УДК 681.3.067

ОБОСНОВАНИЕ ПЕРИОДА ПЕРЕСМОТРА МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ

В. Ю. Осипов[a], *доктор техн. наук, профессор*
И. А. Носаль[a], *аспирант*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, Санкт-Петербург, РФ*

Цель: *поиск гибких подходов, позволяющих в зависимости от сложившейся ситуации оперативно находить целесообразный период пересмотра мероприятий по защите информации.* ***Методы:*** *для расчета вероятностей нахождения процесса защиты информации в интересующих состояниях при альтернативных значениях периода пересмотра мероприятий использован математический аппарат марковских процессов. При поиске этого периода учитывается структура процесса, неоднократность получения доступа к защищаемым информационным ресурсам, возможности его блокирования, интегральные по времени потери, ценность информации, ее устаревание, другие факторы.* ***Результаты:*** *предложена система типовых моделей и алгоритм поиска целесообразного периода пересмотра мероприятий по защите информации, ориентированные на широкий круг условий, отражающих объективные закономерности реальных процессов. Приведены результаты моделирования и сформулированы практические рекомендации по управлению защитой информации.* ***Практическая значимость:*** *показано, что за счет гибкой оптимизации процессов защиты информации с учетом изменения текущих целей и условий их достижения можно существенно повысить информационную безопасность, снизить возможные потери. При управлении защитой информации рекомендуется придерживаться предложенного алгоритма действий, предусматривающего использование разработанной системы типовых моделей.*

Ключевые слова *— защита информации, модель, алгоритм, период, мероприятия.*

Введение

Одной из актуальных задач в области информационной безопасности (ИБ) выступает поиск целесообразного периода пересмотра мероприятий (ППМ) по защите информации. От успешности ее решения во многом зависят как расходы на обеспечение ИБ, так и потери от нарушения этой безопасности. Слишком частый пересмотр мероприятий по защите информации влечет дополнительные временные и материальные расходы. При редких пересмотрах этих мероприятий велики риски нарушения ИБ и потерь ценности защищаемых информационных ресурсов.

В настоящее время при определении ППМ по защите информации специалисты руководствуются международными и отечественными стандартами [1—6], требованиями государственных регуляторов и рекомендациями производителей средств защиты. По большей части эти требования основываются на предыдущем опыте и субъективном мнении экспертов.

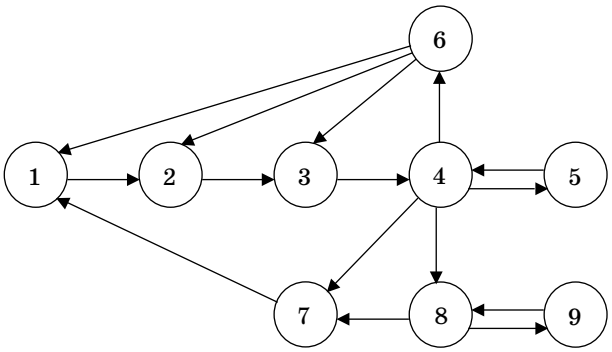
Известны также математические методы решения этой задачи [7—14]. Однако в этих работах не учитывается ряд особенностей, свойственных реальным процессам обеспечения ИБ, в том числе связанных с многократностью проводимых мероприятий, с изменением внешних и внутренних условий, целей защиты информации. В каждом конкретном случае необходимо рассматривать свои модели ИБ. Не во всех случаях при поиске целесообразного ППМ защиты можно обойтись одним и тем же основным показателем эффективности. Условия его расчета также могут существенно отличаться.

Необходимо выработать гибкие подходы, позволяющие оперативно в зависимости от сложившейся ситуации находить целесообразный ППМ по защите информации.

В качестве решения предлагаются система моделей и алгоритм поиска такого периода, ориентированные на широкий круг условий, отражающих объективные закономерности реальных процессов обеспечения ИБ.

