МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОСНОВНЫЕ КОНЦЕПЦИИ

***Дорофеев Александр Владимирович**, CISSP, CISA*
***Марков Алексей Сергеевич**, кандидат технических наук, старший научный сотрудник, CISSP*

Публикация открывает серию статей, посвященных подготовке к сертификации специалистов по информационной безопасности. Рассмотрены основные понятия информационной безопасности: свойства, угрозы, уязвимости, риски, меры безопасности. Приведены классификация и примеры угроз информационной безопасности. Дано описание системы менеджмента информационной безопасности. Рассмотрены меры безопасности в контексте ISO 27001. Представлен порядок использования политик, стандартов, руководств.

***Ключевые слова**: сертификация специалистов, информационная безопасность, CISSP, менеджмент информационной безопасности, СМИБ.*

INFORMATION SECURITY MANAGEMENT: BASIC CONCEPTS

***Alexander Dorofeev**, CISSP*
***Alexey Markov**, Ph.D., Associate Professor, CISSP*

Publication opens a series of articles devoted to preparation for certification for information system security professionals. The basic concepts of information security such as properties, threats, vulnerabilities, risks, controls are reviewed. The classification and examples of information security threats are given. The information security management system is described. The measures of security in the context of ISO 27001 are discussed. The order of using of policies, standards and guidelines is shown.

***Keywords**: experts certification, information security, security controls, CISSP, information security management, ISMS, PDCA–model.*

Основные понятия информационной безопасности

Залогом успешной сдачи экзамена CISSP является хорошее понимание концепции управления информационной безопасностью в организации [1].

Прежде всего, следует разобраться, что стоит за такими понятиями как информационная безопасность, актив, угроза, уязвимость, контроль и риск.

Под *информационной безопасностью* (ИБ) обычно понимают состояние (свойство) защищенности ресурсов информационной системы в условиях наличия угроз в информационной сфере. Защита информации - это процесс, направленный на обеспечение информационной безопасности.

Определяющими факторами информационной безопасности являются угроза (threat) и риск (risk). *Угрозой* называют потенциальную причину (событие, нарушение, инцидент), снижающую уровень информационной безопасности системы, т.е. потенциально способную привести к негативным последствиям (impact) и ущербу (loss) системы или организации.

Риск представляет собой возможный ущерб, т.е. комбинацию (как правило, произведение) вероятности реализации угрозы и ущерба от нее.

Отметим, что угроза и риск определяются не вообще, а относительно конкретного защищаемого ресурса. В терминологии менеджмента бизнес-процессов вместо ресурса используется синонимическое понятие - *актив* (asset), под определение которого подпадает все, что имеет ценность для организации. В информационной сфере примерами активов являются: информация, программное обеспечение, аппаратное обеспечение, информационная система (сложный актив, включающий предыдущие), человек, имидж организации. В итоге, активами представляются все те объекты, которые подлежат защите путем выстраивания процессов информационной безопасности.

Таблица 1.

Примеры угроз информационной безопасности

Направления обеспечения безопасности	Техногенные		Природные
	Преднамеренные	Случайные	
Контроль физического доступа	Бомбардировка	Сон вахтерши	Торнадо
Сохранность оборудования	Вандализм	Запыление	Шаровые молнии
Управление коммуникациями	Прослушивание сети	Флуктуации в сети	Магнитные бури
Защита информационных хранилищ	Взлом парольной системы	Сбой криптосредств	Грибки
Управление непрерывностью деятельности	Последствие DOS-атаки	Последствия тестов на проникновения	Карстовые процессы
Соответствие законодательству	Компьютерное пиратство	Тиражирование персональных данных	Природные пожары

Угрозы классифицируют по ряду критериев:

- по причине возникновения (природные или техногенные, в том числе преднамеренные или случайные);
- по расположению источника (внешние или внутренние);
- по компрометируемой подсистеме или сегменту (сетевые, криптографические и др.);
- по этапу формирования в жизненном цикле системы (реализационные и эксплуатационные);
- по результирующему действию (нарушают целостность, конфиденциальность, доступность).

