УДК 004.4, 004.6, 004.7

ИСПОЛЬЗОВАНИЕ МАТРИЦЫ ДОСТУПА НА ОСНОВЕ ПРИНЦИПА КРИТИЧНОСТИ ФАЙЛОВ ДЛЯ ЦЕЛЕЙ ОРГАНИЗАЦИИ ЭФФЕКТИВНЫХ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ

[1,2]Жигалов К.Ю., [2]Подлевских А.П., [3]Козырев А.П.

[1]Институт проблем управления им. В.А. Трапезникова РАН, Москва, e-mail: kshakalov@mail.ru;
[2]НОУ ВО «Московский технологический институт», Москва, e-mail: a_podlevskikh@mti.edu.ru;
[3]ООО «Газпром связь», Москва, e-mail: kozyrevap@mail.ru

В статье рассмотрены подходы к решению проблем, возникающих при защите информации от неправомерных действий со стороны пользователей или злоумышленников, представлен анализ систем защиты информации. Для обеспечения функционирования системы защиты информации предлагается использовать систему защиты на основе матриц доступа, созданную и прописанную на основе информации о степени критичности защищаемых файлов. В свою очередь, критерии критичности предусматривают три степени: критично для работы программы в целом; важно для работы программы; не критично для работы программы в целом. Представлен алгоритм процедуры определения критичности по расширению файлов. Предлагаемый способ позволяет своевременно реагировать на все изменения в критичных файлах, что существенно повышает безопасность и практически исключает возможность потери важных данных.

Ключевые слова: резервное копирование, матрица доступа, критичность файлов, таблица критичности расширения файлов, облачные технологии, матрица доступа к файловой системе, мониторинг действия пользователя, настройка системы защиты информации

USAGE OF THE ACCESS MATRIX, BUILDED ON THE PRINCIPLE OF FILES CRITICALITY FOR THE ORGANIZATION OF EFFECTIVE SYSTEMS OF INFORMATION SECURITY

[1,2]Zhigalov K.Y., [2]Podlevskich A.P., [3]Kozyrev A.P.

[1]V.A. Trapeznikov Institute of Control Sciences of Russian Academy of Sciences, Moscow, e-mail: kshakalov@mail.ru;
[2]Moscow Technological Institute, Moscow, e-mail: a_podlevskikh@mti.edu.ru;
[3]Gazprom connection LLC, Moscow, e-mail: kozyrevap@mail.ru

In article is submitted the analysis of systems of information security solution of the information security problems, arising from illegal actions from users or malefactors, the analysis of systems of information security is submitted. It is offered to use the system of protection on the basis of access matrixes created on the basis of information on degree of criticality of the protected files for ensuring functioning of system of information security. In turn criteria of criticality provide three degrees: 1 – critical for work of the program in general; 2 – important for work of the program;3 – isn't critical for work of the program in general. The algorithm of procedure of determination of criticality for extension of files is presented in the article. The offered way allows to react in due time to all changes in critical files that significantly increases safety and practically excludes possibility of loss of important data.

Keywords: backup, access matrix, criticality of files, table of criticality of extension of files, cloudy technologies, matrix of access to file system, monitoring of action of the user, control of system of information security

Согласно статистическим данным, в настоящее время около 90% всех атак на информацию происходит со стороны ныне работающих или уволенных из компании сотрудников.

Основной особенностью современных информационных систем предприятия является то, что компоненты системы распределены в пространстве, а физическая связь между ними осуществляется посредством сетевых соединений (витая пара, оптоволокно, Wi-Fi и т.д.) и программно при помощи протоколов в виде пакетов обмена.

В настоящее время в связи с развитием локальных и глобальных вычислительных сетей удаленные атаки на информационную инфраструктуру предприятия занимают лидирующие позиции по количеству попыток и успешности их применения. В связи с чем контроль за программной частью инфраструктуры на файловом уровне становится все более актуальным.

