УДК 056+002:004.056

Обзор нормативно-правовых источников и практик управления инцидентами информационной безопасности

А. О. Логинова

В стремлении обеспечить защищенность информационной среды любая организация должна принимать во внимание угрозы, связанные с информационными активами. Обозначить поле всех возможных угроз для каждого конкретного бизнеса не представляется возможным: появление новых неучтенных угроз может быть обусловлено сменой внутренних или внешних условий работы организации, развитием новых технологий, а также изменениями иного рода. Для организации работы с инцидентами рекомендуется использовать проверенные временем стандарты и лучшие мировые практики.

Ключевые слова: инциденты информационной безопасности, управление инцидентами, нормативно-правовые акты, практики управления инцидентами, международные стандарты, зарубежные стандарты, российские стандарты, отраслевые документы, руководящие документы.

1. Введение

Тема управления инцидентами информационной безопасности (ИБ) не является новой для организаций, достигших высокого уровня зрелости, но она по-прежнему не теряет своей актуальности. Неготовность организации своевременно купировать новые инциденты из-за отсутствия четко проработанной процедуры реагирования на них способна снизить скорость восстановления бизнес-процессов, а значит, нанести финансовый ущерб организации. Следует отметить, что ключевую информацию для оценки работоспособности системы менеджмента ИБ поставляет процесс управления инцидентами.

Целью данной статьи является выявление спецификаций нормативно-правовых источников и практик управления инцидентами ИБ для упрощения задачи выбора стандартов и руководств по управлению инцидентами ИБ среди всего их многообразия с учетом индивидуальных особенностей и потребностей организаций.

В «Указаниях по хорошей практике» [1] – руководстве для профессионалов в области развития бизнеса и формирования его устойчивости представлен жизненный цикл менеджмента непрерывности бизнеса (рис. 1). На этапе проектирования авторами уделяется особое внимание структуре реагирования на инцидент. Такая структура должна определять чёткий пошаговый алгоритм работы с инцидентом, при этом процедура управления инцидентом должна быть регламентирована.

Рис. 1. Жизненный цикл менеджмента непрерывности бизнеса [1]

В настоящее время существует достаточно большой выбор различных стандартов и руководств по управлению инцидентами (менеджмент инцидентов). В рамках данной статьи рассмотрены 4 группы документов [2, 3] (табл. 1).

2. Нормативные источники и практики управления инцидентами ИБ

Основной стандарт по менеджменту инцидентов ИБ – ISO/IEC 27035:2016 Information technology – Security techniques – Information security incident management [4]. Стандарт предусматривает масштабируемость: он применим к организациям разного типа и величины. Достоинство данного стандарта выражается в доступном представлении принципов и этапов менеджмента инцидентов ИБ. Стандарт описывает следующие этапы работы с инцидентом: обнаружение, регистрация, оценка и реагирование, а также применение полученного опыта работы с инцидентами.

В главном руководстве по управлению инцидентами США – NIST SP 800-61 Revision 2 (2012) Computer Security Incident Handling Guide [5] подчёркивается, что способность быстро реагировать на инцидент, минимизировать разрушительные последствия его реализации, а также своевременно устранять слабые места в работе вычислительных систем прямо пропорционально зависит от уровня навыков работы с инцидентом, информированности сотрудников: их подготовленности к возникновению инцидента, наличия политики реагирования на инцидент, установленных процедур и правил работы с инцидентом, а также обмена информацией с экспертным сообществом. Как и в стандартах семейства ISO/IEC, касающихся вопросов менеджмента, в основу данного документа положена циклическая модель менеджмента инцидентов – цикл Деминга (PDSA cycle); фазами цикла являются: подготовка, обнаружение и анализ, обработка инцидента (сдерживание, устранение последствий инцидента, восстановление нормальной работы), извлечение уроков. В руководстве рассматриваются все этапы получения навыка реагирования на инцидент: от начальной подготовки до усвоения опыта произошедшего инцидента и извлечения уроков; в руководстве представлены примеры различных инцидентов и ряд вопросов, возникающих при их обнаружении и дальнейшей обработке.

