УДК 004.056

КОНЦЕПЦИЯ УПРАВЛЕНИЯ ПРОЦЕССОМ ОБЕСПЕЧЕНИЯ ДОСТОВЕРНОСТИ ИНФОРМАЦИИ В ИТКС В УСЛОВИЯХ ИНФОРМАЦИОННОГО ПРОТИВОДЕЙСТВИЯ

Монахов М.Ю., Полянский Д.А., Монахов Ю.М., Семенова И.И.

ФГБОУ ВПО «Владимирский государственный университет имени А.Г. и Н.Г. Столетовых», Владимир, e-mail: osobaii@gmail.com

В работе рассматриваются особенности современных информационно-телекоммуникационных систем (ИТКС), влияющие на процессы обеспечения достоверности информации в системе. В работе предлагается концепция управления процессами обеспечения достоверности информационных ресурсов (ИР) в современных информационно-телекоммуникационных системах (ИТКС), отличающаяся учетом работы систем в условиях: дестабилизирующих факторов, оказывающих влияние на достоверность информации в ИТКС; активного информационного противодействия; мониторинга и динамического определения уровня достоверности источников информации. На основе общепринятых классификаций угроз информационной безопасности составлена карта угроз достоверности ИР. Выявлены функции с целью создания и поддержания условий обеспечения достоверности ИР в условиях информационного противодействия. Приведено соответствие мер и средств обеспечения достоверности ИР выявленным функциям.

Ключевые слова: информационно-телекоммуникационная система (ИТКС), достоверность информации, качество источников информации, конфликтная среда, средства управления, меры обеспечения достоверности

THE CONCEPT OF CONTROL PROCESS OF ENSURE OF INFORMATION RELIABILITY IN ITCS UNDER INFLUENCE OF THE INFORMATION THREATS

Monakhov M.Y., Polyanskiy D.A., Monakhov Y.M., Semenova I.I.

Vladimir State University named after A. and N. Stoletovs, Vladimir, e-mail: osobaii@gmail.com

The paper discusses the features of modern information-telecommunication systems (ITCS), which affect processes the ensure of information reliability in the system. This article proposes a concept of processes ensure the reliability of information resources in modern information-telecommunication systems (ITCS). The concept takes into consideration: the destabilizing factors in ITCS; active information opposition; monitoring and dynamically determine the reliability level of information sources. We have made a map of threats for the reliability of the information resources on the basis of generally accepted classifications of information security threats. We have identified the functions to create and maintain conditions to ensure reliability of information resources in the information opposition. We have associated measures and means to ensure the reliability of information resources to identified functions.

Keywords: information-telecommunication system (ITCS), information reliability, quality of information sources, conflict environment, management tools, measures to ensure the reliability

На данный момент наука располагает существенными возможностями в области построения и организации эффективного функционирования информационно-телекоммуникационных систем (ИТКС). При этом одним из наиболее значимых факторов, влияющих на эффективность ИТКС, является качество информации. Важнейшими взаимосвязанными характеристиками качества информации выступают ее полезность (ценность) и достоверность. Данная работа посвящена вопросам достоверности информации.

Основные компоненты концепции обеспечения достоверности информации

Под объектом управления в работе понимается процесс обеспечения достоверности информации (ОДИ). Можно предложить следующие компоненты концептуальной модели процесса ОДИ на первом (самом высоком, наиболее абстрактном) уровне декомпозиции: информационные ресурсы (ИР); источники информации (ИстИ); угрозы достоверности информации; источники угроз достоверности информации; цели злоумышленников; функции ОДИ; меры ОДИ; средства ОДИ; показатели достоверности информации.

Информационные ресурсы и их источники

Информация – объективная категория, формирующая дополнительные знания (по Шеннону) о каком-либо объекте или явлении. Информация проявляется в сообщениях ИстИ, где сообщение – выбранная порция информации, имеющая законченный смысл. Информационные сообщения, как объективная реальность, абсолютно достоверны всегда.

