7. Радиолокационные станции обзора Земли / Г.С. Кондратенков, В.А. Потехин, А.П. Реутов, Ю.А. Феоктистов; под.ред. Г.С. Кондратенкова. – М.: Радио и связь, 1983. – 218с.

8. Саблин В.Н. Разведывательно-ударные комплексы и радиолокационные системы наблюдения земной поверхности / В.Н. Саблин. – М.: Радиотехника, 2002. – 258с.

9. Неронский Л.Б. Микроволновая аппаратура дистанционного зондирования поверхности Земли и атмосферы. Радиолокаторы с синтезированной апертурой антенны / Л.Б. Неронский, В.Ф. Михайлов, К.В. Брагин.–СПб.: Санкт-Петербургский государственный университет аэрокосмического приборостроения, 1999. – 234 с.

10. Вакин С.А. Основы радиоэлектронной борьбы / С.А. Вакин, Л.Н. Шустов.– М.: ВВИА им. Н.Е. Жуковского, 1998.– 366 с.

УДК 517.978.21

Толюпа С.В. д.т.н.; **Торошанко Я.И.** к.т.н.; **Мороко А.Ю.,** асп.
(*Государственный университет информационно-коммуникационных технологий*)

ПУТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ЭЛЕКТРОННЫХ ХРАНИЛИЩ

Толюпа С.В., Торошанко Я.І., Мороко О.Ю. В умовах інформатизації суспільства завданнязабезпечення безпеки сховищ електронних документів стає усе більш важливим. На основі аналізу світового досвіду захисту інформаційних систем автори цієї статті формулюють і обговорюють принципи створення, експлуатації і забезпечення надійної безпеки довірених електронних сховищ.

***Ключові слова*:** ЕЛЕКТРОННЕ СХОВИЩЕ, ІНФОРМАЦІЙНА БЕЗПЕКА

Толюпа С.В., Торошанко Я.И., Мороко А.Ю. В условиях информатизации общества задача обеспечения безопасности хранилищ электронных документов становится всё более важной. На основе анализа мирового опыта защиты информационных систем авторы данной статьи формулируют и обсуждают принципы создания, эксплуатации и обеспечение надежной безопасности доверенных электронных хранилищ.

***Ключевые слова*:** ЭЛЕКТРОННОЕ ХРАНИЛИЩЕ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Toliupa S.V., Toroshanko Ia.I., Moroko O.Iu. In the conditions of informatization of society the task of providing of safety of depositories of electronic documents becomes more important. On the basis of analysis of world experience of defence of the informative systems of автори of this article formulate and discuss principles of creation, exploitations and providing of reliable safety of the trusted electronic depositories.

***Keywords*:** ELECTRONIC DEPOSITORY, INFORMATIVE SAFETY

Вступление. Постановка задачи. До недавнего времени многие ИТ-администраторы встречали вопрос о безопасности данных недоуменным взглядом. В общем, ИТ-безопасность воспринимается как оборона на периметре сети. Для защиты всей информации в сети обычно достаточно предотвратить несанкционированный доступ в сеть.

Однако опытные сетевые администраторы понимают, что существуют и другие проблемы, относящиеся к безопасности хранилищ данных, наиболее актуальная из которых – добиться, чтобы только доверенные лица имели доступ к данным.

Традиционно, одной из самых больших трудностей при защите хранимых данных было отслеживание мест хранения. Серверы, настольные компьютеры и ноутбуки разбросаны по всей компании, и защита информации на всех доступных пользователям устройствах – весьма трудоемкая задача, почти невозможная, если не применить централизованных методов. Для этого требуется строго контролировать доступ к данным, настроив учетные записи пользователей так, чтобы данные хранились на безопасных сетевых устройствах, и ограничить доступ мобильных пользователей. Процедура защиты данных должна предусматривать меры для безопасного, надежного архивирования. Не имеет смысла защищать данные, если резервные копии хранятся в ненадежном месте.

Чрезвычайно важно настроить меры защиты так, чтобы не только пользователи, но и соответствующие приложения и аппаратные устройства получили необходимый доступ. Ошибки в конфигурации безопасности могут помешать корректной работе приложений (или совсем остановить их), нарушив документооборот в компании. Многие параметры безопасности можно изменять “на ходу”, поэтому стандартные политики безопасности, которые определяют круг лиц, имеющих право вносить изменения – еще один важный компонент модели безопасности хранилищ данных.

