УДК 339.13

08.00.00 Экономические науки

**ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ УЧЕТА АКТИВОВ ПРИ СЕРТИФИКАЦИИ СИСТЕМ МЕНЕДЖМЕНТА**

Мирошниченко Марина Александровна
к.э.н, доцент, SPIN – код 3997-9450
marina_kgu@mail.ru

Мирошниченко Алексей Александрович
к.э.н, SPIN – код 6533-0359
mir_ko@mail.ru

Максимова Ольга Владимировна
магистрант, 2 курса Менеджмент,
Olga.Maksimova@foodunion.lv

*Кубанский государственный университет, Краснодар, Россия*

В статье показано, как выбрать для организации активы при проектировании системы менеджмента информационной безопасности. Как спроектировать, внедрить и сертифицировать систему менеджмента информационной безопасности при различных требованиях

Ключевые слова: АУДИТ, МЕНЕДЖМЕНТ РИСКОВ, ОБЪЕКТ ЗАЩИТЫ, СИСТЕМА МЕНЕДЖМЕНТА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, СИСТЕМА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

UDC 339.13

Economics

**INFORMATION SECURITY OF THE ACCOUNTING OF ASSETS AT CERTIFICATION OF MANAGEMENT SYSTEMS**

Miroshnichenko Marina Aleksandrovna
Cand.Econ.Sci., associate professor,
RSCI SPIN – code 3997-9450, marina_kgu@mail.ru

Miroshnichenko Alexey Aleksandrovich
Cand.Econ.Sci., RSCI SPIN – code 6533-0359
mir_ko@mail.ru

Maximova Olga Vladimirovna
2nd-year master student of the Management Department
Olga.Maksimova@foodunion.lv
*Kuban state university, Krasnodar, Russia*

Process of a choice for the organization of assets at design of information security management system is presented in article. There is the way in article how to design, introduce and certify information security management system at various requirements

Keywords: AUDIT, RISK MANAGEMENT, OBJECT OF PROTECTION, INFORMATION SECURITY MANAGEMENT SYSTEM, SYSTEM OF ENSURING OF INFORMATION SECURITY

## Информационная безопасность учета активов при сертификации систем менеджмента

Проблема внедрения результативной системы менеджмента информационной безопасности (СМИБ) в соответствии с требованиями стандартов ISO серии 27000 [1, 2] актуальна на сегодняшний день. Требования к проведению аудитов систем менеджмента (СМ) изложены стандарте [3]. В ряде источников доступны стандарты на системы обеспечения информационной безопасности (СОИБ), которые в своей основе содержат некоторые требования стандартов [1, 2]. Объективно существуют различия в требованиях СОИБ организации, которые могут

препятствовать успешному внедрению СМИБ (например, различия в понятиях «актив» и «объект защиты») и проведению независимой оценки (сертификации) требованиям базового сертификационного стандарта [1]. В том случае, когда топ менеджмент организации принимает решение о подготовке существующей СМИБ сертификационному аудиту, представляется необходимым проанализировать требования СОИБ организации и принять решение о комплексе мероприятий, которые следует выполнить для обеспечения соответствия требованиям [1]. Для реализации управляемых условий данного процесса необходимо провести идентификацию и оценку активов.

**Учет различий при выявлении и оценки активов (объектов защиты) СМИБ.**

Если организация решает применять национальный или международный стандарт, она вынуждена проводить сопоставление своих процессов, реализованных изначально только под конкретные, отраслевые требования. При этом возможны упущения при выполнении анализа рисков нарушения информационной безопасности (ИБ) и недостаточно полное изучение уязвимости процессов переработки информации в автоматизированных системах. Ситуация может иметь более серьезные последствия, если конкретная отраслевая система (в частности СОИБ) изначально создавалась на базе зарубежных стандартов, но не актуализировалась при их изменении.

В данной статье будут рассмотрены два основных фундаментальных различия, которые, на наш взгляд, могут иметь критичные последствия для освоения и успешной сертификации СМИБ организации на соответствие требованиям стандарта [1]. Эти несоответствия могут стать причиной торможения замысла создания СОИБ организации и потери важного преимущества любой успешно внедренной системы менеджмента – содействие достижению целей бизнеса. Второе негативное последствие

выявленных различий, имеющее измеримое значение, – дополнительные издержки по приведению СМИБ к уровню, достаточному для адекватного выполнения требований стандарта [1].

Отметим, что в практике создания СМИБ важно сконцентрировать экспертные усилия на формировании достоверных моделей и методов проведения внутреннего аудита и эффективного мониторинга состояния объектов, находящихся под воздействием угроз ИБ.

