УДК 004.78:655.1

И.В. Левыкин, А.И. Хорошевский

Харьковский национальный университет радиоэлектроники, Украина

ФАКТОРЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ УДАЛЁННОЙ ИЗДАТЕЛЬСКОЙ СИСТЕМЫ

В статье производится анализ факторов, повышающих безопасность информационных удалённых издательских систем (ИУИС), при помощи метода анализа иерархий, метода обработки экспертной информации и метода одномерного шкалирования. Анализ производится в два этапа. На первом этапе производится обработка множества факторов повышения безопасности ИУИС с помощью метода анализа иерархий. На втором этапе осуществляется процесс определения приоритетности среди наиболее важных факторов и формируется вектор приоритетности факторов. Анализ позволяет сделать обоснованный выбор применяемых действий по повышению защищённости ИУИС от несанкционированного доступа.

Ключевые слова: *htaccess, SSH-доступ, SSL сертификат, USB-токен, выделенный IP адрес, информационная удалённая издательская система, метод анализа иерархий, метод обработки экспертной информации, метод одномерного шкалирования.*

Введение

Постановка проблемы. Информационные удалённые издательские системы (ИУИС) позволяют автоматизировать приём заказов на полиграфическом предприятии по средствам глобальной сети интернет. При этом в системе хранится конфиденциальная информация о клиентах и их заказах. Например, фамилия, имя, отчество, контактные данные, история заказов продукции с датами отгрузки, суммами к оплате, периодичности заказов, номера кредитных карт и даже макеты самих заказов.

WEB сайт является элементом ИУИС, который находится на сервере и к которому можно получить доступ с любой точки мира. Следовательно, ИУИС подвержена всем рискам, которым подвержен любой веб-проект.

Конфиденциальность данных клиентов для любой фирмы является важной задачей и полиграфические предприятия не являются исключением. В условиях повышенной конкуренции следует прикладывать максимум усилий для того, чтобы получить доверие клиентов и постоянно поддерживать его на высоком уровне.

Потеря доверия клиентов вследствие утечки их персональных данных может привести к катастрофическим последствиям. Всемирно известная компания COMODO понесла большие убытки в результате компрометации их серверов со стороны злоумышленников [1]. Компания DigiNotar после подобного инцидента была вынуждена объявить о банкротстве [2]. Это яркие примеры того, как кража конфиденциальных данных компании может привести к негативным последствиям для бизнеса самой компании и её клиентов.

Некоторые зарубежные полиграфические предприятия используют систему в качестве основного способа привлечения клиентов и совершения сделок. В связи с этим остановка или замедление работы ИУИС влечёт за собой прямые финансовые убытки для предприятия. Также стоит отметить тот факт, что восстановление системы после атаки может занять длительный период и потребовать привлечения дополнительных средств для устранения сложившейся ситуации. Для полиграфических предприятий это означает полное прекращение поступления дохода от продаж продукции в интернете и подрыв авторитетности предприятия. При условии того, что ИУИС является основным средством сбыта продукции, её остановка может повлечь серьёзное снижение прибыли предприятия.

Анализ последних исследований и публикаций. Авторы [3 – 10] выявили ряд факторов, влияющих на безопасность информационных систем. Однако не все из них возможно применить к информационным удалённым издательским системам. Так, например, требовать применения системы аутентификации веб-ресурсов [18] для всех пользователей ИУИС, включая клиентов, не целесообразно. Так как у клиента может не оказаться USB-токена. В результате чего он не сможет стать клиентом полиграфической фирмы. Применение SSL сертификатов шифрования доступно не для всех ИУИС, так как требует от сервера определённых программных возможностей. Безусловно, применение всех известных средств повышения безопасности веб-ресурса повысит сохранность пользовательских данных, снизит риск вывода ИУИС из строя и минимизирует вероятность потери доверия со стороны клиента.

Несмотря на это необходимо выбрать только те факторы повышения безопасности ИУИС, которые будут соответствовать возможностям и потребно-

стям каждого конкретного предприятия. При условии того, что эти факторы будут давать максимальный эффект с минимальными затратами и сохранением функциональности и удобства пользования ИУИС со стороны клиентов и работников полиграфического предприятия.

Таким образом, остаётся открытым вопрос важности того или иного фактора повышения безопасности ИУИС, простоты его реализации в условиях ограниченных программно-аппаратных средств и сохранения удобства использования системы.

Решение данного вопроса требует дальнейшей проработки в рамках модельной реализации на основе использования экономико-математического инструментария.

Целью данной статьи является исследование сущности, определение важности и простоты практической реализации факторов, влияющих на повышение безопасности информационных удалённых издательских систем.

Новизна данного исследования состоит в определении наиболее важных факторов, влияющих на повышение безопасности ИУИС (от несанкционированного доступа, вывода системы из строя, нарушения её нормального функционирования), и выявления приоритетности (по простоте) их практической реализации.