Согласно данным, полученным исследовательским центром DataPro Research, Computer Security Institute, ФБР и компании Ernst&Young, компании во всем мире теряют около 6% доходов из-за инцидентов, связанных с различными способами обмана и кражи информации. Количество преступлений в данной области по странам:

– США – 80%;

– Великобритания – 85 %;
– Германия – 75 %;
– Франция – 80 %;
– Российская федерация – 90 %.

К существенным недостаткам существующих на сегодняшний день систем защиты информации можно отнести:

● видимость для конечных пользователей присутствия программ защиты;

● большие объемы хранимой резервной информации.

В данном конкретном случае, как известно, предупрежден – значит, вооружен.

От случайного или преднамеренного уничтожения либо изменения файлов пользователями, имеющими к ним полный доступ, позволяет защититься лишь методика проведения резервного копирования [3, 4].

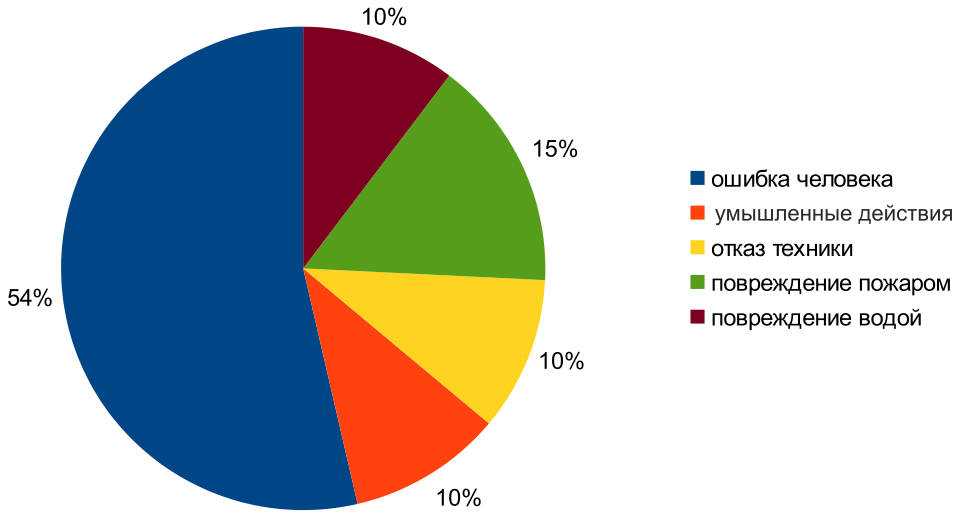

Рис. 1. Основные причины повреждений информации

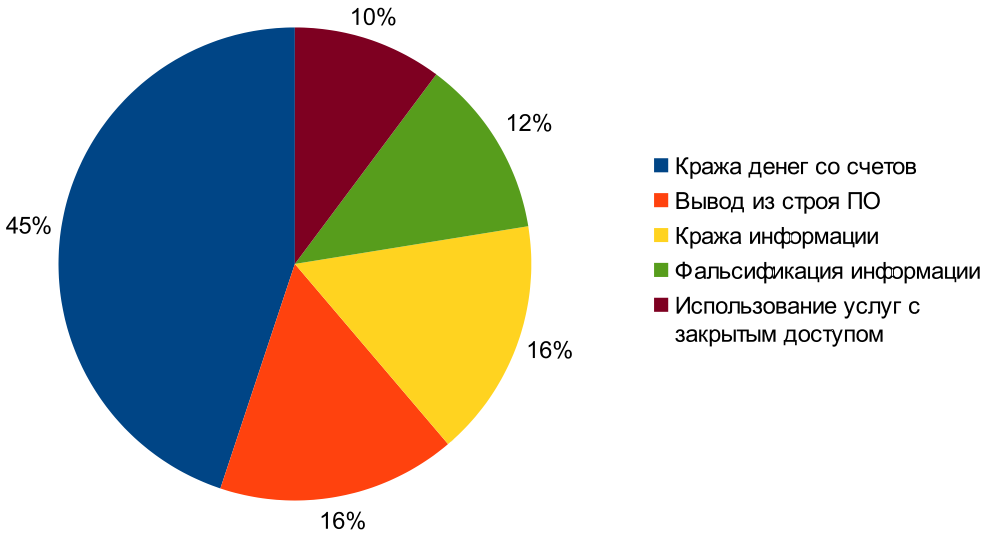

Рис. 2. Основные исполнители действий

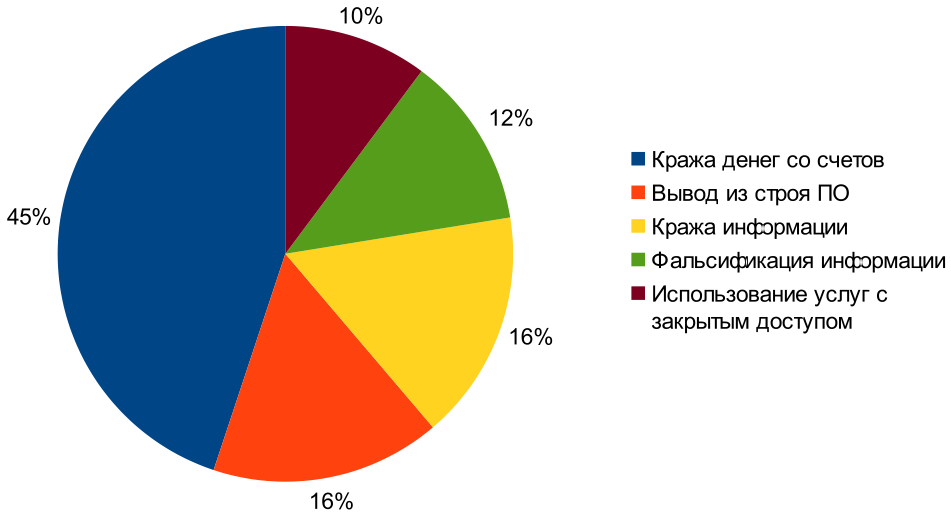

Рис. 3. Действия, предпринятые злоумышленниками при получении доступа к информации

Резервное копирование – дублирование информации с целью обеспечения возможности последующего восстановления этой информации, поврежденной в результате сбоя, ошибки или умысла.

Резервирование – применение независимых, функционально равноценных программ и файлов.

Тем не менее, у существующих методов резервного копирования есть несколько недостатков, к основным из которых относятся:

● необходимость больших объемов физических хранилищ для размещения файлов резервного копирования. Как показывает практика, объем резервных хранилищ часто превышает объем используемых компанией данных в 2–3 раза даже в заархивированном виде [4, 5];

● значительное время, требующееся на восстановление данных из резервных копий. Это связано с поиском необходимого архива, распаковкой файлов и пересылкой их по сети на сервер или рабочую станцию, на которой они использовались до потери;

● отсутствие системы автоматизированного мониторинга целостности файлов. Этот аспект существенно осложняет поиски утраченной информации, так как возникновение аварийного случая может быть обнаружено пользователем лишь по истечении некоторого времени;

● существенная загрузка сети при проведении процедур резервного копирования с нескольких компьютеров (в связи с чем данный вид работ выполняется в основном в ночное время);

● отсутствие технической возможности проверки корректности процедур резервного копирования.

Для минимизации факторов, связанных с большими объемами ежедневного архивирования и перемещением этих данных по сети, применяется «инкрементное» копирование. В этом случае программными средствами определяются и фиксируются изменения, сделанные в файловой системе с момента прошлого резервного копирования (следует отметить, что программное средство должно быть запущено на компьютере все время его работы). Тем не менее, данный способ увеличивает влияние другого, иногда более важного фактора – времени на разархивирование, так как системе архивного хранения необходимо просматривать всю цепочку файлов архива. Система становится уязвима к хранению всей цепочки. Ведущими разработчиками систем такого рода в настоящий момент являются Acronis, IDC и Microsoft.