В ИТКС циркулируют данные – обработанные сообщения, представленные в формализованном виде (например, в виде

цифрового кода), пригодном для передачи, переработки и представления в некотором информационном процессе (ИП) для решения задач пользователей. В них может присутствовать информация об объекте или явлении. Заметим, что пользователь, как правило, не является непосредственным наблюдателем объекта или явления, а должен довольствоваться данными об объектах, которые получает от некоторого ИстИ, который является либо непосредственным «наблюдателем» объекта или явления, либо транслирует данные, получаемые от других источников, в лучшем случае от первоисточников. При этом ИстИ могут перекрывать друг друга и формировать противоречивую информацию. Конфликты значений в противоречащих источниках часто систематические и вызваны свойствами различных источников [10].

Информационные сообщения до времени «скрыты» в ИстИ, проявляются же в виде данных в момент инициирования задач пользователей путем фиксации на физических носителях или при передаче по физическому каналу связи в ИТКС. Эти данные сохраняются, подвергаются переработке, представляются пользователям, которые посредством данных процессов обработки принимают информационные сообщения. Далее сообщения «растворяются» в потребителях (пользователях).

Данные, получаемые при кодировании сообщений, могут оказаться правдивыми (правдоподобными, неправдоподобными), полными (недостаточно полными для задач пользователей), актуальными (устаревшими для решаемой задачи) и т.п. Степень доверия к таким данным определяется их семантической и «временной» искаженностью.

Зафиксированную в ИТКС совокупность данных будем называть информационным ресурсом (ИР). Законодательно ИР – это «отдельные документы и отдельные массивы документов, документы и массивы в информационных системах» [1]. ИР – это данные различного характера, материализованные в виде документов, баз данных и баз знаний. В процессе производственной деятельности ИР рассматриваются как экономическая категория, которая является важнейшим элементом информационного менеджмента [3].

Внешние ИР формируются внешней информационной средой предприятия и отражают отношения между предприятием и экономическими и политическими субъектами, действующими за его пределами.

Внутренние ИР формируются внутренней информационной средой, т.е. совокупностью структурных подразделений предприятия и работающих специалистов, технологическими, социальными, экономическими и другими отношениями между ними. Внутренние ИР определяются внутренними бизнес-процессами [5]. При использовании ИР в предприятиях к ним предъявляются определенные требования, в том числе получение ИР в установленные сроки, полноту и неискаженность как поступающих, так и полученных ИР и т.д.

Эффективность бизнес-процессов определяется качеством ИП, реализуемых корпоративной ИТКС. Здесь важны следующие аспекты:

– решающее значение имеет реальная доступность ИР, которая на практике ограничена;

– экономическая полезность ИР определяется фактором времени и качеством. Устаревшая или неполная информация может не только оказаться полностью обесцененной, но и привести к значительным потерям стоимости производимых на ее основе работ.

ИП направлены на целесообразное использование ИР и снабжение ими всех элементов ИТКС. Эффективность функционирования ИП определяется наличием современных средств вычислительной техники (СВТ), распределенных БД, сетей телекоммуникаций, возможностью их модернизации и модификации, изменения структуры, включения новых компонентов и т.д., что позволяет обеспечить эффективную циркуляцию и переработку ИР. По назначению и характеру использования выделим два основных класса ИП:

– системные (обеспечивающие) ИП – представляют собой процедуры исполнения отдельных системных операций, связанных с представлением, преобразованием, хранением, обработкой или передачей данных;

– прикладные ИП – задачи пользователей. Основная цель прикладных ИП – получать посредством переработки первичных ИР информацию, на основе которой вырабатываются управленческие решения.

Будем считать, что в ИТКС циркулируют информационные ресурсы четырех типов: $ИР_1$ – исходные данные, полученные на хранение и обработку от ИстИ (включая потребителей и взаимодействующих ИТКС); $ИР_2$ – производные данные, то есть данные, полученные в ИТКС в процессе переработки исходных и производных данных; $ИР_3$ – программы, используемые для обработки данных, организации и обеспечения функционирования ИТКС; $ИР_4$ – нормативно-справочные и служебные данные.