Исследование базируется на использовании такого экономико-математического инструментария как метод анализа иерархий (для определения важности факторов влияния), метода обработки экспертной информации на основе использования метода одномерного шкалирования (для выявления и определения приоритетности факторов влияния) [19].

Изложение основного материала

На основании работ авторов [3 – 10] был сформирован следующий перечень факторов, влияющих на безопасность веб-ресурсов его можно применить и для ИУИС, так как она, как правило, разрабатывается на базе системы управления содержимым.

1. *Надёжный хостинг с хорошей технической поддержкой*. ИУИС находится на сервере, где есть своё программное обеспечение, которое также подвержено атакам со стороны злоумышленников (хакеров). Виртуальный хостинг – не лучшее место для размещения ИУИС, так как вместе с вашей системой на сервере находится множество других веб-проектов. Нарушив работоспособность одного из них, можно нарушить работоспособность всех. Обеспечение надлежащей безопасности ИУИС на виртуальном хостинге будет очень сложной или нерешаемой задачей. Поэтому лучше размещать ИУИС на отдельном сервере или на виртуальном выделенном сервере.

2. *Резервное копирование данных*. В случае несанкционированного доступа к ИУИС, выведения её из работоспособности резервные копии позволят за минимальное время восстановить нормальное функционирование системы.

3. *Ограничение права доступа к файлам и директориям пользователям*. Разрешив минимально необходимый доступ к файлам и директориям для пользователей, можно минимизировать вероятность несанкционированной подмены, модификации или удаления важных файлов ИУИС.

4. *Настройки сервера при помощи .htaccess файла для повышения безопасности сайта*. Повысить безопасность ИУИС на уровне сервера можно при помощи применения специальных настроек, размещаемых в файле .htaccess.

5. *Использование выделенного IP адреса сайта*. Это позволяет увеличить скорость доступа к сайту, положительно скажется на позициях выдачи вашего сайта в поисковых системах и повысит защищённость ИУИС от веб-проектов, размещённых на одном и том же сервере, даже в случае виртуального хостинга. Также это даст возможность применения SSL-сертификатов и повысит защищённость от DDoS-атак.

6. *Вынесение файлов конфигурации системы управления содержимым за пределы директории public_html*. В подобных файлах хранится критически важная для ИУИС информация, например, логин и пароль доступа к базе данных ИУИС. Вынесение файла конфигурации за пределы директории public_html затруднит несанкционированный доступ к нему.

7. *Использование SSH-доступа к ИУИС*. Позволит повысить защиту соединения между компьютером сотрудника предприятия и сервером ИУИС.

8. *Использование SSL-сертификата*. Позволит шифровать соединения между всеми пользователями системы и самой ИУИС. Также возможно применение SSL-сертификата для повышения репутации ИУИС в интернете в глазах пользователей.

9. *Создание копии ИУИС на другом сервере*. Для минимизации рисков простоя ИУИС в результате выхода из строя сервера или всего дата-центра хостинга, рекомендуется создавать «зеркало» ИУИС на другом сервере и в другом дата-центре.

10. *Ведение логов*. Позволит анализировать события при успешном несанкционированном доступе к ИУИС и в дальнейшем устранить найденные проблемы в безопасности.

11. *Регулярное обновление системы управления содержимым и сторонних расширений до самых последних версий*. Если ИУИС базируется на системе управления содержимым совместно со сторонними расширениями, то их обновление позволит не только повысить стабильность и функциональность ИУИС, но и устранит найденные уязвимости без-

опасности.

12. *Изменение стандартного пути доступа к панели управления ИУИС.* Получив доступ к форме ввода логина и пароля для административной части ИУИС, злоумышленник может применить метод подбора паролей или выяснить название и версию системы управления содержимым, на которой базируется ИУИС. После чего он может применить известные скрипты для получения несанкционированного доступа к системе.

13. *Ограничение доступа по IP адресу к административной панели ИУИС, FTP и панели управления хостингом.* Рекомендуется ограничивать доступ ко всем критически важным областям системы для сотрудников предприятия по IP адресу. Это затруднит доступ к этим областям посторонних лиц.

14. *Удаление признаков, указывающих на базе какой системы управления содержимым создана ИУИС.* Определив название и версию системы управления содержимым, на которой базируется ИУИС, злоумышленник может применить известные скрипты для получения несанкционированного доступа к системе и выведения её из строя.

15. *Использование расширений для защиты ИУИС от SQL, PHP, LFI, XSS инъекций и DDoS-атак в режиме реального времени.* SQL, PHP, LFI и XSS атаки могут вывести ИУИС из строя и открыть доступ к конфиденциальным данным, хранящимся в системе.

16. *Использование безопасных паролей.* Это защитит ИУИС от средств подбора паролей. Так как подбор безопасного пароля может занять очень продолжительное время.

17. *Хранение паролей и других конфиденциальных данных в зашифрованном виде.* Даже если злоумышленнику удастся получить доступ к базе данных ИУИС, то при условии шифрования данных ему будет сложно воспользоваться полученной информацией.

