Published in the Russian Federation
Sochi Journal of Economy
Has been issued since 2007.
ISSN: 2541-8114
2017, 11(1): 29-36

www.vestnik.sutr.ru

UDC 338.14 + 004.056

Management of Security Incidents in the Information System as a Means of Reducing Economic Loss

Vladlena S. Oladko [a, *], Ekaterina A. Vitenburgh [b], Anna I. Pushkarskaya [b]

[a] Financial University under the Government of the Russian Federation, Russian Federation
[b] Volgograd State University, Russian Federation

Abstract

The article considers the actual problem of counteraction to risks and economic damage arising from the impact of various threats. The relationship between the economic success of an enterprise, the quality and safety of its information system is shown. The threats and causes of the security breach of the information system are analyzed. The consequences and possible risks of threats are described. The need to control events and security incidents occurring in the information system justified. Algorithm for monitoring events and managing incidents of information security is developed. The application of this algorithm should ensure localization of damage and minimization of risks.

Keywords: event, information security, monitoring, attack, threat, risk, enterprise, business process, decision making, classification, intruder.

1. Введение

В условиях сложной экономической ситуации, сопровождающейся жесткой и порой недобросовестной конкурентной борьбой все больше организаций сталкиваются с рядом проблем обусловленных, недостаточной эффективности управления информационной безопасностью (ИБ) как в организации в целом, так и в ее информационной системе (ИС). Анализ статистических данных исследований ведущих компаний в области ИБ [1-3] за 2016 год показывает, что около 76 % ИС являются уязвимыми к угрозам, источниками которых являются внутренние и внешние атаки злоумышленника, а также дестабилизирующих воздействий случайного характера. Результатом реализации угроз являются сбои и отказы ИС, прерывание бизнес-процессов, нарушение конфиденциальности, целостности и доступности информации. В источниках [4, 5] показано, что подобные проблемы часто становятся причиной возникновения рисков и экономического ущерба различного характера и тяжести, последствием которых могут стать большие финансовые потери, снижение репутации и конкурентоспособности организации, а также при самом негативном сценарии ситуации – полное прекращение деятельности.

Для локализации рисков международный стандарт ISO 27001:2013 [6] рекомендует применять процедуры управления инцидентами ИБ, обеспечивающие своевременное реагирование на инциденты ИБ, устранения их последствий и возможных причин. Следовательно, актуальным решением в области контроля и предотвращения экономического ущерба является применение систем мониторинга и управления

* Corresponding author
E-mail addresses: oladko.vs@yandex.ru (V.S. Oladko)

инцидентами ИБ. В задачи входит сбор и корреляция событий безопасности, контроль защищенности, своевременное выявление несанкционированных изменений и их последствий, а также помощь в принятии решений при построении или модификации системы защиты информации.

2. Материалы и методы

Для написания статьи были использованы материалы научной, учебной литературы, законодательство Российской Федерации, статистические данные, собранные из печатных и электронных источников информации.

В качестве основных методов исследования при выполнении работы были использованы: метод описания, системного анализа, аналогии и обобщения, а также элементы теории принятия решений и экспертных систем.

3. Обсуждение

Информационная система предприятия

В соответствии с ISO/IEC 2382:2015 [7] ИС использует технологии и организационные ресурсы (человеческие, технические, финансовые и т. д.), которые обеспечивают хранение, поиск, обработку и распространение информации. Целью ИС является удовлетворение конкретных информационных потребностей в рамках определенной предметной области, повышение эффективности работы персонала [8] и автоматизация бизнес-процессов предприятия. Результат функционирования ИС – информационная продукция, к которой относят документы, информационные массивы, базы данных и информационные услуги. Соответственно от надежности и безопасности ИС напрямую будет зависеть качество производимой информационной продукции, непрерывность бизнес-процессов, а следовательно, экономическая успешность и конкурентоспособность предприятия - владельца ИС на рынке.

Процесс функционирования ИС регулируется на четырех уровнях и должен рассматриваться в контексте эксплуатационной среды [9, 10] (см. рисунок 1).