Многие администраторы обращаются в поисках решения к сетям хранения данных. Несмотря на многие преимущества SAN и NAS (при их правильном использовании), у этих технологий есть уязвимые места, когда дело касается защиты информации. Фактически, данные SAN и NAS концентрируются в одном месте, но эта особенность часто не учитывается в модели безопасности.

Для надежной безопасности хранилища требуется многоуровневая модель защиты, в которой учтены месторасположение данных, потребности доступа пользователей, требования системного доступа и резервного копирования и защиты данных. Многоуровневый подход к защите данных, в отличие от универсального способа, обеспечивает более детализированный контроль над доступом к данным и позволяет изменять модель безопасности при изменении потребностей компании. Вместо того, чтобы полностью перестраивать инфраструктуру защиты данных, нужно изменять только фрагменты, затронутые переменами в деловой деятельности, при постоянстве базовой модели. Суровые меры защиты, ограничивающие готовность и гибкость доступа к данным, могут быть полезными в статической среде, но для динамичной бизнес-модели требуется тщательно продуманный, чрезвычайно гибкий подход к защите хранилищ даннях [1].

Современные корпорации сталкиваются с бурным ростом объемов данных, необходимых для их повседневной работы. Этот рост вызван потребностью постоянно иметь “на кончиках пальцев” финансовую, маркетинговую, техническую, статистическую и другую информацию для оперативного реагирования на изменения рыночной ситуации, поведение конкурентов и клиентов.

Однако высокая степень централизации корпоративной информации делает ее более уязвимой и упрощает задачу злоумышленнику, который поставил себе цель получить доступ к этой информации. Ситуация усугубляется тем, что современные технологии хранения данных, начиная от обычного файл сервера и заканчивая такими архитектурами, как SAN или NAS, практически не предусматривают встроенных средств разграничения доступа и защиты информации.

Таким образом, часто, если не всегда, конфиденциальная информация, которая представляет ценность для компании и утечка которой чревата серьезными неприятностями – ущербом для деловой репутации, судебными исками или потерей конкурентных преимуществ, практически никак не защищена от ряда угроз [2].

Рассмотрим решения для построения системы управления событиями информационной безопасности, управления угрозами и инцидентами. В качестве платформы для построения системы управления событиями информационной безопасности (SIEM–SecurityInformationandEventManagement) предлагается использовать программные и аппаратные решения компании Arcsight.

Для того чтобы надежно управлять безопасностью хранилищами данных необходимо осуществлять аудит действий пользователей информационных систем предприятия и электронных хранилищ. При этом персонал ИТ-подразделений вынужден вручную собирать разрозненную информацию из журнальных файлов (лог-файлов) тех или иных приложений и вручную обрабатывать эти данные. Учитывая огромные объемы таких данных и большое количество применяемых на современном предприятии информационных систем, подобный подход к проблемам аудита является заведомо неэффективным и весьма трудоемким.

При обработке данных аудита вручную возникает еще одна проблема – нарушения политик информационной безопасности выявляются поштучно, эпизодически. Целостную

картину, включающую в себя объективные данные по всем системам и приложениям, построить сложно, а порой и нельзя.

Нередкой является и ситуация, когда контроль соблюдения политик информационной безопасности ложится на администраторов приложений и систем предприятия. При этом сами администраторы оказываются неподотчетными никому, средств для контроля их деятельности нет, что создает почву для возможных злоупотреблений должностными полномочиями.

Очевидно, что в этих условиях крайне сложно организовать оперативное обнаружение атак и прочих угроз, а также своевременные действия по их ликвидации. Обслуживающий персонал вынужден постоянно отслеживать текущие параметры функционирования огромного количества элементов ИТ-инфраструктуры (например, операционных систем серверов и автоматизированных рабочих мест (АРМ), сетевого оборудования, почтовых и веб-серверов и т. п.), просматривать лог-файлы, данные аудита и пр. Подобный подход не только требует привлечения большого количества высококвалифицированных специалистов, приводит к повышенным трудозатратам, но и является малоэффективным: многие атаки обнаруживаются постфактум, велика вероятность вообще не выявить те или иные злонамеренные действия.

Большинство компаний при организации системы управления информационной безопасностью уделяет значительное внимание защите от внешних угроз, используя межсетевые экраны, средства предотвращения вторжений, антивирусные средства. Однако, как показывает общемировая статистика, наибольший ущерб информационным ресурсам наносят внутренние пользователи (около 80 % всех инцидентов безопасности).