Достоверность информации (степень доверия к данным), содержащейся в информационных ресурсах $ИР_1$, $ИР_3$, $ИР_4$,

во многом определяется качеством их источника [10, 11]. Следовательно, необходимо говорить о достоверности информации как достоверности ИстИ (точнее, о степени доверия потребителя-пользователя к конкретному источнику), который искажает (неосознанно или с умыслом) формируемые им данные, делая информацию, содержащуюся в них, недостоверной.

Достоверность ИстИ – апостериорная оценка, получаемая в результате наблюдения за его (источника) «информационной активностью». Источнику можно верить или нет – он субъект, может сообщать системе дезинформацию, может быть достоин доверия или недоверия.

Достоверность информации, содержащейся в $ИР_2$, $ИР_3$, $ИР_4$, в основном определяется качеством и устойчивостью процессов (функций) хранения, переработки и представления данных, происходящих в рамках технической подсистемы ИТКС при выполнении задач пользователей [6, 7]. Такая функциональная устойчивость системы достигается надежностью технических и программных средств, живучестью структурного построения системы, квалификацией и навыками в работе персонала, обеспечением безопасности ИР [8, 9]. В данном случае следует связать понятие достоверности информации с категориями целостности и доступности ИР. Целостность ИР обеспечивается, если он нелегитимно не изменяется, доступность – если легитимный процесс получает ИР за приемлемое время. Все это должно быть обеспечено при функционировании ИТКС в условиях случайных или преднамеренных информационных воздействий [2].

Таким образом, каждое звено прохождения (обработки) информации накладывает на нее свой (информационный) фильтр, вносящий свои «ослабления и запаздывания», т.е. искажения. Природа таких искажений чаще всего случайна. В итоге «достоверность информации», которую мы оцениваем, есть априорная оценка вероятности того, что сообщение для пользователя при решении определенной задачи будет содержать неискаженные данные.

Угрозы достоверности информации и их источники

На основе общепринятых классификаций угроз информационной безопасности [1, 4] составлена карта угроз достоверности ИР, представленная на рисунке, и разработан расширенный перечень таких угроз. Выделены следующие угрозы достоверности:

1. Саботаж или преднамеренная угроза – умышленное нарушение ИП, уклонение от работы или недобросовестное ее выполнение. Субъекты угрозы – персонал (внутренние нарушители – инсайдеры), пользователи (внешние нарушители). Данная угроза может эксплуатировать организационную уязвимость ИТКС – недовольство персонала, например, условиями труда. Относительно пользователей в качестве уязвимых могут эксплуатироваться их психофизиологические свойства.

В качестве средств осуществления угрозы могут выступать: вандализм – вывод из строя всех или отдельных элементов ИТКС (устройств, носителей, персонала); дезорганизация функционирования системы – неправомерное отключение оборудования, изменение режимов работы технических средств (ТС) или программного обеспечения (ПО); умышленное злоупотребление ресурсами (в том числе сетевыми); злоупотребление правами; внедрение вредоносного ПО; нелегитимная имперсонация – «маскарад», в том числе незаконное подключение к линиям связи; разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, пропусков и т.п.); замена, вставка, удаление или изменение данных в информационном потоке в канале связи; вскрытие используемых алгоритмов шифрования; недобросовестное исполнение обязанностей персоналом; ведение агентурной работы.

2. Несанкционированный доступ (НСД) к ИР – первопричина несанкционированной модификации, подмены или уничтожения ИР. Это угроза нарушения целостности и доступности ИР. Субъект данной угрозы чаще всего внешний нарушитель. Данная угроза может эксплуатировать уязвимости ИТКС: недостатки ИТКС и ее компонентов (например, уязвимости ПО). В качестве средств осуществления угрозы могут выступать: нелегитимная имперсонация, разглашение, передача или утрата атрибутов разграничения доступа; внедрение вредоносного ПО; удаление или изменение данных в информационном потоке в канале связи; вскрытие используемых алгоритмов шифрования.

3. Спровоцированный отказ – нарушение работоспособности элементов ИТКС: ТС, ПО, кабельной системы (КС). Это угроза нарушения доступности ИР. Субъект данной угрозы – внешний нарушитель. Данная угроза может эксплуатировать уязвимость ИТКС – недостатки ИТКС и ее элементов. В качестве средств осуществления угрозы могут выступать: вандализм; дезорганизация функционирования системы; нелегитимная имперсонация, разглашение, передача или утрата атрибутов разграничения доступа; умышленное злоупотребление ресурсами; внедрение вредоносного ПО.