18. *Использование токена для аутентификации в ИУИС.* Это минимизирует угрозу компрометации паролей доступа к важным областям ИУИС.

19. *Использование уникального префикса для таблиц баз данных ИУИС.* Данный фактор усложнит работу скриптов злоумышленников, ориентированных на работу с базой данных.

20. *Использование SEF ссылки.* Затрудняет анализ используемого программного обеспечения в ИУИС, повышает защищённость от SQL атак.

21. *Организация круглосуточной технической поддержки ИУИС.* Необходимо круглосуточное наблюдение за сайтом со стороны квалифицированного администратора. Это поможет своевременно предпринимать адекватные действия при обнаружении попыток несанкционированного доступа или нарушения работы ИУИС.

22. *Разграничение права доступа для пользователей и групп пользователей.* Необходимо чётко разграничить права доступа к различным модулям системы для различных пользователей с целью минимизации выполнения несанкционированных действий. Умышленно или по неосторожности.

23. *Организация оповещения администратора сайта на электронную почту и телефон о важных (с точки зрения безопасности) событиях ИУИС.* Своевременное автоматическое оповещение администратора сайта о попытках несанкционированного доступа к ИУИС позволит оперативно применить, например, блокировку атакующего IP адреса.

24. *Минимизация использования сторонних расширений (модулей).* Любое дополнительное расширение (модуль) несёт дополнительные риски, связанные с наличием в его коде уязвимостей.

25. *Использование капчи и систем автоматической фильтрации спама.* При помощи, например, массовой регистрации в системе, которая создаётся злоумышленником, можно нарушить работоспособность ИУИС.

26. *Обеспечение безопасности загружаемых пользователями файлов с и в ИУИС.* Необходимо обеспечить проверку загружаемых с и в ИУИС файлов на наличие двойного расширения или вредоносного программного обеспечения.

27. *Обеспечение информационной безопасности всех компьютеров, с которых производится доступ административной части ИУИС.* Защищённость компьютера, с которого сотрудники предприятия получают доступ к FTP, базе данных и административной зоне ИУИС, не влияет напрямую на безопасность самой ИУИС. Но некоторые вирусы нацелены специально на кражу паролей. Также злоумышленник может получить возможность удалённого управления Вашим компьютером.

28. *Регулярное проведение аудитов безопасности ИУИС.* Аудит безопасности позволит выявлять и устранять недочёты в безопасности ИУИС, тем самым минимизирует вероятность компрометации критических данных и нарушения работоспособности ИУИС.

В процессе исследования сущности факторов, влияющих на повышение безопасности ИУИС [3, 4, 5, 6, 7, 8, 9, 10], были выявлены присущие им сложности и недостатки, которые рационально, в дальнейшем, рассматривать как аналитико-теоретические данные (D_i, при $i = \overline{1, k}$), необходимые для проведения экспертного оценивания сложности реализации факторов. Рассмотрим основные из них.

Использование SSH-доступа к ИУИС. Сервер должен поддерживать данную возможность. Её использование требует определённых технических навыков, как при настройке сервера, так и при ис-

пользовании сотрудниками предприятия.

Использование SSL-сертификата. Сервер должен поддерживать данную возможность. Её использование требует определённых технических навыков при настройке сервера. Стоимость SSL-сертификата RapidSSL составляет 49 – 279$ [11] за один год использования. Стоимость SSL-сертификатов VeriSign составляет 399 – 1499$ [12] за один год использования.

Использование токена для аутентификации в ИУИС. Сложность настройки. Стоимость USB-токена составляет 690 рублей [13]. Сложность использования, связанная с необходимостью постоянного наличия у сотрудников предприятия USB-токена.

Ограничение доступа по IP адресу к административной панели ИУИС, FTP и панели управления хостингом. Использование выделенного IP адреса сайта. Стоимость одного выделенного IP адреса составляет 3$ в месяц [14].

Надёжный хостинг с хорошей технической поддержкой. Стоимость виртуального выделенного сервера базовой конфигурации с минимальной технической поддержкой 240 грн. в месяц [16]. Использование виртуального выделенного сервера требует наличия в штате (или внештатного) системного администратора высокой квалификации.

Настройки сервера при помощи .htaccess файла для повышения безопасности сайта. Требует наличия в штате (или внештатного) системного администратора.

Обеспечение безопасности загружаемых пользователями файлов с и в ИУИС. Требует специального серверного программного обеспечения.

Регулярное обновление системы управления содержимым и сторонних расширений до самых последних версий. Требует наличия в штате (или вне- штатного) системного администратора высокой квалификации и его круглосуточной работы. Так как обновление программного обеспечения необходимо производить в часы наименьшей нагрузки на сервер. Как правило, с двух до трёх ночи.

Хранение паролей и других конфиденциальных данных в зашифрованном виде. Сложность в настройке. Требует наличия в штате (или вне- штатного) системного администратора высокой квалификации.

