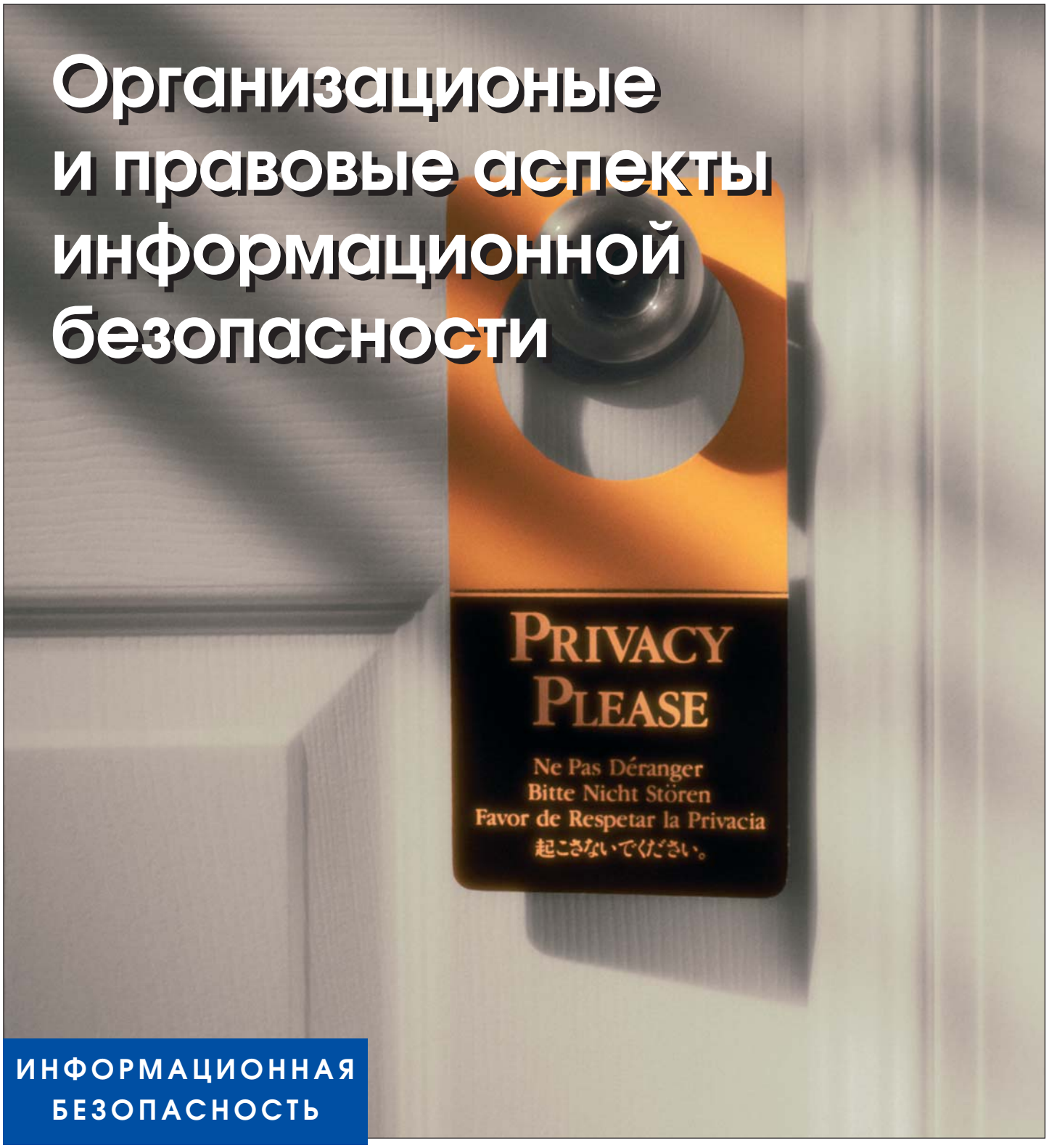
Jet Info

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ № 1 (164)/2007

Организационые и правовые аспекты информационной безопасности



ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Организационые и правовые аспекты информационной безопасности

СОДЕРЖАНИЕ

В настоящее время роль информационной безопасности во всех областях деятельности человека непрерывно возрастает. В условиях быстрого развития информационных технологий постоянно расширяется и спектр рисков. В обеспечении информационной безопасности помимо технической не менее важна и организационная сторона. Кроме того, очень большое значение имеют в этой сфере правовые вопросы. Особое место в правоотношениях при обмене информацией занимает институт государственной тайны. Существуют нормы законов, регулирующие вопросы защиты информации, однако часто бывают ситуации, когда возникает риск нарушения конфиденциальности сведений по техническим и другим причинам.

В данном выпуске бюллетеня читателю предлагаются материалы, в которых рассматриваются вышеназванные проблемы.

Информационная безопасность для организаций с высоким уровнем риска: новые угрозы и возможные подходы к их нейтрализации

Научный редактор обзора И. Чибрикин

Общие положения

Обеспечение информационной безопасности (ИБ) — это не только и не столько техническая, сколько организационная проблема, для решения которой необходима определенная корпоративная культура и поддержка на всех уровнях, начиная от высшего руководства компании.

Информационная безопасность — это не продукт, а процесс. Ее нельзя купить раз и навсегда. Эффективность средств обеспечения информационной безопасности необходимо постоянно повышать, иначе в условиях непрерывного развития информационных технологий (ИТ) даже самая современная система ИБ очень быстро устареет, уровень информационной безопасности в компании снизится.

Информационную безопасность необходимо поддерживать для сложных аппаратно-программных информационных систем (ИС), насчитывающих десятки и сотни миллионов электронных компонентов и строк исходных текстов, подверженных

сбоям, отказам, проявлениям внутренних ошибок и уязвимостей, а также ошибкам и упущениям обслуживающего персонала и пользователей.

Меняются производственные процессы, совершенствуются информационные технологии, появляются новые возможности, а вместе с ними — новые угрозы и новые, все более изощренные, способы атак, которые необходимо нейтрализовать. В условиях постоянно изменяющегося производственного контекста необходимо следить за состоянием информационной безопасности, чтобы она не нарушалась.

Современные тенденции изменения спектра ИТ-рисков

Рассмотрим тенденции изменения спектра ИТ-рисков, характерные для крупных современных организаций, активно использующих передовые информационные технологии.