Примеры угроз представлены в табл.1.

Довольно подробные каталоги угроз подготовлены немецким федеральным агентством по информационной безопасности (BSI) [2].

Одной из основных угроз ИБ компьютерных систем является возможность реализации уязвимости (vulnerability) в ресурсах системы. Под *уязвимостью* понимают реализационный дефект («слабость»), снижающий уровень защищенности ресурсов от тех или иных угроз. Отметим, наличие уязвимости становится угрозой, если ее можно реализовать так, что это приведет к недопустимому ущербу организации. Например, наличие сетевых уязвимостей в программном обеспечении изолированного компьютера не является угрозой.

Умышленная реализация уязвимостей в компьютерных системах, приводящая к ущербу организации, называется *атакой* на ресурсы.

Защищенность системы достигается обеспечением совокупности свойств ИБ ресурсов и инфраструктуры, основными из которых являются:

- конфиденциальность (confidentiality),
- целостность (integrity),
- доступность (availability).

В зарубежных учебниках свойства конфиденциальности, целостности, доступности часто графически представляются в виде ссылки на треугольник CIA.

Конфиденциальность - свойство системы, определяющее ее защищенность от несанкционированного раскрытия информации.

Целостность - свойство, определяющее защищенность от несанкционированного изменения. Разделяют логическую и физическую целостность. Физическая целостность подразумевает неизменность физического состояния данных на машинном носителе. Логическая целостность отражает корректность выполнения процессов (транзакций), полноту и непротиворечивость информации, например, в СУБД, файловых системах, электронных архивах, хранилищах данных, системах управления документооборотом и т.д.

Доступность - характеристика, определяющая возможность за приемлемое время получить требуемую информационную услугу авторизованному пользователю. С доступностью часто связывают такую характеристику системы как готовность - способность к выполнению заявленных функций в установленных технических условиях. Атаки, имеющие целью нарушить степень доступности получили название атак на отказ в обслуживании (DOS-атаки).

Кроме названных, часто в качестве наиболее важных свойств ИБ системы, для выражения значимости, упоминают аутентичность, подотчетность, неотказуемость, надежность и др.

Повышение и обеспечение заданных уровней конфиденциальности, целостности и доступности ресурсов осуществляется путем применения мер (механизмов) безопасности, которые на профессиональном жаргоне часто называются контролями (от. англ. слова controls - инструменты/средства управления). Очень важно не путать этот жаргонизм с привычным словом «контроль», имеющим другое значение: наблюдение за поведением управляемой системы с целью обеспечения ее оптимального функционирования.

Контроли могут иметь технический (technical), организационный (administrative) и физический (physical) характер. Под понятие «технические контроли» подпадают программные и программно-аппаратные средства защиты, такие как антивирусы, межсетевые экраны, системы обнаружения вторжений, средства шифрования данных и т. п. В качестве организационных контролей выступают правила, обязательные для исполнения сотрудниками. Например, наличие согласования заявки на предоставление доступа к системе у ее владельца (как правило, руководителя бизнес-подразделения, отвечающего за процессы, которые поддерживаются данной системой). Хорошими примерами физических контролей являются двери, решетки, заборы, ограничивающие физический доступ к нашим активам.

Контроли могут придерживаться различных целей, например, быть превентивными (preventive), детективными (detective), корректирующими (corrective), восстанавливающими (recovery) и другими. Более подробно контроли мы рассмотрим в следующей публикации, касающейся вопросов обеспечения безопасного доступа.

Применение различных видов и типов контролей тесно связано с концепцией эшелонированной обороны (defense in depth, multilevel security), представляющей идеологию проектирования систем защиты с несколькими уровнями мер (механизмов) безопасности, позволяющими обеспечить эффективную защиту даже в случае «пробивания» обороны на одном уровне.

Управление информационной безопасностью

Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом уровне ИБ организации, называются управлением (менеджментом[1]) информационной безопасностью.