Для одновременной минимизации всех факторов целесообразно использовать системы защиты принципиально другого уровня, на основе матриц доступа, созданных, в свою очередь, на основе информации о степени критичности тех или иных файлов.

Матрица доступа – таблица, отображающая правила разграничения доступа.

Критичность файла (в данной статье) – это способность программного средства, к которому относится файл, работать в случае его утраты.

Таблица 1

Таблица критичности расширений файлов

Версия ОС	Название ПО	Версия ПО	Расширение файла	Критерий критичности (1, 2, 3)
Windows 7	Avast	13	.exe	1
Windows 8	MS Office	2013	.dll	2

Рассмотрим подробнее подход к определению критичности тех или иных файлов. Строго говоря, корпорация Microsoft в своей операционной системе (далее – ОС) на базе Windows уже несколько лет использует критерии критичности некоторых файлов в методах резервного копирования, служащих для [6, 7, 8]:

● восстановления предыдущего состояния ОС;

● восстановления работоспособности ОС.

В первом случае операционная система ведет журнал всех изменений конфигурационных файлов.

Во втором случае Microsoft предлагает переписывать важные системные файлы из первоначального хранилища (образа установки операционной системы).

Оба этих метода практически не влияют на дополнительное программное обеспечение (далее – ПО), установленное пользователем самостоятельно и не относящееся к разработкам Microsoft. Кроме того, такого рода системы не предназначены для работы в сети. Тем не менее, идея Microsoft может быть реплицирована на ПО сторонних разработчиков. Как показали исследования, не все файлы, устанавливаемые вместе с программами, имеют критичное значение для их корректной работы.

Критерии критичности делятся на три степени:

– критично для работы программы в целом. При утрате этих файлов программа не запускается или не выполняет основные свои функции;

– важно для работы программы (обычно это файлы различных модулей программы). При утрате данной группы файлов программа запускается, но не выполняет некоторые второстепенные функции;

– некритично для работы (текстовые файлы-инструкции, резервные файлы для восстановления работоспособности ПО, файлы предыдущих обновлений, файлы, предназначенные для разных конфигураций персонального компьютера, файлы логов). При утрате этой группы файлов программа способна запускаться и выполнять основные свои функции.

Все производители ПО создают его индивидуально, в связи с чем нет единого перечня расширений файлов, относящихся к описанным выше группам ни впрямую, ни косвенно. Этот факт вынуждает нас проводить тестирование каждой программы и каждого ее файла вручную и заносить результаты в таблицу (см. табл. 1). Для упрощения процесса целесообразно первоначально группировать файлы по расширениям и проверять все файлы, имеющие данное расширение одновременно.

Алгоритм процедуры проверки выглядит следующим образом:

1. Копируем директорию, содержащую программу, в архив.

2. Находим файлы с одним общим расширением и удаляем их.

3. Пробуем запустить программу, и, если получается, провести тестирование программы. Если программа не запустилась – относим файлы к категории (1). Если программа запустилась и выполняет только базовые функции – относим эти файлы к категории (2). Если программа запустилась и выполняет свои функции – относим файлы к категории (3).

4. Заносим результат в таблицу.

5. Возвращаем удаленные файлы из архива.

6. Повторяем процедуру с другим типом файлов.

Тестирование программы проходит методом «черного ящика». Принцип метода основывается на том, что тесты проходят в соответствии со спецификацией ПО или иных документов, описывающих требования к системе. Выполняются всё те же действия, которые должны выполняться при штатной работе ПО. Корректность работы программы можно определить, изучая выходные данные, полученные в исходном и измененном состоянии ПО.

