ПРЕДИСЛОВИЕ

Учебное пособие «Управление рисками информационной безопасности» является второй частью серии учебных пособий «Вопросы управления информационной безопасностью».

При подготовке данного учебного пособия были поставлены следующие задачи:

1) определить основные понятия, относящиеся к управлению рисками информационной безопасности (ИБ);

2) детально рассмотреть составляющие процесса управления рисками ИБ (ПУРИБ);

3) описать различные подходы к анализу и оценке рисков ИБ;

4) проанализировать систему управления рисками ИБ (СУРИБ);

5) рассмотреть необходимое документальное обеспечение и применяемые в настоящее время инструментальные средства управления рисками ИБ (УРИБ).

Исходя из поставленных задач, была определена структура учебного пособия «Управление рисками информационной безопасности», которое состоит из введения, 6 глав, приложения, глоссария и списка литературы из 35 наименований.

Во введении обоснована актуальность темы учебного пособия.

Далее кратко анализируется нормативное обеспечение управления рисками ИБ, последовательно вводится понятие риска ИБ и определяются процесс и система управления рисками ИБ.

В основных главах учебного пособия детально рассматриваются составляющие ПУРИБ, а именно:

- установление контекста УРИБ с определением базовых критериев принятия решений и определения области действия и границ УРИБ;
- оценка рисков ИБ, состоящая из двух этапов — анализ (с идентификацией активов, угроз ИБ, существующих элементов управления, уязвимостей и последствий) и оценивание (с определением последствий, вероятностей и количественной оценки рисков) рисков ИБ;

- обработка рисков ИБ, включающая снижение, сохранение, предотвращение и перенос;
- принятие, коммуникация, мониторинг и переоценка рисков ИБ.

Также анализируются различные подходы к оценке рисков ИБ — высокоуровневая, детальная, комбинированная и базовая оценка рисков ИБ и подход к оценке рисков ИБ Банка России. В завершении основной части учебного пособия кратко описываются кадровое и документальное обеспечение и инструментальные средства УРИБ.

В заключении кратко выделяется взаимосвязь изученных понятий, относящихся к УРИБ, а также устанавливается связь между материалом учебного пособия и составляющими профессиональных компетенций.

В приложении приводится информация справочного характера по инструментальным средствам УРИБ и принятым сокращениям.

Освоение материалов данного учебного пособия формирует у обучающихся следующие профессиональные компетенции:

- способность участвовать в управлении ИБ объекта в части оценки и обработки рисков ИБ;
- способность участвовать в проектировании и разработке системы управления ИБ объекта в части применения методов оценки и обработки рисков ИБ, т. е. СУРИБ.

Эти профессиональные компетенции необходимы для решения задач, относящихся к таким видам профессиональной деятельности в сфере управления ИБ, как проектная и организационно-управленческая.

После изучения учебного пособия «Управление рисками информационной безопасности» обучающиеся будут

Знать:

- современные подходы к УРИБ и направления их развития;
- особенности отдельных процессов УРИБ в рамках СУИБ;
- основные международные и российские стандарты, регламентирующие УРИБ.

Уметь:

- анализировать текущее состояние ИБ на предприятии с целью разработки требований к разрабатываемым процессам УРИБ;
- определять цели и задачи, решаемые разрабатываемыми процессами УРИБ;
- разрабатывать процессы УРИБ, учитывающие особенности функционирования предприятия и решаемых им задач;
- практически решать задачи формализации разрабатываемых процессов УРИБ;

- проектировать СУРИБ.

Владеть:

- терминологией в области УРИБ;
- навыками анализа активов организации, их угроз ИБ и уязвимостей в рамках УРИБ.

Материалы, вошедшие в учебное пособие «Управление рисками информационной безопасности» обеспечивают учебно-методической базой любую учебную дисциплину, относящуюся к управлению ИБ. Однако в полной мере данное учебное пособие может быть востребовано при подготовке профессионалов в области управления ИБ. Поэтому оно может быть рекомендовано студентам высших учебных заведений, обучающимся по программам магистратуры направления 10.04.01 — «Информационная безопасность».

Кроме того, учебное пособие из серии «Вопросы управления информационной безопасностью» может быть полезным при реализации программ дополнительного образования (курсы повышения квалификации или переподготовки кадров).

Важно подчеркнуть, что для приступающих к ознакомлению с данным учебным пособием есть определенные требования по предварительной подготовке. Например, следует знать основы теории ИБ и комплексный подход к обеспечению ИБ (ОИБ), уязвимости и угрозы ИБ в информационной среде. Следует рекомендовать предварительное ознакомление с материалом первой части серии учебных пособий «Основы управления информационной безопасностью».

Авторы признательны коллегам по НИЯУ МИФИ, а также всем рецензентам.

Авторы, естественно, не претендуют на исчерпывающее изложение всех названных в работе аспектов проблемы управления ИБ организации, поэтому с благодарностью внимательно изучат и учтут критические замечания и предложения читателей при дальнейшей работе над учебным пособием.