Рис. 1. Уровни типовой ИС

Правовой уровень включает в себя все нормативные документы и требования определенные законодательством РФ, политику безопасности, инструкции руководства и пользователей ИС в соответствии с которыми должна быть организовано проектирование,

эксплуатация и защита ИС.

Организационный уровень ИС включает пользователей, данные, а также информационные и бизнес-процессы в которые они вовлечены. Под пользователем понимается зарегистрированные установленным порядком персоны наделенные определенными полномочиями и правами доступа. В рамках своих полномочий пользователь может осуществлять только разрешенные ему действия с использованием общесистемного и прикладного ПО.

К элементам программного уровня ИС относят установленное программное обеспечение (ПО), которое включает три уровня организации:

–низкоуровневое программное обеспечение, обеспечивающее взаимодействие с аппаратным обеспечением (драйверы);

–операционную систему (ОС);

–прикладные программы и службы, предназначенные для использования пользователями ИС и выполнения бизнес-процессов.

Элементами аппаратного уровня являются:

–автоматизированные рабочие места пользователей – это рабочие станции, оборудованные необходимыми средствами для выполнения пользователями своих должностных обязанностей;

–сервера – высокопроизводительные ЭВМ, предназначенные для реализации централизованных функций ИС, управления вычислительными процессами, предоставления удаленного доступа к ресурсам и данным;

–сетевое оборудование – система активных и пассивных технических средств, обеспечивающих передачу данных между рабочими станциями ИС посредством каналов связи;

–каналы связи – среда распространения сигналов, представляет собой проводные линии связи или радиоканал.

Таким образом, ИС является сложной системой, включающей разнообразные элементы с большим числом пользователей, обладающим разными правами, множеством ресурсов и технологий доступа к ним (см. рисунок 2).

Сложность, гетерогенность компонентов и обеспечения ИС, архитектура, способы доступа к общим информационным ресурсам оказывают непосредственное влияние на показатели безопасности и надежности ИС.

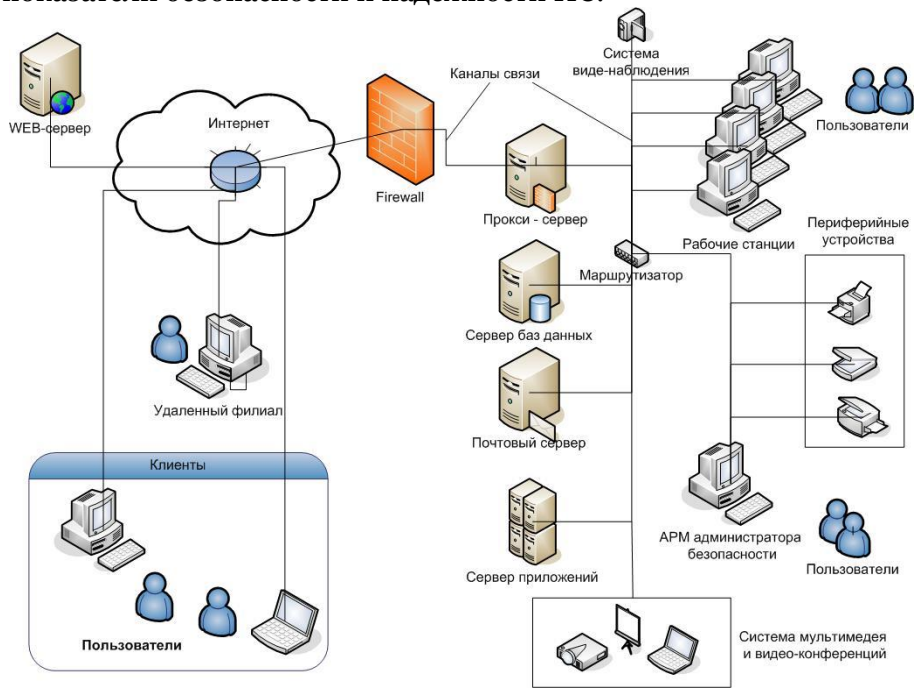

Рис. 2. Структура типовой информационной системы предприятия

Чем сложнее ИС и больше в ней сложных взаимовлияющих друг на друга компонентов, тем больше возможностей для внешнего и внутреннего негативного

воздействия существенной среды [11], проявляющихся в виде природных, техногенных угроз и воздействий злоумышленника (см. рисунок 3).

