the results of the analysis of regulatory legal acts in the field of information protection, such stages are identified as: identification and analysis of information assets; formation of information protection requirements; determination of measures to neutralize threats; creation of an information protection system. A brief description of each stage and the components of the sub-stages, as well as recommendations for their implementation are given. The approbation of the implementation of these stages was carried out during the preparation by undergraduate students of course and final qualification works on the design of information security systems. All such works have been successfully protected.

Keywords: *information security system, design, threat neutralization.*

Вопросы проектирования систем защиты информации в настоящее время вызывают у специалистов серьезный интерес и были исследованы в работах В.И. Аверченкова [1], М.Ю. Рытова [2] и многих других. Однако, авторы, в основном, уделяют внимание математическому моделированию отдельных процессов или этапов функционирования систе-

мы, что, на наш взгляд, является трудно применимым для решения конкретных прикладных задач в области проектирования систем защиты информации.

Также возникают сложности и при подготовке таких специалистов, занимающихся защитой информации. В частности, студенты, обучающиеся по направлениям и профилям подготовки, связанным с информационной безопасностью, сталкиваются с необходимостью написания курсовых и выпускных квалификационных работ по проектированию систем защиты информации. Это вызывает у обучающихся определенные затруднения, связанные с необходимостью систематизации информации, полученной ранее в процессе обучения. Поэтому возникает необходимость четкого системного определения и описания этапов подготовки таких работ.

В связи с этим в статье предлагается ориентированный на специалистов-практиков вариант последовательности этапов проведения работ по проектированию систем защиты информации, основу которого составляют требования нормативно-правовых актов Российской Федерации, связанных с обеспечением защиты информации.

Понятие системы защиты информации и другие термины и определения в области защиты информации рекомендуется трактовать в соответствии с ГОСТ Р 50922 – 2006 [3] и иными нормативно-правовыми актами (законы, постановления правительства и т.д.), актуальными для объекта защиты.

Начальным этапом проведения работ по проектированию системы защиты информации является выявление и анализ информационных активов. Основным активом является та информация, которая требует защиты: персональные данные, коммерческая тайна и т.п. Фиксация такой информации позволяет установить места ее хранения и обработки, а также выявить каналы связи, которые используются при передаче такой информации. На основании этого определяются информационные системы, в которых обрабатывается защищаемая информация.

Выделим два подхода к выявлению информационных активов. Первый подход основан на анализе вычислительной инфраструктуры организации. Он предполагает исследование серверов, автоматизированных рабочих мест, коммутационного оборудования и описания информации, обрабатываемой на каждом средстве вычислительной техники, а также информационных потоков в вычислительной инфраструктуре. Результатом применения такого подхода является схема вычислительной инфраструктуры организации.

Второй подход предполагает анализ организационно-штатной структуры организации. При этом подходе путем интервьюирования представителей подразделений организации получают ответы на следующие типовые вопросы:

- Какая информация обрабатывается в подразделении?
- Какова значимость этой информации для подразделения?
- Какие средства вычислительной техники участвуют в обработке информации?
- Какие информационные технологии применяются при обработке информации?
- Каким подразделениям или сторонним организациям передается информация в процессе обработки?

Результатом применения второго подхода является схема информационных потоков подразделения или организации, предусматривающая выявление входящих и исходящих информационных потоков. Для достижения наиболее достоверных результатов первого этапа предлагается комбинировать оба описанных подхода и использовать информацию, полученную в рамках одного подхода, для проверки и уточнения информации, полученной в рамках другого подхода.

В результате выявления и анализа информационных активов организации должны быть определены: перечень защищаемой информации; перечень информационных систем, в которых обрабатывается защищаемая информация; сведения о средствах вычислительной техники и технологиях, применяемых для обработки защищаемой информации; сведения об используемых методах, средствах защиты информации, съемных носителях защищаемой информации, каналах связи; а также сведения о взаимодействии информационных систем.