Система менеджмента информационной безопасности (СМИБ, ISMS) организации основывается на подходе бизнес-риска и предназначена для создания, реализации, эксплуатации, мониторинга, анализа, поддержки и повышения ИБ. В рамках СМИБ рассматривают структуру системы, политики, действия по планированию, обязанности, практики, процедуры, процессы и ресурсы организации.

Концепция СМИБ определяется в международном стандарте ISO/IEC 27001. В предыдущих редакциях стандарта требования к СМИБ были довольно явно сопоставлены с элементами модели Шухарта-Деминга «Планирование (Plan) - Реализация (Do) - Проверка (Check) – Совершенствование (Act)» (PDCA)[2]. По сути, цикл PDCA отражает руководство здравым смыслом при внедрении какого-либо процесса: прежде чем что-нибудь сделать мы планируем, затем это выполняем, после чего контролируем, что то, что сделали, соответствует тому, что хотели, а выявленные недостатки и отклонения устраняем. Из новой версии стандарта, вышедшей в 2013-м году, данная модель изъята, чтобы не ограничивать организации в выборе концепций управления процессами.

Рассмотрим, что требует от нас стандарт ISO 27001:2013 для построения системы управления информационной безопасностью[3].

В первую очередь необходимо определить контекст, в котором работает организация и четко понимать потребности и ожидания всех сторон, заинтересованных в функционирующей системе управления информационной безопасностью. К заинтересованным сторонам можно отнести владельцев бизнеса, клиентов, партнеров, регулирующие органы, сотрудников и др.

Важно, что стандарт позволяет задать границы системы управления информационной безопасностью, то есть дает возможность внедрить СМИБ «вокруг» определенных критичных бизнес-процессов, а затем уже при необходимости расширять область действия СМИБ на другие процессы.

Внедрение СМИБ невозможно без реальной поддержки со стороны топ-менеджмента организации, определяющего четкую политику информационной безопасности, включающую цели и обязательства выполнять все применимые требования (законодательства, партнеров, клиентов

1 Термин управление в данном разделе тождественен понятию менеджмента, используемому в системах качества по ISO 9000.

2 ISO/IEC 27001:2005 Information technology - Security techniques - Information security management systems – Requirements

3 ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems – Requirements

и т.п.). Руководство компании должно определить роли и обязанности в области ИБ и дать соответствующие полномочия сотрудникам, занимающимся внедрением СМИБ.

Введение в оценку рисков

На этапе планирования внедрения СМИБ в первую очередь формализуется процесс оценки рисков (risk assessment) информационной безопасности.

Методология оценки рисков в первую очередь должна определять критерии оценки и условия принятия рисков (рис. 1).

Методология должна быть разработана таким образом, чтобы его можно было повторить и получить сравнимые результаты.

В соответствии с ISO 27001:2013 в ходе процесса анализа рисков необходимо в первую очередь идентифицировать риски ИБ (risk identification) и определить владельцев рисков. Затем провести анализ рисков (risk analysis), в ходе которого определить вероятность риска, размер ущерба и соответственно определить уровень рисков. После чего провести оценивание риска (risk evaluation) относительно установленных критериев принятия рисков и задать приоритеты для обработки рисков (risk treatment).

Необходимо отметить, что отсутствует общепризнанное разделение процессов идентификации, анализа и оценивания рисков, поэтому в ходе экзамена кандидату необходимо в первую очередь обращать внимание на контекст, в котором используется тот или иной термин.

Очень важно понимать, что подходы к оценке рисков предусматривают также оценку уязвимостей (vulnerability assessment) и существующих контролей (control evaluation) для минимизации угроз.

Конкретные подходы к проведению оценки рисков информационной безопасности более подробно мы рассмотрим в следующем номере журнала.

В отношении рисков, значения которых не соответствуют критериям принятия, важно определиться с решением относительно их обработки. Приступая к выбору варианта «реагирования» на риск менеджмент компании, как правило, рассматривают различные аспекты, среди которых: соотношение стоимости затрат на внедрение предлагаемого контроля к возможному ущербу от реализации угрозы, соответствие контрмеры культуре компании, законодательству и т.п.