Таблица 1. Нормативные источники и практики управления событиями и инцидентами ИБ

Тематика нормативного источника или практики	Стандарты		Другие руководящие документы
	международные и зарубежные	российские	
управление инцидентами ИБ	ISO/IEC 27035:2016 Information technology – Security techniques – Information security incident management (актуальна версия)	Нет аналога	NIST SP 800-61 Revision 2 (2012) NIST SP 800-83 Revision 1 (2013) NIST SP 800-86 (2006) CMU/SEI-2004-TR-015
	ISO/IEC 18044:2004 Information technology – Security techniques – Information security incident management (не действует)	ГОСТ ИСО/МЭК 18044-2007	
управление ИБ и управление рисками ИБ	ISO/IEC 27001:2013 Information security management systems – Requirements (актуальная версия)	Нет аналога	MEHARI Business continuity institute. Good practice guidelines 2018
	ISO/IEC 27001:2005 Information security management systems – Requirements (не действует)	ГОСТ ИСО/МЭК 2700-2006	
	ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management (актуальная версия)	Нет аналога	
	ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management (не действует)	ГОСТ ИСО/МЭК 27002-2012	
	ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity		
	ISO/IEC 27005:2018 (актуальная версия)	Нет аналога	
	ISO/IEC 27005: (не действует)	ГОСТ ИСО/МЭК 27005-2010	
	BS 7799-3:2017 Information security management systems. Guidelines for information security risk management		
работа с ИТ в целом	ISO/IEC 20000:2018 Information technology – Service management (актуальная версия)	Нет аналога	COBIT5 Федеральный закон № 149-ФЗ (ст. 16, п. 4) Федеральный закон № 152-ФЗ (ст. 19, п. 2)
	ISO/IEC 20000:2011 Information technology – Service management (не действует)	ГОСТ ИСО/МЭК 20000-2014	
отраслевые документы	PCI DSS v 3.2:2016		РС БР ИББС-2.5-201

NIST SP 800-83 Revision 1 (2013) Guide to Malware Incident Prevention and Handling for desktops and laptops [6] содержит рекомендации по предотвращению инцидентов, вызванных вредоносными программами, которые на данный момент представляют собой наиболее распространённую угрозу безопасности: чаще всего именно вредоносные программы являются причиной массовых сбоев в работе и повреждений систем. В руководстве также используется модель PDSA. Большое внимание уделяется существующим средствам защиты от вредоносных программ и действий нарушителей.

NIST SP 800-86 (2006) Guide to Integrating Forensic Techniques into Incident Response [7] содержит практические рекомендации по расследованию инцидентов компьютерной безопасности посредством проведения криминалистической экспертизы. Фактически руководство по интеграции криминалистических техник в процедуры по реагированию на инцидент раскрывает принципы применения приёмов и техник криминалистики в работе с инцидентами ИБ. Рекомендации предусматривают внесение ряда изменений в организационную структуру и политику ИБ организаций, заинтересованных в использовании таких техник. В данном руководстве четвёртый этап модели PDSA, обычно характеризуемый как этап извлечения уроков и подготовки отчётности, представлен этапом сбора доказательств.

Технические рекомендации CMU/SEI-2004-TR-015 Defining incident management processes for CSIRT(Critical Incident Stress Response Team) [8] созданы на основе опыта работы различных подразделений, в чьи обязанности входит обработка и реагирование на инцидент, с использованием опыта различных компаний, а также на основе различных исследований в области управления инцидентами ИБ. По мнению авторов, этот документ поможет выделить ключевые компоненты процесса менеджмента инцидентов. CMU/SEI-2004-TR-015 определяет набор требований и критериев, с их использованием любой бизнес сможет оценить свой уровень организации процесса управления инцидентами ИБ.

3. Нормативные источники и практики управления информационной безопасностью и рисками

Стандарты серии ISO/IEC 27000 достаточно популярны в международной практике, к тому же они периодически актуализируются, что делает их наиболее жизнеспособными в условиях быстро развивающихся информационных технологий. Стандартами по вопросам управления ИБ являются: ISO/IEC 27001 [9], ISO/IEC 27002 [10] и косвенно ISO/IEC 27031 [11], а также ISO/IEC 27005 [12] в области менеджмента риска ИБ.

В Приложении А стандарта ISO/IEC 27001 Information security management systems – Requirements [13] четко обозначены задачи управления и средства их реализации, отдельный раздел в этом приложении отводится управлению инцидентами ИБ [14]. Эта версия стандарта претерпела ряд ключевых изменений (предыдущая версия стандарта датирована 2005 г.): проработана совместимость с другими стандартами по вопросу создания систем управления; учтены изменения, вызванные технологическим прогрессом, в частности, учтено использование мобильных технологий в работе организации. Стандарт ISO/ICE 27002 Information technology – Security techniques – Code of practice for information security management [15], представляющий собой дополнение к ISO/IEC 27001 [13] с развернутыми рекомендациями, тоже претерпел некоторые изменения: в обновленной версии исключены все дублирования «дополняемого» стандарта; также учтены произошедшие в информационно-телекоммуникационной сети изменения.