Вторым этапом проведения работ по проектированию системы защиты информации является формирование требований, связанных с защитой информации. В рамках этого этапа проводится выделение требований нормативно-правовых актов к защите информации, моделирование нарушителей и угроз безопасности информации, а также категорирование (классификация) защищаемой информации.

Выделение требований нормативно-правовых актов к защите информации выполняется путем выявления требований законов, указов Президента РФ, постановлений правительства РФ, ведомственных и внутриорганизационных нормативных правовых актов в области защищаемой информации. Результаты такого выделения рекомендуется оформить таблично с указанием наименований нормативных правовых актов и требований к защите информации, связанных с каждым таким актом.

Модель нарушителя и угроз безопасности информации представляет собой документ, в котором описаны внешние и внутренние нарушители, а также актуальные угрозы безопасности защищаемой информации. Документ разрабатывается на основании действующих ведомственных нормативных правовых актов, например, методического документа ФСТЭК России [4].

Категорирование или классификация объектов защиты проводится на основании критериев, утвержденных в нормативных правовых актах, и состоит в отнесении объекта информатизации или обрабатываемой на нем информации к определенной категории (классу или уровню защищенности). Например, для персональных данных определяются уровни защищенности, а для государственных информационных систем классы защищенности. По результатам категорирования (классификации) оформляется специальный акт.

Формирование требований к защите информации завершается разработкой технического задания на проектирование системы защиты информации, в котором приводится, в том числе, краткое описание информационных систем.

Третьим этапом проведения работ по проектированию системы защиты информации является определение мер для нейтрализации угроз безопасности информации. В рамках этого этапа проводится выделение базового набора мер, его адаптация, уточнение и дополнение. В соответствии с приказами ФСТЭК России [5–8] в зависимости от вида объекта защиты определяется базовый набор мер. Адаптация базового набора мер представляет собой исключение из базового набора мер, связанных с характеристиками, не свойственными объекту защиты. Уточнение адаптированного базового набора мер как добавление мер проводится в соответствии с моделью угроз безопасности информации. По результатам заполняется Таблица 1, в ячейках которой должны хотя бы по разу присутствовать все меры из базового набора.

Затем выполняется дополнение уточненного адаптированного набора мерами, которые обусловлены требованиями других нормативных правовых актов, характерных для обеспечения безопасности объекта защиты. Результаты такого дополнения рекомендуется оформить таблично с указанием наименований нормативных правовых актов и мер, необходимых для дополнения набора и связанных с каждым таким актом.

Если на объекте защиты отсутствует возможность реализации отдельных мер из дополненного уточненного адаптированного

Таблица 1

Адаптация и уточнение базового набора мер

Угроза безопасности информации (УБИ), актуальная для объекта защиты (из модели УБИ)	Обозначение и номер меры или группы мер из базового набора мер (сопоставляется каждой УБИ, включенной в модель угроз)	Обозначение, номер меры или группы мер, которые включаются в адаптированный базовый набор мер дополнительно
УБИ 1	Мера 1, …, Мера k	-
…	…	…
УБИ n	-	Включенная мера 1, …, Включенная мера m
Меры, исключенные из базового набора (связаны с характеристиками, не свойственными объекту защиты):	Исключенная мера 1 (обоснование исключения меры из базового набора), …, Исключенная мера f (обоснование исключения меры из базового набора)	

базового набора, то необходимо также провести разработку компенсирующих мер. Для этого заполняется Таблица 2.

Таким образом, определяются все меры для нейтрализации угроз безопасности информации.

Четвертый этап проектирования системы защиты информации включает в себя создание самой системы: выбор средств защиты информации (желательно сертифицированных ФСТЭК России и / или ФСБ России), их установку на подверженные угрозам компьютеры и серверы, а также настройку параметров безопасности. Далее необходимо разработать организационно-распорядительную документацию по защите информации, определяющую правила и процедуры использования средств защиты информации, а также ответственность за их нарушение.

