УДК 004.056
DOI 10.21685/2587-7704-2017-2-2-5

Open Access RESEARCH ARTICLE

Вероятностные модели инцидентов информационной безопасности на основании их факторов

А. Ю. Щербакова
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

О. В. Липилин
Пензенский государственный университет, Россия, 440026 г. Пенза, ул. Красная, 40

Аннотация. Описаны принцип построения факторных моделей инцидентов ИБ, а также вероятностные модели инцидентов ИБ на основании факторов нежелательных событий ИБ, которые могут привести к инцидентам ИБ. Анализ и оценка вероятностей инцидентов ИБ на основании их факторов позволяют обеспечить эффективное планирование системы управления информационной безопасностью объекта с точки зрения предотвращения инцидентов ИБ и снижения затрат на реализацию стратегий управления инцидентами ИБ.

Ключевые слова: инцидент ИБ, нежелательное событие, фактор, вероятность, модель.

Probabilistic incident models for information security based on their factors

A. Yu. Shcherbakova
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

O. V. Lipilin
Penza State University, 40 Krasnaya Street, 440026, Penza, Russia

Abstract. The construction principle of a factor model for information security (IS) incidents, as well as probabilistic models for IS incidents based on the factors of undesirable events leading to IS incidents, are described. A probability analysis and assessment of IS incidents based on their factors allows to ensure an effective planning of the object security information management system in terms of IS incidents prevention and costs reduction for implementation of IS incident management strategies.

Key words: IS incident, undesirable event, factor, probability, model.

Введение

Под инцидентом информационной безопасности (ИБ) понимается одно или серия нежелательных событий ИБ, которые имеют значительную вероятность компрометации бизнес-операций и угрожают информационной безопасности [1]. Последствиями инцидентов ИБ могут быть прерывания бизнес-процессов, нарушение конфиденциальности, целостности или доступности активов объекта, что в свою очередь приводит к потере производительности, ущербу с точки зрения материальных затрат или репутации. Управление инцидентами информационной безопасности является важной частью системы обеспечения информационной безопасности объекта. Эффективное обнаружение происходящих инцидентов ИБ, а также прогнозирование возможных инцидентов ИБ играют ключевую роль при управлении инцидентами ИБ. Идентификация и оценка инцидентов ИБ могут производиться на основании факторов нежелательных событий, ведущих к инцидентам ИБ [2].

1. Сценарии инцидентов ИБ. Факторы нежелательных событий инцидентов ИБ

Инцидент ИБ как последовательность нежелательных событий ИБ может быть представлен в виде совокупности сценариев, описывающих взаимосвязи между этими событиями. Сценарии инцидентов строятся на основе метода дерева отказов [3]. Примеры сценариев инцидентов ИБ представлены в [4]. Нежелательные события в сценариях инцидентов делятся на два уровня. Нежелательные события второго уровня являются непосредственными причинами инцидента ИБ, нежелательные события первого уровня являются прямыми причинами нежелательных событий второго уровня. Реализация нежелательных событий первого уровня свидетельствует о том, что инцидент ИБ может произойти в неопределенный момент времени, он является потенциальным. Реализация нежелательных событий второго уровня свидетельствует о том, что инцидент произошел, он является реальным.

Идентификация потенциальных и реальных инцидентов ИБ может производиться на основании факторов, указывающих на нежелательные события в сценариях инцидентов ИБ определенного вида. Такие факторы, например, как замедление работы и отказы системы, изменение стартовой страницы браузера, всплывающие окна, рекламные сообщения, нетипичный набор запущенных в ОС процессов и другие, могут свидетельствовать о реализации инцидентов внедрения вредоносного программного обеспечения. А такие факторы, как, например, сообщения антивирусной системы о наличии потенциально опасных файлов, сообщения средств проверки подлинности программ об использовании на узле нелицензионного ПО, о наличии файлов с неизвестным системе расширением и другие, могут свидетельствовать о возможности реализации инцидента ИБ в неопределенный момент времени. Модель сценариев инцидентов ИБ представлена на рис. 1, где ФНСп – факторы нежелательных событий первого уровня, ФНСв – факторы нежелательных событий второго уровня.