Обеспечение безопасности загружаемых пользователями файлов с и в ИУИС. Требует наличия специализированного программного обеспечения. Необходим системный администратор высокой квалификации для его выбора, установки и настройки.

Использование SEF ссылки. Необходимо, чтобы все расширения (модули) поддерживали данную возможность. Она увеличивает нагрузку на сервер.

Изменение стандартного пути доступа к панели управления ИУИС. Использование уникального префикса для таблиц баз данных ИУИС. Требуется начальная конфигурация ИУИС и её базы данных.

Использование капчи и систем автоматической фильтрации спама, например, BotScout, Spamhaus. Это может затруднить регистрацию пользователей в ИУИС.

Использование расширений для защиты ИУИС от SQL, PHP, LFI, XSS инъекций и атак в режиме реального времени. Требует наличия специализированного программного обеспечения.

Регулярное проведение аудитов безопасности ИУИС. Стоимость качественного, глубокого анализа безопасности ИУИС может потребовать значительной суммы денег. Она зависит от сложности ИУИС.

Резервное копирование данных. Стоимость 1 гигабайта дискового пространства на сервере резервных копий в сутки может составлять от 0.02$ [15], при условии аренды, до 10 гигабайт дискового пространства.

Создание копии ИУИС на другом сервере. Стоимость создания работоспособной, актуальной копии ИУИС на другом сервере по времени и затратам соизмерима со стоимостью создания ИУИС (самой ИУИС как программного обеспечения).

Реализация остальных факторов, влияющих на повышение безопасности ИУИС, требует минимальных затрат и технической квалификации.

Общий вид процесса определения важности и сложности практической реализации факторов, влияющих на повышение безопасности ИУИС, предлагается представить в следующем виде (рис. 1).

На рис. 1 приняты следующие обозначения:

F_V – множество факторов, влияющих на повышение безопасности ИУИС, при $v = \overline{1, n}$;

F_{V1} – множество наиболее важных (значимых) факторов, при $v1 \in \overline{1, n}$;

S_{V1} – нормированный показатель простоты реализации факторов влияния;

R_{V1} – результирующий ранг каждого фактора.
Обозначение D_i

Этап 1 начинается с обработки множества факторов влияния F_V, при $v = \overline{1, 28}$, с помощью метода анализа иерархий. В результате обработки определяются весовые коэффициенты каждого из факторов влияния. Факторы, имеющие наименьшие значения весовых коэффициентов, отсекаются из дальнейшего рассмотрения как такие, что вносят малый вклад в процесс обеспечения безопасности ИУИС.

Рассмотрим реализацию данного этапа подробнее.

В табл. 1 приведены факторы, влияющие на повышение безопасности ИУИС, и соответствующие им весовые коэффициенты, которые дают возможность выбрать только наиболее значимые из анализируемых факторов.

Рис. 1. Общая схема обработки факторов влияния на повышение безопасности ИУИС

Таблица 1

Факторы влияния на повышение безопасности ИУИС

Фактор		Весовой коэффициент $\mu_i^u(F_i)$
обозначение	наименование	
f1	Использование SSL-сертификата	0,05
f2	Использование токена для аутентификации в ИУИС	0,05
f3	Использование SSH-доступ к ИУИС	0,003
f4	Ограничение доступа по IP адресу к административной панели ИУИС, FTP и панели управления хостингом	0,02
f5	Надёжный хостинг с хорошей технической поддержкой	0,1
f6	Хранение паролей и других конфиденциальных данных в зашифрованном виде	0,01
f7	Ограничение права доступа к файлам и директориям пользователям	0,05
f8	Минимизация использования сторонних расширений (модулей)	0,026
f9	Регулярное обновление системы управления содержимым и сторонних расширений до самых последних версий	0,1
f10	Настройки сервера при помощи htaccess файла для повышения безопасности сайта	0,03
f11	Обеспечение безопасности загружаемых пользователями файлов с и в ИУИС	0,003
f12	Использование расширений для защиты ИУИС от SQL, PHP, LFI, XSS инъекций и атак в режиме реального времени	0,046
f13	Удаление признаков, указывающих на базе каких систем управления содержимым создана ИУИС	0,02
f14	Использование SEF ссылки	0,05
f15	Изменение стандартного пути доступа к панели управления ИУИС	0,01
f16	Использование капчи и систем автоматической фильтрации спама	0,002
f17	Использование уникального префикса для таблиц баз данных ИУИС	0,002
f18	Регулярное проведение аудитов безопасности ИУИС	0,09
f19	Создание копии ИУИС на другом сервере	0,05
f20	Резервное копирование данных	0,05
f21	Использование безопасных паролей	0,05
f22	Использование выделенного IP адреса сайта	0,07
f23	Разграничение права доступа для пользователей и групп пользователей	0,01
f24	Ведение логов	0,003
f25	Вынесение файлов конфигурации системы управления содержимым за пределы директории public_html	0,002
f26	Организация круглосуточной технической поддержки ИУИС	0,05
f27	Обеспечение информационной безопасности всех компьютеров, с которых производится доступ к административной части ИУИС	0,05
f28	Организация оповещения администратора сайта на электронную почту и телефон о важных (с точки зрения безопасности) событиях ИУИС	0,003

Учитывая тот факт, что рынок программного обеспечения развивается очень быстро, перечень критериев может быть откорректирован и дополнен новыми данными, исходя из необходимости.