Изменение в любом из компонентов ИС предприятия под воздействием существенной среды требует изменений в других компонентах и оказывает непосредственное влияние на деятельность предприятия, может повлечь ущерб различного вида. В результате могут возникнуть риски [4, с.75]: кредитный риск, риск ликвидности, ценовой риск, операционный риск, риск несоответствия, стратегический и репутационный риски.

Рис. 3. Взаимосвязь между предприятием, информационной системой и существенной средой

Следовательно, для снижения негативного эффекта необходимо контролировать состояние ИС в течение всего жизненного цикла, блокировать или снижать тяжесть воздействий существенной среды, особенно тех которые связаны с действиями злоумышленника.

Угрозы безопасности в информационной системе

Анализ источников [12, 13] показывает, что угрозы безопасности в ИС можно разделить на две основных категории это непреднамеренные и умышленные угрозы.

К непреднамеренным угрозам относятся:

- ошибки в проектировании ИС;
- ошибки в разработке программных средств ИС;
- случайные сбои в работе аппаратных средств ИС, линий связи, энергоснабжения;
- ошибки пользователей ИС;
- воздействие на аппаратные средства ИС физических полей других электронных устройств.

К умышленным угрозам относятся:

- несанкционированные действия обслуживающего персонала ИС (например, ослабление политики безопасности администратором, отвечающим за безопасность ИС);

– несанкционированный доступ к ресурсам ИС со стороны пользователей ИС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями;

– удаленные атаки;

В зависимости от целей преднамеренные угрозы в ИС делятся на три основные группы [14]:

– угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в ИС или передаваемой от одной ИС к другой;

– угроза нарушения целостности, т.е. преднамеренного воздействия на информацию, хранящуюся в ИС или передаваемую между ИС;

– угроза нарушения доступности информации, т. е. отказа в обслуживании, вызванного преднамеренными действиями одного из пользователей ИС (нарушителя), при котором блокируется доступ к некоторому ресурсу ИС со стороны других пользователей ИС.

Так же анализируя угрозы ИБ в ИС, следует учитывать, что ИС, имеет выход в сеть общего пользования. Внутренние пользователи должны получать выход в глобальные сети, а внешние пользователи должны получать доступ к ИС. Это создает ряд угроз общего характера, которые могут дать злоумышленнику возможность воспользоваться уязвимостью, через которую он может проникнуть к важным сетевым ресурсам.

Алгоритм управления инцидентами информационной безопасности

Каждый этап реализации злоумышленником атаки на ИС и ее объекты, сопровождается рядом событий, происходящих в ИС. Событие ИБ –действие, идентифицируемое появлением определенного состояния системы, сервиса или сети, указывающее на возможное нарушение политики ИБ или отказ защитных мер, а также возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности. Инцидент ИБ – следствие одного или нескольких нежелательных или неожиданных событий ИБ, которые имеют значительную вероятность компрометации операции бизнеса или создания угрозы ИБ.

Таким образом, события ИС, возникшие в результате деятельности злоумышленника или дестабилизирующего фактора случайной природы носят нежелательный характер, могут нанести ущерб и влияют на состояние ИБ ресурсов и объектов ИС. Поэтому необходимо проводить регулярный мониторинг состояния ИС и происходящих в ней событий [15], оценивать риск и опасность каждого события с целью контроля аномальной активности, своевременного обнаружения признаков атак и инцидентов ИБ. Предлагаемая авторами схема алгоритма мониторинга событий и управления инцидентами ИБ в ИС представлена на рисунке 4.

В процессе мониторинга происходит распределенный сбор данных с журналов подсистем регистрации ИС, осуществляется корреляция событий, анализируются источники событий, типы событий и их тяжесть для ИС. Решаются задачи классификации событий и состояний ИС на три множества: нормальное состояние (событие), аномальное состояние (событие), опасное состояние (событие), алгоритм и формализация процедуры классификации, подробно рассмотрен авторами в работе [15].