Для создания системы защиты информации рекомендуется подбирать средства защиты информации и организационные меры таким образом, чтобы каждая определенная выше мера для нейтрализации угрозы была реализуема с помощью хотя бы одного такого средства защиты и хотя бы одной организационной меры. Для разработки варианта реализации всех мер для нейтрализации угроз безопасности информации заполняется Таблица 3.

Таблица 2

Разработка компенсирующих мер

Мера из дополненного уточненного адаптированного базового набора мер, реализация которой невозможна	Обоснование невозможности реализации меры из дополненного уточненного адаптированного базового набора мер	Компенсирующая мера (меры), обеспечивающая нейтрализацию угроз безопасности информации	Обоснование применения компенсирующей меры (мер)
Мера 1	Обоснование невозможности реализации меры 1	Компенсирующая мера (меры) 1	Обоснование применения компенсирующей меры (мер) 1
…	…	…	…
Мера k	Обоснование невозможности реализации меры k	Компенсирующая мера (меры) k	Обоснование применения компенсирующей меры (мер) k

Таблица 3

Реализация мер для нейтрализации угроз безопасности информации

Мера для нейтрализации угроз безопасности информации	Вид средства защиты информации (СЗИ), позволяющий реализовать меру	Наименование организационно-распорядительного документа (ОРД), позволяющего реализовать меру
Мера 1	СЗИ 1	ОРД 1
…	…	…
Мера n	СЗИ n	ОРД n

Выбор конкретного средства защиты информации рекомендуется проводить с помощью метода анализа иерархий [9, с. 98–109] или другим обоснованным способом. Установка и настройка выбранного средства защиты информации производится способом, позволяющим реализовать конкретную меру для нейтрализации угроз безопасности информации. Необходимо привести схему мест установки выбранных средств защиты и скриншоты настроек.

Также разрабатывается система организационно-распорядительных документов по защите информации (положения, политики, приказы, инструкции и т.п.), содержание которых должно быть непротиворечиво и позволять реализовать конкретную меру для нейтрализации угроз безопасности информации.

Дополнительно при необходимости возможно проведение оценки соответствия объекта информатизации требованиям по защите информации, в рамках которой выполняется анализ защищенности и анализ рисков информационной безопасности. Анализ защищенности проводится путем использования

специальных средств анализа защищенности, например, «Сканер-ВС», MaxPatrol, XSpider, RedCheck и т.д. По результатам анализа не должно быть выявлено критичных уязвимостей. Анализ рисков информационной безопасности рекомендуется проводить в соответствии с ГОСТ Р ИСО/МЭК 27005 – 2010 [10]. Также возможно проведение анализа рисков по другим методикам с учетом особенностей объекта защиты. Сравнительная характеристика таких методик представлена в статье Е.К. Барановой [11]. По результатам анализа должно быть отмечено снижение рисков информационной безопасности до допустимых для объекта защиты значений. Также дополнительно возможно проведение тестирования на проникновение, например, с помощью Kali Linux [12].

Таким образом, описаны все этапы проведения работ по проектированию систем защиты информации. Наименования этапов и подэтапы представлены в Таблице 4.

Таблица 4

Этапы проведения работ по проектированию системы защиты информации

№	Наименование этапа	Подэтапы
1	Выявление и анализ информационных активов	Сбор информации о предприятии: определение защищаемой информации, анализ информационных потоков.
2	Формирование требований к защите информации	Выделение требований нормативно-правовых актов к защите информации. Моделирование нарушителей и угроз безопасности информации. Категорирование (классификация) информации.
3	Определение мер для нейтрализации угроз	Определение базового набора мер. Адаптация и уточнение базового набора мер. Дополнение уточненного адаптированного базового набора мер.
4	Создание системы защиты информации	Выбор, установка и настройка средств защиты информации. Разработка организационно-распорядительной документации по защите информации.

