УДК 681.322 Вестник УрФО № 3(29) / 2018, с. 50–54

Карташевский В. Г., Крыжановский А. В. DOI: 10.14529/SECUR180308

АНАЛИЗ МЕТОДОВ И СРЕДСТВ ВЫЯВЛЕНИЯ ИНЦИДЕНТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Анализируются возможности наиболее распространённых стандартов в области менеджмента инцидентов информационной безопасности. Анализируется методика выявления инцидентов на основе операционных и технических процедур с точки зрения управления бизнес - процессами и технической перспективы. Оцениваются возможности основных этапов (шагов): сбор информации об уязвимостях, проверка информации и оценка риска, выбор метода распространения информации. Рассмотрены возможные инциденты информационной безопасности и разработана соответствующая классификация. Сформулированы требования к техническим средствам и системам выявления инцидентов информационной безопасности.

Ключевые слова: *инциденты информационной безопасности, классификация инцидентов информационной безопасности, обнаружение инцидентов информационной безопасности и управление ими, международные и национальные стандарты менеджмента инцидентов информационной безопасности.*

Kartashevskiy V. G., Kryzhanovsky A. V.

ANALYSIS OF METHODS AND MEANS OF DETECTING INFORMATION SECURITY INCIDENTS

We analyze here the possibilities of the most common standards in the field of management of information security incident. We also analyze the methodology of incident detection based on operational and technical procedures from the point of view of business process management and technical perspective. The possibilities of the main stages (steps) are evaluated: collection of information about vulnerabilities, verification of information and risk assessment, choice of the method of information dissemination. Possible incidents of information security are considered and the corresponding classification is developed. We formulate requirements to technical means and systems of detection of information security incidents.

Keywords: *information security incidents, classification of information security incidents, detection and management of information security incidents, international and national standards of management of information security incident.*

Под инцидентами информационной безопасности (ИБ) понимаются различные происшествия, приводящие к нарушениям безопасности компании. Эти нарушения могут привести к серьёзным последствиям, поэтому сотрудники безопасности фирмы должны подготовиться к своевременному противодействию возникающим угрозам. Кроме того, специалистам, обеспечивающим, ИБ необходимо фиксировать все произошедшие на предприятии случаи нарушений безопасности для дальнейшего их анализа. Для лучшей организации процедур выявления угроз специалист должен скомпоновать обнаруженные им случаи нарушения защиты в строго выделенные группы. Данные базовые действия регламентированы соответствующими нормативными документами, поэтому каждый высококвалифицированный специалист должен строго следовать принятой политике безопасности, чтобы организовать комплекс мер по обнаружению и управлению инцидентами ИБ [1,2].

ренцировать обязанности должностных лиц в области менеджмента инцидентов ИБ, в результате риск возникновения инцидентов ИБ на предприятии значительно уменьшается [3].

В качестве примера стандарта, регламентирующего процедуры менеджмента инцидентов ИБ, рассмотрим стандарт ENISA «CSIRT Setting up Guide in Russian». Этот европейский регламентирующий документ «Пошаговое руководство по созданию CSIRT» детально описывает процесс создания Computer Security and Incident Response Team (CSIRT — группа реагирования на инциденты компьютерной безопасности) с точки зрения управления бизнес - процессами, а также технической перспективы [4].

Методика выявления инцидентов на основе операционных и технических процедур иллюстрируется на рис. 1.

Процесс обработки информации состоит из трёх основных этапов (шагов).