- Сложность информационных систем стала самостоятельным фактором риска. Согласно принятым стандартам кодирования, исходный текст программы считается хорошим, если на тысячу строк приходится не более пяти ошибок. Современные операционные системы (ОС) насчитывают несколько десятков миллионов строк исходного текста. Даже если применить трудоемкие и дорогостоящие меры по поиску и исправлению ошибок, уменьшающих их количество до одной на двадцать тысяч строк, их все равно останется несколько тысяч. В новых версиях могут исправляться старые ошибки, но добавляться новые. Ошибки и уязвимости постоянно присутствуют не только в ОС, но и в приложениях. В июле 2006 года известный специалист по ИБ Мур (Moore) успешно реализовал собственный амбициозный проект — каждый день находить и обнародовать по крайней мере один дефект в Интернет-навигаторе. (Интересно отметить, что уже после первой недели работы он получил возмущенное письмо из России от одного из хакеров, который жаловался, что Мур обнародовал использовавшуюся им (хакером) уязвимость). Сложность многократно возрастает в многокомпонентной, многопротокольной среде, включающей многочисленные аппаратно-программные компоненты разных производителей.
- Сокращение времени разработки и тестирования аппаратно-программных продуктов с целью скорейшего выхода на рынок. Это усугубляет проблему сложности, увеличивает число ошибок и уязвимостей в коммерческих продуктах всех видов — от микропроцессоров до программных приложений.
- Расширение спектра рисков, проведение атак, компрометирующих все основные аспекты информационной безопасности: доступность, конфиденциальность и целостность данных и систем, появление новых целей атак, таких как пользовательские устройства. Примером расширения спектра рисков и появления новых угроз может служить запрет, наложенный корпорацией Samsung на использование ее служащими на рабочих местах последней модели мобильного телефона Samsung с памятью на 8 Гб, поскольку реальной становится угроза несанкционированного раскрытия практически всей корпоративной информации. Пользовательские мобильные устройства могут также подвергнуться атаке вредоносного программного обеспечения (ПО), что для компонентов информационной системы, обычно администрируемых непрофессионалами, особенно опасно. Расширяет спектр рисков и массовое внедрение новых информационных сервисов и технологий, таких как беспроводные коммуникации, IP-телефония, многочисленные Web-приложения. Иногда традиционные защитные средства уже не могут быть применимы к подобным нововведениям. Они либо не обеспечат необходимый уровень информационной безопасности, либо будут мешать нормальной работе новых приложений.
- Автоматизация и усложнение атак, организация масштабных, распределенных, многоэтапных нападений, требующих минимального вмешательства злоумышленников и оставляющих минимум следов. Упомянем проект Metasploit — ПО с открытыми исходными текстами для автоматизации использования уязвимостей. Фактически уже сейчас средства эксплуатации уязвимостей появляются существенно раньше, чем соответствующие программные коррекции.
- Сочетание внешних и внутренних угроз, компрометация внутренних оконечных систем как этап атаки на информационную систему организации в целом.
- Развитие и массовое внедрение в пользовательские системы шпионского ПО, руткитов, потайных входов, ботов, организация ботсетей (сетей «зомбированных» компьютеров), способных наращивать вредоносную функциональность и выполнять масштабные вредоносные действия по команде из центра управления.
- Сочетание технических и психологических методов атак. Эта тенденция наиболее полно

реализована в фишинговых атаках, направленных на кражу персональных данных.
- Криминализация ИТ вообще и Интернет в особенности, хакерство ради материальной выгоды, существование рынка уязвимостей и средств их использования, перепродажа незаконно добытых данных, вымогательство под угрозой компрометации информационной системы организации и/или хранимых, обрабатываемых и передаваемых ею данных, наличие у злоумышленников значительных интеллектуальных и материальных ресурсов, повышение уровня мотивации.

Специфика ИТ-рисков для организаций нефтегазовой отрасли

Нефтегазовой отрасли присущи высокие уровни финансовых, экологических и гуманитарных рисков. Ущерб от реализации ИТ-угрозы, приведшей даже к кратковременной остановке работы добывающего и/или транспортирующего оборудования, измеряется миллионами. Любая авария, если ее не удалось оперативно выявить, локализовать и ликвидировать, наносит значительный экологический ущерб. Перенос добычи в отдаленные, труднодоступные регионы со сложными климатическими условиями затрудняет взаимодействие с персоналом и своевременное оказание ему необходимой помощи.

Учитывая вышеизложенное, следует признать важными и актуальными следующие задачи:
- максимальная автоматизация технологических процессов;
- максимально эффективное централизованное использование квалифицированных кадров для обслуживания нескольких удаленных подразделений;
- обеспечение информационной безопасности процесса управления удаленными подразделениями.

Последняя задача особенно сложна, так как требуется поддерживать исключительно высокий уровень всех основных аспектов информационной безопасности — доступности, конфиденциальности и целостности — в условиях физически незащищенных коммуникаций и удаленного оборудования, в том числе компонентов ИС, высокой стоимости и значительных сроков технического обслуживания и восстановления работоспособности аппаратного и программного обеспечения.

Обратим особое внимание на необходимость обеспечения полноты и достоверности информации, поступающей из удаленных подразделений, а также контроля за выполнением централизованно инициируемых управляющих воздействий.

Сложность и борьба с ней

Современное аппаратное и программное обеспечение характеризуется, с одной стороны, возрастанием сложности, а с другой — сокращением сроков разработки, стремлением производителей к скорейшему выходу на рынок с новыми изделиями. Совокупность этих двух тенденций, очевидно, отрицательно сказывается на информационной безопасности современных систем, приводит к квадратичному нарастанию числа известных уязвимостей в наиболее широко используемых операционных системах.

В такой ситуации попытки повысить информационную безопасность путем реализации в операционных системах дополнительных механизмов безопасности (например, мандатного управления доступом) дают скорее противоположный результат, поскольку увеличивают сложность систем. Системы небезопасны не потому, что в них не хватает каких-то защитных средств; они уязвимы, потому что сложны. Требуются принципиально новые концептуальные и архитектурные решения.

С проблемой сложности специалисты по технологии программирования столкнулись в шестидесятых годах двадцатого века. Для решения этой проблемы сначала было предложено структурированное программирование, затем, как его развитие, — объектно-ориентированный подход. Последний остается наиболее эффективным инструментом в технологии программирования больших систем и в настоящее время. К сожалению, в информационной безопасности он еще не стал общепринятым.

Для нас существенны следующие свойства объектов:
- инкапсуляция: наличие границ между объектами, невозможность манипулирования объектами в терминах их внутренней реализации;
- наличие у объектов определенных интерфейсов и построенных на их основе протоколов, специфицирующих правила обращения к объектам;
- потенциальная активность объектов, возможность их параллельной работы.

Объектно-ориентированные системы строятся в многоуровневой архитектуре, с небольшим числом сущностей на каждом уровне и с умеренным числом связей между объектами, что делает подобные системы познаваемыми и, следовательно, принципиально контролируемыми. Если учесть перечисленные выше свойства объектов, можно считать, что

объектно-ориентированные системы имеют сетевую организацию, поддающуюся управлению.

Использование методов программирования при решении проблем информационной безопасности представляется весьма перспективным, но в настоящее время эти две области неоправданно разобщены.

