УДК 004.056.5

В.Э. Исаева, А.С. Шабуров
Пермский национальный исследовательский
политехнический университет, г. Пермь

АНАЛИЗ РИСКОВ ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ, АГРЕГИРОВАННЫХ ПО УГРОЗАМ ИЛИ ПОСЛЕДСТВИЯМ

В статье произведен анализ рисков информационной безопасности объекта критической информационной инфраструктуры, агрегированных по последствиям или угрозам. Предложен доступный метод идентификации последствий реализации угроз безопасности информации, позволяющий поэтапно привести совокупность последствий определенного вида.

Ключевые слова: информационная безопасность; критическая информационная инфраструктура; риски информационной безопасности.

V.E. Isaeva, A.S. Shaburov
Perm national research polytechnic university, Perm

RISK ANALYSIS OF A CRITICAL INFORMATION INFRASTRUCTURE OBJECT, AGGREGATED THREATS OR BY EFFECTS

Risk analysis of an object of critical information infrastructures, aggregated by consequences or threats has been made in this article. An accessible method for identifying the consequences of the implementation of threats to information security have been proposed, which makes it possible to gradually bring a set of consequences of a certain type.

Keywords: information security; critical information infrastructure; information security risks.

Анализ рисков предполагает рациональное выстраивание процессов ИБ и определяет ресурсы для защиты активов. В свою очередь, оценка рисков учитывает целесообразность мер по митигации рисков. Процесс управления рисками информационной безопасности (ИБ) объекта критической информационной инфраструктуры (КИИ) в первую очередь включает следующие процедуры: идентификация рисков ИБ объекта КИИ; оценка рисков ИБ объекта КИИ; митигацию рисков ИБ объекта КИИ.

Работы по идентификации и оценке рисков ИБ объекта КИИ должны проводиться с учетом требований к процессам управления рисками ИБ объекта КИИ. Риски ИБ объекта КИИ должны быть идентифицированы. Основой идентификации рисков является идентификация и анализ возможных последствий нарушения защищаемых свойств информации объекта КИИ.

С целью идентификации рисков ИБ объекта КИИ, необходимо идентифицировать следующие элементы риска ИБ, представленные на рис. 1.

Рисунок 1 – Идентификация элементов риска ИБ объекта КИИ

Для идентификации последствий реализации угрозы безопасности информации (УБИ) используется метод «дерево событий». Данный метод позволяет проследить последовательность отдельных возможных инцидентов, как правило, неисправностей или каких-либо отказов.

Пример дерева событий представлен на рис. 2.

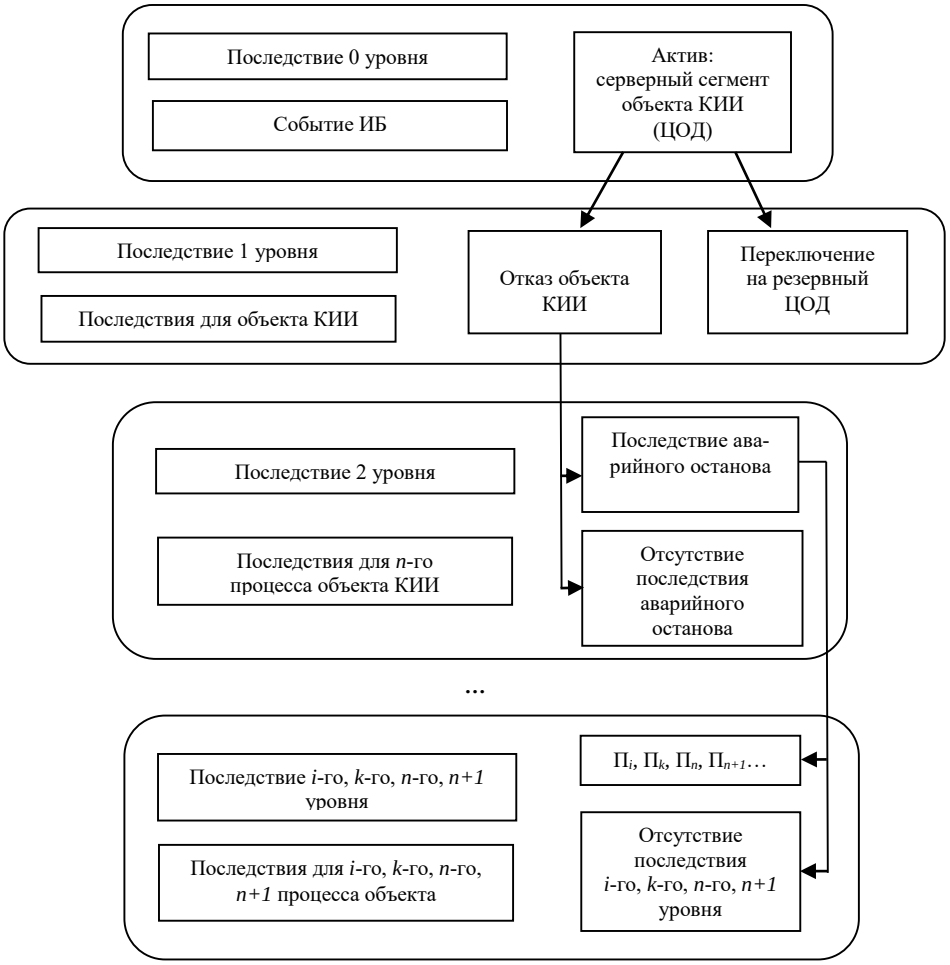

Рисунок 2 – Дерево событий объекта КИИ

В качестве нарушения критериев ИБ объекта КИИ рассматриваются нарушения следующих свойств информации, обрабатываемой в объекте КИИ: конфиденциальность, целостность, доступность информации. Это будет являться корнем дерева событий.