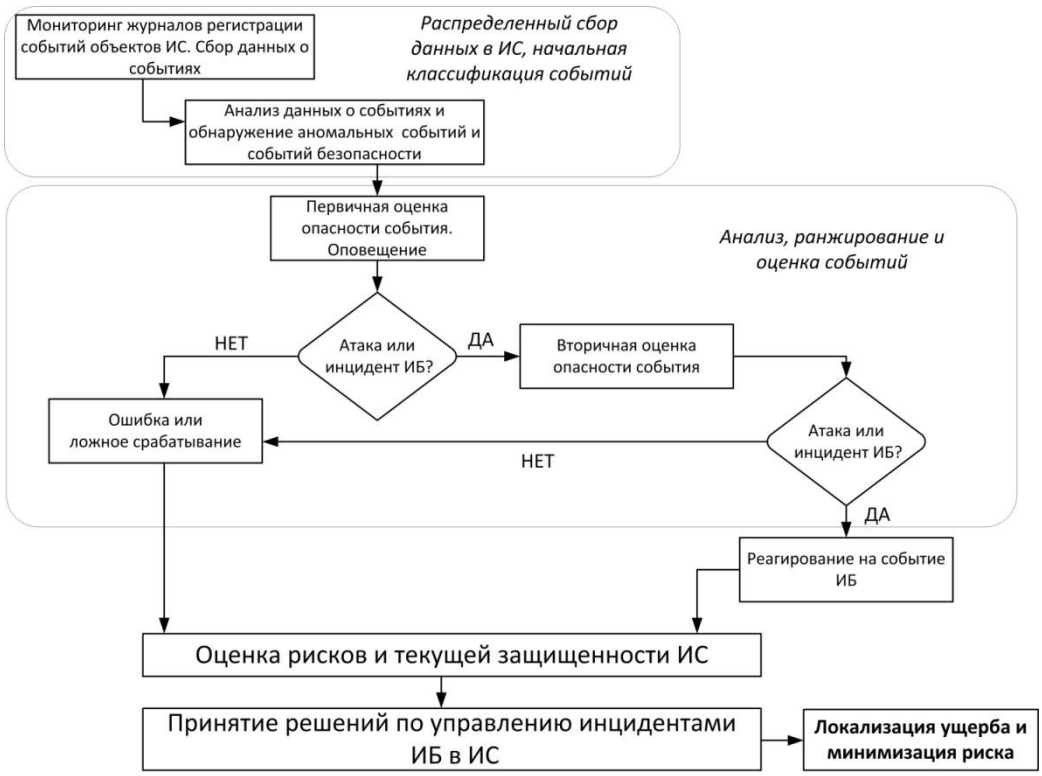

Рис. 4. Алгоритм мониторинга событий и управления инцидентами ИБ в ИС

Таким образом, минимизация риска является частью процесса управления инцидентами ИБ и строится на трех базовых стратегиях:

1) принятие риска - отказ от превентивных мероприятий, воздействие на источник риска, самострахование, диверсификация активов;

2) полная или частичная передача рисков – страхование, хеджирование, синдицирование;

3) избежание рисков – отказ от применения ИС, применение превентивных и профилактических мер по воздействию на источник риска, прогнозирование и предотвращение инцидентов.

4. Заключение

Успешное существование современного предприятия зависит от множества факторов, среди которых не последние позиции занимает ИБ информационной инфраструктуры предприятия. Поэтому для контроля и предотвращения различных видов экономического ущерба и рисков, которые могут оказать негативное влияние на деятельность предприятия необходимо применять процедуры мониторинга событий и мониторинга инцидентов ИБ. Ведь чем быстрее будет обнаружен инцидент и раньше приняты меры по его локализации и устранению последствий, тем меньший ущерб получить предприятие. Предложенный авторами алгоритм мониторинга событий и управления инцидентами ИБ в ИС позволит:

–идентифицировать и контролировать, вызывающие подозрения операции;

–оценивать риск, исходя из конкретных типов событий ИС;

–обращать внимание на любую операцию, превышающую порог «нормальной» активности ИС;

–обращать внимание на усиление активности в ИС или ее подсистемах, особенно тех, которые могут стать объектами сомнительных операций;

–установить правила классификации состояний ИС и пороговые значения для профилей «нормального» и «опасного» функционирования ИС и ее подсистем и время от времени проверять их чувствительность и адекватность.