Для определения значимых факторов, которые будут участвовать в процессе ранжирования необходимо выполнить ***следующие шаги*:**

1) построить матрицу парных сравнений факторов $F = \|f_{ij}\|$ (при i, j = $\overline{1,n}$). В основу процедуры сравнения положен вопрос: «На сколько один фактор повышает безопасность ИУИС больше, чем другой?». На этот вопрос должны отвечать системные администраторы ИУИС предприятия, исходя из собственного опыта, мнений авторитетных экспертов и результата аудита безопасности. Процесс построения происходит следующим образом: строится матрица, в заголовках строк (i) и столбцов (j) расположены выбранные факторы, по диагонали проставляется значение «1», так как при сравнении каждый фактор сравнивается по значимости не только со всеми, но и с самим собой. Для определения числового значения степени важности попарно сравниваемых факторов используется шкала относительности (шкала степени значимости действий), предложенная Саати в [17, С. 53].

Таким образом, например, при сравнении фактора f5 (Надёжный хостинг с хорошей технической поддержкой) с фактором f7 (Ограничение права доступа к файлам и директориям пользователям) определяется, что фактор f5 в 2 раза более значим при повышении безопасности ИУИС, чем фактор f7, значимость которого составляет 0,25. Фрагмент матрицы расчётов приведён ниже:

$$F = \|f_{ij}\| = \begin{pmatrix} & f_1 & f_2 & f_3 & \dots & f_{28} \\ f_1 & 1 & 0.25 & 6 & \dots & 0.12 \\ f_2 & 4 & 1 & 3 & \dots & 4 \\ f_3 & 0.16 & 0.33 & 1 & \dots & 0.25 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ f_{28} & 8 & 0.25 & 4 & \dots & 1 \end{pmatrix}; \quad (1)$$

2) рассчитать элементы матрицы весовых коэффициентов (в соответствии с (2)):

$$\mu_i^u(F_i) = \frac{f_{ij}}{\sum_{i=1}^{n} f_{ij}}, \quad (2)$$

где $\mu_i^u(F_i)$ – значение весовых коэффициентов i-х факторов в пределах u-го диапазона, при $u \in \overline{0,1}$.

Далее, на основе вычисления по каждому F_i суммы вида $\sum_{j=1}^{n} \mu_i^u(F_i)$ определяются весовые коэффициенты факторов. Это даёт возможность сделать обоснованный выбор при сравнении нескольких факторов влияния на безопасность ИУИС между собой. Так, например, значение весового коэффициента критерия f1 составляет: $\mu_1^u(F_1) = 0{,}05$. Рассчитанные для каждого фактора весовые коэффициенты приведены выше (см. табл. 1).

Стоит отметить, что расчётная сумма всех весовых коэффициентов должна равняться «1»:

$$\sum_{i=1}^{n} \mu_i^u(F_i) = 1; \quad (3)$$

3) выявить наиболее важные (значимые) факторы, влияющие на безопасность ИУИС. Уместность включения факторов в процесс выбора предлагается определить, исходя из сформированного авторами [18, С. 305] вывода о том, что 90% от общей совокупности критериев (факторов) является абсолютно достаточным для дальнейшего рассмотрения, анализа и формирования соответствующих выводов. В данном исследовании это даёт возможность для формирования следующих соотношений:

а) факторы f4, f13, f6, f15, f23, f3, f11, f24, f28, f16, f17, f25 в сумме по значимости набрали меньше 10%. Следовательно, их можно исключить из процесса рассмотрения для ИУИС;

б) факторы f5, f9, f18, f22, f1, f2, f7, f14, f19, f20, f21, f26, f27, f12, f10, f8 в сумме набрали больше 90%. Их целесообразно применять для повышения безопасности ИУИС. Данный набор факторов и будет рассматриваться как элементный состав множества наиболее важных факторов F_{V1}: v1 = {f5, f9, f18, f22, f2, f7, f14, f19, f20, f21, f26, f27, f12, f10, f8}, которое подаётся на вход 2-го этапа исследования.

Этап 2 предназначен для осуществления процесса определения приоритетности (по простоте реализации факторов) среди наиболее важных из F_{V1}. В рамках данного этапа формируется вектор приоритетности факторов, влияющих на повышение безопасности ИУИС, элементами которого являются нормированный показатель простоты реализации факторов (S_{V1}) и их результирующий ранг (R_{V1}). Реализация данного этапа происходит на основе использования одного из методов обработки экспертной информации – метода одномерного шкалирования [19].

Рассмотрим реализацию данного этапа подробнее.