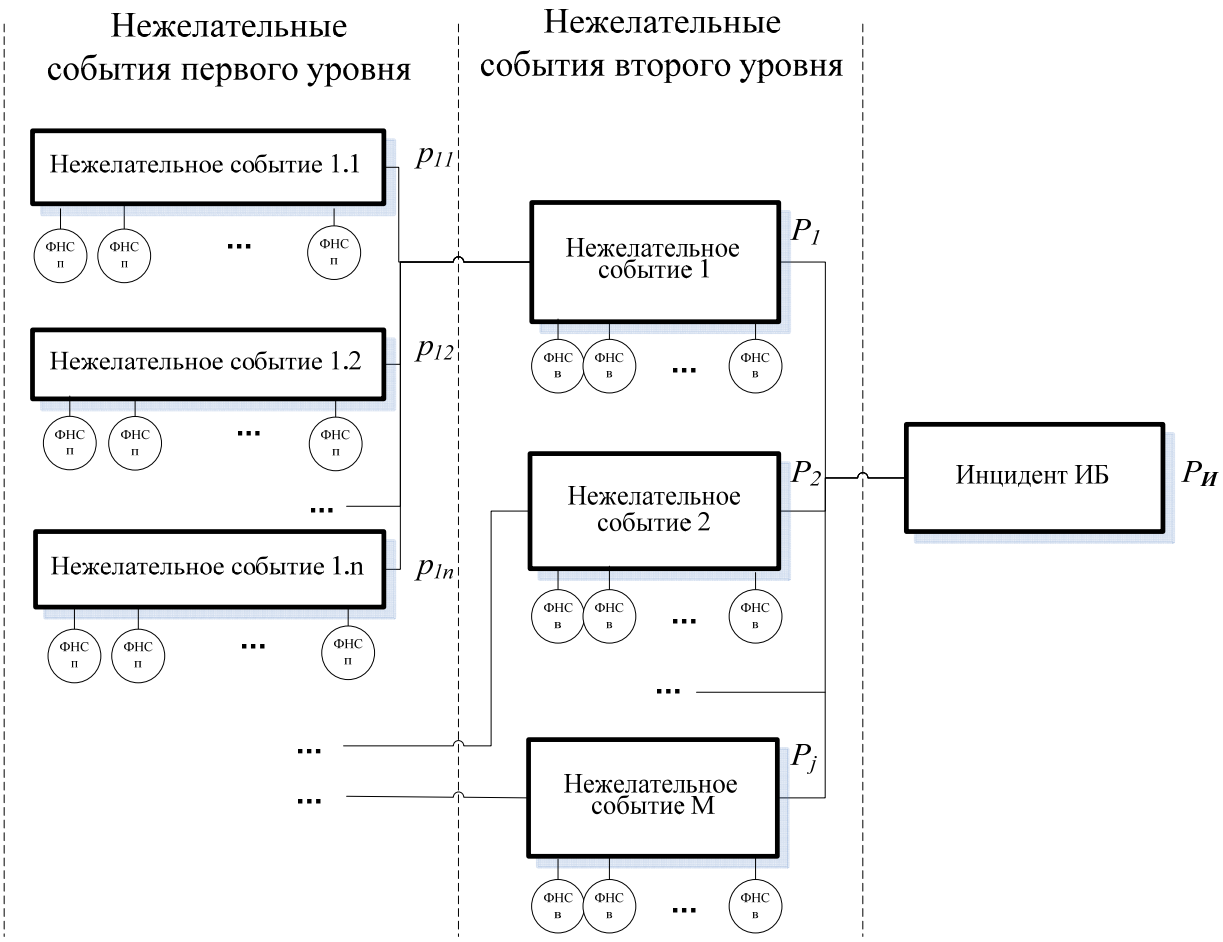

Рис. 1. Модель сценариев инцидентов ИБ

Факторы инцидента ИБ делятся на две группы. К первой группе относятся факторы, указывающие на то, что инцидент может произойти в неопределенный момент времени, ко второй – указывающие на то, что инцидент происходит в настоящий момент. Взаимосвязь между факторами и не-