Не все файлы ПО, имеющие одинаковое расширение, одинаково критичны для работы программы. Если количество файлов достаточно мало, необходимо проверить все эти файлы и критерий критичности присваивать индивидуально каждому файлу. Если же количество файлов весьма велико, можно ограничиться достаточно большой выборкой, чтобы определить процент попадания критичных для работы программы файлов среди «неважных»:

$$К = \frac{\text{Количество критичных файлов}}{\text{Количество проверенных файлов}} \times 100\%, \quad (1)$$

где К – коэффициент критичных файлов среди некритичных. Если в выборке нашлось весьма малое количество критичных файлов, имеет смысл нахождение этих файлов для минимизации архива.

К сожалению, в настоящее время на рынке существует огромное количество программных продуктов, что существенно усложняет занесение файлов данных программ в таблицу критичности. Для решения этого вопроса целесообразно набирать статистические данные о зависимости расширения файлов и критерии критичности. Это позволит систематизировать работу и вычесть из процедуры тестирования новых программ файлы, относящиеся к тому или иному критерию более чем в 80 % случаев.

В дальнейшем, можно использовать «облачные технологии» для целей увеличения таблицы критичности за счет пользователей системы. Для этого необходимо организовать интернет-ресурс, на котором зарегистрированным пользователям будет предоставлена возможность обновления файла базы данных (далее – БД) с информацией о критичности файлов. Одновременно с обновлением, у пользователя будет скачиваться его версия файла данной БД и проверяться на полноту записи. В случае обнаружения расхождений БД сетевого ресурса будет пополняться новыми данными. Идея использования «облачных технологий» для обновления БД посредством пользователей предложена и реализована в программном комплексе «ТАЛКА-ГИС» производства ИПУ РАН [1, 2].

Для целей заинтересованности пользователей в обновлении БД, предлагается ввести поощрительную балльную систему. А именно, за каждые новые 100 записей в БД пользователь получает 1 балл, эти баллы пользователи смогут тратить на приобретение новых лицензий и получение дополнительных консультаций службы поддержки пользователей. В случае превышения определенного порога набора баллов, пользователь получает бесплатную техническую поддержку по данному ПО.

По завершении составления таблиц критичности файлов создается матрица доступа к файловой системе на их основе. По сути, это те же таблицы, только с большим количеством полей (см. табл. 2).

К матрице критичности добавляются варианты действия системы на каждую группу файлов (либо папку в файловой системе) и пользователей (им, в свою очередь, расставляются права на группы файлов и папок).

По проведенным исследованиям были сгруппированы следующие возможные режимы работы программы по каждым группам:

- блокировка чтения (по сути – это блокировка доступа пользователя к данным файлам);
- блокировка записи (пользователь может читать, но не писать файлы);
- мониторинг действий пользователя (в этом случае Программа может вести логирование действий пользователя именно с этими файлами (удалял/читал/редактировал/копировал/запускал);
- безопасный для системы мониторинг (программа ведет логирование действий пользователя и создает на резервном сервере-хранилище папку вида: \дата\логин пользователя\...Сохраняя файловую структуру от корня, копирует файлы, удаленные или измененные пользователем);
- безопасный выборочный мониторинг (программа ведет логирование действий пользователя и создает на резервном сервере-хранилище папку вида: \дата\логин пользователя\... Сохраняет только удаленные или измененные файлы исходя из таблицы критичности файлов).

Как видно, использование таких матриц в системах защиты информации существенно повысит их функционал.

К положительным сторонам матрицы доступа можно отнести:

1. Матрица доступа может быть использована в различного рода программном обеспечении для:

- защиты важных данных, путем разграничения доступа к ним;
- уменьшения места на жестких дисках пользователей в частности и сети в целом путем удаления данных, относящихся к некритичным;
- защиты критически важных данных путем резервного копирования и резервирования.

2. С помощью матрицы можно выбирать необходимый уровень защиты и тем самым экономить ресурсы внутренней сети компании в периоды проведения процедур резервного копирования данных.

