УДК 004.056.5

ЗАЩИТА ИНФОРМАЦИИ ПРЕДПРИЯТИЯ НА УРОВНЕ ЭЛЕКТРОННОЙ ПОЧТЫ

Вадим Евгеньевич Кудряшов
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, обучающийся кафедры информационной безопасности, тел. (953)881-26-16, e-mail: vadkud@inbox.ru

Сергей Николаевич Новиков
Сибирский государственный университет геосистем и технологий, 630108, Россия, г. Новосибирск, ул. Плахотного, 10, доктор технических наук, профессор (совместитель), тел. (913)923-72-34, e-mail: snovikov@ngs.ru

Электронная почта в настоящее время для большинства компаний является основным средством коммуникации, тем более в период пандемии. Переписка необходима для общения внутри самой компании, для обмена данными с партнерами, клиентами, поставщиками, государственными органами и т. д. Ни для кого не секрет, что по электронной почте пересылается масса конфиденциальной информации.

Организация ТОО «Техол-Т» работает на строительном рынке с 1971 года. Для осуществления своей коммерческой деятельности у организации имеется локальная сеть с удаленным доступом. Общение с заказчиками и надзорными органами (федеральная налоговая служба, центр занятости и т.д.) в основном происходит через электронную почту. В связи с этим возникает необходимость провести анализ защищенности информации, которая передается через электронную почту, выявить уязвимости и разработать рекомендации по защите.

В этой связи цель работы – разработка эффективной защиты информации на ТОО «Техол-Т» на уровне электронной почты.

Ключевые слова: электронная почта, шифрование, фишинг, социальная нженерия, коммерческая тайна, персональные данные

PROTECTION OF COMPANY'S INFORMATION AT THE E-MAIL LEVEL

Vadim E. Kudryashov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, Student, Department of Information Security, phone: (953)881-26-16, e-mail: vadkud@inbox.ru

Sergei N. Novikov
Siberian State University of Geosystems and Technologies, 10, Plakhotnogo St., Novosibirsk, 630108, Russia, D. Sc., Professor (part-time), phone: (913)923-72-34, e-mail: snovikov@ngs.ru

E-mail is the main means of communication for most companies, especially during a pandemic. Correspondence is necessary both for communication within the company itself and for exchanging data with partners, customers, suppliers, government agencies, etc. It's a lot of confidential information is sent via corporate e-mail: contracts, invoices, information about the company's products and prices, financial indicators, etc.

“Tehol-T” organization has been operating in the construction market since 1971. To carry out its commercial activities, the organization has a local network with remote access. Communication with customers and supervisory authorities (federal tax office, employment center, etc.) mainly takes place through e-mail. In this regard, it is necessary to analyze the security of information that is transmitted via e-mail, identify vulnerabilities and develop recommendations for protection.

Keywords: email, encryption, phishing, social engineering, trade secrets, personal data

Введение

Организация ТОО «Техол-Т» работает на строительном рынке с 1971 года. Для осуществления своей коммерческой деятельности у организации имеется локальная сеть с удаленным доступом. Общение с заказчиками и надзорными органами (федеральная налоговая служба, центр занятости и т.д.) в основном происходит через электронную почту. В связи с этим возникает необходимость провести анализ защищенности информации, которая передается через электронную почту, выявить уязвимости и разработать рекомендации по защите.

В этой связи цель моей работы – разработать рекомендации по эффективной защите информации на ТОО «Техол-Т» на уровне электронной почты.

Для достижения данной цели в работе решаются следующие задачи:

– определение объекта информатизации;

– составление модели нарушителя;

– анализ существующих инструментов для защиты конфиденциальной информации, передаваемой по электронной почте;

– разработка рекомендаций по защите электронной почты ТОО «Техол-Т».

Методы и материалы

В работе использовались следующие материалы:

– банк данных угроз безопасности ФСТЭК [1];

– список литературы, рекомендованный научным руководителем;

– товарищество с ограниченной ответственностью «Техол-Т» [9];

– местонахождение предприятия – Республика Казахстан, г. Темиртау, Восточная промзона [9];

– численность производственно-промышленного персонала по состоянию на начало 2021-го года – 127 человек [9];

– структура предприятия;

– внешние и внутренние информационные потоки организации;

– структура локальной сети организации;

– ТОО «Техол-Т» использует корпоративную почту от компании «Mail.ru Group»;

– для входа в электронную почту на предприятии используется браузер Google Chrome;

– на персональных компьютерах предприятия установлена ОС Windows 10 Pro.