желательными событиями в сценариях инцидентов определяется факторной моделью применительно к каждому типу инцидентов ИБ.

Пример факторной модели инцидентов ИБ типа «Несанкционированный доступ» представлен в табл. 1. В данном примере факторами нежелательных событий второго уровня (ФНСв) являются:

– наличие неавторизованного инструментария, связанного с безопасностью (ФНСв1.1);

– модификации критичных файлов, отметок времени и привилегий, включая исполняемые программы, библиотеки системы и файлы конфигурации данных на узле (ФНСв1.2);

– сообщения системы обнаружения вторжений об обнаружении вторжений к узлу (ФНСв1.3);

– попытки доступа к критичным файлам узла (ФНСв1.4);

– новая учетная запись пользователя или группы пользователей на административном уровне (ФНСв1.5);

– наличие неавторизованного инструментария (ФНСв1.6).

Таблица 1

Пример факторной модели инцидентов ИБ типа «Несанкционированный доступ»

Инцидент ИБ	Нежелательные события второго уровня		Нежелательные события первого уровня	
	Событие	Факторы	Событие	Факторы
Инцидент несанкционированного доступа	Несанкционированный доступ к узлу	ФНСв1.1 ФНСв1.2 ФНСв1.3 ФНСв1.6	Преодоление механизмов аутентификации на узле	ФНСп1.1 ФНСп1.2 ФНСп1.3 ФНСп1.6 ФНСп1.8
			Использование уязвимостей ОС и приложений на узле	ФНСп1.3 ФНСп1.4 ФНСп1.5 ФНСп1.6 ФНСп1.7
	Несанкционированное использование учетной записи пользователя	ФНСв1.3 ФНСв1.4 ФНСв1.5	Преодоление механизмов аутентификации по сети	ФНСп1.2 ФНСп1.6 ФНСп1.7 ФНСп1.8
			Несанкционированное копирование данных аутентификации	ФНСп1.1 ФНСп1.3 ФНСп1.7 ФНСп1.8

Факторами нежелательных событий первого уровня (ФНСп) являются следующие:

– выявленные факты нарушения политик «чистого стола» и «чистого экрана» (ФНСп1.1);

– выявленное с помощью мониторинга несоответствие требованиям политики парольной защиты (ФНСп1.2);

– выявленное с помощью мониторинга отсутствие процедур проверки внешних носителей, возможность подключения внешних носителей (ФНСп1.3);

– выявленные при мониторинге сведения о версиях ПО и установке последних обновлений и «заплат» для ОС, их несоответствие последним обновлениям, предоставляемым разработчиком (ФНСп1.4);

– нарушения или отказ в процессе обновления программ и ОС на узле (ФНСп1.5);

– многократные попытки регистрации в системе (ФНСп1.6);

– выявленные факты передачи данных аутентификации в открытом виде (в электронном письме, во время телефонного разговора и т.п.) (ФНСп1.7);

– наличие в реестре неизвестных программ (ФНСп1.8).

Рассмотрим применение факторных моделей инцидентов ИБ для прогнозирования инцидентов ИБ и их вероятностной оценки.

2. Вероятностные модели инцидентов ИБ

Реализация нежелательных событий первого уровня в сценариях инцидентов ИБ с определенной вероятностью p_{ij} ведет к реализации нежелательных событий второго уровня. Эта вероятность может быть определена статистически или экспертным путем. Нежелательные события первого уровня, которые могут привести к одному событию второго уровня, являются совместными [5].

