МФЮА
Московский
финансово-юридический
университет

Международная научно-практическая конференция
18 апреля 2017

Современные проблемы и задачи обеспечения информационной безопасности СИБ – 2017

СБОРНИК СТАТЕЙ

Москва
2017

МОСКОВСКИЙ ФИНАНСОВО-ЮРИДИЧЕСКИЙ УНИВЕРСИТЕТ МФЮА

Современные проблемы и задачи обеспечения информационной безопасности

СИБ – 2017

Международная научно-практическая конференция
(г. Москва, 18 апреля 2017 г.)

Сборник статей

Москва МФЮА 2017

УДК 004
ББК 32
С 56

С 56 **Современные проблемы и задачи обеспечения информационной безопасности СИБ – 2017: Международная научно-практическая конференция (г. Москва, 18 апреля 2017 г.) [Текст] : сборник статей / Московский финансово-юридический университет МФЮА. – М. : МФЮА, 2017. – 200 с.**

ISBN 978-5-94811-232-9

Сборник составлени по материалам Международной научно-практической конференции «Современные проблемы и задачи обеспечения информационной безопасности СИБ – 2017» и содержит статьи, подготовленные преподавателями, аспирантами, соискателями и студентами вузов, а также опытными специалистами, работающими в сфере информационной безопасности.

УДК 004
ББК 32

ISBN 978-5-94811-232-9

Содержание

Раздел I. Технологии обеспечения информационной безопасности

Раздел II. Программные и аппаратные средства защиты информации

Раздел III. Перспективные направления обеспечения информационной безопасности

Contents

Section I. The technology of information security

УДК 004.056

РАСЧЕТ ТРУДОЗАТРАТ СОТРУДНИКОВ, ОБЕСПЕЧИВАЮЩИХ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ ОРГАНИЗАЦИИ

С.Б. Вепрев
доктор технических наук, профессор
Московская академия Следственного комитета
E-mail: veprevsb@yandex.ru

С.А. Нестерович
кандидат технических наук
Московская академия Следственного комитета
E-mail: sirial_2005@mail.ru

Аннотация. В статье рассматриваются вопросы определения трудозатрат, необходимых для реализации задач в области организации системы информационной безопасности. На основе формализации качественных параметров предлагаются правила оценки трудозатрат для принятия решения о количественном и качественном составе сотрудников системы защиты информации.

Ключевые слова: информационная безопасность, организация, количество сотрудников, общие трудозатраты, трудозатраты сотрудников, серверы безопасности, доменная архитектура.

CALCULATION OF LABOR COSTS OF EMPLOYEES ENSURING THE INFORMATION SECURITY ORGANIZATION

S.B. Veprev, S.A. Nesterovich

Abstract. The article deals with the definition of labor necessary for the implementation of the organization's information security problems. On the basis of the formalization of quality parameters include labor assessment rules for decision-making on quantitative and qualitative composition of the staff of information security systems.

Keywords: information security, organization, number of employees, total labor costs, labor costs of employees, security servers, domain architecture.

Одной из важных задач создания системы защиты информации является задача обеспечения функционирования её технических, программных и информационных средств. В связи с этим перед руководством организации возникают следующие вопросы:

- какое количество сотрудников отдела информационной безопасности необходимо для охвата всех проблем информационной безопасности;
- какой квалификацией должны обладать сотрудники информационной безопасности.

В небольших учреждениях за организацию бесперебойной работы, администрирование рабочих мест и обеспечение информационной безопасности, как правило, отвечает один человек. В более крупных учреждениях к работам по обеспечению безопасности привлекаются уже несколько человек, причем часто полномочия по задачам обеспечения функционирования системы и обеспечения безопасности могут разделяться, соответственно, между информационным отделом и отделом безопасности. В крупных банках и компаниях за информационную безопасность отвечают специальные отделы.

Основополагающими документами, на основе которых строится политика информационной безопасности, являются:

- Федеральный Закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных», устанавливающий основные принципы и условия обработки персональных данных; права, обязанности и ответственность участников отношений, связанных с обработкой персональных данных;
- «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных», утверждённая заместителем директора ФСТЭК России 15 февраля 2008 г.;
- «О требованиях к защите информации в платежной системе Банка России», Положение от 24 августа 2016 г. № 552-П [4].

На основании данных документов строится концепция безопасности организации и определяются мероприятия по обеспечению безопасности информации на перспективу и на ближайший календарный год.

Основной проблемой в решении данного вопроса является расчет трудозатрат для проведения всех мероприятий. Исходя из полученных результатов можно рассчитать как количество необходимых сотрудников, так и их среднюю нагрузку.