Для защиты почты были использовано следующее программное обеспечение:

– GPG4Win для шифрования содержания отправляемых писем внутри организации [6];

– LanAgent для контроля входящих и исходящих писем сотрудников организации [7].

Результаты

С помощью программы GPG4Win была реализована возможность шифрования по алгоритму RSA писем сотрудников для передачи конфиденциальной информации внутри предприятия (рис. 1) [8].

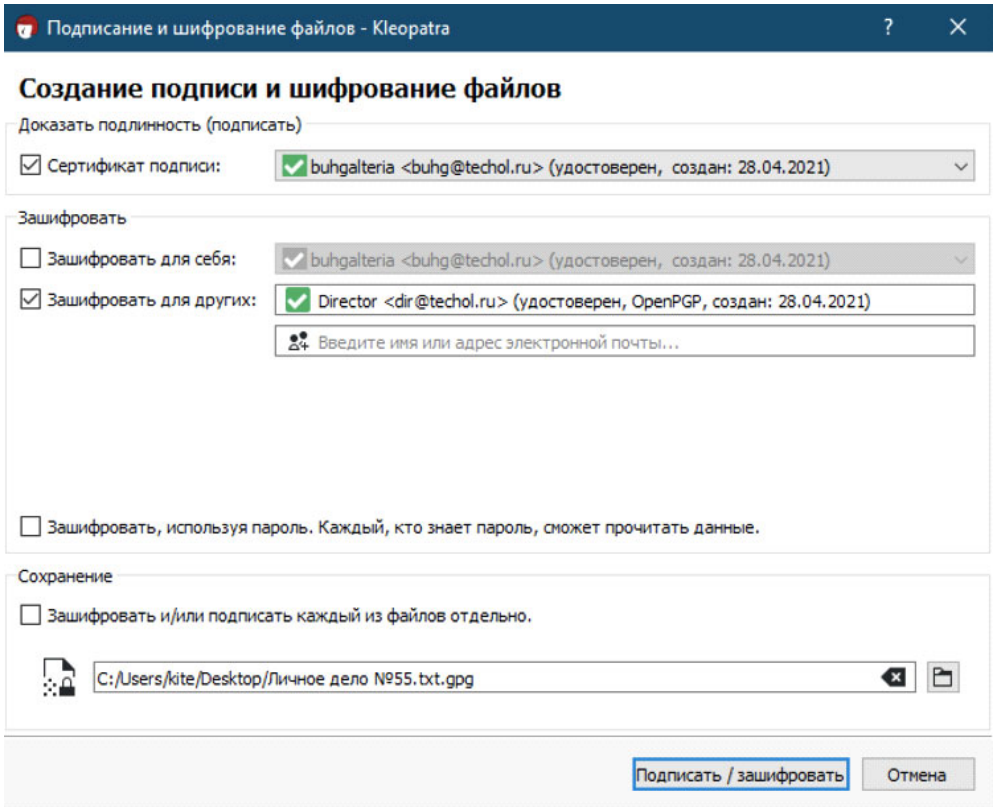

Рис. 1. Пример шифрования письма от бухгалтерии к директору

С помощью программы LanAgent была реализована возможность контроля входящих и исходящих писем сотрудников (рис. 2).