При этом наибольшую опасность могут представлять злоумышленники с высокими полномочиями доступа администраторов сетей, операционных систем, приложений, баз данных, так как могут легко замаскироваться под системными учетными записями или записями приложений, произвести удаление журналов событий безопасности и т.п.

Решения Arcsight обеспечивают распознавание инцидентов информационной безопасности путем корреляции информации, собранной из различных источников: операционных систем, СУБД, электронных хранилищ, приложений, сетевых устройств, средств безопасности, мэйнфреймов, приведение полученных больших объемов информации о событиях безопасности к удобному для восприятию виду, выявление наиболее критичных событий безопасности, оперативное уведомление о нарушениях политики безопасности, расследование инцидентов, контроль за действиями внутренних пользователей, привилегированных пользователей, сторонних консультантов, контроль непрерывности хранения журналов безопасности, контроль соответствия нормативным требованиям.

Службы внутреннего контроля и безопасности, а также ИТ-подразделения, понимают важность эффективной организации сбора, хранения и анализа информации для выявления рисков, автоматизации проверки соответствия и проведения аудита, быстрого выявления угроз и оптимизации соглашений об уровне обслуживания.

С целью решения перечисленных задач, любая система сбора данных должна обеспечивать возможность сбора информации о событиях из широкого диапазона источников — от устройств сетевой и периметровой безопасности до баз данных и приложений собственной разработки.

В дополнение к поддержке широкого спектра устройств и высокой производительности агрегации данных, для обеспечения соответствия нормам и требованиям, а также возможности расследования инцидентов, система должна обеспечивать аудиторское качество сбора и хранения информации. Только сбор информации о событиях на месте их возникновения позволит обеспечить комплексную безопасность, надежность и доступность данных. Для этого необходимо иметь готовое к немедленной эксплуатации масштабируемое решение для сбора информации из журналов, которое можно просто развернуть и эксплуатировать в сотнях или даже тысячах подразделений, что гарантирует комплексный сбор информации обо всех корпоративных событиях.

После сбора данных, их необходимо хранить на протяжении различных периодов времени, часто несколько лет, в соответствии с требованиями, например, закона Сарбейнса-Оксли, стандарта PCI, федерального закона США об управлении информационной безопасностью (FISMA), акта HIPAA и акта GLBA, или в соответствии с принятыми корпоративными политиками хранения. Поэтому необходимо внедрить экономически эффективное решение для длительного хранения информации в электронных хранилищах. Инфраструктура сбора данных об информационной безопасности должна предоставлять возможности хранения и передачи информации в централизованные репозитории, где обеспечивается сжатие и безопасное хранение данных, при этом вся информация должна быть доступна для анализа.

В корпоративной среде и в государственном управлениивсе шире используются электронные документы, вытесняя бумажные аналоги. Традиционные бумажные технологии делопроизводства и архивирования постепенно уходят в прошлое. Однако сегодня, в условиях глобализации, роста объема информации, активизации информационного обмена, электронные документы подвергаются серьезным угрозам безопасности. Так, развитие технологий Web, XML, мобильной и беспроводной связи, стандартизация форматов данных и протоколов их обмена делают информационную среду организаций всё более открытой и беззащитной перед криминализирующимся Интернетом.

В распространившихся системах автоматизированного управления накапливается и обрабатывается огромный объём внутренней корпоративной информации, а в системах CRM– персональных данных клиентов. В то же время рост емкости и миниатюризация носителей памяти, увеличение мощности каналов связи предоставляют широкие технические возможности для краж данных недобросовестными сотрудниками.

В таких условиях всё большее значение приобретают технологии защиты систем электронных документов как от внешних, так и от внутренних угроз. Следует учитывать, что электронные документы являются, по сути говоря, наборами единиц и нулей, и к ним невозможно применять такие традиционные методы защиты, как оттиск печати, собственноручная подпись и водяные знаки на бумаге. Вместо указанных средств используются электронная цифровая подпись, цифровые отпечатки и другие технические и организационные методы, учитывающие специфику жизненного цикла электронных документов и их носителей.

В настоящей статье мы рассматриваем принципы создания и эксплуатации доверенных хранилищ электронных документов, т. е. хранилищ, предусматривающих защиту от основных классов угроз. Мы не будем касаться вопросов актуальности документов хранилища, сохранения их логических взаимосвязей, глубины ретроспективы и других аналитических возможностей. Рассматриваются только аспекты безопасности.