Карта угроз достоверности ИР

4. Отказ ТС, ПО, КС, сервисов – это случайная угроза, вызывающая нарушение доступности ИР. Субъекты данной угрозы: внешняя среда, персонал, производители компонентов ИТКС, организации, предоставляющие услуги, и их работники. Данная угроза может эксплуатировать уязвимости ИТКС: агрессивная внешняя среда, низкая квалификация персонала, неопытность персонала, низкая надежность ТС, ПО, КС, носителей, недостатки структуры ИТКС, недостатки организационного обеспечения (ОО), низкая надежность организаций, предоставляющих услуги. В качестве средств осуществления угрозы могут выступать: неумышленное отключение оборудования или изменение режимов работы устройств и программ персоналом; злоупотребление ресурсами ИТКС; неумышленное использование несанкционированных программ и обработка данных; ошибки персонала (при установке, настройке оборудования и программ и т.п.); ошибки пользователей.

5. Ошибки пользователей при обработке ИР – это случайная угроза, вызывающая нарушение целостности и доступности ИР. Субъекты угрозы – пользователи. Данная угроза может эксплуатировать такую уязвимость ИТКС, как низкая квалификация пользователей.

Функции, меры и средства обеспечения достоверности ИР

Для обеспечения требуемого уровня достоверности ИР необходимы: механизмы практической реализации гарантированного обеспечения требуемого уровня достоверности; средства рациональной реализации необходимых действий по ОДИ; способы оптимальной организации и проведения всех действий по ОДИ в процессе функционирования ИТКС.

С целью построения концепции, удовлетворяющей всей совокупности требований, предлагается система концептуальных решений (по аналогии с концепциями обеспечения информационной безопасности [4]):

– формирование полного множества функций обеспечения достоверности ИР (ФОДИР);

– формирование полного множества мер и средств реализации ФОДИР.

Функция обеспечения достоверности ИР – это присущий ИТКС вид деятельности, осуществляемый с целью создания и поддержания условий обеспечения достоверности ИР в условиях информационного противодействия. Перечислим виды ФОДИР:

1. Предотвращение возникновения угроз (F_1). Угрозы достоверности информации (УгДИ) могут возникнуть случайно или

намеренно, и их источник – как правило, люди. Здесь следует снижать количество источников угроз. Для этих целей необходима работа сотрудников службы безопасности с информаторами в интересах наблюдения и объективной оценки ситуации как внутри коллектива сотрудников, так и вне, среди конкурентов и преступных формирований. В таком предупреждении возникновения угроз весьма существенную роль играет информационно-аналитическая деятельность службы безопасности на основе глубокого анализа криминогенной обстановки и деятельности конкурентов и злоумышленников.

2. Сдерживание угроз (F_2). Главной целью является способствование такому архитектурному построению ИТКС, реализации ИП (включая программное и аппаратное обеспечение) и организационной структуре, чтобы свести к минимуму саму возможность появления уязвимостей в элементах ИТКС, т.е. преследуется упреждающая цель.

3. Обнаружение проявившихся угроз (F_3). Предполагается осуществление таких мер (и, соответственно, использование таких средств) обнаружения угроз, в результате которых проявившиеся УгДИ будут обнаружены еще до того, как они окажут негативное воздействие на достоверность ИР. Иными словами, это функция непрерывного слежения за характеристиками, идентифицирующими конкретные угрозы.

4. Предупреждение воздействия на ИР проявившихся угроз (F_4) – меры, осуществляемые в рамках данной функции, преследуют цель не допустить нежелательного воздействия УгДИ на ИР, если они реально проявились, т.е. данная функция является естественным продолжением предыдущей. Это предполагает использование средств, «устраняющих или ослабляющих воздействие угрозы».

5. Обнаружение воздействия (необнаруженных) угроз (F_5) – функция слежения за ИР с целью своевременного обнаружения фактов воздействия на них необнаруженных (неизвестных) УгДИ. При этом под своевременным понимается такое обнаружение, при котором сохраняются реальные возможности локализации воздействия на информацию.

