Снижение усиления беспроводного канала $G_к$ и, как следствие, увеличение мощности несущей $P_н$ на входе ПРМ позволит, с одной стороны, повысить надежность работы канала, а с другой – снизить угрозу атаки на физический уровень. Для реализации атаки злоумышленнику необходимо располагать передатчик или приемник максимально близко к атакуемой сети, что является основным недостатком атаки на физический уровень.

Проведем оценку работоспособности защищенного беспроводного канала связи в реальных условиях эксплуатации, построенного на основе аппаратуры широкополосного фиксированного радиодоступа Tsunami MP.11 Model 5054-R.

Беспроводной канал имеет следующие технические характеристики в диапазоне частот работы 5,7 ГГц: P_t = 18 дБ, P_r = –76 дБ (для скорости передачи 36 Мбит/с), G_t = 23 дБ, для максимальной длины STP кабеля Cat 5 (≤ 100 м) принимаем $L_t = L_r$ = 3 дБ.

Алгоритм оценки работоспособности беспроводного канала связи заключается в следующем.

1. С учетом (1) и (2) для $К_ш$ = 6 дБ найдем допустимый уровень шумов $P_ш$ на входе ПРМ: $P_ш$ = –76 – 20 + (– 6) = –102 (дБ), $P_ш \le$ –102 дБ.

2. Определим усиление беспроводного канала $G_к$. С учетом выражения (3) получим: $G_к$ = 18 – (–76) = 94 (дБ).

3. С учетом выражения (4) определим допустимый уровень потерь сигнала на радиотрассе: 94 = (3 + L_n + 3) – (23 + 23) (дБ), $L_n \le$ 136 дБ.

4. Определим возможную протяженность беспроводного канала связи по следующей формуле [2, с. 121]:

$$L_n = 101g(\frac{4\pi d}{\lambda})^2,$$

где d и λ – соответственно протяженность канала и длина волны несущего колебания, измеренные в одних единицах.

Для $L_n \le$ 136 дБ $d <$ 26 км.

Для оценки работоспособности беспроводного канала связи в реальных условиях эксплуатации необходимо контролировать уровни несущего сигнала и шумов на входе ПРМ и обеспечивать требуемый запас на затухание $\Delta_к$ сигнала на выходе канала.

Анализ электромагнитной обстановки в местах установки приемных устройств можно проводить встроенными устройствами контроля и измерительными приборами в течение технического обслуживания или регламентных работ элементов ЗТКС и системы в целом.

1. Основы построения систем и сетей передачи информации : учеб. пособие для вузов / В.В. Ломовицкий [и др.] ; под ред. В.М. Щекотихина. М., 2005.

2. Столлингс В. Беспроводные линии связи и сети / пер. с англ. А.В. Высоцкого [и др.]. М., 2003.

УДК 681.324.067

Н.М. Бобович, А.В. Хмарик

ОСОБЕННОСТИ ЗАЩИЩЕННОГО ДОКУМЕНТООБОРОТА В СЭД «ДЕЛО»

Перспективным направлением повышения эффективности деятельности органов внутренних дел является использование в документационном обеспечении управления возможностей и преимуществ электронного документооборота. Работа с документами в электронной форме позволяет однозначно идентифицировать каждый документ; сократить время движения документов и повысить оперативность их исполнения; исключить возможность дублирования документов; находить документ, обладая минимальной информацией о нем; контролировать движение документов по процессам документооборота и принимать управленческие решения, основываясь на данных из отчетов.

Выполнение перечисленных функций возлагается на систему электронного документооборота (СЭД). В качестве такой системы в ОВД используется «ДЕЛО».

СЭД «Дело» представляет собой автоматизированную многопользовательскую систему, которая обеспечивает управление ОВД при выполнении ими своих правоохранительных функций. При этом предполагается, что процесс управления опирается на человекочитаемые документы, содержащие инструкции для сотрудников организации, необходимые к исполнению.

Перемещение в СЭД электронных документов, содержащих конфиденциальную и открытую информацию, по множеству иерархических уровней управления ОВД создает серьезные предпосылки для утраты ценной информации, требует осуществления защищенного электронного документооборота.

Под защищенным электронным документооборотом понимается контролируемое движение электронных документов по регламентированным пунктам приема, обработки, рассмотрения, исполнения, использования и хранения в условиях организационного и технологического обеспечения безопасности как носителя информации, так и самой информации.