Задача обоснования мероприятий информационной безопасности

Известны данные об анализируемом процессе обеспечения ИБ на некотором объекте. К таким данным могут относиться возможные угрозы ИБ; цели и задачи, решаемые объектом и подсистемой защиты информации; текущая ценность защищаемых ресурсов; структура процесса; исходное состояние; некоторые параметры переходов из одного состояния в другое; затраты на реализацию мероприятий защиты. В интересах обеспечения ИБ на объекте периодически должны пересматриваться мероприятия по защите информации. В самых простых случаях в качестве таких мероприятий могут выступать смена паролей доступа лиц к ценным информационным ресурсам; замена карточек доступа (в том числе банковских карточек), специальных электронных ключей. Пример структуры простого процесса обеспечения ИБ по получению доступа к защищенным информационным ресурсам (ЗИР) в одном из уч-



■ ***Рис. 1***. Пример структуры процесса обеспечения информационной безопасности

реждений приведен на рис. 1, где *1* — начальное состояние (проверка соответствия лиц приказу по доступу к ЗИР); *2*, *3* — достоверные авторизационные данные выработаны и загружены, соответственно, в систему; *4* — карточки доступа с достоверными данными выданы пользователям; *5* — получен санкционированный доступ к ЗИР; *6* — сообщение об ошибке доступа направлено администратору безопасности; *7* — состояние необходимости пересмотра мероприятий по защите информации; *8* — несанкционированные пользователи ознакомлены с авторизационными данными; *9* — получен несанкционированный доступ (НСД) к ЗИР.

Опираясь на предельную теорему теории вероятностей для потоков событий, рассматривая этот процесс как марковский, дугам графа на рис. 1 можно поставить в соответствие интенсивности переходов из состояния в состояние. Согласно этому графу, чем меньше процесс находится в состоянии *9*, тем выше уровень ИБ. Варьирование уровнем безопасности в соответствии с рисунком возможно путем изменения параметров переходов из состояния *4* в состояния *7*, *8*, а также из состояния *8* в состояние *7*. Однако заметим, что увеличение времени перехода из *4* в *8*, как правило, связано с заменой применяемых мер защиты. Период же пересмотра мероприятий по защите информации зависит от времени перехода из *4* и *8* в *7*. При этом уменьшение времени перехода из *4* в *7* приводит к снижению вероятности нахождения процесса в состоянии *5* (получение санкционированного доступа), причем на изменение параметров этих переходов требуются также затраты ресурсов.

Общими как для приведенной структуры, так и для других структур процесса обеспечения ИБ являются противоречия между уровнем защищенности и доступности информационных ресурсов; уровнем защищенности и затратами на обеспечение ИБ; затратами на обеспечение ИБ и возможными информационными ущербами со стороны несанкционированных пользователей и др.

В зависимости от преследуемых целей обеспечения ИБ и условий-ограничений, свойственных реальным системам, могут представлять интерес различные по математическим формулировкам задачи поиска целесообразного ППМ по защите информации.

С учетом этих факторов необходимо разработать систему моделей и алгоритм поиска такого периода, ориентированные на широкий круг условий, отражающих объективные закономерности реальных процессов обеспечения ИБ.

Модели информационной безопасности

Принимая во внимание особенности анализируемого процесса, поиск целесообразного ППМ по защите информации предлагается осуществлять в рамках оптимизационных моделей.

Модель 1. В случаях, когда требуется найти такой период Δt_o, при котором на интервале времени T достигается минимум интегральных потерь $S_o(\Delta t_o, T)$, рекомендуется решать задачу следующим образом:

$$S_0(\Delta t_0, T) = \min_{k \in Q} \int_0^T L_k(\Delta t_k, t)\mathrm{d}t; \qquad (1)$$

$$L_k(\Delta t_k, t) = B_k(\Delta t_k, t) + V(t) \cdot P_{k\_\text{í}}(\Delta t_k, t); \qquad (2)$$

$$P_{k\_\tilde{n}}(\Delta t_k, T) \geq P_{\text{ç}}; \qquad (3)$$

$$P_{k\_\text{í}}(\Delta t_k, T) \leq P_{\text{âî ï}}, \qquad (4)$$

$$k = 1, 2, \ldots, K.$$

В модели (1)—(4) приняты обозначения: Q — область допустимых ППМ по защите информации; $L_k(\Delta t_k, t)$ — суммарные потери при k-м значении периода Δt_k пересмотра мероприятий на момент времени t; $B_k(\Delta t_k, t)$ — суммарные затраты на защиту информации при k-м значении периода; $V(t)$ — ценность защищаемых информационных ресурсов; K — число возможных значений ППМ по защите информации; $P_{k\_\text{с}}(\Delta t_k, T)$, $P_{k\_\text{н}}(\Delta t_k, T)$ — вероятности санкционированного и несанкционированного доступа к ЗИР при k-м значении ППМ защиты на момент T; $P_\text{з}$ — заданная нижняя граница вероятности санкционированного доступа; $P_\text{доп}$ — допустимое значение для вероятности НСД.