Для определения S_{V1} и их R_{V1}необходимо выполнить ***следующие шаги:***

1) в качестве входной информации рассматриваются факторы влияния F_{V1}. На основе полученной информации из информационной среды (то есть, аналитико-теоретических данных D_i) экспертной группой производится их ранжирование (по степени простоты реализации по шкале от 1 – очень легко до 16 – очень сложно), рассчитывается сумма рангов и средний ранг по каждому фактору. Результирующие

оценки (независимые мнения), предоставляемые экспертами, группируются в соответствующей таблице, фрагмент которой приведён ниже (табл. 2).

2) сформируем матрицу A размером 16 x 16, в которой указано число случаев, когда один фактор проще другого в реализации. Далее, трансформируем матрицу A (делением каждого элемента «10») в матрицу P, которая показывает вероятность предпочтения i-го фактора j-му. Фрагмент данной матрицы приведен ниже:

Таблица 2

Факторы безопасности ИУИС

№ эксперта	**Наиболее значимые факторы, F_{V1}**									
	f5	**f9**	**f18**	**f22**	**f1**	**f2**	**f7**	**f14**	**…**	**f8**
1	15	7	11	5	14	16	1	6	…	4
2	12	5	7	8	15	13	1	11	…	6
3	14	9	8	5	10	15	3	6	…	4
4	16	8	6	10	14	12	2	5	…	4
5	14	6	9	11	12	13	2	4	…	5
6	15	9	10	6	16	11	4	7	…	3
7	15	6	9	11	13	12	1	4	…	5
8	10	11	7	5	16	15	2	6	…	3
9	13	8	10	6	12	14	2	7	…	1
10	15	6	8	10	12	16	1	5	…	4
Сумма рангов	139	75	85	77	134	137	19	61	…	39
Средний ранг	13,9	7,5	8,5	7,7	13,4	13,7	1,9	6,1	…	3,9

$$P = \left\| p_{ij} \right\| = \begin{pmatrix} & f5 & f9 & f18 & f22 & f1 & ... & f8 \\ f5 & – & 0,1 & 0 & 0 & 0,3 & ... & 0 \\ f9 & 0,9 & – & 0,8 & 0,5 & 1 & ... & 0,1 \\ f18 & 1 & 0,2 & – & 0,5 & 1 & ... & 0 \\ f22 & 1 & 0,5 & 0,5 & – & 1 & ... & 0 \\ f1 & 0,7 & 0 & 0 & 0 & – & ... & 0 \\ ... & ... & ... & ... & ... & ... & ... & ... \\ f8 & 1 & 0,9 & 1 & 1 & 1 & ... & – \end{pmatrix}; \quad (4)$$

3) далее, воспользовавшись функцией Лапласса:

$$P_{ij} = G(Z_{ij}) = \int_{-\infty}^{z_{ij}} \frac{1}{\sqrt{2\pi}} e^{-t^2/2}\, dt = \frac{1}{\sqrt{2\pi}} \int_{0}^{z_{ij}} e^{-t^2/2}\, dt \quad (5)$$

вычисляем элементы матрицы $Z = (Z_{ij})$ (на основе известных p_{ij}), используя таблицы нормального распределения [20]. При этом, Z_{ij} является величиной, которая измеряется в единицах стандартного отклонения.

Учитывая, что $G(-Z_{ij}) = - G(Z_{ij})$, находим элементы матрицы $G(Z_{ij})$:

$$G(Z_{ij}) = \begin{pmatrix} & f5 & f9 & f18 & f22 & f1 & ... & f8 & Сумма\ оценок & Среднее \\ f5 & 0 & –1,28 & –3,9 & –3,9 & –0,52 & ... & –3,9 & –35,56 & –2,22 \\ f9 & 1,28 & 0 & 0,84 & 0 & 3,9 & ... & –1,28 & 5,51 & 0,34 \\ f18 & 3,9 & –0,84 & 0 & 0 & 3,9 & ... & –3,9 & 2,29 & 0,14 \\ f22 & 3,9 & 0 & 0 & 0 & 3,9 & ... & –3,9 & 4,74 & 0,30 \\ f1 & 0,52 & –3,9 & –3,9 & –3,9 & 0 & ... & –3,9 & –36,37 & –2,27 \\ ... & ... & ... & ... & ... & ... & ... & ... & ... & ... \\ f8 & 3,9 & 1,28 & 3,9 & 3,9 & 3,9 & ... & 0 & 35,1 & 2,19 \end{pmatrix}; \quad (6)$$

4) В результате дальнейшего применения метода (после расчета суммы оценок и их средних значений) в соответствии с вышеприведенной формулой (5) находим значение нормальной функции распределения (Ф*). Далее, делением каждого из Ф* на их сумму, находим значение нормированного показателя относительной простоты реализации каждого из факторов (S_{v1}) и производим их ранжировании (R_{V1}). Результат расчетов приведен в табл. 3.