Для обеспечения защищенного документооборота в СЭД «Дело» используются специальные встроенные средства, которые выполняют следующие функции:

базовые функции защиты информации для обеспечения минимально необходимого уровня защиты в случае, когда к СЭД не предъявляются особые требования по информационной безопасности (реализуются в со-

ставе стандартной поставки системы «Дело»). К ним относятся средства аутентификации и разграничения прав доступа пользователей к информации;

расширенные функции информационной безопасности для обеспечения защиты данных от внешних угроз, а также целостности и юридической значимости электронных документов, обрабатываемых в СЭД. Эти функции реализованы в виде так называемых опций: «ЭЦП и шифрование», «Защита от несанкционированного доступа», «Мастер паролей» (поставляются отдельно по желанию заказчика).

Базовые функции защиты информации.

Разграничение прав доступа к информации в системе осуществляется на следующих уровнях:

по картотекам – выделенным секторам единого документального массива;

группам документов – в зависимости от их вида, содержания, порядка обработки и т. п.;

грифам доступа к регистрационным карточкам и к прикрепленным файлам – в соответствии с категорией секретности, к которой отнесена содержащаяся в них информация;

кабинетам должностных лиц, где находятся необходимые им для работы документы.

При этом обеспечивается точное соответствие доступных функций и инструментов реальным должностным обязанностям каждого сотрудника.

Для аутентификации пользователей в системе используются два метода – использование паролей пользователей (ввод имени и пароля пользователя при входе в систему) и аутентификация средствами операционной системы (автоматическая аутентифицикация по имени, которое им предъявлено, при запуске операционной системы Windows).

Расширенные функции информационной безопасности.

1. Опция «ЭЦП и шифрование» используется для организации и ведения защищенного электронного документооборота и позволяет подтвердить личность автора или отправителя корреспонденции, а также гарантирует, что в документ после его подписания не были внесены изменения. Опция реализуется интегрированными в систему «Дело» сертифицированными средствам криптографической защиты информации (СКЗИ) – КриптоАРМ, КриптоПро CSP, СигналКом CSP, Верба OW, Домен-К, Авест, Генкей, решения Microsoft.

Применение ЭЦП предполагает наличие Центра управления ключевой системой (ЦУКС) – комплекса программного обеспечения и устройства записи (чтения) носителей, который устанавливается на автономном компьютере, отключенном от линий связи.

Защищенный документооборот организуется двумя способами:

«Корпоративный электронный документооборот» – реализуется криптографическим комплексом «Корпоративный документооборот», который включает: СКЗИ КриптоПро CSP 3.0 или Сигнал-Ком 3.0, система «ДЕ-

ЛО», начиная с версии 8.8.0 (для системы «ДЕЛО» версии 8.6.0 – СКЗИ КриптоПро CSP 2.0);

«Юридически значимый электронный документооборот» – реализуется криптографическим комплексом «Юридически значимый документооборот», который включает: СКЗИ КриптоПро CSP 3.0 или СигналКом 3.0, КриптоАрм СтандартПРО 4.2, система «Дело», начиная с версии 8.8.0.

Кроме поддержки ЭЦП средства криптографической защиты информации, входящие в состав данной опции, обеспечивают шифрование данных, передаваемых по открытым каналам, что позволяет гарантированно защитить конфиденциальную информацию от несанкционированного доступа – прочтения, искажения либо подмены.

2. Защита от несанкционированного доступа:

1) усиленная аутентификация. На основе технологии Windows Single Sign-On осуществляется единая регистрация пользователей и устраняется необходимость дополнительной регистрации в каждом из используемых приложений. Для этих целей используются «eToken» – USB-устройства и смарт-карты, разработанные компанией Aladdin, – средство усиленной двухфакторной аутентификации на основе цифровых сертификатов стандарта X.509 (поддерживает работу с Windows 2000/XP/2003);

2) защита хранилища данных. В СЭД для обеспечения безопасности хранимой информации используется программный продукт Secret Disk Server NG компании Aladdin, который представляет собой систему защиты корпоративных баз и конфиденциальных данных на серверах от несанкционированного доступа, копирования, повреждения, кражи или неправомерного изъятия. Система не только защищает данные, но и скрывает сам факт их наличия на сервере;

3) защита каналов связи при web-доступе. При организации удаленного доступа к данным по web-соединениям пользователи глобальной сети Интернет получают возможность работать с внутренней информацией СЭД, содержащейся в документах. Тем самым возникает опасность несанкционированного доступа к ним, а также компрометации конфиденциальной информации, так как передача данных осуществляется по заведомо недоверенным каналам связи.

Для защиты каналов связи при web-доступе рекомендуется использовать криптографическую защиту каналов web-доступа – SSL.

3. Опция «Мастер паролей» (управление паролями пользователей).