Суммарные затраты на защиту информации и ценность ЗИР в (2) могут выражаться в виде функций от времени как

$$B_k(\Delta t_k, t) = b_{0k} + at / \Delta t_k; \qquad (5)$$

$$V(t) = V_0 \cdot \exp(-\gamma t), \qquad (6)$$

где a, γ, V_0 — константы; b_{0k} — суммарные затраты на $t=0$, в частном случае они могут не зависеть от Δt_k.

В результате вместо (2) имеем

$$L_k(\Delta t_k, t) = b_{0k} + at / \Delta t_k + \\ + V_0 \cdot \exp(-\gamma t) \cdot P_{k\_\text{í}}(\Delta t_k, t). \quad (7)$$

Из (5) следует, что чем меньше Δt_k, тем больше затраты. Выражение (6) отражает эффект устаревания информации во времени без учета НСД. Величину V_0 можно определить с использованием известного подхода [14]. В частном случае она равна минимуму затрат на восстановление утраченной информации, если нет других последствий.

Особенность этой модели в том, что она учитывает как затраты на реализацию мероприятий по защите информации, так и возможный информационный ущерб от нарушения ИБ. Кроме этого, интеграция возможных потерь осуществляется по времени.

Модель 2. Когда интерес представляет минимум суммарных потерь на конкретный момент времени T, при ограничениях на вероятность НСД и на время блокирования доступа в чрезвычайных ситуациях поиск Δt_o можно осуществлять с использованием следующей модели:

$$L_o(\Delta t_o,\ T) = \min_{k \in Q} L_k(\Delta t_k,\ T); \quad (8)$$

$$P_{k\_\text{í}}(\Delta t_k,\ T) \le P_{\text{äîï}}; \quad (9)$$

$$T_{k\_\text{á}} \le T_{\text{äîï}}, \quad (10)$$

$$k = 1, 2, ..., K.$$

Здесь $T_{k\_\text{á}}$ — время блокирования доступа при k-м ППМ защиты (в качестве его применительно к структуре процесса на рис. 1 может выступать время перехода из состояния *8* в состояние *7*); $T_{\text{доп}}$ — допустимое время блокирования доступа. Другие обозначения такие же, как и в (1)—(4). Заметим, что при решении задачи (8)—(10) в частных случаях можно ограничиться только потерями в виде возможного информационного ущерба [второе слагаемое в правой части выражения (2)].

Модель 3. В ситуации, когда требуется найти Δt_o, исходя из максимума оставшейся ценности защищаемой информации на конкретный момент времени T при ограниченных суммарных затратах на ее защиту, с учетом (5), (6) применима модель

$$V_{\text{opt}}(\Delta t_o,\ T) = \\ = \max_{k \in Q}(V_0 \cdot \exp(-\gamma T)(1 - P_{k\_\text{í}}(\Delta t_k,\ T)); \quad (11)$$

$$B_k(\Delta t_k, T) = b_{0k} + aT / \Delta t_k \le B_\text{ç}. \quad (12)$$

Модель 4. Когда предоставляется возможность иметь интегральные потери, не превышающие допустимых $S_{\text{доп}}$, а наибольший интерес представляет минимизация вероятности НСД, для определения Δt_o предлагается использовать модель

$$P_{o\_\text{í}}(\Delta t_o,\ T) = \min_{k \in Q} P_{k\_\text{í}}(\Delta t_k,\ T); \quad (13)$$

$$\int_0^T L_k(\Delta t_k,\ t)\mathrm{d}t \le S_{\text{äîï}}, \quad (14)$$

$$k = 1, 2, ..., K.$$

Специфика модели (13), (14) состоит в расчете основного показателя и в проверке условия (14). Причем основу интегральных потерь в ней составляют, прежде всего, суммарные затраты на защиту информации [первое слагаемое в выражении (2)]. Что касается второго слагаемого в $L_k(\Delta t_k, t)$, то при минимизации вероятности НСД к ЗИР одновременно минимизируются возможные потери ценности этих ресурсов.

