О.В. Казарин, М.М. Репин

Модель процесса мониторинга состояния информационной безопасности платежной системы

Процесс мониторинга состояния информационной безопасности платежной системы является основой для оценки и анализа рисков информационной безопасности.

Важным аспектом задачи по мониторингу состояния информационной безопасности платежной системы является необходимость оценки взаимосвязей между инициирующими событиями и их влияния на уязвимости платежной системы.

Данные взаимосвязи могут быть описаны с помощью логико-вероятностных моделей, применение которых рассматривается в настоящей работе.

Ключевые слова: платежная система, мониторинг информационной безопасности, логико-вероятностные модели, риск информационной безопасности, инициирующие события.

На стадии эксплуатации платежной системы (далее – ПС) оценку и анализ рисков информационной безопасности (далее – ИБ) проводят на основе определенных сценариев с использованием результатов мониторинга потенциальных уязвимостей ПС, особенностей эксплуатации, компетентности и состава обслуживающего персонала, данных об актуальных угрозах и нештатных ситуациях в ПС (далее – НШС).

Под НШС понимается ситуация, при возникновении которой произошло нарушение штатного функционирования информационно-вычислительных, телекоммуникационных, инженерных систем, систем связи, систем и средств защиты информации, ПС и технологии обработки платежных документов, повлекшее нарушение регламента обработки платежной информации или предоставления отчетности.

Процесс возникновения нештатных ситуаций в ПС

Рассмотрим процесс возникновения НШС. Пусть $V = \{v_1, \dots, v_n\}$ – множество уязвимостей ПС, $E = \{e_1, \dots, e_k\}$ – множество событий в ПС, $I = \{i_1, \dots, i_m\}$ – множество инцидентов ИБ в ПС, $SNS = \{sns_1, \dots, sns_l\}$ – множество сценариев НШС, NS – НШС. На рис. 1 представлен пример процесса возникновения НШС. Событие e_2, связанное с уязвимостью v_2, совместно с событием e_3, не связанным с существующими уязвимостями, порождают инцидент i_2, в свою очередь, подпадающий под сценарий НШС sns_1 и реализующий данную НШС. Аналогично можно описать представленную НШС по сценарию sns_{i-1}. События могут не являться инцидентом ИБ. На рис. 1 данный случай представлен на примере события e_{k-1}.

Таким образом, решение задачи по мониторингу состояния ИБ ПС осложняется необходимостью не только проводить анализ рисков ИБ, но и оценивать взаимосвязи между инициирующими событиями, степень их влияния на уязвимости ПС.

Рис. 1. Процесс возникновения НШС в ПС

Использование сценарного подхода к процессу возникновения НШС позволяет применить для его описания логико-вероятностные модели. Особенности их применения рассматриваются в следующем разделе.

Логико-вероятностная модель процесса мониторинга ИБ в ПС

Постановка задачи. Существующие методы оценки и управления операционными рисками, в том числе и рисками ИБ[1], не предоставляют механизмов, позволяющих описывать сложные зависимости между объектами анализа (событиями, инцидентами, уязвимостями и т. д.), а также связь внутренних и внешних событий, инициирующих риск ИБ.

Данные зависимости могут быть описаны с помощью логико-вероятностных (далее – ЛВ) моделей, показывающих высокую эффективность в решении задач по экономическим направлениям, в том числе при оценке кредитного риска, риска портфеля ценных бумаг[2].

Таким образом, задачу построения модели процесса мониторинга состояния ИБ ПС можно сформулировать следующим образом. Необходимо построить ЛВ-модель процесса мониторинга ИБ ПС. Логико-вероятностная модель процесса мониторинга ИБ ПС должна быть комплексной и включать в себя модели мониторинга обеспечения ИБ ПС и обеспечения безопасности платежных технологий с учетом возможности как внутренних, так и внешних событий, инициирующих НШС.

Структура событий процесса мониторинга ИБ ПС. Задачей процесса мониторинга ИБ ПС является своевременное выявление событий, которые могут инициировать риски возникновения НШС.

Реализация рисков в ПС, включающих также риски ИБ, может иметь два вида последствий, в том числе и одновременных. Первое последствие – это нарушение процесса функционирования ПС, непрерывность которого является одним из важнейших условий для проведения клиентских платежей. Вторым последствием является потеря денежных средств клиентом из-за неправильной обработки электронных платежных сообщений, содержащих данные о платежах. Нарушение процесса непрерывного функционирования, в свою очередь, может быть вызвано как реализацией угроз ИБ, так и ошибками системного программного обеспечения ПС.