В ходе построения данного дерева, ветви выбираются таким образом, чтобы совокупность последствий некоторого вида результирующих событий представляла совокупность множества возможных исходов события, соответствующих *i*-му, *k*-му, *n*-му, *n+1* уровню, появление одного из событий в таком случае исключает появление других – несовместные события. Их совместная реализация невозможна, то есть может произойти только одного некоторое событие, либо иное, следовательно, исходя из теоремы сложения вероятностей, которая применима к любому числу несовместных событий [1, с. 41], вытекает следующее следствие, если последствия A_1, A_2, …, A_{n+1} соответствующего уровня образуют полную группу несовместных событий, то сумма их вероятностей равна единице. [1, с. 42]

$$\sum_{i=1}^{n+1} p_{i,k,n,n+1}\,(A_{i,k,n,n+1}) = 1 \qquad (1)$$

где $p_{i,k,n,n+1}(A_{i,k,n,n+1})$ – вероятность *i, j, k, n, n+1* последствия события на соответствующем *i, j, k, n, n+1* уровне.

На дереве событий может быть отражено более *n* уровней последствий. В случае реализации УБИ объекта КИИ это может привести к лавинообразному развитию событий.

Как правило, реализация УБИ объекта КИИ является причиной возникновения нарушения безопасности информации объекта КИИ. Также это связано с отсутствием мер, предотвращающих возможные последствия.

Пусть $E_{Zi,j,k,n,n+1}$ эффективность защитной меры. Меры направлены на снижение вероятности совокупности множества возможных исходов события.

В каждом конкретном случае необходимо целесообразно идентифицировать УБИ объекта КИИ, а также уязвимостей, соответствующих *n*-ой УБИ.

Идентификация угроз и уязвимостей, вызывающих нарушение ИБ осуществляется в рамках моделирования УБИ в соответствии с требованиями по обеспечению безопасности информации объекта КИИ [2, 3] как правило с использованием [4].

Такого типа соответствие *n*-й УБИ далее будет использоваться при сочетании *n*-го последствия УБИ в рамках идентификации рисков ИБ. Чаще всего используется экспертный метод, который бывает взаимно противоречив.

Поэтому выразим риск ИБ объекта КИИ конкретной формулой:

$$\text{Р} = \text{Р}\{\text{П}_{i,k,n,n+1}\} \text{ в результате реализации } \{\text{УБИ}_{i,k,n,n+1}\} \qquad (2)$$

где Р – риск ИБ;

$\text{Р}\{\text{П}_{i,k,n,n+1}\}$ – риск последствия для компонента объекта КИИ или для ин-

формационной системы объекта КИИ, или для *n*-го процесса объекта КИИ в результате реализации УБИ;

УБИ$_{i,k,n,n+1}$ – соответствующая УБИ.

В таком случае, в зависимости от целей оценки рисков ИБ объекта КИИ осуществляется идентификация суммарных рисков ИБ объекта КИИ. Агрегирование рисков ИБ объекта КИИ может выполняться и по последствиям реализации УБИ объекта, и по УБИ объекта КИИ. Агрегирование выражается формулой 2, при этом рассматривается риск реализации УБИ для компонента объекта КИИ или информационной системы объекта КИИ, или для *n*-го процесса объекта КИИ в результате реализации УБИ.

Аналитическим аппаратом для принятия решений также является и вероятностный метод.

В качестве последствий реализации определенной группы УБИ объекта КИИ выбираются наихудшие последствия реализации УБИ на каждом уровне последствий. Тогда U_{E1}, U_{E2}, …, $U_{E(n+1)}$ оценка ущерба, вызванного последствием A_1, A_2, …, A_{n+1}, с учетом защитной меры $E_{i,j,k,n,n+1}$ и U_1, U_2, …, U_{n+1} оценка ущерба, вызванного последствием A_1, A_2, …, A_{n+1}, без учета защитной меры.