Вероятность нежелательного события второго уровня P_j определяется как вероятность суммы событий первого уровня, ведущих к нему, и может быть вычислена следующим образом:

$$P_j = 1 - \prod_i (1 - p_{ji}), \quad (1)$$

где p_{ji} – вероятность i-го нежелательного события первого уровня, которое может привести к j-му нежелательному событию второго уровня.

Реализация инцидента ИБ обусловлена реализацией хотя бы одного из нежелательных событий второго уровня его сценариев. Нежелательные события второго уровня, которые ведут к реализации одного инцидента ИБ, являются совместными. Вероятность реализации инцидента ИБ $P_{\text{И}}$ может быть вычислена следующим образом:

$$P_{\text{И}} = 1 - \prod_j (1 - P_j). \quad (2)$$

Используя (1) и (2), получим значение вероятности инцидента ИБ, выраженное через вероятности нежелательных событий первого уровня:

$$P_{\text{И}} = 1 - \prod_j \prod_i (1 - p_{ji}). \quad (3)$$

Факторы нежелательных событий (ФНС) инцидентов ИБ свидетельствуют о реализации инцидентов ИБ. Введем два множества показателей наличия ФНС инцидентов ИБ: $\chi_i \in \text{X}$ для первой группы факторов и $\varphi_j \in \Phi$ – для второй. Показатели принимают значение 0 в случае отсутствия факторов и значение 1 – при наличии хотя бы одного фактора соответствующего нежелательного события. Если выявлен хотя бы один фактор нежелательных событий второго уровня, то соответствующее ему нежелательное событие произошло, т.е. инцидент ИБ считается реальным, его вероятность равна 1. В случае если факторы нежелательных событий второго уровня отсутствуют, но выявлены факторы нежелательных событий первого уровня, то инцидент считается возможным. Тогда его вероятность может быть вычислена следующим образом:

$$P_{\text{И}} = \begin{cases} 1 - \prod_j \prod_i (1 - \chi_i p_{ij}), & \text{если } \varphi_j = 0; \\ 1, & \text{если } \varphi_j = 1, \end{cases}$$

где χ_i – показатель наличия факторов i-го нежелательного события первого уровня; φ_j – показатель наличия факторов j-го нежелательного события второго уровня.

Заключение

Представленная вероятностная модель инцидентов ИБ на основании их факторов может быть использована для прогнозирования и вероятностной оценки инцидентов ИБ на объекте, которые обеспечат возможность при необходимости предпринять превентивные защитные меры для предотвращения потенциальных инцидентов ИБ или обеспечить своевременное реагирование на происходящие инциденты ИБ.

Библиографический список

1. ГОСТ Р ИСО/МЭК 18044:2007 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности.
2. Зефиров, С. Л. Оценка инцидентов информационной безопасности / С. Л. Зефиров, А. Ю. Щербакова // Доклады Томского государственного университета систем управления и радиоэлектроники. – 2014. – № 2 (32). – С. 77–81.
3. ГОСТ Р 54144-2010 Менеджмент рисков. Руководство по применению организационных мер безопасности и оценки рисков. Идентификация инцидентов.
4. Щербакова, А. Ю. Модель сценариев инцидента внедрения вредоносного программного обеспечения / А. Ю. Щербакова // Информация и безопасность. – 2013. – № 3. – С. 375–378.
5. Вентцель, Е. С. Теория вероятностей / Е. С. Вентцель. – Изд. 4-е стер. – М. : Наука, 1969. – 576 с.

Щербакова, А. Ю.
Вероятностные модели инцидентов информационной безопасности на основании их факторов / А. Ю. Щербакова, О. В. Липилин // Инжиниринг и технологии. – 2017. – Vol. 2(2). – DOI 10.21685/2587-7704-2017-2-2-5