Для построения ЛВ-модели процесса мониторинга ИБ ПС, по аналогии с подходом, применяемым для финансовых рисков[3], рассмотрим НШС в качестве сложного события Y, состоящего из объединения логической (Л) операцией *И* внутренних Y_{in} и внешних Y_{out} производных событий.

В свою очередь, внутренние и внешние производные события могут вызываться инициирующими событиями с Л-связью ИЛИ из групп Y_s (некорректная работа средств и систем защиты информации в ПС) и Y_{pay} (нарушение платежных технологий). В каждом из событий из групп Y_s и Y_{pay} для внутренних производных событий Y_{in} выделяют события Y_{ins_1}, ... , Y_{ins_n}, Y_{inpay_1}, ... , Y_{inpay_n}, объединенные Л-связью ИЛИ. Внешнее производное событие Y_{out} вызывает события Y_{outs_1}, ... , Y_{outs_n}, Y_{outpay_1}, ... , Y_{outpay_n} , объединенные Л-связью ИЛИ. Структура событий процесса мониторинга ИБ ПС представлена на рис. 2.

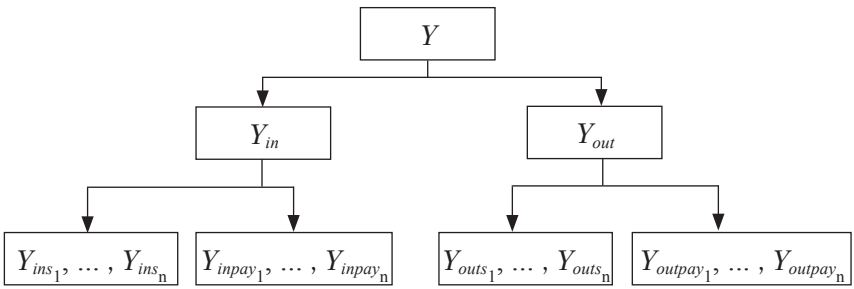

Рис. 2. Структура событий процесса мониторинга ИБ ПС

Производные и инициирующие события ЛВ-модели процесса мониторинга информационной безопасности в ПС. Опишем для общего случая события, мониторинг которых позволит определить наличие нарушений ИБ ПС (см. рис. 3, в котором для упрощения приведены только индексы в обозначении событий).

В качестве основного события Y_1 будем рассматривать общий процесс мониторинга. Событие Y_1 появляется от действия внутреннего производного события Y_2 и внешнего Y_3. Событие Y_3 – производное событие внешних инициирующих событий, включающее в себя события Y_8 и Y_9.

Y_8 – контроль взаимоотношений с внешними организациями: Y_{10} – контроль соблюдения лицензионных требований и наличия лицензий у внешних организаций, Y_{11} – контроль ведения договорной работы с внешними организациями.

Y_9 – контроль платежного процесса при взаимодействии с внешними организациями: Y_{12} – мониторинг статуса клиента, Y_{13} – мониторинг статуса (корректности) электронных платежных сообщений клиента, Y_{14} – мониторинг ликвидности клиента.

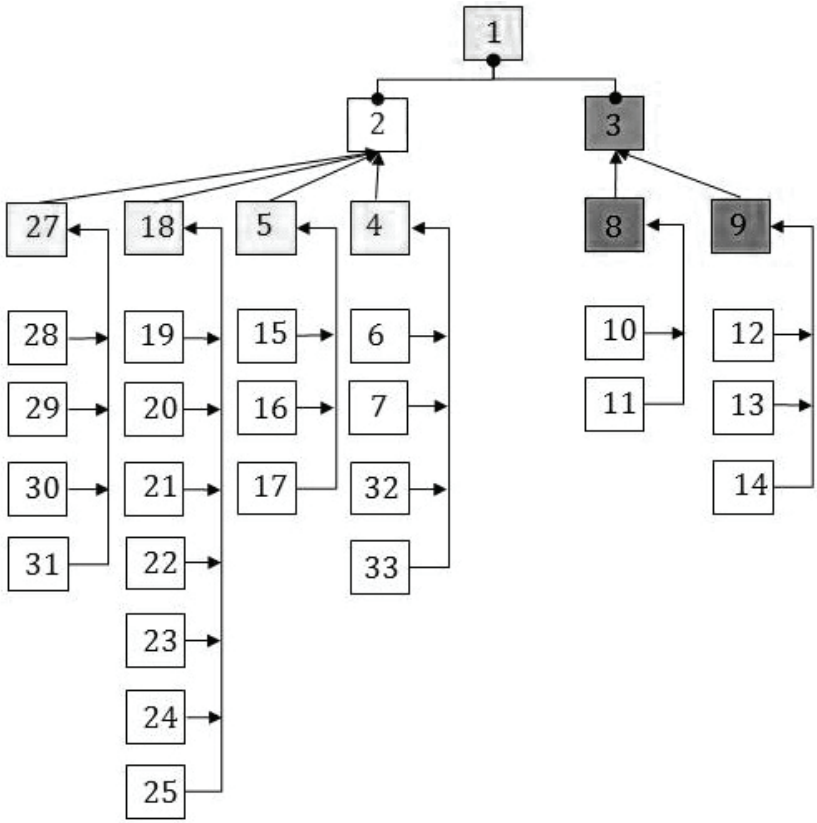

Рис. 3. Структурная модель процесса мониторинга ИБ в ПС

Y_2 – производное событие внутренних инициирующих событий, включающее в себя события:

