УДК 004

Филиппов А. С., Астахова Л. В.

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ КАК ОБЪЕКТ ИЗУЧЕНИЯ В ВУЗЕ

В данной статье обоснован процесс управления инцидентами информационной безопасности на основе российских и зарубежных стандартов как объект изучения будущими специалистами по защите информации в высшем учебном заведении.

Ключевые слова: *инциденты, информационная безопасность.*

Filippov A. S., Astakhova L. V.

INCIDENT MANAGEMENT INFORMATION SAFETY AS AN OBJECT OF STUDY IN HIGH SCHOOL

In this paper based process management of information security incidents based on Russian and foreign standards as an object of study of the future of information security experts in higher education.

Keywords: *accidents, information security.*

В процессе подготовки специалистов по защите информации в вузе важную роль играет освоение процессов управления инцидентами информационной безопасности на основе российских и зарубежных стандартов.

Для управления инцидентами информационной безопасности нужны специальные знания: основ законодательства Российской Федерации, а также международных и национальных стандартов;

В российском законодательстве используются различные национальные стандарты в области информационных технологий и информационной безопасности, например ГОСТ Р ИСО/МЭК 18044-2007 [1]. Стандарт описывает инфраструктуру управления инцидентами информационной безопасности в рамках циклической модели PDCA, дает подробные спецификации для стадий планирования, эксплуатации, анализа и улучшения процесса и рассматривает вопросы обеспе-

чения нормативно-распорядительной документацией и ресурсами и рекомендации по необходимым процедурам. Стандарт ГОСТ Р 53647 [2] содержит руководящие указания по внедрению системы менеджмента непрерывности бизнеса в организации, предназначен для организаций всех форм собственности и специалистов, ответственных за обеспечение непрерывности бизнеса организации.

Международные и национальные стандарты, например ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭ 27001:2005 [3], устанавливают требования к системе управления информационной безопасностью в целом, а также отдельно - к процессу управления инцидентами информационной безопасности. Данные стандарты обращают особое внимание на необходимость создания процесса управления инцидентами информационной безопасности и поддерживающей его работу документации, необходимой для регулирования и управления работой в рамках разработанного процесса и определения обязанностей, и необходимых действий сотрудников.

Технические рекомендации CMU/SEI-2004-TR-015 [4] описывают методологию планирования, внедрения, оценки и улучшения процессов управления инцидентами информационной безопасности. При этом основной упор делается на организацию работы группы или подразделения, обеспечивающего сервис и поддержку предотвращения, обработки и реагирования на инциденты информационной безопасности. Вводятся ряд критериев, на основании которых можно оценивать эффективность данных сервисов, приводятся подробные процессные карты.

Нормативный документ США NIST SP 800-61 [5] представляет собой сборник «лучших практик» по построению процессов управления инцидентами информационной безопасности и реагирования на них. Подробно разбираются вопросы реагирования на разные типы инцидентов, такие как атаки «отказ в обслуживании» (DoS), распространение вредоносного программного обеспечения, несанкционированный доступ, нерегламентированное использование и распределение (многокомпонентные) атаки.

Международный стандарт ISO/IEC 27035:2011 [6] содержит структурированный и планомерный подход к обнаружению, составлению отчетов и оценке инцидентов информационной безопасности, к осуществлению ответной реакции и управлению инцидентами информационной безопасности, к обнаружению, оценке и устранению уязвимостей и к постоянному улучшению управления информационной безопасности и инцидентами информационной безопасности.

В стандарте ISO/IEC 27031:2011 [7] содержатся концепции и принципы, информационных и телекоммуникационных технологий как необъемлемой части критической инфраструктуры любой организации по обеспечению непрерывности ее бизнеса.

Британские стандарты серии BS 25999 [8] содержат общие рекомендации по управлению непрерывностью бизнеса, устанавливают и детализируют конкретные требования к системам управления непрерывностью бизнеса, причем только те, соблюдение которых может быть объективно проверено.

Требования и рекомендации Стандарта Банка России СТО БР ИББС-1.0-2014 [9] направлены на минимизацию рисков возникновения инцидентов и снижения потерь от сбоев в работе. На базе этих требований можно построить программу обучения для студентов в высшем учебном заведении, а также управлять непрерывностью бизнеса для целей обеспечения непрерывности ключевых бизнес-процессов рамках области действия системы управления информационной безопасностью. Стандарты в соответствии с лучшими практиками позволяют студентам убедиться в том, что процессы работают правильно и эффективно. Это особенно важно в том случае, если организация или государственный орган работает с большими объемами ценной информации или обрабатывает и хранит важную информацию своих клиентов и работников. При изучении стандартов полученный опыт рассматривается не только в рамках отдельного инцидента, но и проводится проверка на наличие тенденций (закономерностей) появления предпосылок к инцидентам, которые могут быть использованы в интересах определения потребности в защитных мерах или изменениях подходов к устранению инцидентов. После инцидента, связанного с применением информационных технологий, целесообразно проведение тестирования информационной безопасности, в особенности - для оценки уязвимостей. Информация, получаемая в процессе инцидента, будет направляться для анализа тенденций (закономерностей), что на основе предшествующего опыта и документированных знаний в значительной мере способствует

ранней идентификации инцидентов, а также обеспечивает предупреждение о том, какие инциденты могут возникнуть в будущем. Технологии эффективного функционирования системы для банковской сферы деятельности на основе стандартов по информационной безопасности, имеющие ярко выраженную специфику, описывает в своей работе С.В. Попов [10].

