УДК 004.056

А.А. Костырин[1]

КИБЕРБЕЗОПАСНОСТЬ СЕТЕЙ СВЯЗИ И РАЗРАБОТКА СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

Статья посвящена актуальному вопросу. Дается характеристика угроз киберсреды, их перечень и виды. Также ценным в этой статье является описание стадий создания системы защиты информации.

Ключевые слова: *кибербезопасность, киберсреда, угрозы безопасности, уровни безопасности, защита информации.*

A.A. Kostyrin

CYBERSECURITY OF COMMUNICATION NETWORKS AND DEVELOPMENT OF DATA PROTECTION SYSTEMS

The article is devoted to topical issues. The characteristic of cyberthreats and types of their list are given. Just valuable in this article is to describe the steps of creating a system of information protection.

Keywords: *cybersecurity, cyberenvironment, threats to security, levels of security, information security.*

В настоящее время сравнительно легко можно получать информацию, общаться, наблюдать и управлять системами IT на значительных расстояниях. Современные сети играют ключевую роль во многих инфраструктурах государственной важности: электронной торговле, передаче данных и голоса, коммунальных услуг, финансовой, здравоохранения, транспорта и обороны.

Однако широкий доступ и слабая связь взаимосвязанных систем IT может стать первичным источником широко распространенной уязвимости. Для систем, объединенных в сеть, возрастают угрозы, такие, как: взлом в виде «отказ в обслуживании», кража финансовых и личных сведений, сбои в работе сети, нарушение речевой связи и дистанционной передачи данных.

Угрозы для автоматизированных систем быстро возрастают. Вирусы, черви, троянские кони, кража идентичности, спам и кибератаки находятся на подъеме. Необходимо понимание кибербезопасности для построения фундамента тех знаний, которые помогут обезопасить сети завтрашнего дня.

В современных сетях границы между внутренними и внешними сетями становятся более размытыми. Предполагается, что между этими уровнями обеспечена безопасность. Уровневый подход к проблеме безопасности дает возможность создания множества уровней защиты, направленных против угроз.

[1] Преподаватель Военно-космической академии им. А.Ф. Можайского.

Технологии кибербезопасности могут использоваться для гарантирования готовности систем, целостности, аутентичности, конфиденциальности и строгого выполнения обязательств. Технологии кибербезопасности могут использоваться для гарантий соблюдения личной тайны пользователя. Технологии кибербезопасности могут использоваться для установления достоверности пользователя.

Технологии, такие, как беспроводные сети и передача голоса по Интернету, расширяют область влияния и масштаб Интернета. В связи с этим, киберсреда включает пользователей, Интернет, компьютерные устройства, которые подключены к нему, все приложения, услуги и системы, которые могут напрямую или опосредованно подключаться к Интернету, и среду сетей последующих поколений, доступных для общего и частного применения. При использовании технологий Интернета даже настольный телефон может является частью киберсреды.

Даже изолированные устройства также могут являться частью киберсреды, если они могут пользоваться информацией совместно с компьютерными устройствами, подключаемыми с помощью сменных носителей. И, следовательно, на них могут оказывать воздействие разнообразные вредоносные программы – вирусы, черви, троянские программы, перехватчики и подобные им программы. В целях противодействия возможным атакам рекомендуется применять специальные меры борьбы с ними, например анти-

вирусные программы и иные новые разработки специалистов в области защиты киберсреды.

В киберпространство входит программное обеспечение, которое работает в компьютерных устройствах, информация, которая сохраняется (и передается) в этих устройствах, или информация, которая создается этими устройствами. Оборудование и здания, в которых расположены эти устройства, также являются частью киберпространства. Такие элементы должны приниматься в расчет для обеспечения безопасности.

Кибербезопасность подразумевает:

– совокупность политик и действий, которые должны быть предприняты для защиты соединенных сетей (включая компьютеры, устройства, аппаратные средства, хранящуюся информацию и передаваемую информацию) от несанкционированного доступа, изменения, кражи, разрушения и других угроз;

– текущую оценку и мониторинг вышеуказанных политик и действий для гарантии непрерывного качества безопасности перед лицом изменяющейся природы угроз.

К элементам, составляющим киберсреду, следует относить не только базовые станции, коммутаторы и абонентские терминалы. В ее состав входят также и периферийные устройства, такие, как принтеры, сканеры, факсимильные аппараты, которые сегодня в большинстве случаев являются сетевыми.

Любой элемент киберсреды может рассматриваться, как риск для безопасности, который в общем случае воспринимается как комбинированная оценка угрозы. В анализ угрозы входит задача описания типа возможных взломов, методы осуществления попытки нарушения защиты и последствия в случае успешных взломов. Оценка рисков вместе с анализом угрозы позволяют организации просчитать потенциальный риск для своей сети.

