ИНФОРМАЦИЯ БЕЗ ОПАСНОСТИ

СОВЕРШЕНСТВОВАНИЕ ПОЛИТИКИ ПОЧТОВОЙ БЕЗОПАСНОСТИ РУП «БЕЛПОЧТА»

А.М. ПРУДНИК,
канд. техн. наук,
старший научный сотрудник
кафедры защиты информации
УО «БГУИР»

И.С. ХУДОЛЕЙ,
ассистент кафедры
организации и технологий
почтовой связи
УО «ВГКС»

Защита информации – это целая наука; вопросы безопасности – важная часть концепции внедрения новых информационных технологий во все сферы жизни общества.

Сегодня почтовый сектор претерпевает изменения, являющиеся результатом некоторых внешних влияний, наблюдаемых в почтовой деятельности. Разрабатывая почтовые стратегию и политику, следует принимать во внимание интересы других многочисленных участников сектора.

Во многих странах в соответствии с существующей тенденцией почтовая администрация рассматривается как одно действующее лицо на рынке, имеющем более сложную конъюнктуру.

В большинстве государств существует четкое разделение между национальной почтовой политикой и адекватным регулированием и перспективами эксплуатации для национальных операторов. Несмотря на ярковыраженный курс к интегрированному всемирному почтовому сектору, продолжают сохраняться многочисленные различия вследствие региональной и местной культуры, а также уровня развития.

Необходимость совершенствования политики почтовой безопасности РУП «Белпочта» вызвана следующими основными факторами:

- созданием условий для вступления Республики Беларусь в ВТО;
- переходом на электронный документооборот в почтовой связи;
- определенными требованиями (рекомендациями), которые предъявляют отраслевые или общие, местные или международные стандарты;
- совершенствованием технических средств, используемых в процессе обработки почтовых отправлений и информации;
- перспективой использования информационно-технологических систем почтовой связи в качестве сети передачи финансовой информации;
- необходимостью роста публичных показателей предприятия – позиции в рейтинге, уровня надежности и т. д.

Широкомасштабное использование компьютерной техники и телекоммуникационных систем в рамках территориально-распределенной сети, переход на этой основе к безбумажной технологии в почтовой связи, увеличение объемов обрабатываемой информации и расширение круга пользователей

приводят к качественно новым возможностям несанкционированного доступа к ресурсам и данным информационной системы, к их высокой уязвимости. Поэтому и возникает необходимость в защите этой информации.

Почтовая связь проводит операции с коммерческой информацией своих клиентов и, следовательно, должна обеспечить безопасность этой информации.

Для оптимизации мероприятий, направленных на обеспечение безопасности почтовых отправлений и передаваемой информации, большое значение имеет выбор приоритетных направлений. Это требуется для того чтобы:

- использовать технические и аппаратно-программные средства обеспечения почтовой безопасности с наибольшей эффективностью;
- четко распределять обязанности, которые необходимо закреплять за различными категориями работников объектов почтовой связи;
- защищать почтовые отправления и информацию, наиболее подверженные противоправным действиям со стороны злоумышленников;
- проводить централизацию управления для обеспечения своевременного реагирования на возникающие угрозы безопасности почтовых отправлений и коммерческой информации клиентов почтовой связи.

Если подходить к политике почтовой безопасности более формально, то она видится в форме набора неких требований к функциональности системы обеспечения безопасности почтовых отправлений, закрепленных в ведомственных документах. Однако защиту такой большой информационно-технологической системы, какой обладает РУП «Белпочта» на сегодняшний день, невозможно обеспечить без грамотно разработанной документации по информационной безопасности. Именно она помогает, во-первых, убедиться в том, что ничто важное не упущено из виду, и, во-вторых, установить четкие правила обеспечения безопасности. Только всесторонняя и экономически целесообразная система защиты будет эффективной, а информационная система в этом случае защищенной.

По мере развития РУП «Белпочта» увеличивается ее информационная система. Естественно, что, чем обширнее она становится, чем больше интегрирована с другими системам, тем важнее и труднее обеспечивать ее информационную безопасность. Компонентов становится много, проследить их взаимосвязь сложно, следовательно, увеличивается и количество средств защиты. В такой ситуации основной задачей становится не столько обеспечение безопасности, сколько ее целесообразность и эффективность.