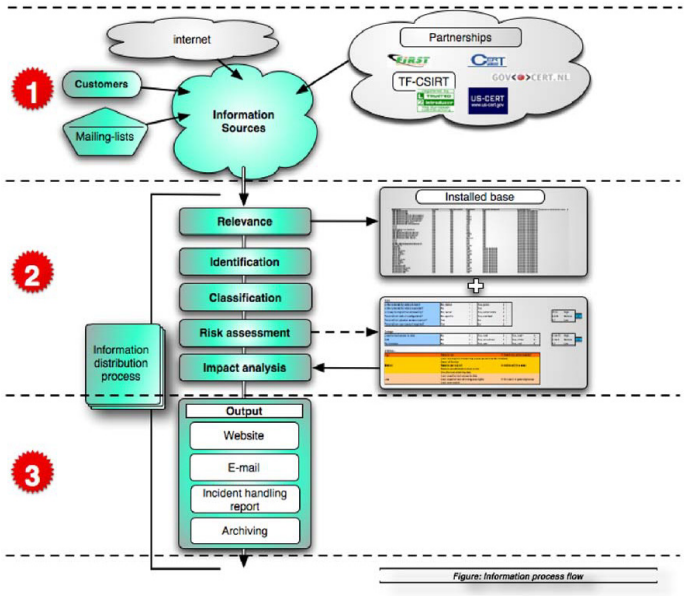

Рис.1. Процесс обработки информации

В области менеджмента инцидентов ИБ, в основном, применяются три национальных стандарта: российский (ГОСТ), европейский (ENISA-European Network and Security Information Agency -европейское агентство сетевой и информационной безопасности) и американский (NIST-National Institute of Standarts and Technology - национальный институт стандартов и технологий). Рекомендации этих стандартов помогают разграничить полномочия сотрудников компании и диффе-

Шаг 1 — сбор информации об уязвимостях.

Обычно существует два основных типа источников информации, которые предоставляют исходную информацию для сервисов:

– информация об уязвимости IT-системы;

– отчёты об инцидентах.

Шаг 2 — проверка информации и оценка риска.

Этот шаг приведёт к анализу последствий

специфической уязвимости на IT-инфраструктуру клиента. Основные критерии анализа — идентификация, актуальность и классификация.

Шаг 3 —выбор метода распространения информации.

CSIRT может выбрать один из нескольких методов распространения, в зависимости от пожеланий клиентов и корпоративной коммуникационной стратегии: веб-сайт, электронная почта, отчёты, архивирование и исследования.

Инцидентами информационной безопасности, представленными на рис. 2, являются: утрата услуг и сбой оборудования, системные сбои или перегрузки, ошибки пользователей, несоблюдение политики или рекомендаций по ИБ, нарушение физических мер защиты, неконтролируемые изменения систем, сбои программного обеспечения и отказы технических средств, нарушение правил доступа [5].

Инциденты информационной безопасности можно классифицировать по ряду признаков, изображённых на рис. 3 [6].