Сетевая организация информационных систем может проявляться и использоваться различными способами. Информационная система строится из объектов с необходимой степенью гранулярности, а границы между объектами по возможности делаются физическими, поддерживаемыми аппаратно (объекты разносятся по узлам сети). Таким образом, в качестве концептуальной основы обеспечения информационной безопасности сложных систем предлагается их объектная организация с физическими границами между объектами.

Коротко правило построения архитектурно безопасных ИС можно сформулировать как «один сервис на узел сети» или как «разнесение сервисов по узлам сети».

Объектная организация с физическими границами между объектами может применяться не только к аппаратным компонентам, но и к потокам данных. Целесообразно физически разграничить пользовательские и административные потоки данных, потоки, связанные с деятельностью администраторов безопасности, внутренние и внешние потоки, потоки с разной политикой безопасности и т.п. У интеллектуальной сетевой карты может быть по крайней мере три сетевых интерфейса. Через один из них проходят пользовательские данные, через другой осуществляется конфигурирование и чтение регистрационных данных, через третий может направляться сигнал тревоги администратору безопасности или осуществляться вмешательство последнего в работу системы.

Отметим, что организация описанной «многожильной» сети не обязательно требует прокладки множества дорогих кабелей. Стандарт безопасности для беспроводных сетей с инфраструктурой IEEE Std 802.11i предусматривает достаточные защитные средства канального уровня.

Разработка информационно безопасного программного обеспечения

Информационная безопасность современных ИС определяется не только и не столько наличием защитных средств, сколько качеством используемого в них программного обеспечения. Наличие в базовом и прикладном ПО многочисленных уязвимостей многократно усложняет защиту ИС и увеличивает ее стоимость, поэтому повышение информационной безопасности разрабатываемого в организации программного обеспечения — необходимое условие успешной, экономически оправданной защиты. Прикладное ПО должно не столько включать какие-то специфические защитные средства, такие как аутентификация или криптография, сколько быть устойчивым к атакам, содержать минимальное число уязвимостей.

Информационная безопасность программного обеспечения должна формироваться и поддерживаться на всех этапах жизненного цикла — от инициации до выведения из эксплуатации. Для решения этой задачи необходимо использовать как организационные, так и технические инструменты.

К первым относится формирование смешанных коллективов из разработчиков ПО и специалистов по информационной безопасности для выработки целей и требований безопасности. Эти цели и требования могут формулироваться в терминах «Общих критериев» (стандарт ГОСТ Р 15408-2002).

На стадии проектирования приложений следует проводить моделирование и анализ угроз, инициировать процесс управления рисками как основу выбора технически и экономически оправданных решений. На этой же стадии должны применяться архитектурные принципы информационной безопасности, такие как минимизация привилегий, разделение полномочий, эшелонированность обороны и, главное, выбор простых апробированных решений. Важнейший вопрос — совместимость с существующей инфраструктурой, в том числе защитной.

Необходимо ответить, по крайней мере, на два вопроса:

- будут ли существующие защитные средства обеспечивать информационную безопасность разрабатываемого приложения?
- Не помешают ли существующие защитные средства нормальной работе разрабатываемого приложения?

На стадии реализации целесообразно использовать такой технический инструмент контроля качества ПО, как статический анализатор исходных текстов, а также их аудит независимыми специалистами-оценщиками. На завершающих этапах реализации может начинаться тестирование проникновением. Параллельно должна разрабатываться документация, в частности, руководство по безопасному использованию приложения.

На стадии внедрения и опытной эксплуатации проверяется качество нового приложения, уровень его защищенности, определяются рекомендуемые значения конфигурационных параметров.

Уровни зрелости Аспекты метрик Типы метрик	Уровень 1. Разработана политика безопасности Намечены конечные цели	Уровень 2. Разработаны процедуры безопасности Определены промежуточные цели	Уровень 3. Процедуры и регуляторы реализованы Метрики реализации	Уровень 4. Процедуры и регуляторы оттестированы Метрики эффективности	Уровень 5. Процедуры и регуляторы интегрированы Метрики воздействия
Автоматизация сбора данных	Отсутствует	Низкая	Умеренная	Высокая	Полная
Трудоемкость сбора данных	Очень высокая	Высокая	Умеренная	Умеренная или низкая	Низкая
Доступность данных	Данные отсутствуют	Есть часть данных	Могут быть собраны	Доступны	В стандартном хранилище

Таблица 1. Соответствие между уровнями зрелости процессов информационной безопасности организации и различными аспектами применения метрик

На стадии эксплуатации анализируются данные о функционировании нового приложения, а также информация об уязвимостях, выявленных в его (приложения) инфраструктуре. По результатам анализа выполняется соответствующая доработка приложения и инфраструктуры, в частности, разработка и установка программных коррекций.

На стадии выведения из эксплуатации основное внимание должно быть уделено безопасности данных, ассоциированных с приложением.

С организационной точки зрения процесс обеспечения информационной безопасности ПО можно подразделить следующим образом:

- оперативное управление объединенным коллективом разработчиков ПО и специалистов по ИБ;
- выработка типовых для данной организации проектных и архитектурных подходов и решений;
- накопление базы знаний об угрозах, рисках, уязвимостях и способах их нейтрализации;
- информирование и обучение персонала, вовлеченного в разработку ПО;
- оценка безопасности разрабатываемого ПО;
- общий контроль за уровнем информационной безопасности разрабатываемого ПО.

Должны быть определены ответственные за каждый вид деятельности; общий контроль (равно как и активная поддержка мер повышения информационной безопасности) должен оставаться за руководством организации.

Количественный подход к информационной безопасности

Информационная безопасность требует затрат, поэтому важно понимать, какие результаты они приносят и насколько они эффективны. Наличие и применение количественных мер и метрик — обязательный элемент зрелого, экономически оправданного управления информационной безопасностью.

Меры и метрики могут быть как абсолютными (например, число инфицированных компьютеров за определенный период времени), так и относительными (например, процент системных администраторов, прослушавших курс информационной безопасности). Важно, чтобы с их помощью можно было реально оценить результативность программ, процессов и процедур, направленных на повышение информационной безопасности организации.

Метрики безопасности могут применяться на разных уровнях — от отдельных систем до организации в целом. Метрики системного уровня детальны; по мере подъема на более высокие уровни они агрегируются с возможным отбрасыванием менее значащих показателей.

Метрики информационной безопасности связаны с целями безопасности. Последние представляют собой желаемый результат; первые отображают прогресс в его достижении. Чтобы отслеживать прогресс, метрики нужно применять многократно и достаточно часто, например, ежеквартально, раз в полгода или, в крайнем случае, раз в год. Чтобы выявлять краткосрочные, среднесрочные и долгосрочные тенденции, соответственно нужно ранжировать и метрики вместе с частотой сбора данных для них, анализом результатов и генерацией отчетов.