Следует отметить, что на анализируемые данные оказывают влияние многие параметры. Это факторы, связанные с составом и структурой системы, степенью её технической оснащённости, использованием соответствующих программных продуктов, степенью решения проблем информационной безопасности на конкретных объектах системы в целом и т.д.

Так, например, при анализе данных следует различать использование централизованной сети с использованием домена и одноранговое использование отдельных вычислительных машин. В случае использовании домена на основе ActiveDirectory имеется возможность администрирования всех компьютеров сети с помощью средств удалённого администрирования, вследствие чего уменьшается время на обслуживание компьютерной сети учреждения. К данному вопросу можно отнести обновление антивирусных баз, обновление операционной системы в случае нарушении безопасности, санкционирование доступа к персональному компьютеру, фильтрация трафика от сайтов с нежелательным вредоносным кодом, проверка парольной политики и так далее. При использовании доменной сети, имеются возможности одновременной настройки всех элементов сети на основе политик безопасности.

В случае же использования отдельных вычислительных машин количество требуемых сотрудников безопасности многократно увеличивается в силу необходимости настройки оборудования и соответственно его проверки на рабочем месте пользователя; изменяются и требования к квалификации персонала.

За основу методики расчета численности сотрудников информационной безопасности можно взять базовую формулу расчета количества сотрудников N предприятия [7]:

$$N = \frac{T_0}{Z_н} K_н \qquad (1)$$

где:

N – расчётная численность сотрудников предприятия;

T_0 – общие трудозатраты (полезное рабочее время) на объём работы в днях или часах;

$Z_н$ – предполагаемый нормативный фонд рабочего времени, требуемого на одного сотрудника в организации;
$K_н$ – коэффициент, учитывающий возможные невыходы сотрудника.

Общие трудозатраты T_0 получаются суммированием всех трудозатрат на нормированные и ненормированные работы (операции), а также внеплановые задания и работы, связанные с непредвиденными ситуациями. Используемые в организациях нормы труда содержат нормативы времени и выработки каждого сотрудника. Расчет трудозатрат на работы по основной и дополнительной деятельности выражается в рабочих днях или часах.

Предполагаемый нормативный фонд $Z_н$ рабочего времени, требуемого на одного сотрудника в организации, определяется нормативными документами организации. В качестве $Z_н$ обычно в расчетах используется 2000 часов или 250 рабочих дней.

Коэффициент $К_н$, учитывает отпуск сотрудника, возможные невыходы по причине болезни или в силу других обстоятельств. Обычно в качестве упрощения принимается доля невыхода на работу в качестве 10 % от общего количества трудовых дней, то есть, как правило, значение $К_н$ берётся равным 1,1.

Очевидно, что самой сложной является задача расчета трудозатрат.

Для определения общих трудозатрат работников отдела безопасности необходимо охватить весь круг обязанностей сотрудников отдела безопасности и вычислить необходимое время выполнения работ, связав их с компетентностью сотрудника.

Рассмотрим и соотнесем средние трудозатраты сотрудников информационно-технологического отдела на обслуживание АРМ (автоматизированных рабочих мест) в одноранговой и доменной системах (табл. 1).

Таблица 1

Нагрузка на сотрудника безопасности при использовании отдельных автоматизированных рабочих мест [6]

	Наименование работ	*Время на работы (в часах за год)*
1	Разработка частной модели угроз	2
2	Установка систем безопасности (включая установку спецсредств, плат безопасности)	3
3	Составление паспорта безопасности рабочего места	3
4	Установка антивирусных средств	2
5	Составление перечня защищаемых помещений и технический паспорт защищаемого помещения	5
6	Разграничение прав доступа к информационным ресурсам	2
7	Резервное копирование данных(с учетом записи на съёмные носители и сдача в архив)	20
8	Ведения журнала учета съемных носителей информации	1

	Наименование работ	*Время на работы (в часах за год)*
9	Ведение журнала учета криптографических средств информации	1
10	Ведение журнала учета средств криптографической защиты информации	1
11	Восстановление работоспособности технических средств	1
12	Внесение в список сотрудников, допущенных к работе с персональными данными	1
13	Составление актов о уничтожении персональных данных и уничтожение данных	1
14	Составление плана мероприятии и включение данного АРМ в список мероприятии по защите информации	1
15	Внесение в план поверок и составление перечня проверяемых субъектов на данном АРМ	1
16	Установка обновлении систем безопасности	4
18	Внесение сотрудника в матрицу доступа к сведениям конфиденциального характера, и сверка имеющихся ресурсов	4
19	Проведение проверок рабочих мест	5
	Итого (в часах на одно рабочее место)	*58*

Данные приведены при использовании отдельных компьютеров, без использования отдельных серверов безопасности, из расчета 2000 рабочих часов в год. Сотрудник отдела безопасности в состоянии поддерживать в корректной работе 2000 / 58 = 34 компьютера с учетом того, что все работы проводятся в строго отведённое время (хотя в реальной жизни время проведения работ часто точно не учитывается в сторону переработки). С учетом замещающего сотрудника безопасности на случай отпуска и других непредвиденных ситуаций в организации их должно быть не менее двух человек. Если организация ввела доменную систему, то возможности сотрудника безопасности значительно возрастают (табл. 2).