**Различие 1. Идентификация (классификация) активов.**

Для анализа первого различия рассмотрим требования стандарта [1] в части управления активами и требования организации по классификации объектов защиты. Известно определение: «Активы – это все, что имеет ценность для организации» [1]. Для установления ценности активов организация должна определить все свои активы на соответствующем уровне детализации. Там же сказано, что могут различаться два вида активов: основные, включающие бизнес-процессы, бизнес-деятельность и информацию, и вспомогательные (поддерживающие), от которых зависят основные составные части, включающие аппаратные средства, программное обеспечение, информационную сеть, персонал, место функционирования организации и структуру организации.

В фазе «План» цикла PDCA предложенного Шухартом–Демингом указано, что организация должна, определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий [1]. В свою очередь, в требованиях СОИБ организации по классификации объектов защиты (ОЗ) приводятся другие термины и определения, где ОЗ трактуется в терминах: автоматизированная система (АС), информационный актив (ИА), программное обеспечение (ПО).

Согласно требованиям организации, под ОЗ понимают информационные активы, технические и программные средства их

обработки, передачи, хранения. Этот перечень ОЗ является закрытым, объективно явно меньшим, чем список активов, представленный в [2]. Соответственно одним из критичных рисков при сертификации объективно может быть явная неполнота идентифицированных и принятых к защите ОЗ в СОИБ организации. Так, в требованиям к организации никак не учтены активы по следующим категориям: персонал, место расположения (объекты) и структура организации. Необходимо обратить внимание, что предложенный подход в системе СОИБ организации вносит существенные сложности в текущий процесс поддержания и обеспечения ИБ, в частности в области управления инцидентами ИБ и рисками ИБ.

В ГОСТ Р ИСО/МЭК 18044-2007 используются примеры инцидентов ИБ, связанных с персоналом, и в новом стандарте ISO серии 27040 по обеспечению безопасности хранящихся данных учитывается важнейшая роль внутреннего и внешнего персонала в обеспечении требуемого уровня ИБ на объектах инфраструктуры. В стандарте организации зафиксированы правила идентификации ОЗ и требование установить собственника, владельца и пользователя конкретного ОЗ. Каждый ОЗ должен быть отнесен только к одному из следующих типов: ИА, ПО, ТС (технические средства обработки, хранения и передачи информации).

Также в требованиях организации перечислены правила определения критичности ОЗ. На основании полученных данных ОЗ вносят с одну из групп максимального, среднего или минимального уровня критичности.

В требованиях организации представлены правила учета ОЗ. Основными задачами учета являются сбор, обработка и систематизация данных об ОЗ. Отмечается, что должна проводиться обязательная регистрация фактов создания, приобретения, передачи, дублирования, снятия с эксплуатации и уничтожения ОЗ.

Таким образом, можно сделать вывод по первому различию. Для разработки и успешной сертификации СМИБ по стандарту (в таблице 1

для наглядности приведены примеры классификации групп активов СМИБ) только выполнения требований, предъявляемых к СОИБ организации, объективно недостаточно, так как учитывается крайне ограниченное множество сущностей, которые объективно можно назвать критичными активами для бизнеса.

Таблица 1 – Классификация групп активов СМИБ организации

| № | Группа | Код |
|---|---|---|
| 1 | Автоматизированные системы | АС |
| 2 | Информационные сервисы пользователя | ИСП |
| 3 | Информационные инфраструктурные сервисы | ИИС |
| 4 | Помещения | Пом. |
| 5 | Средства защиты информации | СЗИ |
| 6 | Персонал | Перс. |
| 7 | Активы на бумажных носителях | Бум. |

**Различие 2. Оценка рисков информационной безопасности.**

Рассмотрим требования [1, 2] в части управления рисками ИБ и требования СОИБ организации по анализу и оценке рисков. Основные определения, необходимые для анализа второго различия, приведены в [1]. Требования по управлению рисками ИБ удобно разложить по фазам цикла PDCA, аналогично различию 1: в фазах «Планируй», «Делай» и «Проверяй» соответственно [4].

В свою очередь, в требованиях СОИБ организации по анализу и оценке рисков выполняются следующие основные процедуры: идентификация, анализ и оценивание риска. Оценка рисков осуществляется для АС, в состав которых входит хотя бы один ОЗ с максимальным уровнем критичности, определяемым в соответствии с требованиями организации. Таким образом, объективно есть критичный риск для успешной сертификации СМИБ, при котором деятельность по оценке рисков в терминах только СОИБ может вообще не проводиться.