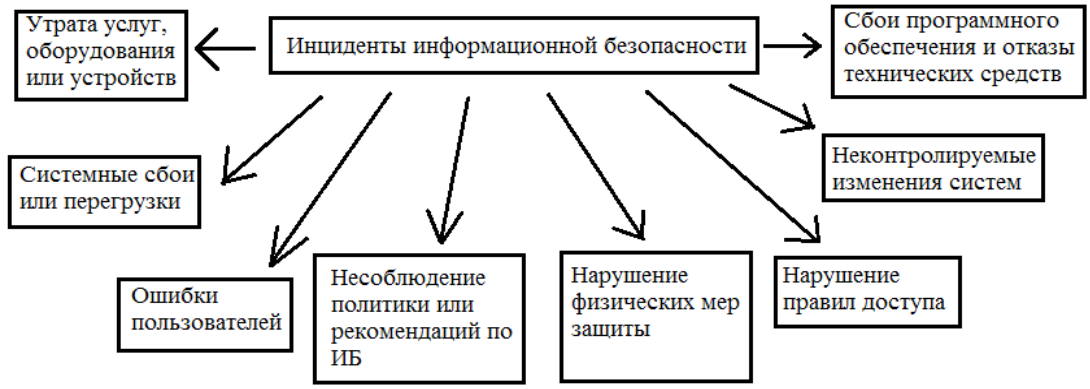

Рис. 2. Инциденты информационной безопасности

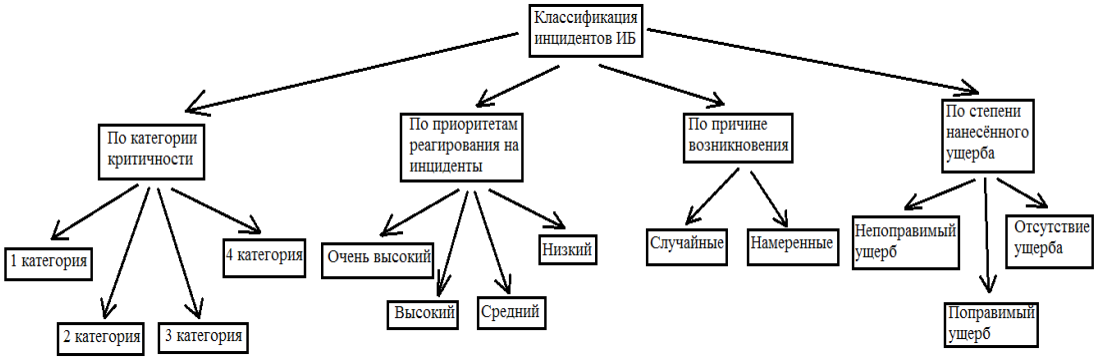

Рис. 3. Классификация инцидентов ИБ

1. По категории критичности:

1 категория: инцидент может привести к значительным негативным последствиям (ущербу) для информационных активов или репутации организации;

2 категория: инцидент может привести к негативным последствиям (ущербу) для информационных активов или репутации организации;

3 категория: инцидент может привести к незначительным негативным последствиям (ущербу) для информационных активов или репутации банка;

4 категория: инцидент не может привести к негативным последствиям (ущербу) для информационных активов или репутации.

2. По приоритетам реагирования на инциденты:

– очень высокий: соответствует 1-й категории критичности, время реагирования не более 1 часа;

– высокий: соответствует 2-й категории критичности, время реагирования не более 4 часов;

– средний: соответствует 3-й категории критичности, время реагирования не более 8 часов;

– низкий: соответствует 4-й категории критичности, время реагирования не определено.

3. По причине возникновения: случайные; преднамеренные.

4.По степени нанесенного ущерба: непо-

правимый ущерб; поправимый ущерб; отсутствие ущерба.

В качестве основных целей структурированного, хорошо спланированного менеджмента инцидентов ИБ ГОСТ 18044-2007 выделяет следующие цели [7,8]:

– обнаружение и эффективная обработка событий ИБ, выделение из их числа инцидентов ИБ;

– оценка и разрешение идентифицированных инцидентов ИБ наиболее оптимальным способом;

– минимизация негативных воздействий инцидентов ИБ соответствующими защитными мерами;

– извлечение уроков из инцидентов ИБ с целью их предотвращения в будущем, улучшения общей система менеджмента инцидентов ИБ (СМИИБ).

Литература

1. ГОСТ Р ИСО/МЭК 20000-2-2012.Издания. Международная стандартная нумерация книг. – М.: Изд-во стандартов, 2011. Часть 2 – 35 с.

2. ГОСТ Р ИСО/МЭК 27002-2013.Издания. Международная стандартная нумерация книг. – М. : Изд-во стандартов, 2014. – 104 с.

3. ГОСТ Р ИСО/МЭК 27037-2014.Издания. Международная стандартная нумерация книг. – М. : Изд-во стандартов, 2014. – 47 с.

4. СТО БР ИББС-1.3-2016.Издания. Международная стандартная нумерация книг. – М. : Изд-во стандартов, 2016. – 49 с.

5. Карташевский В.Г., Крыжановский А.В., Раков А.С. Особенности реализации в ПГУТИ ФГОС ВПО специальности 10.05.02 с учётом специфики Самарской области и отраслевой направленности вуза. Материалы XIX пленума УМО по образованию в области информационной безопасности. Научно-практический журнал «Информационное противодействие угрозам терроризма» № 25, том 2, Таганрог, 2015.-с.122-128.

6. Крыжановский А.В., Кухарев С.Н., Афанасьев В.Н. Реализация лабораторного практикума дисциплины «Информационная безопасность телекоммуникационных систем» специальности 10.05.02. Материалы XIX пленума УМО по образованию в области информационной безопасности. Научно-практический журнал «Информационное противодействие угрозам терроризма» № 25, том 1, Таганрог, 2015.- с.224-234.

7. Карташевский В.Г., Крыжановский А.В., Раков А.С., Алексеев А.П.,

8. Борисенков А.В. О подготовке специалистов в области информационной безопасности в ПГУТИ. Материалы XX юбилейного пленума федерального учебно-методического объединения в системе высшего образования по укрупненной группе специальностей и направлений подготовки10.00.00 «Информационная безопасность», 23-28 ноября 2016: Москва- с.79-85.