3. Наличие матрицы критичности файлов существенно сокращает время на настройку системы защиты информации, так как полностью автоматизирует работу при выборе необходимых файлов.

К отрицательным сторонам использования матрицы доступа можно отнести:

- необходимость тестирования всех программ вручную на начальном этапе;
- наличие матрицы в руках злоумышленника позволит ему быстрее копировать себе важные данные, а также проводить эффективное их уничтожение.

Таблица 2

Матрица доступа (пример)

Данные обобщенно	Данные по группам	Расширения файлов	Пути папок	Критичность файлов 1–3
1	2	3	4	5
Файлы ПО	Файлы ОС	.dll		1
		.sys		1
	Файлы устан. ПО	.exe		1
		.bat		1
	Врем. файлы	.tmp		3
	Логи сист и ПО	.log		3
Файлы данных	Текст. документы	.doc		3
		.docx		1
		.odt		
		.txt		
	БД	.1cd		1
		.lgp		
		.sql		1
		.mdf		
		.rdf		
	Граф. файлы	.jpeg		2
		.raw		3
		.bmp		
		.gif		
Резервные копии				1
				2

Окончание табл. 2

Режимы работы ПО					Индив. ключи поим. пользователя или группы	
6					7	
Блок чтения	Блок записи	Монит. действ	Безоп. сист. мониторинга	Безоп. выбор. монит.	Semenov	Sale Support
xx	yy	zz	vv	Uu		
	yy				1	1
	yy				1	1
–		zz			1	1
		zz			1	1
		z			3 2	3
				Uu	4	3 2
			vv		3	3
xx	yy yy				1	1

К положительным сторонам использования матрицы доступа можно отнести:

● Возможность быстро настраивать систему защиты информации в полуавтоматическом режиме (необходимо лишь занести пользователей и либо расставить им права доступа, либо включить их в группы);

● Возможность использования для систем наблюдения за действиями пользователей.

Согласно проведенным исследованиям, на компьютере может содержаться в среднем от 30% (для компьютеров с ОС Windows) до 50% (для компьютеров под управлением ОС Linux/Unix) не критичных

для работы файлов. Данное обстоятельство позволяет предположить, что защита важных файлов сократит объем как хранимых резервных копий, так и данных, передаваемых по сети во время проведения копирования в среднем на те же величины процентов.

Предложенный подход к обеспечению безопасности информации, имеет определенный потенциал. Данный способ позволит своевременно реагировать на все изменения в критичных файлах (удаление файла), что существенно повышает безопасность и практически исключает возможность потери важных данных в связи со слишком большим промежутком времени, прошедшим с момента их изменения/удаления.

Список литературы

1. Восстановление системы: вопросы и ответы // Microsoft [электронный ресурс] URL: http://windows.microsoft.com/ru-ru/windows/system-restore-faq#1TC=windows-7 (дата обращения: 15.07.2015).

2. Выбор расширенного метода восстановления // Microsoft [электронный ресурс] URL: http://windows.microsoft.com/ru-ru/windows7/choosing-an-advanced-recovery-method (дата обращения: 15.07.2015).

3. Жигалов К.Ю. Методики построения современных геоинформационных систем с учетом новых компьютерных и сетевых технологий // Альманах современной науки и образования. – 2013. – № 7 (74). – С. 66–68.

4. Жигалов К.Ю. Принципы построения локальной вычислительной сети для решения задач автоматизации мониторинга и управления на строительных объектах // Фундаментальные исследования. – 2014. – № 9–7. – С. 1436–1440.

5. Жигалов К.Ю., Сюняев Ш.И. Модели движения строительной техники в процессах автоматизации строительства объектов // Актуальные инновационные исследования: наука и практика (Электронное научное издание). – 2013. – Т. 3. URL: http://www.actualresearch.ru/nn/2013_3/Article/geosciences/zhigalov2013_3.htm. (дата обращения 20.08.2014).