5) Окончательным шагом в процессе применения метода является осуществление проверки на непротиворечивость, результаты которой приведены в табл. 4. В таблице сравниваются исходные (P_{ij}) и расчётные вероятности (Ф*), рассчитывается среднее отклонение по формуле (7), при k=120:

$$Sr(\Delta_{ij}) = \sum_{\substack{i,j=1 \\ i<j}}^{k} \left| \Delta_{ij} \right| / (k * (k-1)) / 2 . \quad (7)$$

Таблица 3

Относительная простота реализации факторов и их результирующий ранг

Факторы	Среднее значение оценок	Значение Ф*	S_{V1}	R_{V1}
f5	–2,22	0,0139	0,0017	9
f9	0,34	0,6331	0,0792	5
f18	0,14	0,5557	0,0695	8
f22	0,30	0,6179	0,0773	6
f1	–2,27	0,0107	0,0013	10
f2	–2,47	0,0062	0,0008	11
f7	3,05	0,9986	0,1249	**1**
f14	0,76	0,7764	0,0971	3
f19	–2,55	0,0062	0,0008	11
f20	2,88	0,9981	0,1249	**1**
f21	2,89	0,9981	0,1249	**1**
f26	0,29	0,6141	0,0768	7
f27	–2,55	0,0062	0,0008	11
f12	–1,19	0,1170	0,0146	8
f10	0,40	0,6554	0,0820	4
f8	2,19	0,9861	0,1234	**2**
	Сумма по Ф*:	7,9937		

Таблица 4

Оценочные разности расчётной и исходной относительной важности первопричин проблемы

По фактору	Разности средних значений оценок	Расчётное значение, Ф*	Исходное значение, P_{ij}	Отклонение, Δ_{ij}
f5	–2,5669	0,0047	0,1	-0,0953
	-2,3656	0,0082	0	0,0082
	-2,5188	0,0062	0	0,0062
	0,0506	0,5199	0,3	0,2199
	0,2519	0,5987	0,6	-0,0013
	…	…	…	…
f9	0,2013	0,5793	0,8	-0,2207
	0,0481	0,5160	0,5	0,0160
	2,6175	0,9953	1	-0,0047
	2,8188	0,9974	1	-0,0026
	-2,7088	0,0035	0	0,0035
	-0,4200	0,3372	0,1	**0,2372**
	2,8944	0,9981	1	-0,0019
	-2,5338	0,0062	0	0,0062
	-2,5481	0,0047	0	0,0047
…	…	…	…	…

Величина среднего отклонения ($Sr(\Delta_{ij})$) составляет 0,11071 (т.е. 13,28575/120), а наибольшее по абсолютной величине расхождение = 0,2372, что свидетельствует о непротиворечивости экспертных ранжировок.

Таким образом, из наиболее важных факторов (F_{V1}), выявленных на 1-м этапе исследования и подлежащим реализации в первую очередь, являются те, у которых на 2-м этапе исследования – показатель относительной простоты реализации (S_{v1}) является наибольшим и, соответственно, результирующий ранг (R_{V1}) наивысшим (1 и 2). Такими факторами являются:

f7: Ограничение права доступа к файлам и директориям пользователям (S_{v1}= 0,1249, R_{V1} = 1);

f20: Резервное копирование данных (S_{v1}= 0,1249, R_{V1} = 1);

f21: Использование безопасных паролей (S_{v1}= 0,1249, R_{V1} = 1);

f8: Минимизация использования сторонних расширений (модулей) (S_{v1}= 0,1234, R_{V1} = 2).

Выводы

Проведённый анализ факторов повышения безопасности информационных удалённых издательских систем от несанкционированного доступа даёт возможность обоснованного принятия решения при выборе тех или иных средств повышения безопасности.

Также руководство и сотрудники полиграфических предприятий могут использовать данные мето-

ды и перечень факторов для нахождения оптимального баланса между безопасностью, целесообразностью применения и удобством пользования ИУИС при проведении профилактических работ по повышению безопасности ИУИС.

Список литературы

1. Независимый информационно-аналитический центр Anti-Malware.ru [Электронный ресурс] / Malware.ru – Режим доступа к ресурсу: http://www.anti-malware.ru/news/2011-03-28/3868 - 31.03.2012 г.

2. РИА НОВОСТИ [Электронный ресурс] / РИА – Режим доступа к ресурсу: http://www.digit.ru/business /20110920/384241851.html. – 31.03.2012 г.

3. Ричард Э. Смит Аутентификация. От паролей до открытых ключей / Э. Смит Ричард. – Addison-Wesley: 2002. – 424 с.

4. Информационная безопасность и защита информации / В.П. Мельников, С.А.Клейменов, А.М. Петраков, С.А.Клейменова. – М.: Издательский центр «Академия», 2008. – 336 с.

5. Духан Е.И. Применение программно-аппаратных средств защиты компьютерной информации / Е.И. Духан, Н.И. Синадский, Д.А. Хорьков. – Екатеринбург: УГТУ-УПИ, 2008. – 182 с.