В стандарте ISO/IEC 27031 Information technology – Security requirements – Guidelines for information and communication technology readiness for business continuity [11] изложены концепции и принципы подготовки информационных технологий (далее – ИТ) к обеспечению не-

прерывности бизнес-процессов. Речь идет о готовности информационно-телекоммуникационных технологий[1], используемых организацией, к последствиям реализации нештатных ситуаций, поэтому стандарт тесно связан с такими понятиями, как событие и инцидент ИБ.

Один из первых стандартов по вопросу менеджмента ИБ – британский стандарт BS 7799 – Part 1 [16] – был без изменений принят на мировом уровне в качестве ISO/IEC 17799 [17] (в дальнейшем этот стандарт получил шифр ISO/IEC 27002 [10]), в нём рассматриваются ключевые аспекты ИБ: политика безопасности, организационные мероприятия по защите информации, работа с персоналом и информационными ресурсами, физическая безопасность, администрирование и т.д. BS 7799 – Part 2 [18] также был принят ISO в качестве уже известного стандарта ISO/IEC 27001 [9]. В этой части стандарт-предшественник рассматривается как перечень требований, которым должна удовлетворять организация. BS 7799 – Part 3 [19] в международной системе кодификации получил шифр 27005 – Information technology – Security techniques – Information security risk management [20]. Последняя версия третьей части британского стандарта от 2017 года была призвана восполнить разрыв между стандартом ISO/IEC 27005, обновление которого было датировано 2011 годом, и уже пересмотренным на тот момент стандартом ISO/IEC 27001 [13] от 2013 года.

В группу II также входит французский документ MEHARI [21], он представляет собой методологию оценки рисков, связанных с обработкой информации. Документ был разработан Французским клубом информационной безопасности[2] и соответствует руководящим принципам, изложенным в стандарте ISO 27005 [20].

4. Нормативные источники и практики использования в работе ИТ в целом

Немаловажную роль в области управления инцидентами ИБ играют документы по вопросам работы с ИТ в целом. Так, например, стандарт ISO/IEC 20000 «Information technology – Service management» [22, 23] определяет требования к организации для создания, внедрения, поддержания и постоянного улучшения системы менеджмента сервиса. Эти требования касаются следующих процессов: планирование, создание, преобразование, доставка и улучшение сервиса для удовлетворения требований непосредственно к качеству сервиса и, как следствие, для увеличения выгоды. В первой части стандарта Information technologies. Specification, описывающей ИТ-процессы, рассматривается группа процессов Resolution Processes, связанных с разрешением инцидентов, возникающих в ИТ-инфраструктуре.

COBIT 5 (Control Objectives for Information and Related Technologies) [23] – это сложная бизнес-ориентированная концепция управления информацией и ИТ. Она призвана помочь организациям получить максимум пользы от использования информации и технологий посредством поддержания баланса между затратами ресурсов, получаемой выгодой и появляющимися рисками. COBIT 5 помогает принимать управленческие решения, касающиеся использования ИТ, с помощью метрик: количества повторяющихся инцидентов, доли крупных инцидентов от всего объёма произошедших инцидентов.

В российском законодательстве действуют законы, предусматривающие требования к наличию процедур работы с инцидентами:

− в пункте (п.) 4 статьи (ст.) 16 Федерального закона от 27.07.2006 № 149-ФЗ (ред. от 18.12.2018) «Об информации, информационных технологиях и о защите информации» [25] речь идёт об обязанности обеспечить «своевременное обнаружение фактов несанкционированного доступа к информации», что является одним из этапов процесса управления инцидентами ИБ;

[1] ICT readiness for business continuity.
[2] CLUSIF – Club de la Sécurité de l'Information Français.

− в п. 2 ст. 19 Федерального закона от 27.07.2006 № 152-ФЗ (ред. от 31.12.2017) «О персональных данных» [26] указано, что одним из условий, соблюдением которого достигается безопасность персональных данных, является обнаружение фактов несанкционированного доступа к персональным данным и принятие мер.

5. Отраслевые документы, затрагивающие вопросы управления инцидентами

Банковские системы являются неотъемлемой частью современной экономики, ошибки в их функционировании оказывают немалое влияние на социально-экономические процессы не только самих банков, но и страны в целом. Этим объясняется заинтересованность банков в применении передового опыта в области управления инцидентами и создания отраслевых стандартов.

В 2014 году были приняты Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности РС БР ИББС-2.5-2014 [27], они основаны на ГОСТ ИСО/МЭК 18044-2007 [28].

