РОЛЬ И МЕСТО ЗАЩИТЫ ИНФОРМАЦИИ В ПРОГРАММЕ ПОДГОТОВКИ IT-СПЕЦИАЛИСТОВ

УДК 378.14

Андрей Иванович Волков,
к.т.н., доцент, профессор кафедры Автоматизированных систем обработки информации и управления Московского государственного университета экономики, статистики и информатики (МЭСИ)
Тел. (495) 442-61-11
Эл. почта: Volkov-AI@mesi.ru

Алла Юрьевна Ермакова,
старший преподаватель кафедры Математического обеспечения информационных систем и инноватики Московского государственного университета экономики, статистики и информатики (МЭСИ)
Тел. (495) 442-80-98
Эл. почта: AYErmakova@mesi.ru

В настоящей статье обсуждается значение проблематики, связанной с защитой информации, в процессе подготовки современных специалистов по информационным технологиям. Отмечается важность изучения IT-специалистами указанной проблематики и необходимость комплексного подхода к выбору и/или разработке систем защиты информации. Определяется содержание программы подготовки по информационной безопасности, а также объем знаний в области математики и информационных технологий, необходимый для освоения этой программы. Формулируются требования к результатам освоения указанной программы и отмечается необходимость включения вопросов защиты информации в курсовую и выпускную квалификационную работы.

Ключевые слова: *информационные технологии, информационная безопасность, угрозы информационной безопасности, средства защиты информации, подготовка IT-специалистов, выпускная квалификационная работа.*

Andrey I. Volkov,
PhD in Technical Sciences, Professor the Department of Automated systems information processing and management, Moscow State University of Economics, Statistics and Informatics (MESI)
Tel. (495) 442-61-11
E-mail: Volkov-AI@mesi.ru

Alla Yu. Ermakova,
Senior Lecturer the Department of Mathematical Software Information Systems and Innovations, Moscow State University of Economics, Statistics and Informatics (MESI)
Tel. (495) 442-80-98
E-mail: AYErmakova@mesi.ru

THE ROLE AND PLACE OF INFORMATION PROTECTION IN THE PROGRAM OF TRAINING OF IT-SPECIALISTS

This article discusses the importance of issues related to the protection of information in the preparation of modern information technology specialists. Notes the importance of studying IT-specialists of this perspective and the need for an integrated approach to the selection and/or development of information security systems. Define the content of training programs on information security, as well as the amount of knowledge in the field of mathematics and information technologies needed for the development of this program. Formulated requirements to the results of development of the program and noted the need to include the protection of information in coursework and final qualifying work.

Keywords: *information technology, information security, information security threats, means protection of information, preparation of IT-specialists, graduation thesis.*

Любое фундаментальное техническое или технологическое новшество, предоставляя возможности для решения одних социальных проблем и открывая широкие перспективы их развития, всегда вызывает обострение других или порождает новые, ранее неизвестные проблемы, становится для общества источником новых потенциальных опасностей. Иными словами, без должного внимания к вопросам обеспечения безопасности, последствия перехода общества к новым технологиям могут быть катастрофическими как для него, так и для его граждан. Именно так обстоит дело с информатизацией общества. Бурное развитие средств вычислительной техники открыло перед человечеством небывалые возможности по автоматизации умственного и физического труда и привело к созданию большого числа автоматизированных, информационных и управляющих систем в различных сферах деятельности.

В связи с этим, неправомерное искажение или фальсификация, уничтожение или разглашение определенной части информации, равно как и дезорганизация процессов ее обработки и передачи в информационно-управляющих системах наносят серьезный материальный и моральный урон многим субъектам (государству, юридическим и физическим лицам), участвующим в процессах информационного взаимодействия.

Острота проблемы обеспечения безопасности субъектов информационных отношений, защиты их законных интересов при использовании информационных и управляющих систем, хранящейся и обрабатываемой в них информации все более возрастает. Проблема защиты вычислительных систем становится еще более серьезной и в связи с развитием и распространением вычислительных сетей, территориально распределенных систем и систем с удаленным доступом к совместно используемым ресурсам.

Доступность средств вычислительной техники и, прежде всего персональных электронно-вычислительных машин, привела к распространению компьютерной грамотности в широких слоях населения, что закономерно, привело к увеличению числа попыток неправомерного вмешательства в работу государственных и коммерческих автоматизированных систем, как со злым умыслом, так и «из спортивного интереса». Несмотря на введение соответствующих статей в Уголовный кодекс РФ, постоянно возрастает число компьютерных преступлений. По оценкам специалистов ущерб от действий злоумышленников, наносимый коммерческим организациям и частным лицам, ежегодно составляет сотни миллионов рублей.