Опытная работа по реализации этих этапов проводилась в 2020–2023 гг. в ФГБОУ ВО «Ярославский государственный технический университет» при подготовке студентами бакалавриата курсовых и выпускных квалификационных работ по проектированию систем защиты информации. Все такие работы были успешно защищены, причем, оценку «Отлично» получили 76% работ, «Хорошо» – 20%, «Удовлетворительно» – 4%.

Литература

1. Аверченков В.И. Автоматизация проектирования систем инженерно-технической защиты информации / В.И. Аверченков, М.Ю. Рытов, Т.Р. Гайнулин // Вестник Белгородского университета потребительской кооперации. – Белгород. – 2006.

2. Актуальные проблемы выбора технических средств защиты информации многомерных структурно-перестраиваемых объектов: монография / Рытов М.Ю., Горлов А.П., Лысов Д.А. и др.; ФГБОУ ВО «Брянский гос. техн. ун-т», Приднестр. гос. ун-т им. Т.Г. Шевченко, Рыбницкий фил. ПГУ им. Т.Г. Шевченко. – Рыбница; Брянск. – 2019. – 170 с.

3. Национальный стандарт Российской Федерации «ГОСТ Р 50922 – 2006. Защита информации. Основные термины и определения» от 27.12.2006 № 373-ст // Федеральное агентство по техническому регулированию и метрологии. – 2006.

4. Методический документ «Методика оценки угроз безопасности информации» от 05.02.2021 // Федеральная служба по техническому и экспортному контролю. – 2021.

5. Приказ «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 18.02.2013 № 21 // Федеральная служба по техническому и экспортному контролю. – 2013.

6. Приказ «Об утверждении требований о защите информации, не составляющей государствен-

ную тайну, содержащейся в государственных информационных системах» от 11.02.2013 № 17 // Федеральная служба по техническому и экспортному контролю. – 2013.

7. Приказ «Об утверждении требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» от 14.03.2014 № 31 // Федеральная служба по техническому и экспортному контролю. – 2014.

8. Приказ «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25.12.2017 № 239 // Федеральная служба по техническому и экспортному контролю. – 2017.

9. Формализация подходов к обеспечению защиты персональных данных: монография / Голембиовская О.М. и др. – Саратов: Ай Пи Эр Медиа, 2019 – 198 с.

10. ГОСТ Р ИСО/МЭК 27005 – 2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» от 30.11.2010 № 632-ст // Федеральное агентство по техническому регулированию и метрологии. – 2011.

11. Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии. – 2015. – №1 (9). – С. 73–79.

12. Шива Парасрам, Алекс Замм, Дамиан Буду, Джерард Йохансен, Ли Аллен, Теди Хериянто, Шакил Али. Kali Linux. Тестирование на проникновение и безопасность. – 4-е изд. – СПб.: Питер, 2018. – 448 с.

References

1. Averchenkov V.I. Avtomatizacija proektirovanija sistem inzhenerno-tehnicheskoj zashhity informacii / V.I. Averchenkov, M.Ju. Rytov, T.R. Gajnulin // Vestnik Belgorodskogo universiteta potrebitel'skoj kooperacii. – Belgorod. – 2006.

2. Aktualnye problemy vybora tehnicheskih sredstv zashhity informacii mnogomernyh strukturno-perestraivaemyh obektov: monografija / Rytov M.Ju., Gorlov A.P., Lysov D.A. i dr.; FGBOU VO «Brjanskij gos. tehn. un-t», Pridnestr. gos. un-t im. T.G. Shevchenko, Rybnickij fil. PGU im. T.G. Shevchenko. – Rybnica; Brjansk. – 2019. – 170 s.