Для большей эффективности мониторинг и управление инцидентами ИБ следует проводить на регулярной или периодической основе, применяя инструментальные средства поддержки принятия решений.

Литература

1. Статистика уязвимостей корпоративных информационных систем 2016 // Аналитика компании Positive Technologies 2016. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Corporate-Vulnerability-2015-rus.pdf (дата обращения 29.09.2016).

2. Positive Research 2016 // Аналитика компании Positive Technologies 2016. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Positive-Research-2016-rus.pdf (дата обращения 29.09.2016).

3. Исследование утечек конфиденциальной информации в первом полугодии 2016 года // Отчет InfoWatch. https://www.infowatch.ru/report2016_half (дата обращения 29.09.2016).

4. Сычев А.М., Ревенков П.А., Дудка А.Б. Безопасность электронного банкинга. М.:РФК-Имидж Лаб, 2016. 188 с.

5. Oladko V.S. The place of risk assessment in the process of business continuity management // Sochi Journal of Economy. 2016. № 3 (41). С. 167-175.

6. Международный стандарт ISO 27001:2013 Информационные технологии. Методы защиты. Системы менеджмента информационной безопасности. Требования. URL: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf (дата обращения 07.04.2017).

7. ГОСТ 33707-2016 (ISO/IEC 2382:2015) Информационные технологии (ИТ). Словарь//Электронный фон правовой и нормативно-технической документации. URL: http://docs.cntd.ru/document/1200139532 (дата обращения 17.04.2017).

8. Малахова Ю.В., Хохлова В.В., Ходос Д.В. Экономическая успешность // Вестник Красноярского государственного аграрного университета. 2014. №1. С. 3-6.

9. Виснадул Б.Д., Лупин С.А., Сидоров С.В. Основы компьютерных сетей: Учебное пособие для среднего профессионального образования (под ред. Гагариной Л.Г.). М: Форум, 2007. 272 с.

10. Варлатая С.К., Шаханова М.В. Программно-аппаратная защита информации: учеб. пособие. Владивосток: Изд-во ДВГТУ, 2007.

11. Аткина В.С. Разработка метода, алгоритмов и программы для анализа катастрофоустойчивости информационных систем // автореферат дис. ... кандидата технических наук: 05.13.19 / Южный федеральный университет. Волгоград, 2013.

12. Соколов С.С. Модель угроз информационной безопасности организаций // Вестник государственного университета морского и речного флота им. адмирала С.О. Макарова. 2009. №2(2). С. 176-180.

13. Бабенко Г.В. Анализ современных угроз безопасности информации, возникающих при сетевом взаимодействии // Вестник Астраханского государственного технического университета. Серия: Управление, вычислительная техника и информатика. 2010. №2. С. 149-152.

14. Леонтьев П.А. Социология интеллектуальной собственности и проблемы информационной безопасности // Sochi Journal of Economy. 2011. № 4. С. 222-224.

15. Пушкарская А.И., Витенбург Е.А., Оладько В.С. Классификация состояний информационной системы по критерию безопасности // Технология, техника, инженерия. 2017. № 2(4). С. 48-52.

References

1. Statistika uyazvimostei korporativnykh informatsionnykh sistem 2016 // Analitika kompanii Positive Technologies 2016. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Corporate-Vulnerability-2015-rus.pdf (data obrashcheniya 29.09.2016).

2. Positive Research 2016 // Analitika kompanii Positive Technologies 2016. URL: http://www.ptsecurity.ru/upload/ptru/analytics/Positive-Research-2016-rus.pdf (data obrashcheniya 29.09.2016).

3. Issledovanie utechek konfidentsial'noi informatsii v pervom polugodii 2016 goda // Otchet InfoWatch. https://www.infowatch.ru/report2016_half (data obrashcheniya 29.09.2016).

4. Sychev A.M., Revenkov P.A., Dudka A.B. Bezopasnost' elektronnogo bankinga. M.: RFK-Imidzh Lab, 2016. 188 s.

5. Oladko V.S. The place of risk assessment in the process of business continuity management // Sochi Journal of Economy. 2016. № 3 (41). S. 167-175.