Помимо уже упомянутого принятия риска (risk accepting), заключающегося в том, что организация соглашается с возможной реализацией угрозы и принимает последствия, вариантами обработки рисков являются:

- *минимизация риска* (risk mitigation, reducing risk) посредством внедрения контролей;

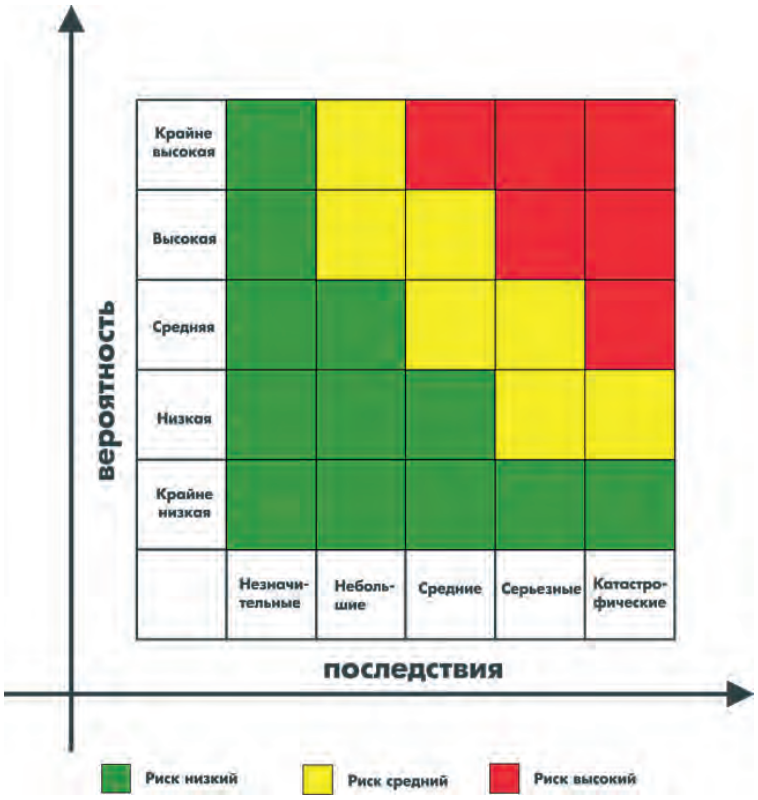

Рис. 1. *Матрица оценки рисков*

- *передача риска* (assigning risk, transferring risk), которая может заключаться как в его страховании, так и передаче подрядчику (в совокупности с процессами, передающимися на аутсорсинг),

- *избежание риска* (rejecting risk, avoiding risk), которое может заключаться в изменении процесса таким образом, что риск становится неактуальным.

Необходимо отметить, что в результате обработки риска остается так называемый *остаточный риск* (residual risk), который принимается менеджментом компании (владельцами рисков).

Внедрение контролей безопасности

На практике для большинства выявленных рисков принимается решение об их минимизации путем внедрения контролей. Стандарт ISO 27001:2013 содержит Приложение А, в котором приведены 114 контролей, распределенных по следующим 14-ти доменам:

A.5: Политики информационной безопасности
A.6: Организационные аспекты информационной безопасности
A.7: Вопросы безопасности, связанные с персоналом
A.8: Управление активами
A.9: Управление доступом
A.10: Криптография
A.11: Физическая безопасность и защита от угроз окружающей среды
A.12: Безопасность операций
A.13: Безопасность коммуникаций
A.14: Приемка, разработка и поддержка систем
A.15: Отношения с поставщиками услуг
A.16: Управление инцидентами информационной безопасности
A.17: Аспекты информационной безопасности в обеспечении непрерывности бизнеса
A.18: Соответствие требованиям

В случае внедрения СМИБ в соответствии с ISO 27001:2013 компания руководствуется Приложением А для выбора контролей, при этом, исключение контроля должно быть обоснованным, как и включение контроля, отсутствующего в стандарте.

Интересно, что контроли неравноценны. В целом контроли из Приложения А относятся к организационным мерам, например, встречаются контроли «Политика контроля доступа» (A.9.1.1), «Правила использования активов» (A.8.1.3), предусматривающие определение правил информационной безопасности в форме политик. Что же касается технически мер, то они формулируются исключительно общими словами, например, «Безопасность сетевых сервисов» (A.13.1.2).