Желательно, чтобы метрики указывали на причины неудовлетворительного функционирования, если таковое имеет место, и/или на диспропорции в распределении ресурсов; в таком случае они действительно помогают планировать и осуществлять корректирующие действия, оперативно выявлять и решать проблемы. Например, если по-

литика безопасности определяет требования к выбору пользовательских паролей, степень следования этой политике может измеряться как доля паролей, удовлетворяющих сформулированным требованиям. Возможна и другая метрика, определяющая долю паролей, которые можно взломать доступными средствами. Если значения по первой метрике близки к 100%, а доля взламываемых паролей относительно велика, значит, требования к выбору паролей сформулированы неудачно и нуждаются в корректировке.

Можно выделить следующие типы метрик информационной безопасности:

- метрики реализации, служащие для измерения степени проведения политики безопасности в жизнь;
- метрики эффективности, служащие для измерения результативности сервисов безопасности;
- метрики воздействия, служащие для измерения влияния действий и событий ИБ на функционирование организации.

Организация может параллельно использовать метрики всех трех типов, однако реальная польза от них зависит от степени зрелости процессов ИБ в организации.

На ранних стадиях формирования этих процессов, когда идет разработка, формализация и внедрение политики и процедур безопасности, доступны данные только для метрик реализации (например, какой процент разработанных процедур документирован и доведен до сведения персонала или какой процент семейств регуляторов охвачен положениями политики безопасности).

Когда политика и процедуры документированы и внедрены, а соответствующие регуляторы безопасности реализованы, можно начинать измерение эффективности последних (например, какой процент систем оказывается инфицированным за определенный промежуток времени или какой процент нарушений безопасности вызван просчетами в конфигурировании регуляторов управления доступом). Для применения метрик этого типа обычно бывают необходимы данные из нескольких источников (например, требуется знание политики и процедур управления доступом, данные о нарушениях безопасности, результаты аудита информационной системы и данные об изменениях в конфигурации информационной системы). Метрики этого типа полезны для принятия решений на уровне службы информационной безопасности с целью выработки оценки сложившейся практики и планирования развития системы, закупки, разработки или совершенствования регуляторов безопасности.

На следующем уровне зрелости, когда для процессов ИБ обеспечены устойчивость и повторяемость, метрики безопасности становятся более надежными и поддающимися автоматизации как на этапе сбора, так и на этапе анализа данных, пригодными для поддержки принятия решений и усилий по совершенствованию процессов ИБ. Только на этом уровне имеет смысл привлекать метрики воздействия, позволяющие оценить экономическую целесообразность деятельности в области информационной безопасности. Для применения метрик воздействия требуются многочисленные данные о ресурсах, а полученные с их помощью результаты являются наиболее ценными для руководства организации.

Таблица 1 помогает уяснить соответствие между уровнем зрелости процессов информационной безопасности организации и различными аспектами применения метрик.

Управляемость — ключевой аспект применения метрик безопасности. Метрик не должно быть слишком много (как правило, от пяти до десяти на одно должностное лицо в каждый момент времени). Только при выполнении этого условия можно сконцентрировать усилия на решении наиболее острых из выявляемых проблем, первоочередном устранении самых существенных недостатков.

Важнейшие регуляторы безопасности

Необходимым условием обеспечения информационной безопасности является выбор и реализация соответствующих регуляторов безопасности, то есть выработка и применение экономически оправданных контрмер и средств защиты. Регуляторы безопасности подразделяются на административные, процедурные и программно-технические и служат для обеспечения доступности, конфиденциальности и целостности информационной системы и обрабатываемых, хранимых и передаваемых ею данных.

Выбор регуляторов безопасности осуществляется на основе результатов категорирования данных и информационной системы. Кроме того, следует учесть, какие регуляторы безопасности уже внедрены и для каких имеются планы реализации, а также необходимо помнить о требуемой степени доверия к эффективности действующих регуляторов.

Адекватный выбор регуляторов безопасности можно упростить, если производить его из предопределенных базовых наборов.

Рекомендуется применение следующих классов административных регуляторов безопасности:

- оценка рисков;
- планирование безопасности;

- закупка систем и сервисов;
- сертификация, аккредитация и оценка безопасности.

К числу рекомендуемых классов процедурных регуляторов безопасности относятся следующие:

- кадровая безопасность;
- физическая защита;
- планирование бесперебойной работы;
- управление конфигурацией;
- сопровождение;
- целостность систем и данных;
- защита носителей;
- реагирование на нарушения информационной безопасности;
- информирование и обучение.

Рекомендуется применение следующих программно-технических регуляторов безопасности:

- идентификация и аутентификация;
- управление доступом;
- протоколирование и аудит;
- защита систем и коммуникаций.

Обратим особое внимание на необходимость реализации следующих элементов информационной безопасности:

- распространение мер безопасности на все этапы жизненного цикла и все компоненты ИС;
- мониторинг безопасности, анализ защищенности, выявление и нейтрализация уязвимостей;
- укрепление существующих систем;
- управление программными коррекциями;
- реализация двухфакторной аутентификации, устойчивой к шпионскому ПО и фишингу;
- применение криптографических средств для обеспечения целостности и конфиденциальности данных во внешних сетях, на мобильных устройствах и резервных носителях;
- эшелонированная защита от вредоносного ПО, контроль и фильтрация информационного наполнения на границах сетей с разными требованиями безопасности, контроль целостности систем, выявление признаков внедрения вредоносного ПО и его оперативная ликвидация;
- обеспечение высокой доступности коммуникаций и критических важных систем;
- защита беспроводных коммуникаций;
- распространение мер информационной безопасности на потребительские устройства как компоненты корпоративной ИС;
- повышение культуры пользователей в области информационной безопасности, обеспечение защиты от мер морально-психологического воздействия.

Заключение

Обеспечение информационной безопасности — проблема исключительной важности и сложности. Решить ее можно только на основе комплексного подхода, привлекающего меры безопасности всех уровней, реализующего динамическую трактовку ИБ как совокупность процессов в постоянно меняющемся окружении.

О правоприменительной практике и технической защите информации в области обмена информацией, содержащей сведения, отнесенные к государственной тайне

С. Нагорный
к.т.н. В. Донцов

Государственная тайна — это информация, которая имеет непосредственное уголовно-правовое значение, связанное с обеспечением государственной безопасности. В соответствии со ст.2 Закона РФ «О государственной тайне» от 21 июля 1993 г. государственную тайну Российской Федерации составляют защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации. Разглашение государственной тайны (придание огласке) означает, что сведения, составляющие государственную тайну, стали достоянием лиц, которые не имеют доступа к работе с такими сведениями или материалами, либо имеют доступ, но не к той информации, которая стала их достоянием в результате разглашения.