9. Крыжановский А.В., Кухарев С.Н., Афанасьев В.Н. Применение бюджетных решений при обучении технической защите информации. Материалы XXI пленума ФУМО: труды Межвузовской научно-практической конференции «Актуальные проблемы обеспечения информационной безопасности». - Самара: Изд-во Инсома-пресс, 2017. -с.111-118.

References

1. GOST R ISO/MEK 20000-2-2012.Izdaniya. Mezhdunarodnaya standartnaya numeratsiya knig. – M.: Izd-vo standartov, 2011. Chast' 2 – 35 s.

2. GOST R ISO/MEK 27002-2013.Izdaniya. Mezhdunarodnaya standartnaya numeratsiya knig. – M. : Izd-vo standartov, 2014. – 104 s.

3. GOST R ISO/MEK 27037-2014.Izdaniya. Mezhdunarodnaya standartnaya numeratsiya knig. – M. : Izd-vo standartov, 2014. – 47 s.

4. STO BR IBBS-1.3-2016.Izdaniya. Mezhdunarodnaya standartnaya nu-meratsiya knig. – M. : Izd-vo standartov, 2016. – 49 s.

5. Kartashevskiy V.G., Kryzhanovskiy A.V., Rakov A.S. Osobennosti realizatsii v PGUTI FGOS VPO spetsial'nosti 10.05.02 s uchotom spetsifiki Samarskoy oblasti i otraslevoy napravlennosti vuza. Materialy XIX plenuma UMO po obrazovaniyu v oblasti informatsionnoy bezopasnosti. Nauchno-prakticheskiy zhurnal «Informatsionnoye protivodeystviye ugrozam terrorizma» № 25, tom 2, Taganrog, 2015.-s.122-128.

6. Kryzhanovskiy A.V., Kukharev S.N., Afanas'yev V.N. Realizatsiya laboratornogo praktikuma distsipliny «Informatsionnaya bezopasnost' telekommunikatsionnykh sistem» spetsial'nosti 10.05.02. Materialy XIX plenuma UMO po obrazovaniyu v oblasti informatsionnoy bezopasnosti. Nauchno-prakticheskiy zhurnal «Informatsionnoye protivodeystviye ugrozam terrorizma» № 25, tom 1, Taganrog, 2015.- s.224-234.

7. Kartashevskiy V.G., Kryzhanovskiy A.V., Rakov A.S., Alekseyev A.P.,

8. Borisenkov A.V. O podgotovke spetsialistov v oblasti informatsionnoy bezopasnosti v PGUTI. Materialy XX yubileynogo plenuma federal'nogo uchebno-metodicheskogo ob"yedineniya v sisteme vysshego obrazovaniya po ukrupnennoy gruppe spetsial'nostey i napravleniy podgotovki10.00.00 «Informatsionnaya bezopasnost'», 23-28 noyabrya 2016: Moskva- s.79-85.

9. Kryzhanovskiy A.V., Kukharev S.N., Afanas'yev V.N. Primeneniye byudzhetnykh resheniy pri obuchenii tekhnicheskoy zashchite informatsii. Materialy XXI plenuma FUMO: trudy Mezhvuzovskoy nauchno-prakticheskoy konferentsii «Aktual'nyye problemy obespecheniya informatsionnoy bezopasnosti». - Samara: Izd-vo Insoma-press, 2017. -s.111-118.

КАРТАШЕВСКИЙ Вячеслав Григорьевич, доктор технических наук, профессор, заведующий кафедрой Информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики». Россия, 443010, Самара, Льва Толстого, д.23. E-mail: kartash@psati.ru

КРЫЖАНОВСКИЙ Анатолий Владиславович, кандидат технических наук, доцент кафедры Информационной безопасности ФГБОУ ВО «Поволжский государственный университет телекоммуникаций и информатики». Россия, 443010, Самара, Льва Толстого, д.23. E-mail: kryzan@mail.ru

KARTASHEVSKIY Viacheslav, Doctor of Engineering Science, Professor, Head of the department of information security of the «Povolzhskiy State University of Telecommunications and Informatics», 23, L.Tolstoy str., Russia, 443010, E-mail: kartash@psati.ru

KRYZHANOVSKY Anatoly, Candidate of Engineering Science, Docent of the department of information security of the «Povolzhskiy State University of Telecommunications and Informatics», 23, L.Tolstoy str., Russia, 443010, E-mail: kryzan@mail.ru