После решения задачи выбора контролей, которые должны быть внедрены, чтобы снизить риски до приемлемого уровня, определяется: что конкретно должно быть сделано, какие ресурсы для этого необходимо задействовать, кто будет ответственным, и как будет проводиться оценка выполнения.

На данном этапе разрабатываются политики, процедуры, инструкции (подробнее о них ниже), внедряются технические средства защиты информации, проводится обучение специалистов, задействованных в процессах обеспечения ИБ, внедряется программа повышения осведомленности сотрудников компании в вопросах безопасности (security awareness program).

Контроль процессов

В результате внедрения контролей должны быть получены работающие процессы СМИБ, которые выполняются, измеряются и контролируются. Необходимо отметить следующие три важных составляющих контроля работы СМИБ:

- операционный контроль;
- внутренний аудит;
- анализ со стороны руководства.

Операционный контроль подразумевает собой текущий контроль со стороны непосредственных руководителей. Например, принятая процедура предусматривает выполнение периодического сканирования на наличие уязвимостей сетевых сервисов, и отвечает за эту функцию конкретный специалист отдела ИБ. Соответственно руководитель отдела следит за тем, чтобы задача выполнялась подчиненным, и он вовремя получал отчет с результатами сканирования.

Внутренний аудит заключается в периодической проверке эффективности контролей. Например, аудитор просит системного администратора предоставить перечень учетных записей, созданных в течение прошлого года, выбирает несколько и просит показать заявки, по которым он может убедиться, что доступ был согласован руководителями сотрудников и владельцами системы.

Анализ со стороны руководства подразумевает, что менеджмент интересуется тем, как работает СМИБ и, в частности, анализирует результаты проведенных аудитов (как внутренних, так и внешних), информацию о количестве произошедших инцидентов ИБ, в каком объеме требуются ресурсы для работы системы и т.п.

Результатом подобных контрольных мероприятий будет информация о недостатках и необходимых улучшениях системы. Концепция постоянного улучшения (continual improvement) СМИБ является одним из основных принципов стандарта.

Политики, процедуры, стандарты

Очевидно, что «спонтанно бессознательная» организация управления неприменима для сложных систем, поэтому СМИБ основывается на наборе внутренних нормативных документов: политиках, процедурах, корпоративных стандартах, руководствах и инструкциях.

Политика (policy) представляет собой документ, в котором определяются цели, задачи и пути их достижения, принципы.

Следует помнить, что часто под политикой информационной безопасности (information security policy) понимается высокоуровневый документ, предназначенный для обеспечения управления ИБ в соответствии с требованиями бизнеса, партнеров, клиентов, законодательной базы.

Высокоуровневая политика безопасности, как правило, представляет собой достаточно статичный документ. Такой документ обычно содержит:

- общую информацию об обеспечении ИБ в организации (в которой мотивировано определена необходимость обеспечения и поддержки режима безопасности);
- заявление о поддержке (commitment) мероприятий по обеспечению ИБ на всех управленческих уровнях;
- основные положения по определению целей ИБ;
- распределение ролей и определение общей ответственности за реализацию мероприятий по обеспечению ИБ (в том числе по разработке и корректировке политик);
- ссылки на низкоуровневые документы, конкретно определяющие порядок реализации тех или иных аспектов, связанных с обеспечением ИБ.

Документированная политика ИБ должна быть утверждена руководством и доведена до сведения всех сотрудников организации и внешних сторон, к которым она относится.

Кроме высокоуровневой политики выделяют низкоуровневые политики (частные политики, подполитики), как правило, отражающие требования в определенной области (домене). В качестве примеров политик низкого уровня можно привести политику управления доступом, политику управления паролями, политику резервного копирования и т.п.

Точный состав частных политик зависит от особенностей организации: ее размера, структуры, корпоративной культуры и т.п.