Следовательно, эффективность внедрения защитной меры определим следующим образом как отношение U_{E1}, U_{E2}, …, $U_{E(n+1)}$ оценки ущерба, вызванного последствием A_1, A_2, …, A_{n+1}, с учетном защитной меры $E_{i,j,k,n,n+1}$ к U_1, U_2, …, U_{n+1} оценка ущерба, вызванного тем же последствием, без учета защитной меры.

$$1 - \frac{U_{Ei,j,k,n,n+1}}{U_{i,j,k,n,n+1}} = E_{Zi,j,k,n,n+1} \quad (3)$$

где $E_{Zi,j,k,n,n+1}$ – эффективность защитной меры относительно последствия A_1, A_2, …, A_{n+1};

$\frac{U_{Ei,j,k,n,n+1}}{U_{i,j,k,n,n+1}}$ – отношение U_{E1}, U_{E2}, …, $U_{E(n+1)}$ оценки ущерба, вызванного последствием A_1, A_2, …, A_{n+1}, с учетном защитной меры $E_{i,j,k,n,n+1}$ к U_1, U_2, …, U_{n+1} оценка ущерба, вызванного тем же последствием, без учета защитной меры.

Оценка ущерба – величина, равная максимальному ущербу от реализации УБИ, входящих в соответствующую группу УБИ. Значит вероятность последствий будет вычисляться как произведение вероятности [1, с. 45] возникновения ущерба на вероятность возникновения последствий соответствующего уровня.

$$\prod_i^{n+1} p_{i,k,n,n+1} = P(A_{i,k,n,n+1}) \quad (4)$$

Для проведения суммирования рисков необходимо выяснить разницу между приемлемым и неприемлемым рисками, для этого впоследствии необходимо оценить ущерб от единичной ситуации реализации УБИ или групп УБИ. В качестве последствий реализации УБИ рассматриваем наихудшие.

Следовательно, вероятность последствий соответствующего уровня для заданной УБИ будет определяться следующим образом (формула 5).

$$P_{Ai,k,n,n+1}(I_{i,k,n,n+1}) \prod_i^{n+1} p_{i,k,n,n+1} = P_{Ii,k,n,n+1}(A_{i,k,n,n+1}) \quad (5)$$

где $P_{Ii,k,n,n+1}(A_{i,k,n,n+1})$ – вероятность последствий соответствующего *i*-го, *k*-го, *n*-го, *n+1* уровня для заданной УБИ;

$P_{Ai,k,n,n+1}(I_{i,k,n,n+1})$ – вероятность заданного *i*-го, *k*-го, *n*-го, *n+1* уровня для соответствующей $I_{i,k,n,n+1}$ УБИ.

Далее для суммирования введем последствие, связанное с нарушением функций компонентов информационной системы объекта КИИ.

Суммирование проводим по УБИ, содержащимся в Банке данных угроз безопасности информации, сформированном ФСТЭК России и Государственным научно-исследовательским испытательным институтом проблем технической защиты информации ФСТЭК России [4] и признании данных УБИ актуальными относительно объекта КИИ. Для суммирования рекомендуется сформировать соответствующую группу УБИ, связанную с множеством возможных исходов событий. Данная группа УБИ может быть связана с несанкционированным управлением синхронизацией и состоянием, и с несанкционированным управлением указателями или иными признаками. Вероятность реализации УБИ вычисляется с учетом защитных мер относительно конкретного объекта КИИ.

Это рекомендуется проводить таким образом для снижения вероятности риска ИБ на определенное время. Вычисления рекомендуется проводить, используя экспертный и вероятностный аппарат относительно конкретной системы объекта КИИ для принятия соответствующего решения.

В результате выполненных действий, получена оценка рисков ИБ объекта КИИ, которая трактуется как вероятность возникновения максимального ущерба в результате реализации соответствующей группы УБИ. Таким образом, идентифицированные агрегированные риски ИБ объекта КИИ впоследствии формируются в единый реестр рисков ИБ объекта КИИ.

Список литературы

1. Вентцель Е.С. Теория вероятностей. – М.: Издательство «Наука», 1969. – 576 с.

2. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

3. Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

4. Банк данных угроз безопасности информации, сформированный ФСТЭК России и Государственным научно-исследовательским испытательным институтом проблем технической защиты информации ФСТЭК России

(https://bdu.fstec.ru/).

5. Шабуров А.С., Зонова В.Э., Модель реализации требований по защите информации объектов критической информационной инфраструктуры // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления = Perm National Research Polytechnic University Bulletin. Electrotechnics, Information Technologies, Controlsystems. - 2019. - № 32- с. 130-147., ВАК

6. Шабуров А.С., Зонова В.Э., Рыжук Н.С. Защита критической информационной инфраструктуры в соответствии с требованиями по обеспечению безопасности информации // Материалы X Международной интернет-конференции молодых ученых, аспирантов, студентов. – 2019. – с. 397–403.

Сведения об авторах

Исаева Виктория Эдуардовна – магистрант Пермского национального исследовательского политехнического университета, Пермь, email: us277@mail.ru

Шабуров Андрей Сергеевич – кандидат технических наук, доцент кафедры «Автоматика и телемеханика», Пермский национальный исследовательский политехнический университет, Пермь, email: shans@at.pstu.ru

About the authors

Isaeva Viktoriya Eduardovna – Student of Perm National Research Polytechnic University, Perm, email: us277@mail.ru

Shaburov Andrey Sergeevich – Ph.D. in Technical Sciences, Associate Professor, the Department of Automation and Telemechanics, Perm National Research Polytechnic University, Perm, email: shans@at.pstu.ru