Доверенное хранилище (ДХ), как правило, представляет собой сложную систему, включающую логически единую базу данных, находящуюся в сети, где над ней производится многопользовательская обработка. По мнению экспертов компании Perimetrix, российского разработчика систем защиты корпоративных секретов от внутренних нарушителей, одним из важнейших принципов построения и эксплуатации ДХ является принцип системности [3].Он подразумевает необходимость защиты электронных документов на всех этапах их жизненного цикла – от создания, обработки и хранения до передачи по каналам связи и уничтожения. Такая защита включает как технические средства, так и меры организационного характера, и должна быть направлена и на сами документы, и на программный комплекс электронного документооборота.

Система защиты ДХ должна обеспечивать конфиденциальность (гарантию доступа к данным только определенных лиц), целостность (защиту от случайных и преднамеренных искажений и подмен) и готовность (возможность в любое время пользоваться документами в соответствии с установленной политикой безопасности) объектов ДХ. Надо отметить, что обеспечение аутентичности и конфиденциальности электронных документов необходимо не только для защиты от утечек и потерь, но и для придания документам юридической силы.

Также при построении ДХ большое значение имеет принцип равнопрочности всех звеньев цепи защиты. Он означает, что следует учитывать все виды рисков, включая вирусное заражение, SQL-инъекции, незаконное копирование, непреднамеренные ошибки, ведущие к искажениям, отказы аппаратных и программных средств и т. д. Защита только от части угроз делает систему безопасности неэффективной, а инвестиции в неё бесполезными. «Для понимания достаточности предпринимаемых мер защиты наилучшим способом, несомненно, является проведение оценки рисков. Методика такой оценки и уровень принятия риска в каждом случае являются предметом обсуждения с подразделениями – владельцами обрабатываемых в доверенном хранилище информационных активов», – говорит Алена Фомина, исполнительный директор и партнёр компании Milestone.

Конфиденциальность данных ДХ обеспечивается путем реализации принципа разграничения доступа. Этот принцип, заключающийся в предоставлении разным пользователям различных полномочий на выполнение конкретных операций над документами, может быть реализован в виде дискреционной (избирательной), ролевой либо мандатной модели.

В ***дискреционной*** модели используется матрица, устанавливающая связь между каждым пользователем, разрешенной операцией и объектом базы данных. Такой подход обеспечивает широкую вариативность доступа, но, к сожалению, он достаточно громоздок.

В ***мандатной*** модели объектам ДХ, его пользователям и процессам приписываются метки, определяющие уровень секретности. Если метки объекта и субъекта совпадают, то последнему разрешается проводить определенные действия над объектом ДХ. Эта модель является весьма жёсткой и подходит для строгой иерархической организации.

В ***ролевой*** модели каждому пользователю и процессу назначается роль, имеющая те или иные права доступа, причем у одного пользователя может быть несколько ролей. Этот подход по жёсткости представляет собой нечто среднее между дискреционной и мандатной моделями.

При построении и эксплуатации ДХ важно соблюдать и принцип многоуровневой и многокомпонентной аутентификации. При многоуровневой аутентификации для доступа к защищённой информации используются дополнительные средства защиты, кроме пароля, — например, USB-ключ или биометрические данные. Многокомпонентность же означает, что для доступа к критически важным документам требуется аутентификация в системе сразу нескольких человек. По принципу действия данный подход можно сравнить с банковской практикой хранения ключей от различных замков особо важного сейфа у разных сотрудников. Для открытия сейфа требуется их совместная деятельность, а значит, обеспечивается взаимный контроль [3].

В последнее время в связи с увеличением вычислительной мощности компьютеров, стало возможным шифрование объектов ДХ, которое используется для обеспечения конфиденциальности и целостности данных. Применяются как протоколы симметричного шифрования, требующие управления большим количеством ключей, так и ассиметричные схемы, обладающие повышенной ресурсоемкостью. Довольно часто используются гибридные схемы, позволяющие максимально использовать достоинства обоих подходов.

Для рядового пользователя наиболее удобно так называемое “прозрачное” шифрование, выполняющееся в автоматическом режиме, когда управление ключами осуществляется системными средствами. Другим вариантом является задание ключа самим пользователем, что требует от системы безопасности контроля выполнения всех необходимых протоколов. В отношении шифрования важнейшим принципом создания ДХ, по мнению специалистов, является принцип открытости криптографических алгоритмов. Он обеспечивает стойкость применяемых протоколов шифрования объектов ДХ, поскольку говорит о том, что они прошли многократную публичную проверку.