Модель 5. В ситуации, когда трудно определить суммарные или частные потери, связанные с защитой информации, для поиска Δt_o можно использовать модель

$$\Delta t_o = \max_{k \in Q} \Delta t_k; \quad (15)$$

$$P_{k\_\text{í}}(\Delta t_k,\ T) \le P_{\text{äîï}}, \quad (16)$$

$$k = 1, 2, ..., K.$$

В соответствии с (15), (16) ищется наибольший ППМ по защите информации, при котором вероятность НСД на момент T не превышает допустимого значения $P_{\text{доп}}$. В этой модели максимизация ППМ в какой-то мере равносильна минимизации текущих расходов на защиту информации.

Кроме приведенных моделей, возможны также и другие варианты, учитывающие при поиске целесообразного ППМ по защите информации ограничения на время восстановления доступа, на длительность однократного доступа и другие, от которых зависят вероятности санкционированного и несанкционированного доступа к ЗИР. Системообразующим ядром всех этих оптимизационных моделей выступает модель процесса ИБ в виде графа состояний.

В интересах обеспечения ИБ с использованием этих оптимизационных моделей рассмотрим обобщенный алгоритм действий.

Алгоритм

Этот алгоритм можно представить в виде следующей последовательности шагов.

1. Анализ текущей ситуации с защитой информации на объекте.

2. Уточнение или пересмотр целей защиты информации и условий их достижения на качественном уровне.

3. Выбор в соответствии с этими целями и условиями адекватной оптимизационной модели ИБ из имеемого конечного множества. В нашем случае это пять моделей (1)—(16).

4. При необходимости — уточнение или разработка новой марковской модели процесса ИБ в виде графа состояний.

5. Определение текущих параметров переходов процесса из одних состояний в другие.

6. Задание начальных и интересующих состояний процесса.

7. Генерация альтернативных значений ППМ защиты или параметров отдельных переходов, от которых они зависят.

8. Расчет вероятностей нахождения процесса в интересующих состояниях при альтернативных значениях ППМ защиты и определение значений других показателей эффективности процесса, входящих в выбранную оптимизационную модель.

9. Проверка выполнимости условий, связанных с этими вероятностями и другими показателями, зависящими от значений ППМ защиты.

10. Поиск экстремума основного показателя эффективности (целевой функции), удовлетворяющего всем условиям задачи.

11. Принятие в качестве целесообразного периода того значения, при котором достигнут экстремум целевой функции.

12. Практический пересмотр параметров защиты информации в соответствии с этим периодом.

13. Если отсутствует необходимость защиты информации, то завершение процесса.

14. Если есть необходимость защиты информации и ситуация с ИБ изменилась, то переход к шагу 1.

В соответствии с этим алгоритмом выбор конкретной оптимизационной модели следует осуществлять, исходя из наибольшего соответствия ее реальной ситуации с учетом возможностей и неопределенностей.

При необходимости уточнения или разработки новой марковской модели процесса ИБ в виде графа состояний следует исходить из целесообразного уровня формализации. Излишняя детализация влечет за собой повышение затрат на разработку модели процесса и определение ее параметров. Грубая формализация позволяет оперативно получать интересующие оценки, однако не обеспечивает необходимой точности результатов.

Определение текущих параметров (интенсивностей) переходов процесса из одних состояний в другие осуществимо путем сбора и обработки статистических данных. В ряде случаев, когда известны начальные и конечные состояния процесса на некотором интервале времени, определить исходные интенсивности можно также путем подбора параметров с использованием метода наименьших квадратов.

Для расчета вероятностей нахождения процесса в интересующих состояниях при альтернативных значениях ППМ защиты в соответствии с построенным графом составляется система дифференциальных уравнений. Затем она разрешается относительно заданных начальных и интересующих состояний. Для этого применимы пакеты прикладных программ MatLab, MathCad и др.