Примером международного стандарта является Payment Card Industry Data Security Standard 3.2 [29], разработанный Советом по стандартам безопасности индустрии платёжных карт. Он включает в себя 12 подробно изложенных требований к обеспечению безопасности данных, принадлежащих держателю платёжной карты. Целью стандарта является повышение уровня защищённости данных держателя карты и интеграция единых требований к обеспечению безопасности таких данных на международном уровне.

6. Заключение

Широкий выбор документов, содержащих регламент работы с инцидентами ИБ или вспомогательные материалы по работе с ними, вызывает затруднения при выборе стандарта/руководства/практики управления инцидентами ИБ для определённого бизнеса [30]. В связи с этим разработаем матрицу характеристик нормативно-правовых источников и практик управления инцидентами ИБ (табл. 2).

Процесс управления инцидентами является составной частью общей системы управления ИБ организации, поэтому стоит учитывать не только действующее законодательство, но и использовать стандарты, руководства и признанные мировые практики для достижения наилучших показателей защищённости информационной системы. При выборе таких «инструкций» по управлению инцидентами ИБ необходимо учитывать индивидуальные особенности и потребности организации.

Таблица 2. Матрица характеристик нормативно-правовых источников и практик управления инцидентами ИБ

Наименование группы документов	Наименование стандарта/руководства/практики	Основные темы	Характеристики. В документе рассмотрено/предусмотрено:					
			вид деятельности организации	создание группы по реагированию на инцидент ИБ	примеры инцидентов ИБ	работа с внешними организациями	подготовка организации к реагированию на инцидент ИБ	вспомогательные материалы (опросники, пошаговые инструкции и т.д.)
управление инцидентами ИБ	ISO/IEC 27035:2016 Information technology – Security techniques – Information security incident management	основные понятия в области управления инцидентами ИБ, этапы работы с инцидентом	нет ограничений	+	+	+	-	-
	NIST SP 800-61 Revision 2 (2012)	практики по построению процессов управления инцидентами ИБ	нет ограничений	+	+	-	+	-
	NIST SP 800-83 Revision 1 (2013)	инциденты ИБ, связанные с вредоносными программами	нет ограничений	-	-	-	+	+
	NIST SP 800-86 (2006)	расследование инцидентов компьютерной безопасности и устранение проблем в работе ИТ-инфраструктуры	нет ограничений	+	+	-	+	+
	CMU/SEI-2004-TR-015	организация работы группы реагирования на инцидент, этапы работы с инцидентом	нет ограничений	+	-	-	-	+
управление ИБ и управление рисками ИБ	ISO/IEC 27001:2013 Information security management systems – Requirements	поддержание работоспособности и улучшение системы менеджмента ИБ, требования к оценке и обработке рисков ИБ	нет ограничений	-	-	-	+	+
	ISO/IEC 27002:2013 Information technology – Security techniques – Code of practice for information security management	общие правила выбора, внедрения и управления средствами контроля, учитывающие риски ИБ организации	нет ограничений	-	-	+	+	-
	ISO/IEC 27031:2011 Information technology – Security techniques –	концепции и принципы обеспечения готовности	нет ограничений	-	-	-	-	+

	Guidelines for information and communication technology readiness for business continuity	ИКТ к обеспечению непрерывности бизнеса						
	ISO/IEC 27005:2018	менеджмент рисков ИБ	нет ограничений	-	-	-	-	+
	BS 7799-3:2017 Information security management systems. Guidelines for information security risk management	менеджмент рисков ИБ	нет ограничений	-	-	-	+	-
	MEHARI	метод анализа рисков	нет ограничений	-	-	-	+	-
	Business continuity institute. Good practice guidelines 2018	обеспечение непрерывности бизнеса	нет ограничений	+	-	-	+	-
работа с ИТ в целом	ISO/IEC 20000:2018 Information technology – Service management	требования к созданию, внедрению, поддержке и улучшению системы управления услугами	нет ограничений	-	-	+	-	+
	COBIT 5	управление информацией и ИТ	нет ограничений	-	-	-	+	-
	Федеральный закон № 149-ФЗ (ст. 16, п. 4)	информация, ИТ, защита информации	нет ограничений	-	-	-	+	-
	Федеральный закон № 152-ФЗ (ст. 19, п. 2)	персональные данные	нет ограничений	-	-	-	+	-
отраслевые документы	PCI DSS v 3.2:2016	безопасность данных платёжных карт	финансовая организация	-	-	+	+	+
	РС БР ИББС-2.5-201	обеспечение ИБ организации банковской системы	финансовая организация	+	-	-	+	+