ВВЕДЕНИЕ

Любая организация практически всегда подвергается ряду рисков ИБ, которые могут рассматриваться как одна из основных категорий бизнес-рисков или быть отнесены к другим категориям, наряду со стратегическими и операционными рисками. Такие риски желательно выявить как можно раньше и еще до того, как они реализовались (в этом случае принятие соответствующих мер обычно требует меньших ресурсов). После выявления риска ИБ необходимо принять решение об ответных действиях, позволяющих снизить вероятность неблагоприятного события или уменьшить его последствия в случае реализации риска. При этом желательно, чтобы расход ресурсов был минимальным.

Основу методологии управления рисками информационной безопасности (УРИБ) составляет системный подход.

Такой подход к УРИБ как к непрерывному процессу помогает идентифицировать потребности организации в обеспечении ИБ (ОИБ) и создать эффективную систему управления ИБ (СУИБ).

В определении СУИБ отмечается, что это часть общей системы управления, основанная на оценке рисков ИБ [1, 2].

В основных стандартах, посвященных вопросам УРИБ, — ISO/IEC 27005:2018 и ГОСТ Р ИСО/МЭК 27005–2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности» (идентичный первой редакции ISO/IEC 27005:2008) — также указывается, что риск-ориентированный подход содействует адекватному обеспечению ИБ (ОИБ) [3, 4].

Деятельность по ОИБ обеспечивает своевременное и эффективное реагирование на риски ИБ там и тогда, где и когда это наиболее необходимо.

Почему такое значение уделяется процессу УРИБ (ПУРИБ) в рамках СУИБ? Вся информация организации, системы, приложения, сети и оборудование, которое поддерживает их работу, — это важные активы организации. Против этих активов могут быть ре-

ализованы угрозы ИБ, которые могут привести не только к финансовому ущербу, но и к потере репутации организации, что в современном мире конкуренции может быть даже более существенно.

Для этого необходимо применять меры ОИБ — действия, процедуры или средства, которые могут защищать от реализации угроз ИБ, обнаруживать нежелательные события и инциденты ИБ, ограничивать их негативные последствия, а также способствовать восстановлению активов организации после инцидента ИБ.

Построение эффективной системы обеспечения ИБ (СОИБ) в условиях ограниченности всех видов ресурсов и времени, с учетом ценности активов и их уязвимостей и вероятных угроз ИБ для активов, а, значит, и выбор адекватных мер ОИБ, необходимых для достижения достаточного уровня ИБ, должен основываться на результатах анализа рисков ИБ.

Эти результаты являются отправной точкой для установления и поддержки эффективного управления ИБ и обязательно используются при написании всех политик обеспечения ИБ (кратко политика ИБ — далее ПолИБ) организации — корпоративной и частных — и выработки требований по ОИБ.

Решения о расходах на мероприятия по управлению ИБ также должны приниматься с учетом возможного ущерба, нанесенного в результате нарушения ИБ организации.

Именно современные методики УРИБ, проектирования и сопровождения СОИБ дают возможность организации осуществить следующее [5]:

- количественно оценить текущий уровень ИБ, обосновать приемлемые риски ИБ, разработать план мероприятий по поддержанию требуемого уровня ИБ на организационно-управленческом, технологическом и техническом уровнях;
- рассчитать и экономически обосновать размер необходимых вложений в СОИБ, соотнести расходы на ОИБ с потенциальным ущербом и вероятностью его возникновения;
- выявить и провести первоочередные мероприятия для устранения наиболее опасных уязвимостей до осуществления атак на уязвимые ресурсы;
- определить функциональные отношения и зоны ответственности при взаимодействии подразделений и лиц, ответственных за ОИБ в организации, создать или модифицировать необходимый пакет организационно-распорядительной документации;
- разработать и согласовать со службами организации и надзорными органами проект внедрения необходимых комплексов за-

щиты, учитывающий современный уровень и тенденции развития информационно-коммуникационных технологий (ИКТ);

- организовать поддержание внедренного комплекса защиты в соответствии с изменяющимися условиями работы организации, регулярными доработками организационно-распорядительной документации, модификацией технологических процессов и модернизацией технических средств защиты информации (СЗИ).

В учебном пособии подробно рассмотрены основополагающие аспекты, связанные со сложными процессами УРИБ как составной части более общего процесса управления ИБ и с построением СУРИБ как части СУИБ.

Все представленные сведения могут быть переработаны для целей создания собственного подхода к оценке рисков ИБ, учитывающего бизнес-цели организации, для которой этот подход разрабатывается. Не существует «правильных» или «неправильных» способов расчета рисков ИБ при условии, что понятия, описанные в электронных обучающих курсах (ЭОК), объединяются некоторым осмысленным образом, и только сама организация может принять решение о том, какой метод оценки рисков ИБ подходит к ее бизнес-требованиям и требованиям по ОИБ. Однако, если перед организацией стоит задача построения формализованной СУИБ, соответствующей требованиям российских или международных стандартов по управлению ИБ, необходимо, чтобы при разработке методики оценки рисков ИБ были учтены и выполнены все требования к процессу оценки рисков ИБ, которые предъявляют стандарты, в соответствии с которыми строится СУИБ.

Все это доказывает необходимость внимательного изучения вопросов УРИБ.

ВНИМАНИЕ: в учебном пособии для единообразия принят термин «управление», даже при цитировании первоисточников, в которых в оригинале или при их переводе на русский используется термин «менеджмент».