Y_4 – контроль действий пользователей ПС и объектов информационной инфраструктуры ПС: Y_6 – контроль средств ввода-вывода информации, Y_7 – контроль работы в подсистемах ПС, Y_{32} – контроль работы с сетью Интернет, Y_{33} – контроль входных/выходных данных.

Y_5 – контроль функционирования компонент ПС: Y_{15} – контроль присутствия эксплуатационного персонала на рабочих местах, Y_{16} – контроль статуса функционирования ИТ-сервисов, Y_{16} – контроль функционирования средств и систем защиты информации.

Y_{18} – контроль заданных настроек ПС: Y_{19} – контроль настроек безопасности, согласно стандартам, Y_{20} – паспортный контроль объектов информационной инфраструктуры ПС, Y_{21} – регистрация и мониторинг событий ИТ-сервисов, Y_{22} – регистрация и мониторинг событий средств и систем защиты информации, Y_{23} – регистрация, учет и контроль используемых носителей информации, Y_{24} – контроль выполняемых критичных операций в ПС, Y_{25} – контроль систем автоматизированного мониторинга и корреляции событий.

Y_{27} – контроль целостности: Y_{28} – контроль целостности архивов и резервных копий, Y_{29} – контроль целостности сред функционирования средств криптографической защиты информации, серверов, автоматизированных рабочих мест, Y_{30} – контроль модификаций программного обеспечения ПС, Y_{31} – контроль целостности регистрационных журналов.

В свою очередь, для наиболее критичных инициирующих событий можно построить индивидуальное дерево событий, отражающее процесс его возникновения.

Рассмотрим одно из важнейших событий для платежных систем Y_9 – контроль платежного процесса при взаимодействии с внешними организациями (см. рис. 4). При получении платежных сообщений от клиента важным аспектом является контроль его корректности Y_{13}. Для Y_{13} можно определить следующие инициирующие события с учетом того, что электронное сообщение (далее – ЭС) представляет собой одиночное сообщение или пакет сообщений в соответствии с альбомом «Унифицированные форматы электронных банковских сообщений»: Y_{34} – контроль корректности конверта ЭС (на соответствие указанному альбому), Y_{35} – контроль корректности электронной подписи отправителя и ее принадлежности и даты формирования, Y_{36} – контроль корректности ЭС/пакета ЭС, Y_{37} – контроль дублирования ЭС/ пакета ЭС, Y_{38} – контроль общей суммы платежей в пакете ЭС (если поступил пакет).

Кортежи для описания производных событий модели процесса мониторинга ИБ в ПС. Для обеспечения гибкости представленной структурной модели введем описание производных событий в виде кортежей. Производные события будут являться значением функции, аргументами которой являются инициирующие события.

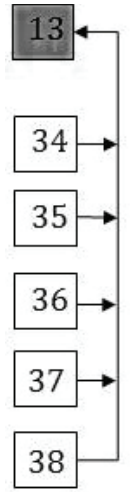

Рис. 4. Структурная модель процесса контроля корректности входящих платежных сообщений ПС

Например:
1(2, 3);
2(27, 18, 5, 4);
3(8, 9);
27(28, 29, 30, 31);
18(19, 20, 21, 22, 23, 24, 25);
5(15, 16, 17);
4(6, 7, 32, 33);
8(10, 11);
9(12, 13, 14).

В записи производных кортежей знак Л-операции опущен, так как он может варьироваться в зависимости от постановки задачи. Также следует отметить, что наличие определенных факторов не является однозначным свидетельством инцидента ИБ (ранее – НШС) и соответствующие им инициирующие события имеют определенную вероятность и являются случайными совместными и независимыми событиями.

Прогнозирование финансовых потерь. При осуществлении процесса мониторинга важно оценить возможные финансовые потери от реализации рисков в ПС.

Рассмотрим подход к анализу возможных потерь на примере процесса контроля корректности входящих платежных сообщений ПС.