Также необходимо отметить, что при проектировании ДХ большое значение имеет и принцип экономической оправданности. Данный принцип заключается в необходимости соблюдения разумного баланса между эффективностью системы защиты, затратами ресурсов на ее создание и поддержание, удобством и психологическим комфортом пользователей.

В наше время информация становится все более ценным экономическим активом. Желанной целью злоумышленников является несанкционированный доступ к электронным документам как из-за пределов корпоративной сети, так и внутри ее периметра. Открытость информационной среды и современные технические средства дают дополнительные возможности для осуществления утечек и порчи документов.

Однако растут возможности и средств защиты. По нашим оценкам, реализация сформулированных в данной статье принципов при проектировании ДХ позволяет создать максимально защищенное хранилище электронных документов, не снижая при этом продуктивность других бизнес-процессов, благодаря чему инвестиции в систему безопасности оправдываются.

Литература

1. Куликов А.А. Создание и експлуатация баз данных / А.А Куликов. В.А. Григович, О.И. Ларипов. – М.: Око-Трендз, 2005. – 184 с.

2. Богуш В.А. Теоретичні основи захищених інформаційних технологій: навч. посіб. / Богуш В.А., Довидьков О.А., Кривуца В.Г. – К.: ДУІКТ, 2010. – 454 с.

3. Кравченко Р. Принципы создания и эксплуатации доверенных хранилищ [Електронний ресурс] / Р. Кравченко – Режим доступу: http://www.pcweek.ru/security/article/detail.php?ID=109629.

УДК 62-83:517

Розорінов Г.М., д.т.н.; **Труш О.В.,** викладач
(*Державний університетт інформаційно-комунікаційних технологій*)

ДОСЛІДЖЕННЯ МОЖЛИВОСТЕЙ РЕАЛІЗАЦІЇ ОПТИМАЛЬНОГО ПО ШВИДКОДІЇ УПРАВЛІННЯ КРОКОВИМ ДВИГУНОМ ПРИВОДУ ОБЕРТАННЯ CD, DVD.

Розорінов Г.М., **Труш О.В. Дослідження можливостей реалізації оптимального по швидкодії управління кроковим двигуном приводу обертання CD, DVD.** Досліджується можливість реалізації оптимального або квазіоптимального по швидкодії управління кроком ротора двигуна за рахунок спеціальної організації багатоканального генератора імпульсів. У статті розглядаються два варіанти управління кроковим двигуном, в одному з них оцінка ефективності проводиться по математичній моделі крокового двигуна, в другому – за експериментальними даними.

Ключові слова: КРОКОВИЙ ДВИГУН. ШВИДКОДІЯ УПРАВЛІННЯ, ГЕНЕРАТОР ІМПУЛЬСІВ

Розоринов Г.Н., **Труш А.В. Исследование возможностей реализации оптимального по быстродействия управления шаговым двигателем привода вращения CD, DVD.** Исследуется возможность реализации оптимального или квазиоптимального по быстродействию управления шагом ротора двигателя за счет специальной организации многоканального генератора импульсов. В статье рассматриваются два варианта управления шаговым двигателем, в одном из них оценка эффективности проводится по математической модели шагового двигателя, во втором – по экспериментальным данным.

Ключевые слова: ШАГОВЫЙ ДВИГАТЕЛЬ. БЫСТРОДЕЙСТВИЕ УПРАВЛЕНИЯ, ГЕНЕРАТОР ИМПУЛЬСОВ

Rozorinov H.M., **Trush O.V. Research of marketabilities optimum for fast-actings foot-pace engine management of occasion of rotation of CD, DVD.** Marketability by the step of rotor of engine optimum or quazi optimum on a fast-acting management is probed due to the special organization of multichannel pulser. Two variants of foot-pace engine management are examined in the article, in one of them the estimation of efficiency is conducted on the mathematical model of foot-pace engine, in the second from experimental data.

Keywords: FOOT-PACE ENGINE. FAST-ACTING MANAGEMENT, MULTICHANNEL PULSER

Вступ. Одним з ефективних і перспективних приводів мікромашин і приладів, які вимагають підвищеної точності позиціонування, є кроковий двигун (КД). У сучасних системах автоматичного управління для забезпечення гарантованого переміщення ротора крокового двигуна на один крок використовуються управляючі імпульси із збільшеною тривалістю, або спеціальні режими роботи. Наприклад, використання мікрокрокового режиму