При использовании доменной архитектуры затрачивается время на настройку сервера (около 200 часов в год и около 31 часов на рабочее место). С учетом приведённых данных можно рассчитать парк компьютеров: (2000 – 200) / 31 = 58. Таким образом, при наличии одного сервера данных сотрудник отдела безопасности может содержать уже парк компьютеров в количестве 58 штук. Данная возможность достигается за счёт того, что при использовании домена можно автоматизировать рутинные операции, такие как резервное копирование данных, обновление систем безопасности, настройка рабочих мест.

Таблица 2

Нагрузка на сотрудника безопасности при использовании домена

	Наименование работ	*Время в часах за год*	*Примечание*
1	Разработка частной модели угроз	2	
2	Установка систем безопасности	3	
3	Составление паспорта безопасности рабочего места	3	
4	Установка антивирусных средств	0	Централизованно
5	Составление перечня защищаемых помещений и технический паспорт защищаемого помещения	5	
6	Разграничение прав доступа к информационным ресурсам	0,5	Централизованно
7	Резервное копирование данных (с учетом записи на съемные носители и сдача в архив)	1	Централизованно
8	Ведения журнала учета съемных носителей информации	1	
9	Ведение журнала учета криптографических средств информации	1	
10	Ведение журнала учета средств криптографической защиты информации	1	
11	Восстановление работоспособности технических средств	1	
12	Внесение в список сотрудников, допущенных к работе с персональными данными	1	
13	Составление актов о уничтожении персональных данных и уничтожение данных	1	
14	Составление плана мероприятий и включение данного АРМ в список мероприятий по защите информации	1	
15	Внесение в план поверок и составление перечня проверяемых субъектов на данном АРМ	1	
16	Установка обновлении систем безопасности	0	Централизованно
18	Внесение сотрудника в матрицу доступа к сведениям конфиденциального характера, и сверка имеющихся ресурсов	4	
19	Проведение проверок рабочих мест	5	
	Итого	*31*	В часах на одно рабочее место

Например, если учесть, что организация использует парк из 150 рабочих мест, подключенных в домен 3 сервера и около 50 компьютеров, работающих отдельно, то общие трудозатраты будут: 150 x 31 + 50 x 58 + 3 x 200 = 4650 + 2900 + 600= 8150 часов.

Общее число сотрудников вычисляется по формуле (1). Подставив в исходную формулу значение N = (8150 / 2000) x 1,1, получим примерную нагрузку на сотрудника информационной безопасности, равную 4,48 человека.

Еще одним моментом, который может влиять на расчет трудозатрат, является компетентность сотрудников. Приведенные выше расчеты основываются на знаниях и умении среднестатистического сотрудника. Особенность тематики информационной безопасности заключается в возможной минимизации штата сотрудников за счет привлечения более компетентных специалистов. Все знают примеры случаев, когда один компьютерный гуру заменял целый коллектив сотрудников. Но, следует отметить, что каких-либо формальных критериев на этот счет вообще не имеется. Предлагается следующий подход к определению компетентности сотрудника:

- оценка степени доверия к сотруднику – A;
- оценка общей компетентности – B;
- опыт работы в данной области – C.

Каждая из трех оценок является дополнительным коэффициентом к расчетному значению трудозатрат, определяемых в соответствии с табл. 1 или табл. 2.

Работа с документами, имеющими определённый гриф, а также с соответствующими техническими средствами и носителями информации требует дополнительных затрат. Поэтому знания, умения и соответствующий допуск к данным тоже имеет очень важное значение. Оценка степени доверия (A) к сотруднику в государственных организациях легко реализуема через наличие той или иной степени допуска. Например, допуск к документам ДСП оценивается как 0,5 балла, допуск к секретным документам оценивается в 1 балл, допуск к совершенно секретным документам – в 2 балла. В коммерческих организациях данная оценка может производиться на основе уровня допуска к конфиденциальной информации.

Оценка общей компетентности (B) производится при соотнесении имеющихся у сотрудника навыков с перечнем работ, перечисленных в приводимых выше таблицах. Работа оценивается по трехбалльной шкале: 0,5 балла – имеет представление; 1,0 – имеет навык; 2,0 – владеет в совершенстве.