Стандарт (standard) определяет обязательное требование, практику применения какого-либо решения. Примером корпоративного стандарта является, например, стандарт на конфигурацию серверов под управлением Linux. Такие стандарты можно разрабатывать на основе чеклистов, доступных на сайте Center of Internet Security [3].

Руководства (guidelines) отличаются от стандартов в первую очередь тем, что носят рекомендательный характер. Руководства, в частности, могут определять, как именно следует реализовывать то или иное требование на практике с учётом локальной специфики. Так, например, специалист по информационной безопасности может разработать руководство, описывающее различные алгоритмы генерации надежных паролей, чтобы облегчить задачу выбора пароля пользователю.

Процедура (procedure) представляют собой документ, определяющий последовательность действий по выполнению какой-либо задачи в соответствии с требованиями политик и стандартов. Из процедуры должно быть ясно, кто, что и когда делает. Хорошим примером процедуры является процедура регистрации пользователей в системе, описывающая этапы согласования заявки на доступ.

Необходимо отметить, что, в основном, упомянутые документы ориентированы на специалистов отделов ИТ/ИБ, руководителей подразделений. Для неподготовленных сотрудников содержание данных документов может быть непонятным. В таких случаях разрабатывается документ «Свод правил для сотрудников», в котором доступным языком без использования технических терминов формулируются требования, которые должны выполнять сотрудники. Также функционал по обеспечению ИБ должен быть закреплен в положениях об отделах и должностных инструкциях.

К отдельным видам документов стоит отнести так называемые записи (records). Записи представляют собой те документы, которые создаются при выполнения процедуры, например, заявка на предоставление доступа к системе, журнал системы контроля доступа с информацией о том, кто входил в серверное помещение и т.п.

При внедрении СМИБ названия документов и их состав определяют, исходя из устоявшейся практики в компании. Политика может называться положением, процесс - порядком и т.п.

На рисунке 2 представлен возможный вариант структуры документации СМИБ.

Заключение

В настоящей статье мы рассмотрели ключевые понятия менеджмента информационной безопас-

Рис. 2. *Возможная структура документации СМИБ*

ности, разобравшись в которых можно серьезно повысить свои шансы на успешную сдачу экзамена CISSP [4-7].

Приоритетность изучения данной учебной информации обусловлена тем, что в пройденном разделе представлены основные понятия информационной безопасности, на которые мы будем ссылаться при публикации очередного учебного материала.

В следующем номере мы детально рассмотрим подходы к оценке рисков информационной безопасности.

Литература

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68
2. IT-Grundschutz Catalogues. Bundesamt für Sicherheit in der Informationstechnik, 2005. URL: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html (Дата обращения: 1.03.2014).
3. CIS Security Benchmarks. Center for Internet Security, 2014. URL: https://benchmarks.cisecurity.org/downloads/ (Дата обращения: 1.03.2014).
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012. 968 p.
5. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012. 936 p.
6. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition - McGrawHill, 2012. 1216 p.
7. Eric Conrad, Seth Misenar, Joshua Feldman. CISSP Study Guide, Second Edition - Syngress, 2012. 600 p.

References

1. Dorofeyev A.V. Status CISSP: kak poluchit i ne poteryat? Voprosy kiberbezopasnosti, 2013, No 1(1), pp. 65-68
2. IT-Grundschutz Catalogues, Bundesamt für Sicherheit in der Informationstechnik, 2005, URL: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html
3. CIS Security Benchmarks, Center for Internet Security, 2014, URL: https://benchmarks.cisecurity.org/downloads/
4. Steven Hernandez. Official (ISC)2 Guide to the CISSP CBK, Third Edition. - ISC2 Press, 2012, 968 p.
5. James M. Stewart, Mike Chapple, Darril Gibson. CISSP: Certified Information Systems Security Professional Study Guide, 6th Edition. - Sybex, 2012, 936 p.
6. Shon Harris, CISSP All-in-One Exam Guide, 6th Edition - McGrawHill, 2012, 1216 p.
7. Eric Conrad, Seth Misenar, Joshua Feldman. CISSP Study Guide, Second Edition - Syngress, 2012, 600 p.