6. Устранение (локализация, ограничение) обнаруженного воздействия угроз (F_6). Являясь логическим продолжением предыдущей, данная функция предусмотрена с целью недопущения распространения воздействия («недостоверности») на другие (составные) ИР (за пределы максимально допустимых размеров).

7. Ликвидация последствий реализованной атаки (F_7) – проведение таких мероприятий относительно локализованного воздействия УгДИ на информацию, в результате которых дальнейшая обработка информации может осуществляться без учета имевшего место воздействия. Иными словами, удается восстановить то состояние информационных ресурсов, которое имело место до воздействия УгДИ.

Меры обеспечения достоверности ИР – способы и методики реализации функций обеспечения достоверности ИР за счёт противодействия внутренним и внешним угрозам, снижения воздействия УгДИ на ИР и облегчения восстановления ИР при реализации угроз.

Средства ОДИ – это действия, процедуры, механизмы и устройства, способные с той или иной степенью эффективности реализовать меры обеспечения достоверности ИР.

В таблице приведено соответствие мер и средств обеспечения достоверности ИР функциям ОДИ. Заметим, что каждая функция обеспечивается подмножеством полного множества мер и средств.

Связь функций с мерами и средствами обеспечения достоверности ИР

Функции обеспечения достоверности ИР / Меры и средства обеспечения достоверности	F_1	F_2	F_3	F_4	F_5	F_6	F_7
Организационное обеспечение	+	+		+		+	+
Физическая защита	+	+		+			
Обеспечение целостности данных			+	+	+		+
Контроль доступа				+			
Идентификация и аутентификация				+			
Аудит			+		+		
Контроль носителей данных		+		+			
Обеспечение надёжности инфраструктуры	+	+					
Сетевое администрирование		+		+		+	+
Защита от вредоносного ПО			+	+		+	+
Обнаружение вторжений			+				
Валидация данных				+	+		

Заключение

Таким образом, имеются предпосылки для использования необходимого арсенала мер и средств ОДИ. Для решения вопроса о достаточном их количестве необходимо иметь данные об эффективности использования различных мер при обеспечении выполнения различных функций ОДИ. На текущий момент ведутся работы по проведению серии экспериментов по выявлению метрик, на основе которых будет выполняться комплексная оценка уровня достоверности ИР в ИТКС. Развитие работы видится в построении модели управления процессом обеспечения достоверности, отличающейся учетом работы ИТКС в условиях: дестабилизирующих факторов; активного противодействия; мониторинга и динамического определения уровня достоверности ИстИ; ограничений ресурсов различных классов в ИТКС.

Научная публикация подготовлена в рамках государственного задания ВлГУ № 2014/13 на выполнение государственных работ в сфере научной деятельности.

Список литературы

1. ГОСТ Р 53114-2008 Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения. – М.: СандартинФорм, 2009. – 20 с.

2. Илларионов Ю.А., Монахов М.Ю. Безопасное управление ресурсами в распределенных информационных и телекоммуникационных системах. – Владимир: Владим. гос. ун-т. Владимир, 2004. – 204 с.

3. Костров А.В. Основы информационного менеджмента. – М.: Финансы и стат., 2001. – 336 с.

4. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия-Телеком, 2004. – 280 с.

5. Монахов М.Ю., Файман О.И. Инвентаризация информационных ресурсов как основа безопасного функционирования АСУ // Известия высших учебных заведений. Приборостроение. – 2012. – Т. 55. – № 8. – С. 35–39.

6. Остринская Л.И., Семенова И.И., Дороболюк Т.Б. Теория и практика работы с современными базами и банками данных. – Омск: Изд-во СибАДИ, 2005. – 250 с.

7. Семенова И.И. Аспекты информационной безопасности в системах управления базами моделей // МИК-2012.– Омск: Правительство Омской области, 2012. – С. 246–252.

8. Сухарев М.С., Монахов Ю.М. Модель оценки функциональной устойчивости бизнес-процессов // Вестник Костромского государственного университета. – 2011. – № 5–6. – С. 4–6.