Еще одним весомым аргументом в пользу усиления внимания к вопросам безопасности вычислительных систем является бурное развитие и распространение, так называемых, компьютерных вирусов, способных скрытно существовать в системе и совершать потенциально любые несанкционированные действия.

Из сказанного выше следует, что в настоящее время квалифицированный IT-специалист должен владеть основами информационной безопасности, знать в этой области нормативную базу, уметь анализировать и оценивать угрозы информационной безопасности, иметь опыт применения современных методов и средств защиты информационных систем.

В связи со сложностью задач защиты информации и многообразием угроз информационным системам, следует акцентировать внимание слушателей на необходимости комплексного подхода к выбору и/или разработке систем защиты информации.

Студенты IT-направлений должны знать основные требования безопасности информационных систем, стандарты безопасности, уметь применять правовые, организационные, технические и другие методы и средства защиты информации [1, 2]. В связи с этим, любая программа подготовки IT-специалистов, в части изучения вопросов обеспечения информационной безопасности, должна включать следующие разделы:

– правовые основы защиты информации;

– организационно-технические методы защиты информации;

– программно-аппаратные методы и средства защиты информации;

– криптографические методы защиты информации;

– методы защиты программ, данных и операционных систем от несанкционированного доступа и различных негативных воздействий;

– общие вопросы защиты информационных систем.

Изучение дисциплины «Информационная безопасность» (или «Защита информации») рекомендуется начинать с правовых основ защиты информации и рассмотреть следующие вопросы:

− понятие, содержание и сущность безопасности, виды безопасности;

− место информационной безопасности в системе национальной безопасности РФ;

− источники угроз информационной безопасности;

− правовое обеспечение информационной безопасности в России, законы РФ «Об информации, информационных технологиях и защите информации», «О государственной тайне», «О коммерческой тайне», «О персональных данных».

В разделе, посвященном организационно-техническим мерам защиты информации, следует рассмотреть вопросы:

− цели и задачи защиты информации;

− факторы, воздействующие на защищаемую информацию, классификация источников угроз информации;

− угрозы нарушения конфиденциальности, целостности и доступности информации;

− причины, виды и каналы утечки информации;

− модели нарушителя, построение моделей угроз;

− политика безопасности предприятия, методы оценки рисков;

− физическая защита;

− защита информации от утечек по техническим каналам связи;

− защита поддерживающей инфраструктуры.

Один из центральных разделов курса должен быть посвящен изучению программно-аппаратных методов и средств защиты информации [1, 2]. При этом необходимо рассмотреть следующие вопросы:

− идентификация и аутентификация;

− разграничение прав доступа;

− экранирование и туннелирование;

− протоколирование и аудит;

− контроль целостности;

− антивирусная защита.

Как отмечают специалисты, в настоящее время наиболее надежными средствами защиты информации являются криптографические алгоритмы и построенные на их основе протоколы защищенного обмена информацией и цифровые подписи [3]. Криптографические средства являются неотъемлемой частью штатных средств защиты современных информационных систем и программных продуктов, предназначенных для безопасной передачи и хранения информации [4], в частности, криптографические алгоритмы широко применяются для защиты электронных платежей. В данном разделе целесообразно изучить следующие вопросы:

− определение шифра, простейшие виды шифров;

− основные узлы и блоки симметричных криптографических алгоритмов;

− понятия стойкости криптографических преобразований; временная, практическая, теоретическая стойкость;

− отечественные и зарубежные стандарты шифрования;

− открытое распределение ключей, асимметричные алгоритмы шифрования, схемы шифрования RSA, Эль Гамаля;

− цифровая подпись, хэш-функции;

− криптографические протоколы.

В следующем разделе, посвященному изучению методов защиты программ, данных и операционных систем от несанкционированного доступа и различных негативных воздействий, следует рассмотреть следующие вопросы:

− классификация способов защиты;

− защита от закладок и дизассемблирования;

− способы встраивания закладок в программное обеспечение;

− понятие разрушающего программного воздействия;

− модели взаимодействия прикладной программы и прикладной закладки;

− методы перехвата и навязывания информации;

− методы внедрения программных закладок;

− компьютерные вирусы как особый класс разрушающих программных воздействий;

− защита от разрушающих программных воздействий;

− понятие изолированной программной среды.