Так, в 1998 г. по ст. 283 УК был привлечен к ответственности и осужден бывший сотрудник ГРУ Генштаба Министерства обороны РФ подполковник Владимир Т., передавший своему бывшему сослуживцу по Центру космической разведки слайды с изображением городов некоторых ближневосточных стран, сделанные силами космической разведки. При этом способ разглашения сведений может быть любым (в разговоре, письме, выступлении, публикации, демонстрации схем, чертежей, изделий и т.п.) и на квалификацию содеянного не влияет. Объективная сторона преступления, предусмотренного ст. 283 УК, предполагает:

1) наличие действия или бездействия, заключающегося в разглашении государственной тайны;
2) наступления определенных последствий, когда сведения, не подлежащие огласке, стали достоянием постороннего лица;
3) наличие причинную связь между деянием и последствием.

Отсутствие последствия (например, разглашаемые сведения не были восприняты посторонними лицами) квалифицируются в соответствии со ст. 30 уголовного кодекса РФ как покушение на разглашение государственной тайны. **Лицо не может быть привлечено к ответственности по ст. 283 уголовного кодекса, если оно не знало того, что разглашаемые им сведения являются государственной тайной.**

Так, от ответственности за разглашение сведений, составляющих государственную тайну, был освобожден заместитель генерального директора межотраслевой ассоциации «Совинформспутник» В., передававший в Израиль 186 слайдов, отснятых с секретных фильмов космической съемки. На дубль-позитивах были изображены города Ближнего Востока и Израиля. **Дело прекратили на том основании, что В. не знал о секретном характере слайдов, так как гриф «секретно» на дубль-позитивах отсутствовал.**

Под субъектами, которым тайна стала известна по службе или работе, понимаются лица, специально не допущенные к работе со сведениями, составляющими государственную тайну, но в силу специфики своей работы или службы могущие знать эти сведения (рабочие, выполняющие работу на режимных предприятиях, охрана на этих предприятиях, шоферы, машинистки и пр.). Если разглашение совершает лицо, которому тайна не была доверена и не стала известна по службе или работе, но он узнал о ней от других лиц (например, в частном разговоре), его ответственность по ст. 283 УК исключается в силу отсутствия признаков специального субъекта.

Из вышеизложенного следует, что субъектом уголовного преследования являются физические лица, допустившие нарушения в порядке обращения с информацией, содержащей сведения, отнесенные к государственной тайне.

Учитывая судебную практику, попытаемся реализовать схему обмена информацией, содержащей сведения, отнесенные к государственной тайне, используя средства вычислительной техники.

Сетевая технология — это согласованный набор стандартных протоколов и реализующих их программно-аппаратных средств (например, сетевых адаптеров, драйверов, кабелей и разъемов), достаточный для построения вычислительной сети.

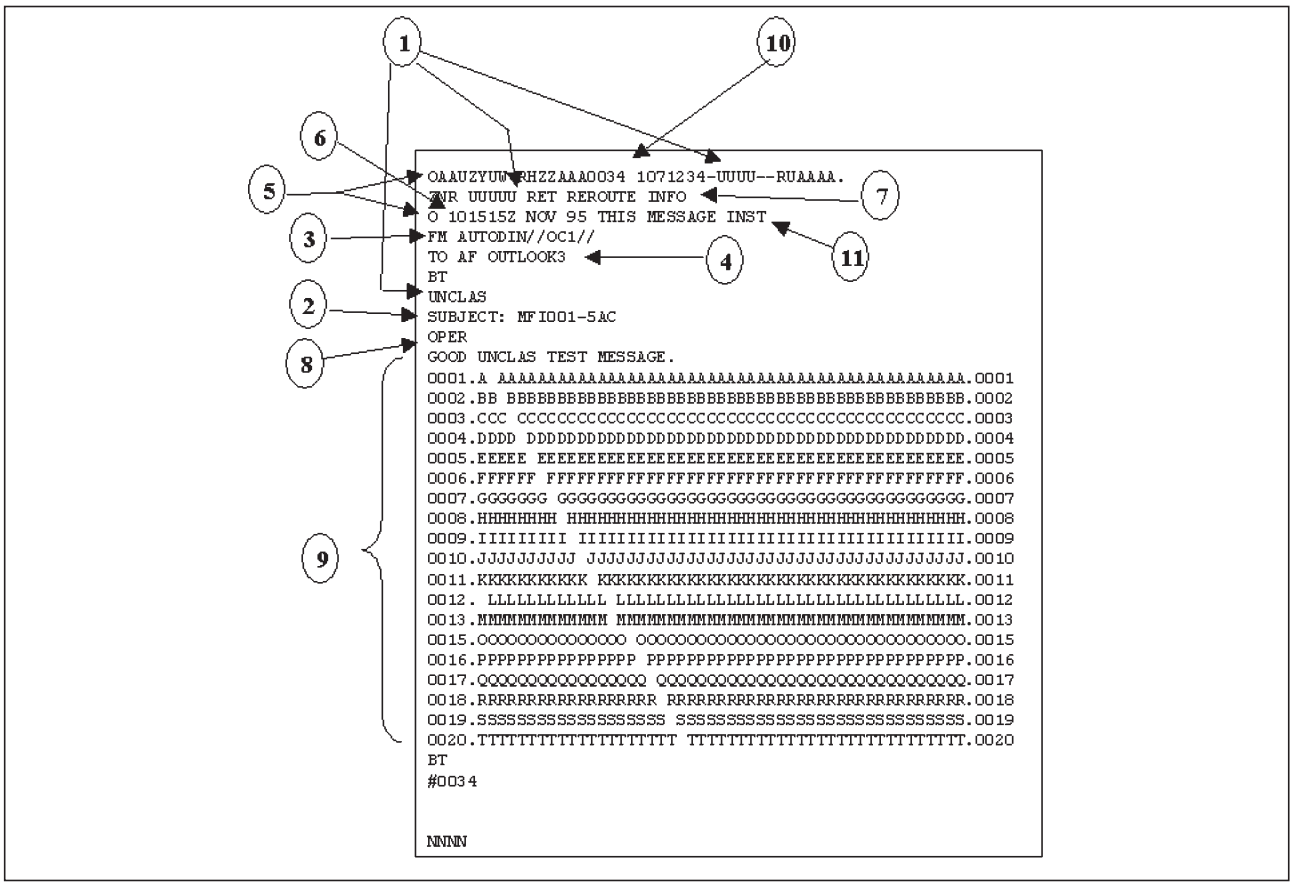
Передача информации с одного компьютера на другой происходит «кадрами». Любая подлежащая передаче информация при передаче с помощью сетевых ресурсов «компьютер-адресат» будет разделена на «кадры», которые впоследствии будут собраны у адресата.