Попытки нарушения защиты могут исходить из киберсреды, такие, как взломы, посредством червей или других вредоносных программ, могут быть прямые попытки нарушения защиты важной инфраструктуры, такой, как кабели электросвязи, или взломы, вызванные действиями доверенного, хорошо осведомленного человека. Сочетание этих попыток нарушения защиты также возможно. Риски обычно характеризуются как высокие, средние и низкие. Уровень риска изменяется среди разных компонентов киберсреды.

Кибербезопасность заключается в управлении рисками. Для управления рисками могут использоваться разные технологии:

– разработка стратегии защиты, определяющая меры противодействия, которые могут быть предприняты при возможных попытках нарушения защиты;

– обнаружение, в которое входит идентификация взлома в момент его развития и впоследствии;

– формулировка отклика на попытку нарушения защиты, в которой определяется совокупность мер противодействия этой попытке для того, чтобы ее остановить или снизить ее влияние;

– формулировка стратегии восстановления, которая дает возможность сети возобновить работу с известного состояния.

Согласно Рекомендации МСЭ-Т X.800 (ITU-T X.800), в перечень угроз для системы передачи данных включены следующие:

– уничтожение информации и/или других ресурсов;

– искажение или изменение информации;

– кража, перемещение или потеря информации и/или других ресурсов;

– раскрытие информации;

– прерывание обслуживания.

В соответствии с ITU-T X.800, угрозы могут классифицироваться как случайные или преднамеренные, и они могут быть активными и пассивными. Случайными угрозами являются такие угрозы, которые возникают без предварительного умысла. Примерами реализованных случайных угроз являются: эксплуатация неисправного оборудования, неквалифицированный ремонт компьютерной и иной цифровой техники, неправильное срабатывание системы, грубые просчеты в работе и ошибки в программном обеспечении.

Преднамеренные угрозы могут классифицироваться от непредусмотренной экспертизы, использующей легкодоступные инструменты мониторинга, до сложных попыток нарушения защиты, использующих специальные системные знания. Преднамеренная угроза, если она реализована, может быть воспринята, как «попытка нарушения защиты».

Пассивными угрозами являются такие, которые, если они реализованы, не приводят к какому-либо изменению информации, заключенной в системе, и при которых не изменяется ни работа, ни состояние системы. Использование пассивного подслушивающего оборудования для наблюдения за информацией, передаваемой по подключенной линии, является реализацией пассивной угрозы.

Активные угрозы для системы включают в себя изменение информации, содержащейся в

системе, или изменения в состоянии или работе этой системы. Злонамеренное изменение таблиц маршрутизации системы несанкционированным пользователем является примером активной угрозы.

Таким образом, до начала разработки системы безопасности нужно идентифицировать конкретные угрозы, против которых понадобится защита. Этот анализ известен как оценка угроз.

В оценку угроз включены:

– идентификация уязвимых мест системы;

– анализ вероятности угроз, нацеленных на использование этих уязвимых мест;

– оценка последствий, если каждая угроза будет успешно выполнена;

– оценка стоимости каждой попытки нарушения защиты;

– расчет стоимости потенциальных мер противодействия;

– выбор механизмов безопасности, которые оправданны (возможно с помощью использования анализа стоимостной выгоды).

В ITU-T X.805 фактором безопасности является совокупность мер безопасности, разработанных для определенного аспекта безопасности сетей. В ITU-T X.805 определяются восемь факторов, которые защищают от всех основных угроз безопасности. Эти факторы не ограничиваются сетями, а также распространяются на приложения и информацию конечного пользователя.

Факторами безопасности являются:

– контроль доступа;

– аутентификация;

– неотказуемость;

– конфиденциальность данных;

– безопасность связи;

– целостность данных;

– готовность;

– секретность.

Для того чтобы обеспечить решение вопроса сквозной безопасности связи, факторы безопасности должны применяться к иерархии сетевого оборудования и группировкам средств, которые рассматриваются как уровни безопасности.

Различают три уровня безопасности:

1) уровень безопасности инфраструктуры;

2) уровень безопасности услуг;

3) уровень безопасности приложений.

Уровни безопасности устанавливают, где в продуктах и решениях принимается во внимание обеспечение безопасности путем предоставления последовательной структуры безопасности сетей. Например, сначала обращаются к уязвимым местам с точки зрения безопасности для уровня инфраструктуры, затем – для уровня услуг и для уровня приложений. Факторы безопасности применяются к уровням безопасности для того, чтобы уменьшить количество уязвимых мест, присутствующих в каждом уровне.