Завершить изучение дисциплины рекомендуется рассмотрением общих вопросов защиты информационных систем таких как:

− защита от сбоев программно-аппаратной среды;

− правила разработки программного обеспечения;

− предотвращение ошибок и неточностей в программном обеспечении;

− защита семантического анализа и актуальности информации;

− построение систем защиты от угроз раскрытия параметров информационной системы;

− иерархический метод разработки программного обеспечения;

− исследование корректности реализации и верификации;

− теория безопасных систем.

Как отмечено выше, задачи обеспечения информационной безопасности являются сложными и многообразными, и для успешного овладения современными методами защиты информации слушатели должны иметь всестороннюю подготовку в области математики и информационных технологий и владеть следующими знаниями и навыками:

− основами теории множеств (понятие множества, теоретико-множественные операции);

− основами теории алгоритмов (понятие и свойства алгоритма);

− элементами вышей алгебры (теория групп, колец, полей);

– знаниями архитектуры средств вычислительной техники и компьютерных сетей;

− основами программирования (типы и структуры данных, процедуры, функции);

− навыками работы с основными операционными системами;

− навыками работы с информацией в глобальных компьютерных сетях.

В результате изучения дисциплины «Информационная безопасность» студенты должны приобрести знания и навыки по:

– анализу и оценке угроз информационной безопасности;

– постановке и решению задачи обеспечения информационной безопасности компьютерных систем и сетей;

– моделированию средств обеспечения безопасности компьютерных систем, в том числе моделирования управления доступом и информационными потоками в компьютерных системах и сетях;

− обеспечению безопасности операционных систем;

– разработке модели угроз и модели нарушителя безопасности компьютерных систем;

– разработке политики безопасности компьютерных систем и сетей, в том числе политики управления доступом и информационными потоками;

– применению технических, программных и криптографических средств для защиты компьютерных систем и сетей;

– анализу показателей качества и критериев оценки эффективности систем и отдельных методов и средств защиты информации.

В соответствии с образовательными стандартами по укрупненной группе направлений «Информатика и вычислительная техника», изучение дисциплины «Информационная безопасность» направлено на формирование следующих компетенций:

− способности разрабатывать формальные модели политик безопасности, политик управления доступом и информационными потоками в компьютерных системах и сетях;

− способности проводить анализ безопасности компьютерных систем и сетей с использованием отечественных и зарубежных стандартов в области компьютерной безопасности;

− способности проводить обоснование и выбор рационального решения по уровню защищенности компьютерной системы с учетом заданных требований;

− способности участвовать в разработке системы защиты информации компьютерной системы и сети;

− способности оценивать степень надежности выбранных механизмов обеспечения безопасности для решения поставленной задачи;

− способности обосновывать правильность выбранной модели решения профессиональной задачи, сопоставлять экспериментальные данные и теоретические решения;

− способности оценивать эффективность систем защиты информации в компьютерных системах и сетях.

В связи со сложностью и многообразием задач и необходимостью получения значительного количества практических навыков, изучение дисциплины «Информационная безопасность» целесообразно проводить в виде лекционных, практических занятий и лабораторных работ.

В рамках проведения самостоятельной работы рекомендуется выполнение студентами курсовой работы. В ходе подготовки курсовой работы студенты должны проанализировать угрозы безопасности конкретной информационной системы или компьютерной сети, выбрать необходимые методы и средства защиты от угроз безопасности и оценить эффективность принятых решений. Для обеспечения необходимого качества подготовки по дисциплине общее количество аудиторных часов должно составлять не менее половины общего количества часов, отведенного на изучение дисциплины. На изучении дисциплины рекомендовано отводить 180 часов.

При проведении лекционных занятий целесообразно применять такую форму как лекция-визуализация, сопровождая изложение теоретического материала презентациями, при этом желательно заблаговременно обеспечить студентов раздаточным материалом.

Основной упор в методике проведения практических занятий и лабораторных работ должен быть сделан на отработке и закреплении учебного материала в процессе выполнения заданий с применением средств вычислительной техники в компьютерном классе. Особое внимание при этом должно быть уделено применению элементов проблемного и контекстного обучения, опережающей самостоятельной работе студентов. Для упрощения подготовки тестовых стендов на практических и лабораторных занятиях целесообразно использовать технологии виртуализации.

Текущий контроль усвоения знаний осуществляется путем выполнения контрольных заданий и тестов, подготовки и защиты отчетов по лабораторным работам.