Соответственно деятельность, предусмотренная СОИБ организации, не будет осуществляться на «законных» основаниях, что, скорее всего, приведет к ошибкам в процессах выявления, идентификации и классификации угроз нарушения ИБ для ОЗ, а также к недостоверному анализу рисков нарушения ИБ и уязвимостей в процессах переработки информации в АС в установленной области применения. Важно подчеркнуть, что так называемая вложенность критичных рисков — невыполнение оценки рисков (различие 2) бывает прямым следствием исключения персонала из активов в СОИБ (различие 1) и объективно может привести к значительным несоответствиям на внешнем сертификационном аудите СМИБ. В рамках работ по идентификации рисков необходимо выполнить идентификацию элементов риска, т.е. ОЗ, угроз ОЗ и уязвимостей ОЗ организации. По анализу рисков определяют:

– возможный ущерб, наносимый в результате нарушений свойств безопасности ОЗ;

– уровень вероятности наступления такого нарушения с учетом идентифицированных угроз и уязвимостей, а также реализованных защитных мер;

– величину риска.

Оценка возможного ущерба производится по трехуровневой качественной шкале: максимальная, средняя и минимальная величина. Как правило, при решении конкретных прикладных задач значения критериев измеряются в пределах определенной шкалы и выражаются в установленных единицах. Применение качественной шкалы для оценки возможного ущерба ИБ представляется не вполне оправданным и методически уязвимым с позиции обеспечения достижения измеримых целей – создание СМИБ, постоянное повышение ее результативности и успешная сертификация на соответствие требованиям [1].

В стандарте организации отмечается, что максимальная величина

возможного ущерба характеризуется максимальным уровнем критичности ОЗ, средняя величина возможного ущерба – средним уровнем критичности ОЗ, минимальная величина возможного ущерба – минимальным уровнем критичности ОЗ. Существуют затруднения для определения уровня возможного ущерба для активов (в терминах стандартов ISO), но не учтенных как ОЗ в системе СОИБ, например: персонал (собственный и посторонний), серверные помещения, помещения для проведения конфиденциальных переговоров и т.п.

Следующий шаг при оценке рисков – сравнение полученных величин риска с заранее определенной шкалой уровня риска организации. Должны быть идентифицированы уровни риска, которые являются приемлемыми и принятыми риски, не превышающие приемлемого уровня. Также должны приниматься риски, превышающие допустимый уровень, если для них отсутствует подходящий способ обработки. Все остальные риски должны обрабатываться. Это положение создает существенное затруднение для подготовки СМИБ к сертификации. Так как известное требование – выполнение анализа СМИБ со стороны руководства [1] явно предусматривает учет в качестве входной «информации об уязвимостях или угрозах, которые не были адекватно рассмотрены в процессе предыдущей оценки риска» [5], и в СОИБ организации не выполняется в силу применяемой парадигмы формирования ОЗ.

Одним из важнейших и принципиальных различий между СМИБ и СОИБ является различие в терминах «актив» и «объект защиты». Соответственно необходимо предложить методический подход, который позволит адаптировать существующую СОИБ к требованиям СМИБ и обеспечить результативность проведения как различных аудитов, так и мониторинга состояния объектов, находящихся под воздействием угроз нарушения ИБ организации. В этом случае необходимо преобразовать принятую в СОИБ систему ОЗ в соответствии с требованиями определения

всех групп активов СМИБ по стандарту [1]. Для наглядности приведены примеры реестра группы активов АС (таблица 2), оценки рисков ИБ для актива АС «Босс Кадровик» (таблица 3) исследуемой организации.

Таблица 2 – Реестр группы активов АС

| № | Код | Наименование | Бизнес-функции | Служба в области сертификации СМИБ | Уровень критичности | Размещение |
|---|---|---|---|---|---|---|
| 1 | Босс | АС «Босс Кадровик» | Обеспечение финансовых данных о зарплате | Служба персонала (в части обработки персональных данных), Служба «А» (в части сопровождения СЗИ), Служба «Б» (в части инфраструктуры связи) | Средний | Здание «А» |

Таблица 3 – Оценка рисков ИБ для актива АС

| № риска | Наименование риска | Критичность актива | Уровень уязвимости | Уровень вероятности реализации угрозы | Величина риска | Уровень риска |
|---|---|---|---|---|---|---|
| 1 | Нарушение конфиденциальности информации в АС «Босс Кадровик» | Средний | Средний | Средний | 4 | Средний |
| 2 | Нарушение целостности информации в АС «Босс Кадровик» | Средний | Максимальный | Минимальный | 4 | Средний |
| 3 | Нарушение доступности информации в АС «Босс Кадровик» | Средний | Средний | Минимальный | 5 | Средний |