В ITU-T X.805 определены три плоскости безопасности для представления трех типов защищенных действий, которые происходят в сети:

1) плоскость управления;

2) плоскость контроля;

3) плоскость конечного пользователя.

Эти плоскости безопасности предназначены для конкретных нужд безопасности, связанных с деятельностью управления сетью, контроля сети или деятельностью по передаче сигналов и деятельностью конечного пользователя, соответственно. В ITU-T X.805 предлагается разрабатывать сети таким образом, чтобы события на одной плоскости безопасности хранились изолированно от других плоскостей безопасности.

Концепция плоскостей безопасности позволяет установить различия в конкретных вопросах безопасности, связанных с этими видами деятельности, и дает возможность обращаться к ним независимым образом.

Разработка систем защиты информации производится подразделением организации или специализированными организациями, имеющими лицензии ФСТЭК (Гостехкомиссии) России. При этом разрабатываются методическое руководство и конкретные требования по защите информации, аналитическое обоснование необходимости создания системы защиты информации (СЗИ), согласовывается выбор основных технических средств и систем (ОТСС) и вспомогательных технических средств и систем (ВТСС), технических и программных средств защиты информации (ЗИ), организуются работы по выявлению возможных каналов утечки информации и нарушения целостности защищаемой информации, аттестация объекта информатизации.

Стадии создания системы защиты информации

1. Предпроектная стадия, включающая предпроектное обследование объекта информатизации, разработку аналитического обоснования необходимости создания СЗИ и технического (частного технического) задания на ее создание.

2. Стадия ввода в действие СЗИ, включающая опытную эксплуатацию и приемо-сдаточные испытания средств защиты информации, а также аттестацию объекта информатизации на соответствие требованиям безопасности информации.

3. Стадия проектирования (разработки проектов), включающая разработку СЗИ в составе объекта информатизации.

По результатам предпроектного обследования разрабатывается аналитическое обоснование необходимости создания СЗИ и задаются конкретные требования по защите информации, включаемые в техническое (частное техническое) задание на разработку СЗИ.

Работы, выполняемые на предпроектной стадии, следующие.

1. Устанавливается необходимость обработки (обсуждения) информации на данном объекте информатизации.

2. Определяется перечень сведений конфиденциального характера, подлежащих защите.

3. Определяются (уточняются) угрозы безопасности информации и модель вероятного нарушителя применительно к конкретным условиям функционирования объекта.

4. Определяются условия расположения объекта информатизации.

5. Определяются конфигурация и топология ОТСС в целом и их отдельных компонентов, физические, функциональные и технологические связи ОТСС с другими системами различного уровня и назначения.

6. Определяются конкретные технические средства и системы, предполагаемые к использованию в разрабатываемой автоматизированной системе (АС), условия их расположения, их программные средства.

7. Определяются режимы обработки информации в АС в целом и в отдельных компонентах.

8. Определяется класс защищенности АС.

9. Определяется степень участия персонала в информации, характер их взаимодействия между собой и со службой безопасности.

10. Определяются мероприятия по обеспечению конфиденциальности информации на этапе проектирования объекта информатизации.

Аналитическое обоснование подписывается руководителем организации, проводившей предпроектное обследование, согласовывается с должностным лицом, обеспечивающим научно-техническое руководство создания объекта информатизации, руководителем службы безопасности и утверждается руководителем организации-заказчика.

Аналитическое обоснование необходимости создания СЗИ включает в себя следующее:

1) информационная характеристика и организационная структура объекта информатизации;

2) характеристика комплекса ОТСС и ВТСС, программного обеспечения, режимов работы, технологического процесса обработки информации;

3) возможные каналы утечки информации и перечень мероприятий по их устранению и ограничению;

4) перечень предлагаемых к использованию сертифицированных средств защиты информации;

5) обоснование необходимости привлечения специализированных организаций;

6) оценка материальных, трудовых и финансовых затрат на разработку и внедрение СЗИ;

7) ориентировочные сроки разработки и внедрения СЗИ;

8) перечень мероприятий по обеспечению конфиденциальности информации на стадии проектирования объекта информатизации.

Техническое задание на проектирование объекта информатизации оформляется отдельным документом, согласовывается с проектной организацией, службой (специалистом) безопасности организации-заказчика и утверждается заказчиком.

Содержание технического задания должно содержать следующее.

1. Обоснование разработки.

2. Исходные данные создаваемого (модернизируемого) объекта информатизации в техническом, программном, информационном и организационном аспектах.

3. Класс защищенности АС.

4. Ссылка на нормативные документы, на основании которых будет разрабатываться СЗИ.