При подготовке выпускной квалификационной работы вопросам обеспечения информационной безопасности целесообразно посвятить отдельный раздел. В нем необходимо рассмотреть вопросы, связанные с угрозами информационной безопасности объекта проектирования, средствами защиты от этих угроз и обоснованием их эффективности

[5], руководствуясь при этом требованиями отечественных и международных стандартов [6, 7]. Для решения поставленной задачи следует провести выявление и учет факторов, воздействующих на защищаемую информацию в конкретных условиях и, составляющих основу для выбора средств защиты информации. При этом в соответствии [6], под фактором, воздействующим на защищаемую информацию, следует понимать явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации или блокировка доступа к ней.

Согласно [6] организация обеспечения информационной безопасности должна носить комплексный характер, а выбор средств основываться на анализе негативных последствий, который предполагает обязательную идентификацию возможных источников угроз, факторов, способствующих их проявлению (уязвимостей) и, как следствие, определение актуальных угроз и возможных рисков информационной безопасности [8]. Исходя из этого, моделирование и классификацию источников угроз и их проявлений, целесообразно проводить на основе анализа взаимодействия в виде логической цепочки (рис. 1).

Под источником угроз при этом понимаются потенциальные антропогенные, техногенные и стихийные угрозы безопасности. Под угрозой (в целом) понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба интересам владельца или пользователя информационной системы. Под угрозой интересам субъектов информационных отношений понимают потенциально возможное событие, процесс или явление которое посредством воздействия на информацию или другие компоненты ИС может прямо или косвенно привести к нанесению ущерба интересам данных субъектов.

Под уязвимостью понимаются причины, присущие объекту информационной системы, приводящие к нарушению безопасности информации на конкретном объекте и обусловленные недостатками процесса функционирования информационной системы, свойствами ее архитектуры, протоколами обмена и интерфейсами, применяемым программным обеспечением и аппаратной платформой, условиями эксплуатации, невнимательностью сотрудников.

Чаще всего угроза является следствием наличия уязвимых мест в защите информационных систем (таких как возможность доступа посторонних лиц к оборудованию или ошибки в программном обеспечении).

Последствия – это возможные действия реализации угрозы при взаимодействии источника угрозы через имеющиеся уязвимости.

К основным угрозам информации относят:

– хищение (копирование информации);

– уничтожение информации;

– нарушение доступности (блокирование) информации;

– уничтожение информации;

– модификация (искажение) информации;

– отрицание подлинности информации;

– навязывание ложной информации.

Знание возможных угроз, а также уязвимых мест, через которые угрозы могут осуществляться, необходимо для того, чтобы выбрать эффективные средства защиты от них.

Система защиты информации (СЗИ) – совокупность взаимосвязанных средств, методов и мероприятий, направленных на предотвращение уничтожения, искажения, несанкционированного получения конфиденциальных сведений, отображенных полями, электромагнитными, световыми и звуковыми волнами или вещественно-материальными носителями в виде сигналов, образов, символов, технических решений и процессов.

Выявление и учет факторов, воздействующих или могущих воздействовать на защищаемую информацию в конкретных условиях, составляют основу для планирования и проведения эффективных мероприятий, направленных на защиту информации на объекте информатизации. Полнота и достоверность выявленных факторов, воздействующих или могущих воздействовать на защищаемую информацию, достигаются путем рассмотрения полного множества факторов, воздействующих на все элементы информационной системы (технические и программные средства обработки информации, средства обеспечения и т. д.) и на всех этапах обработки информации.

При рассмотрении вопросов защиты информационной системы целесообразно использовать четырехуровневую градацию доступа к хранимой, обрабатываемой и защищаемой информации, которая позволит систематизировать как возможные угрозы, так и меры по их нейтрализации:

1. Уровень носителей информации.

2. Уровень средств взаимодействия с носителем.

3. Уровень представления информации.

4. Уровень содержания информации.

Данные уровни введены, исходя из того, что, во-первых, информация для удобства работы с ней чаще всего фиксируется на некотором материальном носителе, которым может быть бумага, компакт диск, USB-флеш-накопитель, кассета и т.д. Во-вторых, если способ представления информации таков, что она не может быть непосредственно воспринята человеком, то возникает необходимость в преобразователях информации в доступный для человека способ представления. Например, для чтения информации

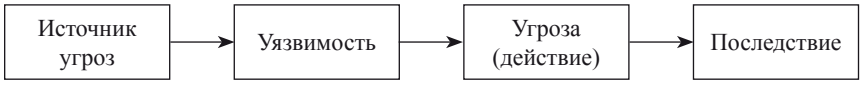

Рис. 1. *Логическая цепочка угроз и их проявлений*

с USB-флеш-накопителя необходим компьютер, оборудованный USB-портом соответствующего типа. В-третьих, как уже было отмечено, информация может быть охарактеризована способом своего представления или тем, что еще называется языком в обиходном смысле. Язык жестов, язык символов и т.п. – все это способы представления информации. В-четвертых, человеку должен быть доступен смысл представленной информации, ее семантика.