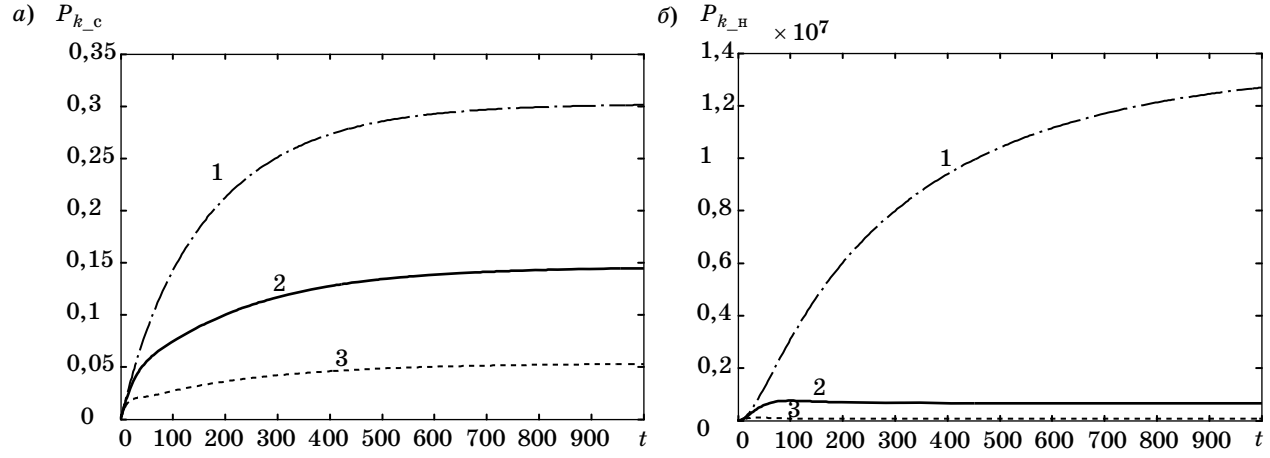
Расчет показателей $L_k(\Delta t_k, t)$, $S_k(\Delta t_k, T)$ в зависимости от этих вероятностей производится по формулам (1), (2).

Результаты моделирования

В целях раскрытия особенностей развития процесса ИБ при различных ППМ защиты осуществлялось математическое моделирование. В качестве структуры процесса в виде графа состояний использовалась модель, представленная на рис. 1. Особенность этой модели в том, что она учитывает многократность санкционированного и несанкционированного доступа к защищаемым информационным ресурсам, возможность пересмотра мероприятий защиты, а также блокирования доступа в случаях нарушения ИБ. Основные интенсивности переходов были определены исходя из средних временных затрат, при стандартном (не экстренном) предоставлении доступа к ЗИР.

Обосновывался целесообразный ППМ защиты в соответствии с моделью (1)—(4).

Результаты моделирования представлены на рис. 2, *а*, *б* и 3, *а*, *б*. На рис. 2 отражены зависимости вероятностей санкционированного $P_{k\_с}(\Delta t_k, t)$ и несанкционированного $P_{k\_н}(\Delta t_k, t)$ доступа к ЗИР от времени для трех различных значений ППМ защиты, которым соответствуют различные интенсивности переходов процесса на рис. 1 из состояния *4* в *7*: кривая *1* получена при $\lambda_{47}=0{,}0022$; кривая *2* — при $\lambda_{47}=0{,}022$; кривая *3* — при $\lambda_{47}=0{,}088$. Напомним, что санкционированному доступу на рис. 1 соответствует состояние *5*, а НСД — состояние *9*. Для результатов, приведенных на рис. 2, процесс на момент $t=0$ находился только в состоянии *4*. Из анализа этих результатов видно, что с увеличением ППМ защиты (с уменьшением соответствующей интенсивности) растет не только вероятность санкционированного доступа $P_{k\_с}(\Delta t_k, t)$, но и вероятность НСД $P_{k\_н}(\Delta t_k, t)$. При этом суммарные потери $L_k(\Delta t_k, t)$ согласно (2) с учетом (5), (6) изменяются по-разному (рис. 3, *а*).