6. Ярочкин В.И. Информационная безопасность / В.И. Ярочкин. – Академический Проект, Гаудеамус, 2004. – 544 с.

7. Курило А.П. Аудит информационной безопасности / А.П. Курило. – БДЦ-пресс, 2006. – 304 с.

8. Леонтьев В.П. Безопасность в сети Интернет / В.П. Леонтьев. – Олма медиа групп, 2008. – 256 с.

9. Кузнецов М.В. PHP. Практика создания Web-сайтов / М.В. Кузнецов, И.В. Симдянов. – BHV-СПб, 2009. – 1264 с.

10. Коровченко Э. Энциклопедия Internet / Э. Коровченко. – Мультимедия, 2005. – 1000 с.

11. Компания Rapidssl [Электронный ресурс] / SSL сертификаты Rapidssl – Режим доступа к ресурсу: http://www.rapidssl.com/switch-ssl/compare-ssl-certificates/index.html - 31.03.2012 г.

12. Symantec Corporation [Электронный ресурс] / SSL сертификаты VeriSign. – Режим доступа к ресурсу: http://www.verisign.com/ssl/buy-ssl-certificates/compare-ssl-certificates/index.html - 31.03.2012 г.

13. Компания «Актив» [Электронный ресурс] / Электронный идентификатор Rutoken. – Режим доступа к ресурсу: http://www.rutoken.ru/buying/price/. – 31.03.2012 г.

14. Компания «PLASMA Хостинг Украина» [Электронный ресурс] / PLASMA Хостинг Украина. – Режим доступа к ресурсу: http://www.plasma.co.ua/category/ip-address/. – 31.03.2012 г.

15. Компания myRepono [Электронный ресурс] / myRepono. – Режим доступа к ресурсу: http://myrepono.com/pricing/. – 31.03.2012 г.

16. Интернет холдинг – Turbogroup [Электронный ресурс] / Хостинг Bitte. – Режим доступа к ресурсу: http://bitte.com.ua/#vds_vps. – 05.04.2012 г.

17. Саати Т. Принятие решений. Метод анализа иерархий: пер. с англ. / Т. Саати. – М.: Радио и связь, 1989. – 316 с.

18. Лямец В.И. Системный анализ. Вводный курс / В.И. Лямец, А.Д. Тевяшев. – 2-е изд., перераб. и доп. – Х.: ХНУРЭ, 2004. – 448 с.

19. Теория выбора и принятие решений: учебное пособие / И.М. Макаров, Т.М. Виноградская, А.А. Рубчинский, В.Б. Соколов. – М.: Наука. Главная редакция физико-математической литературы, 1982. – 328 с.

20. Вентцель Е.С. Теория вероятностей: учеб. для вузов / Е.С. Вентцель. – 7-е изд. стер. – М.: Высш. шк., 2001. – 575 с.

Поступила в редколлегию 15.02.2012

Рецензент: д-р техн. наук, проф. С.Ф. Чалый, Харьковский национальный университет радиоэлектроники, Харьков.

ФАКТОРИ ПІДВИЩЕННЯ БЕЗПЕКИ ІНФОРМАЦІЙНОЇ ВІДДАЛЕНОЇ ВИДАВНИЧОЇ СИСТЕМИ

І.В. Левикін, О.І. Хорошевський

У статті проводиться аналіз чинників, що підвищують безпеку інформаційних віддалених видавничих систем (ІВВС), за допомогою методу аналізу ієрархій, методу обробки експертної інформації і методу одновимірного шкалування. Аналіз проводиться в два етапи. На першому етапі проводиться обробка багатьох чинників підвищення безпеки ІВВС за допомогою методу аналізу ієрархій. На другому етапі здійснюється процес визначення пріоритетності серед найбільш важливих чинників і формується вектор пріоритетності чинників. Аналіз дозволяє зробити обґрунтований вибір дій,що застосовуються з метою підвищення захищеності ІВВС від несанкціонованого доступу.

Ключові слова: *htaccess, SSH-доступ, SSL сертифікат, USB-токен, виділена IP адреса, інформаційна віддалена видавнича система, метод аналізу ієрархій, метод обробки експертної інформації, метод одновимірного шкалування.*

FACTORS WHICH IS INCREASED SAFETY OF INFORMATION REMOTE PUBLISHING SYSTEM

I.V. Levykin, A.I. Horoshevskij

In article, the analysis of the factors raising safety of information remote publishing systems (IRPS) is madding, by means of a method of the analysis of hierarchies, method of processing of the expert information and method one-dimensional scale. The analysis made in two stages. At the first stage processing of set of factors of increase of safety, IRPS by means of a method of the analysis of hierarchies is madding. At the second stage, definition process priority among the most important factors is carried out and the vector priority factors are formed. The analysis allows to make a well-founded choice of applied actions on increase of security IRPS from unapproved access.

Keywords: *htaccess, SSH-access, SSL certificate, USB-token, allocated IP address, information remote publishing system, method of the analysis of hierarchies, method of processing of the expert information, a method one-dimensional scale.*