6. Зегжда Д.П., Ивашко А.М. Основы безопасности информационных систем. – М.: Горячая линия – Телеком, 2000. – 452 с.

7. Медведев Н.В., Гришин Г.А. Модели управления доступом в распределенных информационных системах // Наука и образование. – 2011. – № 1; [электронный ресурс] URL: http://technomag.edu.ru/doc/164245.html (дата обращения: 20.06.2015).

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

9. Подлевских А.П., Жигалов К.Ю. Методы оценки и обеспечения информационной безопасности в корпоративных сетях // Образовательная среда сегодня и завтра. Сборник научных трудов IX Международной научно-практической конференции. – 2014. – С. 322–325.

10. Подлевских А.П., Норец В.А. Обеспечение информационной безопасности от несанкционированного проникновения в сетях // Образовательная среда сегодня и завтра. Сборник научных трудов VIII Международной научно-практической конференции. – 2013. – С. 416–419.

References

1. Vosstanovlenie sistemy: voprosy i otvety // Microsoft [jelektronnyj resurs] URL: http://windows.microsoft.com/ru-ru/windows/system-restore-faq#1TC=windows-7 (data obrashhenija: 15.07.2015).

2. Vybor rasshirennogo metoda vosstanovlenija // Microsoft [jelektronnyj resurs] URL: http://windows.microsoft.com/ru-ru/windows7/choosing-an-advanced-recovery-method (data obrashhenija: 15.07.2015).

3. Zhigalov K.Ju. Metodiki postroenija sovremennyh geoinformacionnyh sistem s uchetom novyh kompjuternyh i setevyh tehnologij // Almanah sovremennoj nauki i obrazovanija. 2013. no. 7 (74). pp. 66–68.

4. Zhigalov K.Ju. Principy postroenija lokalnoj vychislitelnoj seti dlja reshenija zadach avtomatizacii monitoringa i upravlenija na stroitelnyh ob#ektah // Fundamentalnye issledovanija. 2014. no. 9–7. pp. 1436–1440.

5. Zhigalov K.Ju., Sjunjaev Sh.I. Modeli dvizhenija stroitelnoj tehniki v processah avtomatizacii stroitelstva ob#ektov // Aktualnye innovacionnye issledovanija: nauka i praktika (Jelektronnoe nauchnoe izdanie). 2013. T. 3. URL: http://www.actualresearch.ru/nn/2013_3/Article/geosciences/zhigalov2013_3.htm. (data obrashhenija 20.08.2014).

6. Zegzhda D.P., Ivashko A.M. Osnovy bezopasnosti informacionnyh sistem. M.: Gorjachaja linija Telekom, 2000. 452 p.

7. Medvedev N.V., Grishin G.A. Modeli upravlenija dostupom v raspredelennyh informacionnyh sistemah // Nauka i obrazovanie. 2011. no. 1; [jelektronnyj resurs] URL: http://technomag.edu.ru/doc/164245.html (data obrashhenija: 20.06.2015).

8. Melnikov V.P., Klejmenov S.A. Informacionnaja bezopasnost i zashhita informacii. M.: Izdatelskij centr «Akademija», 2008. 336 p.

9. Podlevskih A.P., Zhigalov K.Ju. Metody ocenki i obespechenija informacionnoj bezopasnosti v korporativnyh setjah // Obrazovatelnaja sreda segodnja i zavtra. Sbornik nauchnyh trudov IX Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2014. pp. 322–325.

10. Podlevskih A.P., Norec V.A. Obespechenie informacionnoj bezopasnosti ot nesankcionirovannogo proniknovenija v setjah // Obrazovatelnaja sreda segodnja i zavtra. Sbornik nauchnyh trudov VIII Mezhdunarodnoj nauchno-prakticheskoj konferencii. 2013. pp. 416–419.