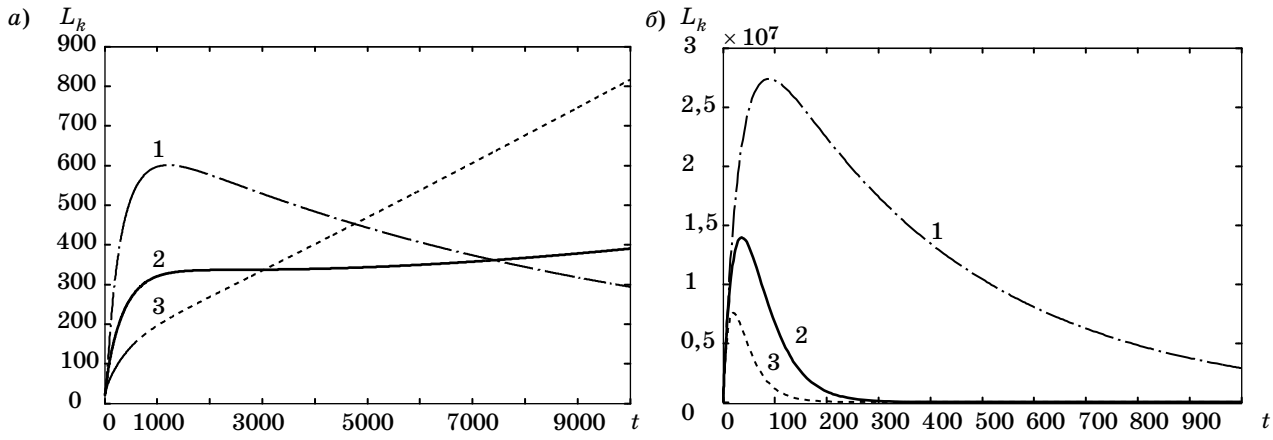


■ ***Рис. 2.*** Зависимость вероятности санкционированного (*а*) и несанкционированного (*б*) доступа от времени для различных значений ППМ защиты

Когда λ_{47}=0,0022 (кривая *1*), суммарные потери $L_k(\Delta t_k, t)$ сначала резко растут из-за редкого пересмотра мероприятий защиты, однако затем они снижаются. Это снижение обусловлено устаревание защищаемой информации. При λ_{47}=0,022 (кривая *2*) потери на интервале от 0 до 1000 условных временных единиц также резко растут, как и в первом случае. Однако этот прирост почти в 2 раза меньше. Затем, в отличие от первого случая, несмотря на устаревание защищаемой информации, из-за суммарных затрат $B_k(\Delta t_k, t)$ на защиту информации потери увеличиваются, но незначительно. В случае λ_{47}=0,088 (кривая *3*) из-за частых пересмотров мероприятий защиты потери быстро растут на всем интервале времени. Анализируя рис. 3, *а*, трудно сказать о приоритетности всех ППМ. Однако осуществив интегрирование полученных зависимостей по времени, мы получаем однозначный ответ. Целесообразным является период Δt_o=1/0,022, при котором получена кривая *2*. За ним следует период, равный 1/0,0022, свойственный кривой *1*, и только затем период 1/0,088 (для кривой *3*). При целесообразном периоде Δt_o=1/0,022 интегральные потери (1) в 1,29 и в 1,34 раза ниже, чем при Δt_k=1/0,0022 и Δt_k=1/0,088 соответственно.

Для других случаев, например, когда процесс на t=0 находится в состояниях *4* и *8* с вероятностями, равными 0,5, ситуация с суммарными потерями $L_k(\Delta t_k, t)$ несколько иная. Основной вклад в них вносят потери ценности информации из-за НСД. Причем на величину этих потерь существенное влияние оказывает время блокирования доступа при обнаружении нарушений. Это время перехода процесса на рис. 1 из состояния *8* в состояние *7*. На рис. 3, *б* приведены зависимости $L_k(\Delta t_k, t)$ для интенсивностей λ_{87}=(0,0025; 0,025; 0,075) — кривые *1*, *2*, *3* соответственно.

Из анализа этих кривых видно, что имеет место резкий всплеск потерь из-за утраты авторизационных данных. При этом чем быстрее происхо-



■ ***Рис. 3.*** Зависимость суммарных потерь от времени для различных значений: *а* — ППМ защиты при нахождении процесса на t=0 в четвертом состоянии с вероятностью $P_4(0)$=1; *б* — параметров блокирования доступа при $P_4(0)$=0,5 и $P_8(0)$=0,5

дит блокирование доступа, тем ниже суммарные потери $L_k(\Delta t_k, t)$.