9. Сухарев М.С., Монахов Ю.М., Файман О.И. Применение системного подхода к оценке функциональной устойчивости бизнес – процессов // Сборник научных трудов Sworld. – 2011. – Т. 5. – № 4. – С. 70–73.

10. Heiko Müller, Johann-Christoph Freytag, Ulf Leser Improving data quality by source analysis // J. Data and Information Quality. – 2012. – № 2, 4. – 38 p.

11. Using information quality for the identification of relevant web data sources: a proposal / Bernadette Farias Lóscio, Maria C.M. Batista, Damires Souza, Ana Carolina Salgado // IIWAS ‘12. – ACM, NY, USA. – 2012. – P. 36–44.

References

1. GOST R 53114-2008 Zashchita informatsii. Obespecheniye informatsionnoy bezopasnosti v organizatsii. Osnovnyye terminy i opredeleniya (Information Security. Ensuring information security in the organization. Basic terms and definitions). M.: SandartinForm, 2009. 20 p.

2. Illarionov YU.A., Monakhov M.YU. Bezopasnoye upravleniye resursami v raspredelennykh informatsionnykh i telekommunikatsionnykh sistemakh (Safe management of resources in distributed information-telecommunication systems). Vladimir: Vladim. gos. un-t. Vladimir, 2004. 204 p.

3. Kostrov A.V. Osnovy informatsionnogo menedzhmenta (Fundamentals of Information Management). M.: Finansy i stat., 2001. 336 p.

4. Malyuk A.A. Informatsionnaya bezopasnost’: kontseptual’nyye i metodologicheskiye osnovy zashchity informatsii (Information security: conceptual and methodological framework for the protection of information). M.: Goryachaya liniya-Telekom, 2004. 280 p.

5. Monakhov M.YU., Fayman O.I. Inventarizatsiya informatsionnykh resursov kak osnova bezopasnogo funktsionirovaniya ASU (Inventory of information resources as a basis for the safe functioning of ACS) // Izvestiya vysshikh uchebnykh zavedeniy. Priborostroyeniye. 2012. Vol. 55. no. 8. *pp*. 35–39.

6. Ostrinskaya L.I., Semenova I.I., Dorobolyuk T.B. Teoriya i praktika raboty s sovremennymi bazami i bankami dannykh (Theory and practice of modern databases and data banks). Omsk: Izd-vo SibADI, 2005. 250 p.

7. Semenova I.I. Aspekty informatsionnoy bezopasnosti v sistemakh upravleniya bazami modeley (Aspects of information security in database management systems models) // MIK-2012. Omsk: Pravitel’stvo Omskoy oblasti, 2012. *pp*. 246–252.

8. Sukharev M.S., Monakhov YU.M. Model’ otsenki funktsional’noy ustoychivosti biznes-protsessov (Model evaluation of functional stability of business processes) // Vestnik Kostromskogo gosudarstvennogo universiteta. 2011. Vol. 17. no. 5–6. *pp*. 4–6.

9. Sukharev M.S., Monakhov YU.M., Fayman O.I. Primeneniye sistemnogo podkhoda k otsenke funktsional’noy ustoychivosti biznes–protsessov (A systematic approach to assessment of functional stability of business-processes) // Sbornik nauchnykh trudov Sworld. 2011. V*щд*. 5. no. 4. *pp*. 70–73.

10. Heiko *Müller, Johann*-Christoph Freytag, Ulf Leser Improving data quality by source analysis // J. Data and Information Quality. 2012. 2, 4. 38 p.

11. Using information quality for the identification of relevant web data sources: a proposal / Bernadette Farias Lóscio, Maria C.M. Batista, Damires Souza, Ana Carolina Salgado // IIWAS ‘12. ACM, NY, USA. 2012. *pp*. 36–44.

Рецензенты:

Александров Д.В., д.т.н., профессор кафедры ИБМ-7, МГТУ им. Н.Э. Баумана, г. Москва;

Бутковский О.Я., д.ф.-м.н., профессор кафедры МиИ, Владимирский филиал финансового университета, г. Владимир.

Работа поступила в редакцию 08.09.2014.