Авторизация пользователей в СЭД обеспечивается программно-аппаратным комплексом, разработанным компанией «Рускард». Кроме того, осуществляется авторизация пользователей при входе в корпоративную сеть и интернет, а также практически в любые Windows-приложения, использующие авторизацию (например, Word, Excel и др.).

Логины и пароли хранятся на специальной смарт-карте, доступ к которой закрывается PIN-кодом. Помимо стандартной смарт-карты памяти

возможно использование процессорной смарт-карты повышенной защищенности (например, интеллектуальной карты).

УДК 681.324.067

Н.М. Бобович, А.В. Шаповалов

ИСПОЛЬЗОВАНИЕ СИСТЕМЫ МОНИТОРИНГА И АРХИВИРОВАНИЯ ПОЧТОВЫХ СООБЩЕНИЙ «ДОЗОР-ДЖЕТ» В СЭД «ДЕЛО»

Отличительной особенностью современного этапа совершенствования документационного обеспечения управления органами внутренних дел Республики Беларусь является внедрение системы электронного документооборота «Дело» и переход на электронный документооборот и технологии дистанционного межведомственного взаимодействия.

Система электронного документооборота (СЭД) «Дело» представляет собой автоматизированную многопользовательскую систему, сопровождающую процесс управления работой ОВД с целью обеспечения выполнения ими основных правоохранительных функций.

Работа с документами в электронной форме позволяет быстро и удобно хранить, обрабатывать и передавать их в рамках СЭД «Дело». Перечисленные функции, как правило, выполняет почтовая система, являющаяся неотъемлемой частью всякого электронного документооборота.

Благодаря таким качествам, как низкая стоимость, простота использования, большое количество пользователей, электронная почта стала одним из распространенных и популярных средств коммуникации.

Однако наряду с многочисленными преимуществами существуют риски, связанные с использованием электронной почты, которые могут привести к значительному снижению эффективности работы ОВД, потере значимой информации.

Основными проблемами, связанными с неконтролируемым использованием электронной почты, являются:

утечка конфиденциальной информации;

передача сообщений неприемлемого содержания;

передача потенциально опасных вложений, вирусов и вредоносных кодов;

передача неприемлемых вложений – большого размера, нежелательного формата и т. д.;

несанкционированные почтовые рассылки («спам»);

ошибочное направление писем;

потери рабочего времени, ресурсов или блокирование почтового сервиса.

В целях реализации корпоративной политики использования электронной почты в части обеспечения информационной безопасности СЭД «Дело» предлагается использовать специализированное программное средство –

систему мониторинга и архивирования почтовых сообщений «Дозор-Джет».

Система «Дозор-Джет» осуществляет мониторинг и контроль всех входящих, исходящих и внутренних почтовых сообщений. При этом анализируются заголовки и структура сообщений, проверяется наличие в тексте сообщения или прикрепленных файлах разрешенных или запрещенных к использованию в почтовых сообщениях слов или последовательностей слов. Результатом мониторинга может стать, например, задержание подозрительных писем.

«Дозор-Джет» позволяет задавать ведомственные правила обработки входящей и исходящей почты в зависимости от тех или иных предопределенных событий, например:

запрет пересылки файлов формата EXE всем, кроме администратора СЭД;

запрет пересылки картинок формата GIF и JPEG отдельным пользователям СЭД;

ограничение на объем и количество присоединенных файлов, направляемых отдельным адресатам;

автоматическое уведомление руководителя подразделения о письмах с определенными пометками или отвечающих поставленным условиям.

В системе реализована гибкая система фильтрации сообщений, что позволяет реализовать практически любую схему прохождения электронной почты.

Например, возможна так называемая отложенная доставка почтового сообщения, когда решение о доставке конечному пользователю принимается только после дополнительного анализа администратором СЭД и другими системами безопасности (проверка на наличие вирусов, контроль массовой рассылки сообщений рекламного характера, наличие неопознанных (закодированных) вложений и пр.).

При попадании в систему «Дозор-Джет» почтовые сообщения проходят процедуру разбора заголовков сообщения (отправитель, получатель, скрытая копия, тело сообщения и пр.) и всей его структуры вне зависимости от количества уровней вложенности. Это позволяет анализировать сообщения, содержащие прикрепленные файлы, а также сообщения, которые были несколько раз перенаправлены корреспондентами.

Процедура анализа разобранных сообщений включает:

определение характеристик сообщения – отправитель, получатель, дата, размер, структура;

определение характеристик вложений – имя, размер, тип, количество;

распознавание форматов вложений – сжатие (архивирование) документов, исполнимых файлов, графических, аудио- и видеофайлов;

анализ текста в заголовках сообщения, теме, теле письма и вложенных файлах.