С учетом полученных результатов можно сформулировать следующие практические рекомендации по повышению эффективности защиты информации:

— целесообразно на объектах с ценной информацией иметь и оперативно использовать оптимизационные модели ИБ;

— при управлении защитой информации предлагается придерживаться предложенного алгоритма действий;

— при определении целесообразных ППМ защиты необходимо правильно определять цели и условия их достижения;

— рекомендуется при обосновании мероприятий по защите информации учитывать интегральные потери на интересующем интервале времени;

— следует непрерывно накапливать и обрабатывать статистические данные, свойственные процессам ИБ, прогнозировать возможные события.

Заключение

В результате выполненного исследования для поиска целесообразных ППМ по защите информации предложена новая система из пяти оптимизационных моделей. Системообразующим ядром ее выступает марковская модель процесса, учитывающая неоднократность доступа к информационным ресурсам, возможности его блокирования, пересмотра мероприятий защиты. Предложенная система оптимизационных моделей позволяет расширить взгляды на оценку потерь и достижение различных целей, связанных с защитой информации. Разработан алгоритм поиска целесообразного ППМ по защите информации, который включен в алгоритм действий лиц при обеспечении ИБ.

Предложенные решения могут найти применение при обосновании мероприятий по защите ценной информации как в процессе эксплуатации систем ИБ, так и при их проектировании.

Литература

1. **Payment** Card Industry Data Security Standard (PCI DSS) – PCI Security Standards Council LLC, Version 2.0. Oct. 2010. 75 p. https://www.pcisecuritystandards.org/documents. (дата обращения: 01.07.2013).
2. **Information** Security Forum. Standard of Good Practice 2007 (ISF «SoGP») – Information Security Forum Limited (01.05.2007). http://www.securityforum.org. (дата обращения: 12.05.2013).
3. **Aceituno V.** Information security management maturity model (ISM3) v2.10/Stansfeld E. – ISM3 Consortium, 2007. http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf (дата обращения: 18.12.2013).
4. **ГОСТ** Р ИСО/МЭК 13335-1–2006. Информационная технология. Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий. Введ. 01.06.2007. – М.: Стандартинформ, 2006. – 23 с.
5. **ГОСТ** Р ИСО/МЭК 27001–2006. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования. Взамен ГОСТ Р ИСО/МЭК 17799–2005; введ. 27.12.2006. – М.: Стандартинформ, 2008. – 26 с.
6. **Стандарт** Банка России СТО БР ИББС-1.0-2010. Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения. Взамен СТО БР ИББСС-1.0–2008; введ. 21.06.2010/ЦСБ РФ. – М., 2010. – 42 с.
7. **Brotby K.** Information security governance. A Practical Development and Implementation Approach. – Hoboken: John Wiley & Sons, Inc., 2009. – 220 p.
8. **Hentea M.** Intelligent System for Information Security Management: Architecture and Design Issues // Issues in Informing Science and Information Technology. 2007. Vol. 4. P. 29–43.
9. **Андреев О. О.** и др. Критически важные объекты и кибертерроризм. Часть 1. Системный подход к организации противодействия/ под ред. В. А. Васенина. – М.: МЦНМО, 2008. – 398 с.
10. **Грибунин В. Г., Чудовский В. В.** Комплексная система защиты информации на предприятии. – М.: Академия, 2009. – 416 с.
11. **Миронов В. В., Носаль И. А.** Моделирование и оценка системы обеспечения информационной безопасности на примере ГОУ ВПО «СыктГУ» // Информация и безопасность. 2011. № 2. С. 209–211.
12. **Осипов В. Ю.** Оценка защищенности информационно-вычислительных ресурсов от несанкционированного доступа // Приборы и системы управления. 1996. № 7. С. 16–19.
13. **Осипов В. Ю., Емелин В. И.** Оптимальное управление информационной безопасностью социально-технических систем// Вопросы защиты информации. 2009. № 3(86). С. 64–67.
14. **Осипов В. Ю., Носаль И. А.** Обоснование мероприятий информационной безопасности // Информационно-управляющие системы. 2013. № 2(63). С. 48–53.