Оказание услуг высокого качества предполагает предоставление гарантий сохранности и безопасности почтовых отправлений. Это, в свою очередь, говорит о целесообразности организации комплексной системы, где важное место занимает защита объектов почтовой связи. Трансформация существующих и появление новых угроз, связанных с переходом на электронный документооборот, вызывает необходимость пересмотра определенных вопросов почтовой безопасности.

В связи с этим можно выделить следующие основные моменты работы в данном направлении:

- анализ источников образования технических каналов утечки информации в объектах почтовой связи;
- четкое категорирование информации, участвующей в почтовом обмене;
- организация многоуровневой защиты объектов, позволяющей модернизировать существующую;
- пересмотр категорий защищенности объектов;
- разработка основных принципов построения интегральных систем защиты объектов почтовой связи;
- применение современных разработок в области защиты информации от утечки по техническим каналам.

В первую очередь следует провести анализ развития методов и систем обеспечения безопасности почтовых отправлений и передаваемой информации; выявить и изучить основные факторы, оказывающие влияние на нарушение безопасности почтовых отправлений на современном этапе развития информационных технологий и перехода к электронному документообороту; провести исследования по основным угрозам безопасности почтовых отправлений и передаваемой информации.

Предлагается классифицировать почтовые отправления и информацию о данных отправлениях по трем основным группам риска нарушения почтовой безопасности.

Первая группа будет включать почтовые отправления и информацию, при нарушении безопасности которых произойдут значительные финансовые потери, будут необходимы существенные людские и информационные ресурсы для преодоления последствий нарушения, а также возникнут предпосылки для потери потенциальных клиентов национального оператора почтовой связи.

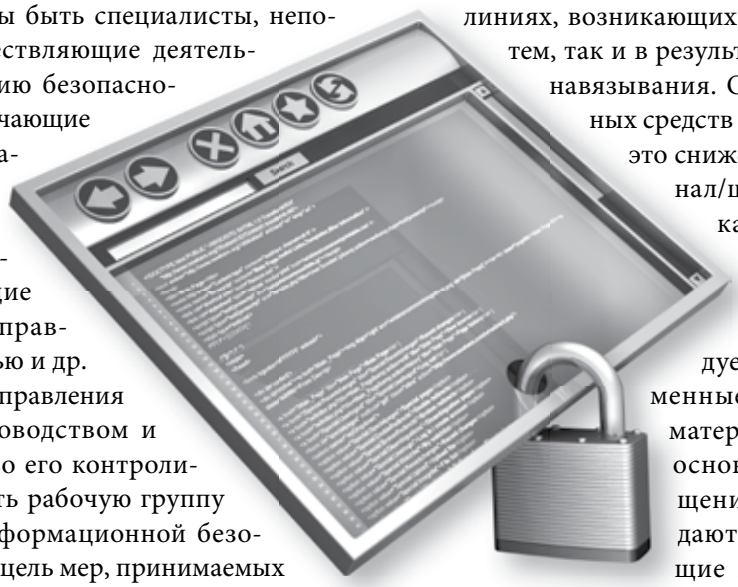
Во **вторую** группу войдут почтовые отправления и информация, при нарушении безопасности которых произойдут незначительные финансовые потери, для преодоления последствий нарушения не будут необходимы существенные людские и информационные ресурсы, однако могут возникнуть

предпосылки для потери потенциальных пользователей услуг почтовой связи и потери авторитета национального оператора почтовой связи.

Третья группа будет включать почтовые отправления и информацию, при нарушении безопасности которых произойдут минимальные финансовые потери, а для преодоления последствий нарушения не понадобится применять людские и информационные ресурсы.

Одним из основных принципов эффективного обеспечения безопасности является вовлеченность руководства в этот процесс. Это важно для того, чтобы все сотрудники понимали, что инициатива обеспечения безопасности исходит не от специалистов по информационной безопасности, а от руководителя организации. Кроме этого, учитывая тот факт, что в настоящее время обеспечение информационной безопасности интересует клиентов и партнеров РУП «Белпочта», подпись главного лица предприятия на основополагающем документе по информационной безопасности гарантирует, что организация серьезно относится к информационной безопасности и пользоваться оказываемыми услугами безопасно.