Защита носителей информации должна обеспечивать минимизацию рисков от реализации всех возможных угроз, направленных как на сами носители, так и на помещенную в них информацию, представленную в виде изменения состояний отдельных участков, блоков, полей носителя. Применительно к автоматизированным системам обработки информации защита носителей информации в первую очередь подразумевает защиту машинных носителей. Вместе с тем, необходимо учитывать, что носителями информации являются также каналы связи, документальные материалы, получаемые в ходе эксплуатации системы. Защита средств взаимодействия с носителем охватывает спектр методов защиты программно-аппаратных средств, входящих в состав автоматизированной системы, таких, как средства вычислительной техники, операционная система, прикладные программы. В основном защита на данном уровне рассматривается как защита от несанкционированного доступа, обеспечивающая разграничение доступа пользователей к ресурсам системы.

Защита информации, представленной в виде последовательности символов, обеспечивается средствами криптографической защиты. Защита содержания информации обеспечивается семантической защитой данных.

Таким образом, для построения защищенной информационной системы, в зависимости от решаемых ею задач, условий эксплуатации и возможных угроз ее безопасности, разработчиками, в качестве которых в рассматриваемой ситуации выступают студенты-дипломники, могут применяться встроенные (штатные) средства защиты информационной системы, а при их недостаточной эффективности могут привлекаться дополнительные организационные и технические (программно-аппаратные, криптографические и др.) средства.

Обязательным элементом построения защиты информационной системы является анализ достаточности применяемых методов и средств. Первым шагом в этом направлении является сопоставление выявленных угроз и предлагаемых защитных механизмов. Более полным обоснованием является оценка рисков нарушения информационной безопасности и сопоставление их с допустимым уровнем потерь.

В заключение следует еще раз подчеркнуть исключительно важную роль изучения вопросов информационной безопасности в процессе обучения современных квалифицированных IT-специалистов. Стоит надеяться, что данные рекомендации помогут при разработке и реализации указанной дисциплины, а также при подготовке выпускной квалификационной работы.

Литература

1. А.С. Кабанов, А.Б. Лось, В.И. Трунцев. Основы информационной безопасности. Учебное пособие. – М.: РИО МИЭМ, 2012.

2. А.С. Кабанов, А.Б. Лось, А.С. Першаков. Теоретические основы компьютерной безопасности. Учебное пособие. – М.: РИО МИЭМ, 2012.

3. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. Основы криптографии. – М: Гелиос, 2001.

4. А.Ю. Ермакова, А.Б. Лось. О защите информации в облачных средах // Научный журнал «Апробация», №12, 2014. – С. 16–20.

5. Волков А.И. Методические вопросы организации дипломного проектирования // «Совершенствование IT-специалистов по направлению «Прикладная информатика» для инновационной экономики»: сборник статей научно-методической конференции (2 декабря 2014 г.). – М.: МЭСИ, 2014. – С. 27–31.

6. Российский стандарт информационной безопасности ГОСТ Р 51275. – 2006.

7. Международный стандарт информационной безопасности ИСО МЭК 27000.

8. А.С. Кабанов, А.Б. Лось, В.И. Трунцев. Основы управления рисками информационной безопасности. Учебное пособие. – М.: РИО МИЭМ, 2012. – 73 с.

References

1. Kabanov A.S., Los A.B., Truntsev V.I. Fundamentals of Information Security. Textbook. – M.: RIO MIEM. – 2012. – 163 p.

2. Kabanov A.S., Los A.B., Pershakov A.S. Theoretical Foundations of Computer Security. Textbook. – M.: RIO MIEM. – 2012. – 245 p.

3. Alferov A.P., Zubov A.Y., Kuzmin A.S., Cheremushkin A.V. Basics cryptography. – M.: Helios. – 2001. – 480 p.

4. Ermakova A.Y., Los A.B. About protection of information in cloud environments // Scientific journal «Aprobatsyia», №12, 2014. – P. 16–20.

5. Volkov A.I. Methodological issues of organizing graduate design // «Improving IT-specialists in Applied Computer Science for the innovation economy»: a collection of articles Scientific Conference. – M.: MESI, 2014. – P. 27–31.

6. Russian information security standards GOST R 51275. – 2006.

7. The international standard ISO information security IEC 27000.

8. Kabanov A.S., Los A.B., Truntsev V.I. Fundamentals of information security risk management. Textbook. – M.: RIO MIEM, 2012. – 73 p.