М.М. Репин

Модели риска возникновения нарушений информационной безопасности в платежной системе

Процесс обеспечения раннего предупреждения рисков информационной безопасности в платежной системе является основным для определения необходимых управляющих воздействий по минимизации данных рисков.

Важным аспектом задачи предупреждения рисков является моделирование процесса их возникновения.

Данные модели могут быть описаны различными способами, в том числе и с помощью логико-вероятностных моделей, применение которых рассматривается в настоящей работе.

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

В процессе функционирования платежной системы (далее – ПС) могут возникать различные нештатные ситуации в ПС (далее – НШС), в том числе связанные с информационной безопасностью ПС. Учитывая тот факт, что область информационной безопасности в ПС имеет расширенные границы и включает в себя обеспечение безопасности платежных технологий, целесообразно рассматривать процесс возникновения НШС в целом, не акцентируя внимание только на классических областях обеспечения информационной безопасности.

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.

НШС можно разделить на три типа:

– НШС 1 типа – нештатная ситуация, влияющая на начало, ход или завершение операционного дня и/или осуществление (завершение) электронных расчетов в текущем операционном дне;
– НШС 2 типа – нештатная ситуация, не влияющая на начало, ход и завершение операционного дня, осуществление электронных расчетов в текущем операционном дне, но влияющая на решение других задач, реализуемых структурными подразделениями;
– НШС 3 типа – нештатная ситуация, не влияющая на начало, ход и завершение операционного дня, осуществление электронных расчетов в текущем операционном дне, а также решение других задач, реализуемых структурными подразделениями.

Рассмотрим процесс возникновения НШС в платежной системе.

Пусть $V = \{v_1, \ldots, v_n\}$ – множество уязвимостей ПС, $E = \{e_1, \ldots, e_k\}$ – множество событий в ПС, $I = \{i_1, \ldots, i_m\}$ – множество инцидентов ИБ в ПС, $NS = \{sns_1, \ldots, sns_l\}$ – множество сценариев НШС, NS – НШС. Например, 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, попадающий под сценарий НШС sns_1 и реализующий данную НШС. Аналогично можно описать представленную НШС по сценарию sns_{l-1}. События могут не являться инцидентом ИБ. Более подробно данный случай на примере события e_{k-2} проиллюстрирован в работе[1].

Использование сценарного подхода к процессу возникновения НШС позволяет применить для его описания логико-вероятностные модели, а также сценарный подход к анализу рисков возникновения НШС.

Возникновение НШС могут вызвать различные инциденты, связанные с объектами информационной инфраструктуры ПС, которые могут быть инициированы рядом факторов. Данные факторы могут быть описаны как ключевые индикаторы рисков в ПС и применены при проведении сценарного анализа риска (см. рис. 1).

Рис. 1. Процесс сценарного анализа рисков возникновения НШС

Под ключевыми индикаторами риска понимаются показатели или параметры, которые отражают актуальный уровень рисков возникновения событий и инцидентов в ПС, являющихся инициирующими событиями для НШС и повышающих риск возникновения НШС.

В качестве основных параметров индикаторов рисков целесообразно рассматривать[2]:

– предмет индикатора (предмет оценки);
– способы получения значений индикатора (формула расчета индикатора);
– пороговые значения индикатора;
– источники информации о состоянии индикатора;
– регулярность контроля индикатора;
– периодичность пересмотра индикатора.

Для примера опишем некоторые из верхнеуровневых факторов (ключевых индикаторов), влияющих на уровень риска возникновения НШС.

X_1 – процент неидентифицированных входящих электронных сообщений (далее – ЭС). Повышение данного показателя может свидетельствовать о наличии ошибок в системах клиентов, либо о попытках тестирования ПС.

X_2 – процент ЭС, забракованных из-за ошибок в их структуре или при наличии некорректного содержимого. Повышение процента подобных ЭС повышает риск проведения несанкционированных платежей и может свидетельствовать о наличии ошибок в системах клиентов или попытках проведения атак на ПС.

X_3 – неисправность серверов ПС (криптосерверов, серверов баз данных, файловых серверов и т. п.). Наличие ошибок в работе серверов ПС может повышать риски возникновения НШС, связанных с корректным функционированием ПС в целом, включая процессы обработки платежей, клиринга и др.