**Оценка результативности ИСМ с учетом требований СМИБ.**

Учет активов в соответствии с требованиями стандарта ISO [1] позволит привнести в интегрированную систему менеджмента (ИСМ) элемент управляемости по единым целям, измеримым в терминах бизнеса. Для ИСМ, в составе которой есть СМИБ, могут быть применены соответствующие метрики. Широко известны примеры формирования простых метрик ИБ, которые позволят получить количественные оценки

(метрики) как доказательства «полезности» для бизнеса. Здесь представляется особенно важным сразу сделать сопоставление с механизмами внутреннего аудита, которые предназначены именно для представления объективных доказательств высшему руководству с целью принятия эффективных управленческих решений [5]. Различные виды метрик для обеспечения ИБ следует сгруппировать следующим образом:

- для оценки основного бизнеса, например, доля на рынке, уровень лояльности клиентов;
- для управления издержками, например, ТСО (совокупная стоимость владения), ROI (оценка возврата инвестиций);
- для оптимизации текущей деятельности, например, оптимизация затрат (прямых и косвенных).

С целью снижения издержек (это одна из приоритетных задач любого бизнеса и наиболее презентабельная форма оценки результативности службы ИБ) применяются метрики, показывающие степень достижения возможного максимума (плана продаж, выполнения в срок проектов и пр.). Соответственно могут быть предложены различные типы:

– простые метрики (например, число выявленных инцидентов ИБ);

– сложные метрики (например, отношение стоимости средств защиты информации к стоимости ИТ-активов);

– комплексные метрики (например, число произошедших инцидентов ИБ, приведших к ущербу или вынужденному простою в АС, определенных как критичные для бизнеса).

При планировании и реализации проектов по сертификации СМИБ организации необходимо принимать во внимание, что множество требований произвольной системы отраслевой сертификации в общем случае не соответствует требованиям сертификационного стандарта ISO серии 27000.

Для адаптации СОИБ необходима продуктивная методика,

основанная на сопоставлении стандартных требований в области ИБ и обеспечивающая достижение целей по проведению внутреннего аудита и эффективного мониторинга состояния объектов, находящихся под воздействием угроз ИБ, на основании сформированных достоверных моделей и методов.

Реализация требований современных стандартов к СМИБ, совмещенных с существующей СОИБ, приводит к необходимости пересматривать фундаментальные требования (например, в отношении понятий «актив» и «менеджмент рисков»). Это обстоятельство напрямую связано с определяемой высшим руководством областью сертификации и с перечнем активов, признанных жизненно важными для организации, и по этой причине подлежащих защите в составе СМИБ.

**Библиографический список**

1 ГОСТ Р ИСО/МЭК 27001-2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования.

2 ГОСТ Р ИСО/МЭК 27005-2010. Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности.

3 ГОСТ Р ИСО 19011-2011. Руководящие указания по проведению аудитов систем менеджмента.

4 Лившиц И.И. Оценки соотношения количественных показателей сертификации систем менеджмента предприятий // Менеджмент качества. 2014. Вып. 2.

5 Лившиц И.И. Совместное решение задач аудита информационной безопасности и обеспечения доступности информационных систем на основании требований международных стандартов BSI и ISO // Информатизация и связь. 2013. Вып. 6.

**References**

1 GOST R ISO/MJeK 27001-2006. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Sistemy menedzhmenta informacionnoj bezopasnosti. Trebovanija.

2 GOST R ISO/MJeK 27005-2010. Informacionnaja tehnologija. Metody i sredstva obespechenija bezopasnosti. Menedzhment riska informacionnoj bezopasnosti.

3 GOST R ISO 19011-2011. Rukovodjashhie ukazanija po provedeniju auditov sistem menedzhmenta.

4 Livshic I.I. Ocenki sootnoshenija kolichestvennyh pokazatelej sertifikacii sistem menedzhmenta predprijatij // Menedzhment kachestva. 2014. Vyp. 2.

5 Livshic I.I. Sovmestnoe reshenie zadach audita informacionnoj bezopasnosti i

obespechenija dostupnosti informacionnyh sistem na osnovanii trebovanij mezhdunarodnyh standartov BSI i ISO // Informatizacija i svjaz'. 2013. Vyp. 6.