Кроме основ законодательства Российской Федерации, государственных стандартов в области информационных технологий (как отечественных, так зарубежных), студентов вуза необходимо обучать судебной практике в области расследования инцидентов информационной безопасности, а также программным продуктам для получения доказательной базы и документированию процесса управления инцидентами в целом. Благодаря этим знаниям и умениям обучающиеся смогут самостоятельно строить алгоритмы управления инцидентами информационной безопасности в организации. Например, с помощью стандарта ГОСТ Р ИСО/МЭК 18044-2007 [1] - описывать систему управления инцидентами информационной безопасности. Анализировать этапы процесса управления инцидентами информационной безопасности, разбиваемого на планирование и подготовку, использование, анализ и улучшение относится к стандарту. Отдельно исследовать подпроцессы обнаружения событий и инцидентов информационной безопасности, и оповещения о них, а также обработка событий и инцидентов информационной безопасности, включая первую оценку и предварительное решение по событию информационной безопасности и вторую оценку, и подтверждение инцидента информационной безопасности. Для этого обучающиеся будут использовать ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭ 27001:2005 [3]. Детально исследовать подпроцесс реагирования на инциденты информационной безопасности и его составляющие будущим специалистам также позволит стандарт: немедленное реагирование, контроль, последующее реагирование, антикризисные действия, правовая экспертиза, передача информации, расширение области принятия решений, регистрация деятельности и контроль за внесением изменений и техническая поддержка реагирования на инциденты ИБ. Для разработки документации системы управления инцидентами информационной безопасности, включая политику и программу, используется ISO/IEC 27035:2011 [6].

Для обучения студентов анализу деятельности группы реагирования на инциденты информационной безопасности должен использоваться британский стандарт BS 25999. На его основе студенты осознают необходимость обеспечения осведомленности и обучения в области инцидентов информационной безопасности. Значительное внимание уделяется сохранению доказательств инцидента информационной безопасности и кратко определяются функции инструментальных средств управления событиями информационной безопасности.

Освоение этих материалов в учебном процессе лежит в основе формирования у обучающихся следующих профессиональных компетенций:

1) Способность участвовать в управлении информационной безопасностью объекта (в части управления инцидентами информационной безопасности и непрерывностью бизнеса);

2) Способность участвовать в проектировании и разработке системы управления информационной безопасностью (система управления информационной безопасностью) объекта (в отношении подсистем управления инцидентами информационной безопасности и непрерывностью бизнеса);

3) Способность участвовать в проведении контрольных мероприятий по определению эффективности и результативности система управления информационной безопасности объекта (в части эффективности и результативности управления инцидентами информационной безопасности и непрерывностью бизнеса).

Таким образом, управление инцидентами информационной безопасности является сложносоставным объектом изучения будущими специалистами по защите информации в вузе. Это – алгоритмический динамический объект, зависящий от постоянно меняющихся стандартов по управлению информационной безопасности и по информационным технологиям, требующий разработки специальных обучающих методик, а потому - пристального внимания выпускающей кафедры.

Примечания

1. ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности». М.: Стандартинформ, 2009.

2. ГОСТ Р 53647 «Менеджмент непрерывности бизнеса. Практическое руководство». М.: Стандартинформ, 2011.

3. ISO/IEC 27001:2005 «Information technology. Security techniques. Information security management systems. Requirements» и ГОСТ Р ИСО/МЭ 27001:2005 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования».

4. CMU/SEI-2004-TR-015 «Defining incident management processes for CSIRT».

5. NIST SP 800-61 «Computer security incident handling guide».

6. ISO/IEC 27035:2011 «Information technology. Security techniques. Information security incident management».

7. ISO/IEC 27031:2011 «Information technology. Security techniques. Guidelines for information and communications technology readiness for business continuity».

8. BS 25999-1:2006 «Business continuity management. Code of practice» и BS 25999-2:2007 «Business continuity management. Specification».

9. Стандарт Банка России СТО БР ИББС-1.0-2014 «Обеспечение информационной безопасности организаций банковской системы Российской Федерации/Общие положения» принят и введен в действие распоряжением Банка России от 17 мая 2014 г. № Р-399.

10. Попова С.В., Повышение эффективности функционирования системы мониторинга инцидентов информационной безопасности банка на основе оценки надежности ее компонентов: дис. канд. техн.наук. - Тамбов, 2012. - 242 с.

Информация об авторах отсутствует на обоих языках