X_4 – неисправность каналов связи и сетевого оборудования. Наличие ошибок при передаче ЭС создает предпосылки для некорректной обработки платежной информации, ошибок при осуществлении клиринговых процессов и повышает риск ошибок функционирования ПС в целом.

X_5 – неисправность функционирования средств и систем защиты информации в ПС. Данные факторы влияют на такие риски, как осуществление несанкционированного доступа к объектам информационной инфраструктуры ПС, компрометация платежной информации и иные инциденты, связанные с нарушением ИБ ПС.

Таким образом, можно выделить множество $X = \{X_1 \cdots X_J\}$ – факторов, повышающих риски возникновения НШС. В то же время данные факторы могут сами являться НШС для подсистем ПС.

Сценарии ошибок функционирования объектов информационной структуры ПС позволяют построить граф-модель риска возникновения НШС[3].

Пусть общему состоянию ПС G соответствуют состояния ее подсистем $S = \{S_1 \cdots S_d\}$, а факторам $X = \{X_1 \cdots X_f\}$ случайные события, обозначаемые логическими переменными. НШС (итоговое событие) произойдет, если произойдет любое одно, два или все из событий множества. Данные производные события могут вызываться инициирующими событиями (факторами) $X = \{X_1 \cdots X_f\}$. Построим обобщенную граф-модель возникновения НШС (см. рис. 2). Граф-модель может содержать не только логические связи OR, но и AND, NOT, а также различные циклы.

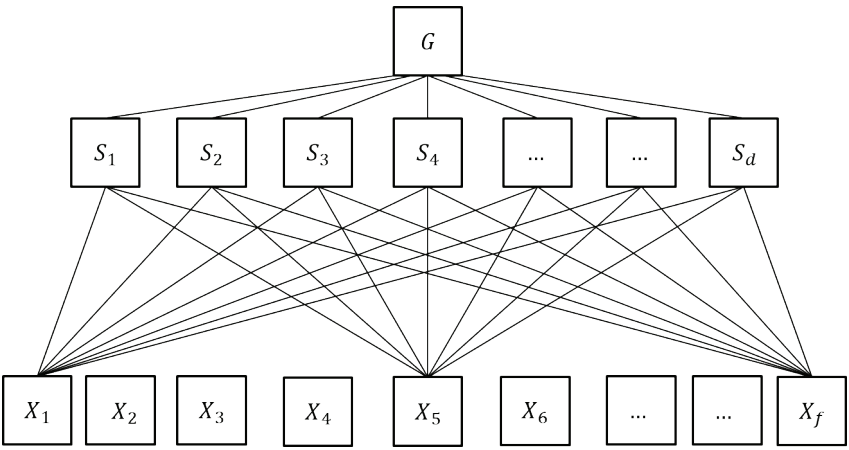

Рис. 2. Граф-модель риска НШС

На основе граф-модели риска можно записать логическую модель риска возникновения НШС:

$$G = S_1\{X_1 \cdots X_f\} \vee S_2\{X_1 \cdots X_f\} \vee S_d\{X_1 \cdots X_f\},$$

имеющую следующую ортогональную форму:

$$G = S_1 \vee S_2 \bar{S}_1 \vee S_3 \bar{S}_2 \bar{S}_1 \vee \cdots$$

Тогда описание вероятностной модели риска возникновения НШС можно представить как

$$P_r = P_1\{G_1 = 1\} = P_1 + P_2\{1 - P_1\} + P_3\{1 - P_2\}\{1 - P_1\} + ...,$$

где P_1, P_2, P_3, ... , P_d – вероятности событий S_1, S_2, S_3, ... , S_d.

В статье приведена модель возникновения НШС, на основе которой предложена структурная, логическая и вероятностная модели риска возникновения НШС.

Рассмотрен сценарный подход к анализу рисков возникновения НШС. Приведены примеры факторов риска (ключевых индикаторов), оказывающих влияние на общий риск возникновения НШС.

Предложенные модели возникновения НШС позволят описывать влияние факторов риска на подсистемы ПС и уровень риска возникновения НШС в целом, а также связь внутренних и внешних событий, инициирующих риски возникновения НШС.

Использование предложенных моделей при описании процессов по предупреждению рисков возникновения НШС позволяет исключить неопределенности, возникающие в процессе оценки влияния различных факторов на уровень ИБ ПС в целом.

Примечания

[1] *Казарин О.В., Репин М.М.* Модель процесса мониторинга состояния информационной безопасности платежной системы // в настоящем номере.

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

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