6. Mezhdunarodnyi standart ISO 27001:2013 Informatsionnye tekhnologii. Metody zashchity. Sistemy menedzhmenta informatsionnoi bezopasnosti. Trebovaniya. URL: http://www.pqm-online.com/assets/files/pubs/translations/std/iso-mek-27001-2013(rus).pdf (data obrashcheniya 07.04.2017).
7. GOST 33707-2016 (ISO/IEC 2382:2015) Informatsionnye tekhnologii (IT). Slovar'//Elektronnyi fon pravovoi i normativno-tekhnicheskoi dokumentatsii. URL: http://docs.cntd.ru/document/1200139532 (data obrashcheniya 17.04.2017).
8. Malakhova Yu.V., Khokhlova V.V., Khodos D.V. Ekonomicheskaya uspeshnost' // Vestnik Krasnoyarskogo gosudarstvennogo agrarnogo universiteta. 2014. №1. S. 3-6.
9. Visnadul B.D., Lupin S.A., Sidorov S.V. Osnovy komp'yuternykh setei: Uchebnoe posobie dlya srednego professional'nogo obrazovaniya (pod red. Gagarinoi L.G.). M: Forum, 2007. 272 s.
10. Varlataya S.K., Shakhanova M.V. Programmno-apparatnaya zashchita informatsi: ucheb.posobie. Vladivostok: Izd-vo DVGTU, 2007.
11. Atkina V.S. Razrabotka metoda, algoritmov i programmy dlya analiza katastrofoustoichivosti informatsionnykh sistem // avtoreferat dis. ... kandidata tekhnicheskikh nauk: 05.13.19 / Yuzhnyi federal'nyi universitet. Volgograd, 2013.
12. Sokolov S.S. Model' ugroz informatsionnoi bezopasnosti organizatsii // Vestnik gosudarstvennogo universiteta morskogo i rechnogo flota im. admirala S.O. Makarova. 2009. №2(2). S. 176-180.
13. Babenko G.V. Analiz sovremennykh ugroz bezopasnosti informatsii, voznikayushchikh pri setevom vzaimodeistvii // Vestnik Astrakhanskogo gosudarstvennogo tekhnicheskogo universiteta. Seriya: Upravlenie, vychislitel'naya tekhnika i informatika. 2010. №2. S. 149-152.
14. Leont'ev P.A. Sotsiologiya intellektual'noi sobstvennosti i problemy informatsionnoi bezopasnosti // Sochi Journal of Economy. 2011. № 4. S. 222-224.
15. Pushkarskaya A.I., Vitenburg E.A., Olad'ko V.S. Klassifikatsiya sostoyanii informatsionnoi sistemy po kriteriyu bezopasnosti // Tekhnologiya, tekhnika, inzheneriya. 2017. № 2(4). S. 48-52.

УДК 338.14 + 004.056

Управление инцидентами безопасности в информационной системе как средство снижения экономического ущерба

Владлена Сергеевна Оладько [a, *], Екатерина Александровна Витенбург [b],
Анна Игоревна Пушкарская [b]

[a] Финансовый университет при Правительстве Российской Федерации, Российская Федерация
[b] Волгоградский государственный университет, Российская Федерация

Аннотация. В статье рассмотрена актуальная проблема противодействия рискам и экономическому ущербу, возникающим в результате воздействия угроз различного характера. Показана взаимосвязь между экономической успешностью предприятия, качеством и безопасностью функционирования его информационной системы. Проанализированы угрозы и причины нарушения безопасности информационной системы, описаны последствия и возможные риски. Обоснована необходимость контроля над событиями и инцидентами безопасности, возникающими в информационной системе. Предложен алгоритм мониторинга событий и управления инцидентами информационной безопасности, применение которого должно обеспечить локализацию ущерба и минимизацию рисков.

Ключевые слова: событие, защита информации, мониторинг, атака, угроза, риск, предприятие, бизнес-процесс, принятие решений, классификация, злоумышленник.

[*] Корреспондирующий автор
Адреса электронной почты: oladko.vs@yandex.ru (В.С. Оладько)