«Сейфуллин оқулары – 12: Ғылым жолындағы жастар-болашақтың инновациялық әлеуеті» атты Республикалық ғылыми-теориялық конференция материалдары = Материалы Республиканской научно-теоретической конференции **«Сейфуллинские чтения-12:** Молодежь в науке - инновационный потенциал будущего" . – **2016**. – Т.1, ч.3 – С.350-353

МЕНЕДЖМЕНТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОСНОВНЫЕ КОНЦЕПЦИИ

Нұрланқызы А.

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

Определяющими факторами информацион- ной 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.

Угрозы классифицируют по ряду критериев [1]:

- 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 идр.);
- по этапу формирования в жизненном цикле системы (реализационные иэксплуатационные);
- по результирующему действию (нарушают целостность, конфиденциальность,доступность).

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

Примерыугрозинформационнойбезопасности

Направлениеобеспечениябезопасности	**Техногенные**		**Природные**
	Преднамеренные	**Случайные**	
Контрольфизическогодоступа	Бомбардировка	Сонвахтерши	Торнадо
Сохранностьоборудования	Вандализм	Запыление	Шаровыемолнии
Управлениекоммуникациями	Прослушиваниесети	Флуктуации в сети	Магнитныебури
Защитаинформационныхресурсов	Взломпарольнойсистемы	Сбойкриптосредств	Грибки

Управлениенепрерывностьюдеятельност	Последствие DOS-атаки	Последствиятестовнапроникнове	Карстовыепроцессы
Соответствиезаконодательству	Компьютерноепиратство	Тиражирование персональныхда	Природныепожары

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

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

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.

Управление информационной безопасностью. Скоординированные действия, выполняемые с целью повышения и поддержания на требуемом называются управлением (менеджментом) 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). 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.

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

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.

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 CenterofInternetSecurity [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.

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. [4]

На рисунке представлен возможный вариант структуры документации СМИБ.

Рис. Возможная структура документации СМИБ

Список литературы

1. Дорофеев А.В. Статус CISSP: как получить и не потерять? // Вопросы кибербезопасности. 2013. № 1(1). С.65-68

2. IT-GrundschutzCatalogues. BundesamtfürSicherheit in der Informationstechnik, 2005. URL: https://www.bsi.bund.de/EN/Topics/ITGrundschutz/itgrundschutz_node.html (Датаобращения: 1.03.2014).

3. CIS Security Benchmarks. Center for Internet Security, 2014. URL: https://benchmarks.cisecurity.org/downloads/ (Дата обращения: 1.03.2014).

4. Tom Lawton, Donna Goddard, Edward P Gibson. Managing Cyber risk: who has your information? Risk management solutions from Thomson Reuters 2015 GRC03174/ 7-15.

Руководитель: Курмангалиева Д.Б.- д.т. н., доцент