В соответствии со ст.2 Закона РФ «О государственной тайне» от 21.07.1993 г, носителем информации, составляющей государственную тайну, является материальный объект, в том числе физическое поле, в котором сведения, составляющие государственную тайну, находят отображение в виде символов, образов, сигналов, технических решений и процессов. При этом на носители сведений, составляющих государственную тайну, наносятся следующие реквизиты:

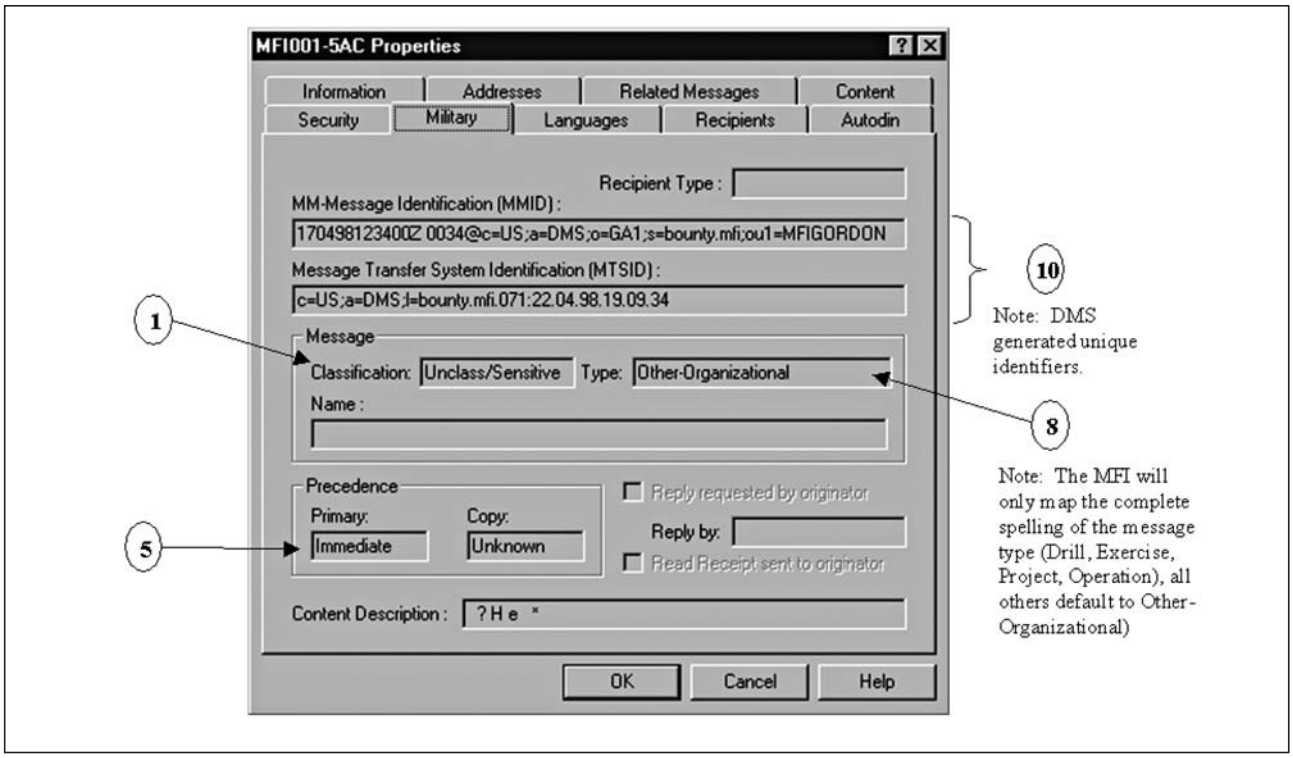
- степень секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти, на данном предприятии, в данном учреждении и организации перечня сведений, подлежащих засекречиванию;
- наименование органа государственной власти, предприятия, учреждения, организации, где осуществлено засекречивание носителя;
- регистрационный номер;
- дата или условия рассекречивания сведений, либо событие, после наступления которого сведения будут рассекречены.

Принимая во внимание положения Закона РФ «О государственной тайне», следует отметить, что нанесение реквизитов на носитель информации является обязательным. Таким образом, возникают две проблемы.

1. Как оповестить добросовестного пользователя сетевого ресурса о том, что он получил доступ к информации содержащей сведения, отнесенные к государственной тайне?
2. Как на носитель сведений, составляющих государственную тайну, нанести реквизиты?



Пример сообщения сети AUTODIN



Пример вида сообщения DMS

В протоколе IP предусмотрены средства передачи информации о безопасности дейтаграммы. Параметры IP обрабатываются всеми узлами IP. Они передаются в необязательных полях, находящихся в конце заголовка. Присутствие параметров в любом конкретном пакете не обязательно, но их поддержка должна быть реализована в обязательном порядке.

Поле безопасности имеет длину 16 бит и определяет один из 16 уровней безопасности, восемь из которых зарезервированы для использования в будущем. Коды безопасности перечислены в таблице 1. Некоторые из кодов используются только во внутренней работе организаций, отвечающих за ИБ.

код	описание
00000000 00000000	Открытая информация
11110001 00110101	Конфиденциальная информация
0Ш1000 10011010	EFTO
10Ш100 01001101	MMMM
01011110 00100110	PROG
10101111 00010011	Информация для служебного пользования
11010111 10001000	Секретная информация
01101011 11000101	Совершенно секретная информация
0011010111100010	Зарезервировано на будущее

Таблица 1. Коды безопасности

Поле дробления имеет длину 16 бит. Если передаваемая информация не дробится, поле состоит из одних нулей. Поле ограничений доступа имеет длину 16 бит.

Организационные сообщения обычно содержат служебную информацию. В сообщениях действующего формата эта информация упорядочена и отформатирована в форматные строки (FL), которые предоставляют специальные услуги и части данных по аналогии с текстом сообщения. Сообщения DMS имеют в конвертах сообщений подобные информационные области служебных данных Типичная служебная информация, содержащаяся в организационном сообщении, перечислена в таблице 2. Маркер на рисунке (круг с номером и стрелка) показывает номер и местоположение информации (в соответствии с номером пункта в таблице и пояснением), содержащейся в примерах сообщений AUTODIN формата JANAP128 и DMS.

Применение технологий, которые на аппаратном уровне будут извещать пользователя о том, что он получает информацию ограниченного использования, позволят в дальнейшем снять вопросы процедурного характера типа — «не знал».

Решение второй проблемы представляет наибольшую сложность. Особенно в части трактовки

Элементы служебной информации	Номер маркера на рисунке
Гриф секретности сообщения	1
Тема (предмет) сообщения	2
Отправитель сообщения	3
Действительный адрес получателей	4
Служебная информация адресации получателей	не показано
Старшинство сообщения (адрес и служебная информация получателей)	5
Дата и время отправки сообщения	6
Инструкции по обработке сообщения	7
Ссылки	не показано
Тип сообщения	8
Текст сообщения	9
Идентификатор (протокола формата) сообщения	10
Инструкции	11

Таблица 2. Служебная информация, содержащаяся в организационном сообщении

закона, что при **«невозможности нанесения таких реквизитов на носитель сведений, составляющих государственную тайну, эти данные указываются в сопроводительной документации на этот носитель»**.