Опыт работы в данной области (C) можно оценивать по стажу общей работы в данной области вообще и на конкретной должности – в частности, предлагается табл. 3.

Из таблицы выбирается наибольшее число, которое и является коэффициентом. Обобщённая формула будет выглядеть следующим образом:

$$N = \frac{T_O}{Z_H ABC} K_H \qquad (2)$$

Проведенные расчеты позволяют сделать только самые первые приблизительные оценки для принятия решения о количественном и качественном составе сотрудников системы защиты информации. Отметим, что решения о выделении средств на защиту информации в государственных учреждениях принимается директивно, а в коммерческих – исходя из оценки возможных

Таблица 3

Опыт работы сотрудника информационной безопасности

	Опыт работы				*Итого*
	Отсутствует	*От одного до двух лет*	*От двух до пяти лет*	*Свыше пяти лет*	
В данной области	1	1,33	1,5	1,67	
В конкретной должности	1	1,5	1,67	2	

финансовых и связанных с ними рисков. И то и другое носит субъективный характер, что во многом определяет экономическую составляющую информационной безопасности.

Литература

1. Трудовой кодекс Российской Федерации от 30 декабря 2001 г. № 197-ФЗ (ред. от 3 июля 2016 г., с изм. и доп., вступ. в силу с 1 января 2017 г.) // Собрание законодательства РФ. 2002. № 1 (ч. 1). Ст. 3.
2. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утв. Заместителем директора ФСТЭК России 14 февраля 2008 г. // СПС КонсультантПлюс. URL: http://www.consultant.ru (дата обращения: 20.02.2016).
3. Методический документ «Меры защиты информации в государственных информационных системах». Утв. ФСТЭК России 11 февраля 2014 г. // СПС КонсультантПлюс. URL: http://www.consultant.ru (дата обращения: 20.02.2016).
4. Положение от 24 августа 2016 г. № 552-П «О требованиях к защите информации в платежной системе Банка России» // СПС КонсультантПлюс. URL: http://www.consultant.ru (дата обращения: 20.02.2016).
5. Требования к защите персональных данных при их обработке в информационных системах персональных данных. Утв. постановлением Правительства РФ от 1 ноября 2012 г., № 1119 // СПС КонсультантПлюс. URL: http://www.consultant.ru (дата обращения: 20.02.2016).
6. *Петренко С., Симонов С., Кислов Р.* Информационная безопасность: экономические аспекты // JetInfoOnline. 2003. № 10.
7. *Шевчук Н.С.* Управление персоналом организации: учебно-методическое пособие. Томск, 2014.

УДК 004.42

КОГНИТИВНЫЕ ИСКАЖЕНИЯ КАК УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И МЕТОДЫ ИХ ПАРИРОВАНИЯ

А.А. Кононов
кандидат технических наук
Институт системного анализа РАН Федерального исследовательского центра «Информатика и управление» Российской академии наук
E-mail: kononov@isa.ru

Аннотация. Показана опасность, которую представляют собой когнитивные искажения, порождаемые систематическими недостатками информирования о существующих проблемах в обеспечении безопасности. По сути они обуславливают ту причину большинства чрезвычайных ситуаций, аварий и техногенных катастроф, которую принято называть «человеческим фактором». Предложено рассматривать когнитивные искажения, как угрозы информационной безопасности. Рассматриваются методы критериального моделирования как способ парирования этих угроз.

Ключевые слова: когнитивные искажения, угрозы информационной безопасности, критически важные объекты, критические инфраструктуры, человеческий фактор, критериальное моделирование.

COGNITIVE BIASES AS INFORMATION SECURITY THREATS AND METHODS OF THEM MITIGATION

A.A. Kononov

Abstract. The danger presented by cognitive biases, generated by systematic shortcomings in informing about existing security problems, is shown. As a matter of fact, they cause that reason of the majority of extreme situations, failures and technogenic accidents which it is accepted to name «the human factor». It is proposed to consider cognitive biases as threats to information security. Criterial modeling methods are considered as a way to mitigate these threats.

Keywords: cognitive biases, threats to information security, critical facilities, critical infrastructures, the human factor, criterial modeling..

Когнитивные искажения в оценках рисков объективно существующих опасностей и уязвимостей являются одной из основных причин техногенных аварий и катастроф, а иногда и тяжелых последствий стихийных бедствий [5]. Особенно актуально это для больших систем критически важных объектв (КВО) и критических инфраструктур (КИ), где проблемы когнитивных искажений, возникающие как на исполнительском, так и на управленческом уровнях, представляют особую опаснсть. Это