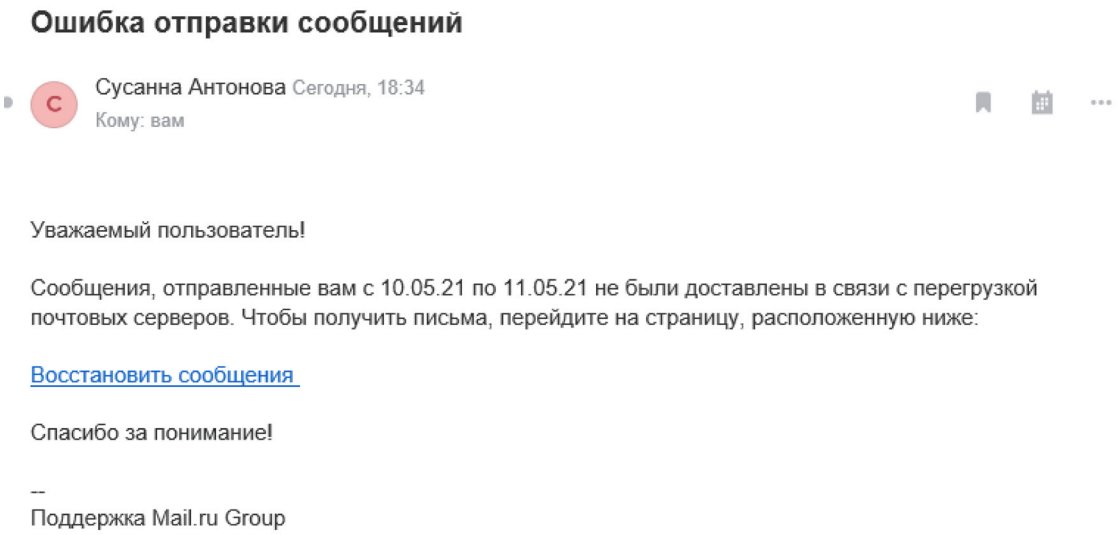

Рис. 2. Фишинговое письмо, пришедшее на почту сотрудника бухгалтерии

Обсуждение

Проанализировав конфиденциальную информацию, обрабатываемую на предприятии, входящие и исходящие информационные потоки на уровне электронной почты и состояние защищенности почты можно сделать вывод, что на предприятии обрабатывается достаточно много конфиденциальной информации. Она ежедневно отправляется по электронной почте, как внутри предприятия, так и за его пределы. Служба безопасности обеспечивает неполную защиту на уровне почты от фишинга, спама и социальной инженерии с помощью инструктажей сотрудников. Такие угрозы как спуффинг и перехват пакетов, могут быть реализованы злоумышленником без особых сложностей [10]. Это может нанести финансовый ущерб предприятию. В данной работе даны рекомендации по минимизации рисков безопасности электронной почты.

Заключение

Одно из направлений развития современных предприятий — информатизация. Использование современных информационных технологий (в том числе и электронной почты) позволяет существенно повысить эффективность производственных и управленческих процессов. Но вместе с применением этих технологий возникает проблема обеспечения комплексной защиты информации, которая может быть отнесена к конфиденциальной [3].

В данном исследовании были рассмотрены основные угрозы информационной безопасности предприятия ТОО «Техол-Т» на уровне электронной почты. Для этого была дана характеристика организации, описана ее структура, проведен анализ организации защиты конфиденциальной информации, проведен ана-

лиз информационных потоков предприятия и защищенности ее локальной сети. Также была разработана модель нарушителя в соответствии с требованиями Федерального законодательства [5].

На основе полученных результатов были разработаны рекомендации по защите информации, передаваемой по электронной почте.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Банк данных угроз безопасности информации [Электронный ресурс]. URL: https://bdu.fstec.ru/vul (дата обращения: 10.04.2021).
2. Гафнер, В.В. Информационная безопасность: учеб. пособие. – Феникс, 2017. – 324 с.
3. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты / В. Домарев // М.: ТИД Диа Софт. – 2006. – 688 с.
4. Кузнецов А. А. Защита деловой переписки (секреты безопасности) / А. Кузнецов // М.: Экзамен. – 2008. – 239 с.
5. Методика определения угроз безопасности информации в информационных системах [Электронный ресурс]. URL: https://fstec.ru/component/%20attachments/download/812 (дата обращения: 10.04.2021).
6. Официальный сайт программного обеспечения «GPG4Win» [Электронный ресурс]. URL: https://www.gpg4win.org (дата обращения: 25.04.2021).
7. Официальный сайт программного обеспечения «LanAgent» [Электронный ресурс]. URL: https://lanagent.ru (дата обращения: 26.04.2021).
8. Панасенко С. Алгоритмы шифрования. Специальный справочник / С. Панасенко // М.: БХВ-Петербург. – 2017. – 576 с.
9. Сайт предприятия ТОО «Техол-Т» [Электронный ресурс]. URL: http://www.tehol.kz/index.php (дата обращения: 01.04.2021).
10. Тимошенков А., Современные угрозы и защита электронной почты. 2008. – [Электронный ресурс]. // Журнал «Information Security» : официальный сайт. – URL: https://lib.itsec.ru/articles2/Oborandteh/sovremennie-ugrozi-i-zaschita-elektronnoi-pochti (дата обращения: 10.04.2021).