Сложившаяся практика предлагает следующий инструмент: если нельзя нанести реквизиты на передаваемые по сетевым ресурсам кадры, то нужно «рассекретить» информацию в сети, применив криптографию. Шифротекст, полученный путем шифрования с помощью средств криптографической защиты информации незашифрованной секретной информации любых грифов, являются несекретными (п.6.13 РД «Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от несанкционированного доступа в автоматизированных системах и средствах вычислительной техники»).

Значительная роль алгоритмов шифрования в вопросе решения задач защиты электронной информации в массовом масштабе обусловила необходимость принятия стандартов шифрования, из которых наиболее известным и широко используемым является американский федеральный стандарт DES, принятый в середине 1970-х годов и послуживший аналогом для российского стандарта ГОСТ 28147-89. В настоящее время существует значительный выбор средств криптографической защиты информации, в том числе для сетевых технологий. Однако остаются открытыми вопросы передачи секретной информации между различными юридическими лицами и аттестации системы в целом.

Бухгалтерская отчетность как источник рассекречивания информации, содержащей сведения, отнесенные к государственной тайне

С. Нагорный
к.т.н. В. Донцов

В системе правоотношений, возникающих при обороте информации, особое место занимает институт государственной тайны. Значимость этого института в эпоху информационных технологий, когда информация становится особенно важным и ценным ресурсом в обществе, многократно возрастает. Государственная тайна существует во всех странах мира и является неотъемлемой составляющей суверенитета и системы управления.

На законодательном уровне правоотношения в сфере государственной тайны регулируются нормами Законов: от 27 июля 2006 г. N 149-ФЗ «Об информации, информационных технологиях и о защите информации», от 05.03.1992 N 2446-1 «О безопасности» (в ред. от 25.07.2002), от 04.07.1996 N 85-ФЗ «Об участии в международном информационном обмене» (в ред. от 30.06.2003) от 21.07.1993 N 5485-1 «О государственной тайне» (в ред. от 30.06.2003).

Закон «О государственной тайне» определяет, что основания для рассекречивания сведений, составляющих государственную тайну (ст. 13), возникают тогда, когда дальнейшая их защита становится нецелесообразной или когда Российская Федерация берет на себя международное обязательство по открытому обмену сведениями, составляющими государственную тайну. Срок засекречивания не может превышать 30 лет, хотя в исключительных случаях он может быть продлен по заключению Межведомственной комиссии по защите государственной тайны. Не реже одного раза в 5 лет проводится оценка соответствующих сведений на предмет их соответствия критериям секретности. Решения должностных лиц по рассекречиванию государственной тайны согласовываются с Межведомственной комиссией по защите государственной тайны. Законом о государственной тайне предусмотрено право граждан или юридических лиц ходатайствовать о рассекречивании государственной тайны. Соответствующее заявление должно быть рассмотрено в течение трех месяцев, а результат его рассмотрения может быть оспорен в суде. Гражданам или юридическим лицам дано право оспаривать в судебном порядке и правомерность отнесения сведений к государственной тайне.

Институт государственной тайны включает в себя две составляющих, одна из которых — критерии отнесения к категории государственной тайны информации, ограниченной для доступа, и соответственно определение степени секретности сведений.

Основным критерием для отнесения информации к государственной тайне является риск нанесения ущерба безопасности Российской Федерации (ст. 2 Закона «О государственной тайне»), возникающий тогда, когда появляется возможность распространения каких-либо сведений.

Такие сведения можно классифицировать следующим образом:

1. Сведения в военной области, касающиеся стратегических и оперативных планов, планов строительства и функционирования вооруженных сил, сведения о технологиях и производствах в военной сфере, о местонахождении и дислокации военных объектов. Сюда же следует отнести сведения из области экономики, науки и техники, связанные с обеспечением обороноспособности и безопасности государства.
2. Сведения в области разведки, контрразведки и оперативно-розыскной деятельности в стране и за ее пределами.
3. Сведения о финансово-кредитной, внешнеэкономической и внешнеполитической деятельности государства, преждевременное распространение которых может нанести ущерб его безопасности.

В соответствии с Законом «О государственной тайне», Указом Президента РФ от 30.11.1995 N 1203 (в ред. от 29.05.2002) определен следующий перечень сведений, отнесенных к государственной тайне:

- сведения в области разведывательной, контрразведывательной деятельности и защиты информации, раскрывающие организацию или фактическое состояние защиты государственной тайны;
- сведения, раскрывающие методы и средства защиты информации, содержащей сведения, составляющие государственную тайну, плани-

руемые и (или) проводимые мероприятия по защите информации от несанкционированного доступа, иностранных технических разведок и утечки по техническим каналам;
- сведения о системе президентской, правительственной, шифрованной связи, в том числе кодированной и засекреченной, о шифрах, их разработке, изготовлении и обеспечении ими, о методах и средствах анализа шифровальных средств и средств специальной защиты, об информационно-аналитических системах специального назначения.

В стандарте ГОСТ Р 50922-96 «Защита информации. Основные термины и определения» дано следующее толкование сведениям, изложенным в Указе Президента РФ от 30.11.1995 N 1203:

1. Мероприятие по защите информации — совокупность действий по разработке и/или практическому применению способов и средств защиты информации.
2. Мероприятие по контролю эффективности защиты информации — совокупность действий по разработке и/или практическому применению методов [способов] и средств контроля эффективности защиты информации.
3. Техника защиты информации — средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.
4. Средства защиты информации — техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации.
5. Средство контроля эффективности защиты информации — техническое, программное средство, вещество и/или материал, предназначенные или используемые для контроля эффективности защиты информации.

При проведении мероприятий в части технической защиты информации организации переходят в область гражданско-правовых отношений и финансового права. Нормы законодательства в части защиты государственной тайны в области финансового права в настоящее время детально не проработаны, поэтому существует возможность создания предпосылок для непреднамеренного рассекречивания информации, содержащей сведения, отнесенные к государственной тайне. В связи с этим авторы данного материала решили подробно остановиться на проблемах соблюдения режима секретности при проведении бухгалтерского учета мероприятий по защите информации.

Законодательство Российской Федерации о бухгалтерском учете включает Федеральный Закон от 21 ноября 1996 г. N 129-ФЗ «О бухгалтерском учете», устанавливающий единые правовые и методологические основы организации и ведения бухгалтерского учета в Российской Федерации, указы Президента Российской Федерации и постановления Правительства Российской Федерации. Основными целями законодательства Российской Федерации о бухгалтерском учете являются: обеспечение единообразного ведения учета имущества, обязательств и хозяйственных операций, осуществляемых организациями; составление и представление сопоставимой и достоверной информации об имущественном положении организаций и их доходах и расходах, необходимой пользователям бухгалтерской отчетности.