Литература

1. *Корнеев И. Р.* Система управления непрерывностью бизнеса: Почему она должна быть внедрена на каждом предприятии? М.: ЛЕНАНД, 2016. 352 с.
2. *Рыженкова А.* Управление инцидентами информационной безопасности: о чем говорят стандарты // CONNECT. На пути к полнофункциональному SOC. 2014. № 7–8. С. 62–65.
3. *Sunil Ladekar*. Best Practices for Information Security Breach Management. East Carolina University, College of Technology and Computer Science, Department of Technology Systems. 2014.
4. ISO/IEC 27035:2016. Information technology – Security techniques – Information security incident management. ISO/IEC, 2016.
5. NIST SP 800-61. Computer Incident Handling Guide. Gaithersburg: NIST, 2012.
6. NIST SP 800-83. Guide to Malware Incident Prevention and Handling. Gaithersburg: NIST, 2013.
7. NIST SP 800-86. Integrating Forensic Techniques into Incident Response. Gaithersburg: NIST, 2006.
8. CMU/SEI-2004-TR-015. Defining incident management processes for Critical Insident Stress Response Team. CMU/SEI, 2004.
9. ISO/IEC 27001:2005. Information security management systems – Requirements. ISO/IEC, 2005.
10. ISO/IEC 27002:2005. Information technology – Security techniques – Code of practice for Information security management. ISO/IEC, 2005.
11. ISO/IEC 27031:2011 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity. ISO/IEC, 2011.
12. ISO/IEC 27005:2018. Information technology – Security techniques – Information security risk management. ISO/IEC, 2018.
13. ISO/IEC 27001:2013. Information security management systems – Requirements. ISO/IEC, 2013.
14. *Царегородцев А. В.* Критичные вопросы оперативного и организационно-технического управления информационной безопасностью облачных вычислений // Национальная безопасность. Nota bene. 2011. № 6 (17). С. 11–17.
15. ISO/IEC 27002:2013. Information technology – Security techniques – Code of practice for Information security management. ISO/IEC, 2013.
16. BS 7799-1:1995. Code of Practice for Information Security Management. London: British Standards Institution, 1995.
17. ISO/IEC 17799:2005. Information technology – Code of practice for information security management. ISO/IEC, 2005.
18. BS 7799-2:1999. Information security management, Specification for information security management systems. London: British Standards Institution, 1999.
19. BS 7799-3. Information security management systems. Guidelines for information security risk management. London: British Standards Institution.
20. ISO/IEC 27005:2008. Information technology – Security techniques – Information security risk management. ISO/IEC, 2008.
21. MÉHARI. CLISIF, 2016.
22. ISO/IEC 20000:2011. Information technology – Service management. ISO/IEC, 2011.
23. ISO/IEC 20000:2018. Information technology – Service management. ISO/IEC, 2018.
24. COBIT 5. ISACA, 2012.
25. Об информации, информационных технологиях и о защите информации: Федеральный закон от 27 июля 2006 г. №149-ФЗ.
26. О персональных данных: Федеральный закон от 27 июля 2006 г. №152-ФЗ.

27. Рекомендации в области стандартизации Банка России «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Менеджмент инцидентов информационной безопасности»: РС БР ИББС-2.5-2014. Банк России, 2014.
28. ГОСТ ИСО/МЭК 18044-2007. Информационная технология – Методы и средства обеспечения безопасности – Менеджмент инцидентов информационной безопасности. М.: Стандартинформ, 2009.
29. PCI DSS v 3.2:2016. PCI Security Standards Council, 2016.
30. *Мещеряков Р. В., Исхаков С. Ю.* О проблемах анализа данных в системах управления инцидентами безопасности роботов // Труды 8-й Всероссийской научной конференции с международным участием «Информационные технологии и системы», Ханты-Мансийск, 2020. С. 108–114.

Статья поступила в редакцию 28.10.2020.

Логинова Алина Олеговна
эксперт отдела научного менеджмента и наукометрии МГЛУ, аспирант кафедры международной информационной безопасности МГЛУ (119021, Москва, Комсомольский проспект, д. 6), e-mail: loginova@linguanet.ru.

An overview of regulatory sources and practices of information security incidents management

A. Loginova

Any organization should take into account the threats to information assets to ensure information environment security. It is impossible to identify an entire field of all possible threats for each specific business: appearance of new threats may be caused by changes in the internal or external working conditions of an organization as well as the development of new technologies and other changes. Using time-tested standards and best international practices is highly recommended for managing incidents.

*Keywords***:** information security incident, incident management, regulatory sources, incident management practices, international standards, foreign standards, Russian standards, industry documents, guidelines.