3. Natsionalnyj standart Rossijskoj Federatsii «GOST R 50922 – 2006. Zashchita informatsii. Osnovnye terminy i opredeleniya» ot 27.12.2006 № 373-st // Federalnoe agentstvo po tekhnicheskomu regulirovaniyu i metrologii. – 2006.

4. Metodicheskij dokument «Metodika otsenki ugroz bezopasnosti in-formatsii» ot 05.02.2021 // Federalnaya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. – 2021.

5. Prikaz «Ob utverzhdenii sostava i soderzhaniya organizatsionnykh i tekhnicheskikh mer po obespecheniyu bezopasnosti personalnykh dannykh pri ikh obrabotke v informatsionnykh sistemakh personalnykh dannykh» ot 18.02.2013 № 21 // Federalnaya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. – 2013.

6. Prikaz «Ob utverzhdenii trebovanij o zashchite informatsii, ne sostavlyayushchej gosudarstvennuyu tajnu, soderzhashchejsya v gosudarstvennykh informatsionnykh sistemakh» ot 11.02.2013 № 17 // Federalnaya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. – 2013.

7. Prikaz «Ob utverzhdenii trebovanij k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsialno opasnykh ob"ektakh, a takzhe ob"ektakh, predstavlyayushchikh povyshennuyu opasnost dlya zhizni i zdorovya lyudej i dlya okruzhayushchej prirodnoj sredy» ot 14.03.2014 № 31 // Federalnaya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. – 2014.

8. Prikaz «Ob utverzhdenii trebovanij po obespecheniyu bezopasnosti znachimykh ob"ektov kriticheskoj informatsionnoj infrastruktury Rossijskoj Federatsii» ot 25.12.2017 № 239 // Federalnaya sluzhba po tekhnicheskomu i eksportnomu kontrolyu. – 2017.

9. Formalizatsiya podkhodov k obespecheniyu zashchity personalnykh dan-nykh: monografiya / Golembiovskaya O.M. i dr. – Saratov: Aj Pi Er Media, 2019 – 198 s.

10. GOST R ISO/MEK 27005 – 2010 «Informatsionnaya tekhnologiya. Metody i sredstva obespecheniya bezopasnosti. Menedzhment riska informatsionnoj bezopasnosti» ot 30.11.2010 № 632-st // Federalnoe agentstvo po tekhnicheskomu regulirovaniyu i metrologii. – 2011.

11. Baranova E.K. Metodiki analiza i otsenki riskov informatsionnoj bezopasnosti // Obrazovatelnye resursy i tekhnologii. – 2015. – № 1 (9). – S. 73–79.

12. Shiva Parasram, Aleks Zamm, Damian Budu, Dzherard Jokhansen, Li Allen, Tedi Kheriyanto, Shakil Ali. Kali Linux. Testirovanie na proniknovenie i bezopasnost. – 4-e izd. – SPb.: Piter, 2018. – 448 s.

НИКИТЕНКО Андрей Владимирович, кандидат педагогических наук, доцент, кафедра «Информационные системы и технологии», ФГБОУ ВО «Ярославский государственный технический университет». 150023, г. Ярославль, Московский проспект, 88. E-mail: andnkt@mail.ru

NIKITENKO Andrey Vladimirovich, Candidate of Pedagogical Sciences, Associate Professor, Department of Information Systems and Technologies, Yaroslavl State Technical University. 150023, Yaroslavl, Moskovsky prospect, 88. E-mail: andnkt@mail.ru

БОЙКОВ Сергей Юрьевич, кандидат технических наук, заведующий кафедрой «Информационные системы и технологии», ФГБОУ ВО «Ярославский государственный технический университет». 150023, г. Ярославль, Московский проспект, 88. E-mail: boykovsy@ystu.ru

BOYKOV Sergey Yuryevich, Candidate of Technical Sciences, Head of Department, Department of Information Systems and Technologies, Yaroslavl State Technical University. 150023, Yaroslavl, Moskovsky prospect, 88. E-mail: boykovsy@ystu.ru