5. Требования к СЗИ на основе нормативно-методических документов и установленного класса защищенности АС.

6. Перечень предполагаемых к использованию сертифицированных средств защиты информации.

7. Обоснование проведения разработок собственных средств защиты информации, невозможности или нецелесообразности использования имеющихся на рынке сертифицированных средств защиты информации.

8. Состав, содержание и сроки проведения работ по этапам разработки и внедрения.

9. Перечень подрядных организаций-исполнителей видов работ.

10. Перечень предъявляемой заказчику научно-технической продукции и документации.

Мероприятия по защите информации от утечки по техническим каналам относятся к основным элементам проектных решений, которые включаются в соответствующие разделы проекта и разрабатываются одновременно с ними.

При вводе в эксплуатацию выполняются необходимые мероприятия, такие, как опытная экс-

плуатация средств защиты информации с другими техническими и программными средствами для проверки их работоспособности в комплексе и отработки технологического процесса обработки (передачи) информации, приемо-сдаточные испытания средств защиты информации по результатам опытной эксплуатации, аттестация объекта информатизации по требованиям безопасности информации.

При этом разрабатываются следующие документы.

1. Приемо-сдаточный акт, подписываемый разработчиком (поставщиком) и заказчиком.

2. Акты внедрения средств защиты информации по результатам их приемо-сдаточных испытаний.

3. Протоколы аттестационных испытаний и заключение по их результатам.

4. Аттестат соответствия объекта информатизации требованиям по безопасности информации.

5. Приказ (указание, решение) о назначении лиц, ответственных за эксплуатацию объекта информатизации.

6. Приказ (указание, решение) о разрешении обработки в АС конфиденциальной информации.

Контроль состояния защиты конфиденциальной информации проводится службой безопасности организации не реже чем один раз в год и федеральными и отраслевыми органами контроля не реже одного раза в два года. При проведении аттестации объектов информатизации и периодическом контроле состояния защиты конфиденциальной информации организациями могут, при необходимости, использоваться «Временные методики оценки защищенности конфиденциальной информации». При необходимости, по решению руководителя организации, могут быть проведены работы по поиску электронных устройств съема информации («закладочных устройств»), возможно, внедренных в технические средства, осуществляемые организациями, имеющими соответствующие лицензии или ФСБ России (ФАПСИ).

Литература

1. Временная методика оценки защищенности основных технических средств и систем, предназначенных для обработки, хранения и (или) передачи по линиям связи конфиденциальной информации. – М. : Гостехкомиссия России, 2002.

2. Временная методика оценки защищённости конфиденциальной информации, обрабатываемой основными техническими средствами и системами, от утечки за счёт наводок на вспомогательные технические средства и системы и их коммуникации. – М. : Гостехкомиссия России, 2002.

3. Временная методика оценки защищенности помещений от утечки речевой конфиденциальной информации по акустическому и виброакустическому каналам. – М. : Гостехкомиссия России, 2002.

4. Временная методика оценки помещений от утечки речевой конфиденциальной информации по каналам электроакустических преобразований во вспомогательных технических средствах и системах. – М. : Гостехкомиссия России, 2002.

5. Международный союз электросвязи. Серия X. Сети передачи данных, взаимосвязь открытых систем и безопасность. – Швейцария, Женева, 2010.

6. Специальные требования и рекомендации по технической защите конфиденциальной информации. – М., 2001. – С. 9.

7. Лохвицкий В.А. Подход к построению системы автоматизированной интеграции информации в базу данных для её своевременной актуализации / В.А. Лохвицкий, С.В. Калиниченко, А.А. Нечай // Мир современной науки. – 2014. – № 2 (24). – С. 8–12.

8. Нечай А.А. Выявление недекларированных возможностей аппаратно-программного обеспечения / А.А. Нечай // Экономика и социум. – 2014. – № 1–2 (10). – С. 457–460.

9. Нечай А.А. Специфика проявления уязвимостей в автоматизированных системах управления критически важными объектами / А.А. Нечай, П.Е. Котиков // Современные тенденции в образовании и науке : сборник научных трудов по материалам Международной научно-практической конференции : в 14 ч. – Тамбов, 2014. – С. 96–97.

10. Нечай А.А. Выбор и обоснование показателей эффективности решения задачи распределения объектов по средствам поражения / А.А. Нечай, С.В. Матвеев, В.М. Сафонов // Мир современной науки. – 2014. – № 2 (24). – С. 13–16.

11. Скородумов Б.И. Современные проблемы отечественного профессионального стандарта информационной безопасности / Б.И. Скородумов // Вестник Российского нового университета. – 2014. – Вып. 4. – С. 156–158.