UDC 681.3.067

Substantiation of the Period of Revision of Information Security Measures

Osipov V. Yu.[a], Dr. Sc. Tech., Professor, Leading Research Fellow, osipov_vasiliy@mail.ru
Nosal I. A.[a], Post-Graduate Student, ironia.i@gmail.com
[a]Saint-Petersburg Institute for Informatics and Automation of RAS, 39, 14th Line, 199178, Saint-Petersburg, Russian Federation

Purpose: To find flexible approaches providing prompt identification of an expedient period of revision of information security measures depending on a current situation. **Methods:** The mathematical apparatus of Markov processes has been used to estimate possibilities of finding information security actions. Searching this period a process structure, multiplicity of receiving access to protected information resources, possibilities of its blocking, integrated time losses, information value, its obsolescence, and other factors are considered. **Results:** There has been proposed a system of typical models and an algorithm for identification of an expedient period of revision of information security measures which are targeted at a large range of conditions reflecting objective rules of real processes. The results of modeling have been given and practical recommendations on management of information security have been formulated. **Practical relevance:** It has been shown that due to flexible optimization of information security processes with account of change of current goals and conditions of their achievement one can increase significantly information security and reduce possible losses. Managing information security it is recommended to follow the proposed algorithm of actions which implies the use of the developed system of typical models.

Keywords — Information Security, Model, Algorithm, Period, Actions.

References

1. *Payment Card Industry Data Security Standard (PCI DSS) – PCI Security Standards Council LLC, Version 2.0*. October 2010. 75 p. Available at: https://www.pcisecuritystandards.org/documents (accessed 1 July 2013).
2. *Information Security Forum. Standard of Good Practice 2007 (ISF "SoGP") – Information Security Forum Limited (01.05.2007)*. Available at: http://www.securityforum.org (accessed 12 May 2013).
3. Aceituno V. *Information Security Management Maturity Model (ISM3) v2.10*. Stansfeld E., ISM3 Consortium, 2007. 96 p. Available at: http://www.lean.org/FuseTalk/Forum/Attachments/ISM3_v2.00-HandBook.pdf (accessed 18 December 2013).
4. State Standard R ISO/MEK 13335-1–2006. Information Technology. Methods and Means of Ensuring of Safety. Concept and Models of Management of Safety of Information and Telecommunication Technologies. Moscow, Standartinform Publ., 2006. 23 p. (In Russian).
5. State Standard R ISO/MEK 27001–2006. Information Technology. Methods and Means of Ensuring of Safety. Systems of Management of Information Security. Requirements. Moscow, Standartinform Publ., 2008. 26 p. (In Russian).
6. Standard of Bank of Russia IBBS-1.0-2010. Ensuring Information Security of the Organizations of a Banking System of the Russian Federation. General Provisions. Moscow, CSB RF Publ., 2010. 42 p. (In Russian).
7. Brotby K. *Information Security Governance: A Practical Development and Implementation Approach*. Hoboken, John Wiley & Sons, Inc., 2009. 220 p.
8. Hentea M. Intelligent System for Information Security Management: Architecture and Design Issues. *Issues in Informing Science and Information Technology*, 2007, vol. 4, pp. 29–43.
9. Andreev O. O., Batov I. S., Bolshakov M. V., Vasenin V. A., Shapchenko K. A., Klimovsky A. A., Markelov K. K., Puchkov F. M., Savkin V. B., Kazarin O. V. *Kriticheski vazhnye ob»ekty i kiberterrorizm. Sistemnyi podkhod k organizatsii protivodeistviia* [Crucial Objects and Cyberterrorism. System Approach to the Counteraction Organization]. Ed. V. A. Vasenin, Moscow, MTsNMO Publ., 2008. 398 p. (In Russian).
10. Gribunin V. G., Chudovsky V. V. *Kompleksnaia sistema zashchity informatsii na predpriiatii* [Complex System of Information Security at the Enterprise]. Moscow, Akademiia Publ., 2009. 416 p. (In Russian).
11. Mironov V. V., Nosal I. A. Modeling and an Assessment of System of Ensuring Information Security. *Informatsiia i bezopasnost'*, 2011, no. 2, pp. 209–211 (In Russian).
12. Osipov V. Yu. Assessment of Security of Information Resources from Unauthorized Access. *Pribory i sistemy upravleniia*, 1996, no. 7, pp. 16–19 (In Russian).
13. Osipov V. Yu., Emelin V. I. Optimum Control of Information Security of Social and Technical Systems. *Voprosy zashchity informatsii*, 2009, no. 3, pp. 64–67 (In Russian).
14. Osipov V. Yu., Nosal I. A. Substantiation of Information Security Measures. *Informatsionno-upravlyayushhie sistemy*, 2013, no. 2, pp. 48–53 (In Russian).