Бухгалтерским документом называется письменное свидетельство, которое подтверждает факт совершения хозяйственных операций, право на их совершение или устанавливает материальную ответственность работников за доверенные им ценности. Бухгалтерскими документами оформляются любые хозяйственные операции в той последовательности, в какой они совершаются. Это обеспечивает:

- непрерывный учет всех объектов учета; юридическое обоснование бухгалтерских записей, которые делают на основании документов, имеющих доказательную силу;
- использование документов для текущего контроля и оперативного руководства хозяйственной деятельностью организаций; контроль за сохранностью собственности, так как документами подтверждается материальная ответственность работников за доверенные им ценности;
- укрепление законности, поскольку документы служат основными источниками сведений для последующего контроля правильности, целесообразности и законности каждой хозяйственной операции при документальных ревизиях.
(Ст. 1 Федерального Закона от 21 ноября 1996 г. N 129-ФЗ «О бухгалтерском учете»).

Форма документа определяется совокупностью показателей (реквизитов) и их расположением в документах. Наименование показателей и их количество в документах зависят, в основном, от содержания отражаемой хозяйственной операции. Некоторые реквизиты являются основными (обязательными) для каждого документа. Они определяют содержание отражаемых операций и придают документу доказательную силу. Сюда относятся: наименование документа (формы); код формы;

дата составления; наименование организации, от имени которой составлен документ; содержание хозяйственной операции; измерители хозяйственной операции (в натуральном и денежном выражении); наименование должностей лиц, ответственных за совершение хозяйственной операции и правильность ее оформления, личные подписи указанных лиц. Перечень должностей лиц, имеющих право подписи первичных учетных документов, утверждает руководитель организации по согласованию с главным бухгалтером.

В зависимости от характера операции и технологии обработки данных в первичные документы могут быть включены дополнительные реквизиты. Первичные документы должны быть составлены в момент совершения операции, а если это не представляется возможным — непосредственно по окончании операции. Ответственность за своевременное и доброкачественное создание документов, передачу их в установленные сроки для отражения в бухгалтерском учете, за достоверность содержащихся в документах данных несут лица, создавшие и подписавшие эти документы (Статья 9 п.4 Федерального закона от 21 ноября 1996 г. N 129-ФЗ «О бухгалтерском учете»). В учреждениях все бухгалтерские документы, связанные с исполнением смет доходов и расходов по бюджетным средствам и средствам, полученным за счет внебюджетных источников, подписываются руководителем учреждения и главным бухгалтером или уполномоченными ими на то лицами. Документы без подписи главного бухгалтера или его заместителя считаются недействительными и не принимаются к исполнению. (Приходные кассовые ордера действительны при наличии подписи главного бухгалтера или его заместителя и кассира.)

Материально ответственные лица представляют первичные документы по приходу и расходу товарно-материальных ценностей при реестре сдачи документов. После проведенной в присутствии материально ответственного лица проверки правильности оформления представленных первичных документов реестр с подписью работника бухгалтерии возвращается материально ответственному лицу. С лицами, ответственными за хранение денежных средств и товарно-материальных ценностей, заключается письменный договор о полной индивидуальной материальной ответственности в установленном порядке.

Инструкция по бюджетному учету (утв. приказом Минфина РФ от 26 августа 2004г. N 70н) утвердила следующие унифицированные формы первичных учетных документов:

1. Перечень форм документов класса 03 Общероссийского классификатора управленческой документации (ОКУД) «Унифицированная система первичной учетной документации».
2. Перечень форм документов класса 05 ОКУД «Унифицированная система финансовой, учетной и отчетной бухгалтерской документации бюджетных учреждений и организаций».
3. Формы первичных учетных документов класса 05 ОКУД «Унифицированная система финансовой, учетной и отчетной бухгалтерской документации бюджетных учреждений и организаций».

Процессы приобретения средств технической защиты информации, их последующая установка и, соответственно, ввод в эксплуатацию находят свое отражение в бухгалтерской отчетности в соответствии с приказом Минфина РФ от 30 марта 2001 г. N 26н «Об утверждении Положения по бухгалтерскому учету «Учет основных средств» ПБУ 6/01».

Указанные операции оформляются следующими формами первичной учетной документации. Поступающие основные средства от других учреждений и организаций принимает комиссия, назначаемая руководителем организации. Для оформления приемки комиссия составляет в двух экземплярах акт приемки-передачи основных средств на каждый объект в отдельности. В актах указываются наименования объекта, год постройки или выпуска заводом, краткая характеристика объекта, первоначальная стоимость, присвоенный объекту инвентарный номер, место использования объекта и другие сведения, необходимые для аналитического учета основных средств. После оформления акт приемки-передачи основных средств передают в бухгалтерию организации. К акту прилагают техническую документацию, относящуюся к данному объекту (паспорт, чертежи и т. п.). На основании этих документов бухгалтерия производит соответствующие записи в инвентарные карточки основных средств, после чего техническую документацию передают в технический или другие отделы организации. Акт утверждает руководитель организации. При передаче основных средств другой организации, акт составляют в двух экземплярах (для сдающей и принимающей основные средства организаций).

Накладная на внутреннее перемещение основных средств применяется при передаче объектов основных средств от одного материально ответственного лица другому внутри учреждения или при централизованном учете — от одного учреждения другому. В акте указывают наименование объекта, его инвентарный номер, краткую характеристику технического состояния объекта, получателя

и сдатчика, с указанием их должностей и подписи, название структурных подразделений (организаций), сдающих и принимающих объект, подпись бухгалтера. Накладную утверждает руководитель организации.

Выдача основных средств со склада производится по накладным (требованиям), которые утверждаются руководителем учреждения. Накладную выписывает в двух экземплярах работник цеха (отдела) сдатчика. Первый экземпляр передают в бухгалтерию для записи в инвентарной карточке, а второй остается у сдатчика для отметки о выбытии соответствующего объекта в инвентарном списке основных средств. В накладной указывают наименование объекта, его инвентарный номер, сдатчика и получателя и другие необходимые сведения по переданному со склада объекту.

Таким образом, получая доступ к бухгалтерской отчетности, можно свободно получить:

- информацию о фактическом состоянии защиты государственной тайны;
- информацию, раскрывающую методы и средства защиты информации, содержащей сведения, отнесенные к государственной тайне;
- сведения о системе шифрованной связи, предназначенной для защиты информации, содержащей сведения, отнесенные к государственной тайне,

то есть получить легальный доступ к сведениям, составляющим государственную тайну.

Jet Info
ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ
Издается с 1995 года
Издатель: компания «Инфосистемы Джет»

Главный редактор: Дмитриев В.Ю. *(vlad@jet.msk.su)*
Редактор: Лапина И.К. *(lapina@jet.msk.su)*
Россия, 127015, Москва, Б. Новодмитровская, 14/1
тел. (495) 411 76 01
факс (495) 411 76 02
email: JetInfo@jet.msk.su http://www.jetinfo.ru

Подписной индекс по каталогу Роспечати 32555