Фрагмент логической модели данного процесса имеет следующий вид.

$$Y = \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \vee \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \vee \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge Y_{37} \wedge Y_{38} \vee \bar{Y}_{34} \wedge \bar{Y}_{35} \wedge Y_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \vee \bar{Y}_{35} \wedge \bar{Y}_{36} \wedge \bar{Y}_{37} \wedge \bar{Y}_{38} \cdots$$

Логическую модель процесса контроля в минимальной дизъюнктивной нормальной форме можно представить следующим образом: $Y = Y_{34} \vee Y_{35} \vee Y_{36} \vee Y_{37} \vee Y_{38}$.

Возможные финансовые потери от рисков реализации НШС можно вычислить по следующей формуле.

$$Q_{13} = P_{34} Q_{34} + P_{35} Q_{35} + P_{36} Q_{36} + P_{37} Q_{37} + P_{38} Q_{38},$$

где $Q_{34} \cdots Q_{38}$ – финансовые ресурсы, которые могут быть потеряны при реализации соответствующего инициирующего события; $P_{34} \cdots P_{38}$ – риски реализации инициирующих событий, под которыми понимается вероятность потери финансовых ресурсов.

В данном примере под финансовыми ресурсами, которые могут быть потеряны, понимаются суммы, направляемые банками клиентов в платежных распоряжениях, соответственно в зависимости от этапа контроля под угрозой могут находиться как отдельные платежные документы, так и пакеты платежей (в случае внутреннего нарушителя).

В том случае, если в банк поступает подложный платежный документ, возникает риск предъявления банку претензий клиента на данную сумму, если данный платеж будет проведен.

Существенное отличие данного подхода заключается в том, что риск возникновения основного события рассчитывается в результате Л-операций со значениями риска инициирующих событий. Значения риска инициирующих событий, например $P_{34} \cdots P_{38}$, основаны на результатах комплексного анализа различных оценок[4]. Также стоит отдельно отметить, что формула расчета финансовых потерь имеет ту же структуру, что и формула Базельского комитета для расчета резервирования под операционный риск[5].

В статье приведена модель возникновения НШС, на основе которой предложена структурная ЛВ-модель процесса мониторинга ИБ ПС, а также отдельно рассмотрен процесс мониторинга безопасности платежного процесса, для которого приведена формула расчета возможных потерь.

Предложенная ЛВ-модель процесса мониторинга ИБ ПС позволит описывать сложные зависимости между объектами анализа (событиями, инцидентами, уязвимостями и т. д.), а также связь

внутренних и внешних событий, инициирующих риски ИБ, как в контексте обеспечения безопасности платежного процесса, так и по направлению обеспечения ИБ ПС в целом.

Использование ЛВ-моделей при описании процессов по обеспечению ИБ позволяет исключить неопределенности, возникающие в процессе оценки влияния различных факторов на уровень ИБ ПС.

Примечания

[1] *Бухтин М.А.* Методика и практика управления операционными рисками в коммерческом банке. М.: ИБД АРБ, 2006; *Сазыкин Б.В.* Управление операционным риском в коммерческом банке. М.: Вершина, 2008; *Михеев В.А., Кузнецов А.В., Репин М.М.* Способ определения степени уязвимости автоматизированной информационной системы в отношении конкретных методов реализации угроз безопасности информации // Вопросы защиты информации. 2013. № 1. С. 20–25; Обеспечение информационной безопасности организаций банковской системы Российской Федерации: Методика оценки рисков нарушения информационной безопасности: Рекомендации в области стандартизации Банка России. РС БР ИББС-2.2-2009. Дата введения 01.01.2010. Приняты и введены в действие распоряжением Банка России от 11 ноября 2009 г. № Р-1190; *Астахов А.М.* Искусство управления информационными рисками. М.: ДМК Пресс, 2010; *Петренко С.А., Симонов С.В.* Управление информационными рисками: Экономически оправданная безопасность. М.: ДМК Пресс, 2005; *Петренко С.А.* Анализ рисков в области защиты информации. СПб.: Афина, 2009.

[2] *Соложенцев Е.Д.* Сценарное логико-вероятностное управление риском в бизнесе и технике. СПб.: Бизнес-пресса, 2004.

[3] *Карасева Е.И., Степанов А.Г.* Логико-вероятностная модель операционного риска банка // Информационно-управляющие системы. 2011. № 2. С. 77–83.

[4] *Бедрединов Р.Т.* Управление операционными рисками банка: Практические рекомендации. М.: Альпина, 2014.

[5] Международная конвергенция измерения капитала и стандартов капитала: новые подходы типа. [Электронный ресурс] URL: http://www.cbr.ru/today/ms/bn/bz_1.pdf (дата обращения: 10.05.2016).