Также в структуре национального оператора почтовой связи должны быть специалисты, непосредственно осуществляющие деятельность по управлению безопасностью, например обучающие сотрудников компании, разрабатывающие критерии для оценки эффективности, планирующие мероприятия по управлению безопасностью и др.



Так как процесс управления инициируется руководством и именно руководство его контролирует, следует создать рабочую группу по управлению информационной безопасностью. Главная цель мер, принимаемых на управленческом уровне, сформировать программу работ в области информационной безопасности и обеспечить ее выполнение с выделением необходимых ресурсов и контролем за состоянием дел. Основой программы является многоуровневая политика безопасности, отражающая подход предприятия к защите своих информационных активов. Использование информационных систем сопровождается определенной совокупностью рисков, которые должны постоянно анализироваться специальными подразделениями информационной безопасности или системными администраторами (для небольших организаций).

Исходя из того, что значительную роль в производственных процессах почтовой связи играет человеческий фактор, следует обратить внимание на защиту внутренней коммерческой информации от разглашения путем намеренного или ненамеренного прослушивания. Перехват или прослушивание речевой информации может иметь для организации очень серьезные последствия, так как при личном контакте обычно передается информация, которая не записывается на иные носители и является наиболее важной. Также при анализе речевой информации можно определить говорящего и классифицировать данную информацию по важности.

Для защиты информации от утечки по акустическому каналу применяется комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей. Существуют пассивные и активные способы защиты акустической информации.

Пассивные способы предполагают ослабление непосредственно акустических сигналов, циркулирующих в помещении, а также продуктов электроакустических преобразований в соединительных линиях, возникающих как естественным путем, так и в результате высокочастотного навязывания. Основная идея пассивных средств защиты информации – это снижение соотношения сигнал/шум в возможных точках перехвата данных за счет снижения информативного сигнала. Для этого следует использовать современные звукоизолирующие материалы и экраны на их основе для защиты помещений, в которых обсуждаются сведения, содержащие коммерческую тайну. Предпочтение следует отдавать материалам, оказывающим влияние на снижение степени разборчивости речи. Разборчивость речи представляет собой интегральную оценку речевого сигнала и определяется как «степень, с которой речь может быть понята (расшифрована) слушателями». Таким образом, это величина, характеризующая уровень понимания слушателями смысла фраз, способность идентифицировать слова, слоги и фонемы. В соответствии с этим различают виды разборчивости: фразовую, словесную, фонемную и слоговую. Среди многочисленных факторов, влияющих на разборчивость речи, прежде всего можно

выделить следующие: наличие посторонних акустических сигналов, процесс реверберации, параметры тракта звукоусиления. Следует отметить, что при проведении исследований в этой области было установлено, что наибольший эффект достигается при комплексном использовании различных материалов.

Активные способы предусматривают создание маскирующих помех, подавление аппаратов звукозаписи и подслушивающих устройств. Средства активной защиты акустической информации условно можно разделить на две группы: средства акустической защиты помещения и средства собственно акустической защиты речи.

К первой группе относятся средства, обеспечивающие заградительную акустическую помеху вдоль ограждающих конструкций. При этом поддерживается невысокий уровень паразитного акустического шума, что позволяет создать комфортные акустические условия для персонала, но объем контролируемого помещения в этом случае остается не защищенным.

Ко второй группе относятся генераторы акустического шума, располагаемые непосредственно в местах проведения переговоров и своим шумом маскирующие речь участников переговоров.

В результате следования основным требованиям политики почтовой безопасности и сопутствующим документам по обеспечению и управлению безопасности защищенность информационной системы организации достигнет требуемого уровня, сотрудники компании будут осознавать свою роль и вовлеченность в процесс обеспечения безопасности. И, как следствие, требуемые информационные активы станут доступны в нужные моменты времени, изменения будут вноситься только авторизованными пользователями, обеспечивая полную конфиденциальность.