УДК 004.056

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА: УГРОЗЫ И СПОСОБЫ ЗАЩИТЫ

Е. Л. Пищалова

Белорусский государственный экономический университет,
Партизанский проспект, 22а, 220070, Минск, Беларусь, lmersee@yahoo.com,
Научный руководитель: Л. С. Черепица, ассистент кафедры информационных технологий

Защита информации – залог успешности бизнеса. Утечка паролей, данных о клиентах или транзакциях может привести к большим финансовым потерям и ущербу репутации фирмы. Доклад подчеркивает важность информационной безопасности для предприятий, обращая внимание на внешние и внутренние угрозы – от DDoS-атак до намеренных действий сотрудников. Для обеспечения безопасности данных необходимо применять комплексный подход, включающий в себя технические меры (шифрование, брандмауэры, антивирусное программное обеспечение), организационные меры (обучение сотрудников, разработка политики безопасности) и физические меры (контроль доступа к серверам, защита от несанкционированного доступа).

Ключевые слова: информационная безопасность бизнеса; утечка информации; ведение бизнеса; способы защиты бизнеса; защита данных; защита веб-сайтов.

Информация, такая как пароли, номера счетов, данные о транзакциях, отчеты, контакты клиентов и история покупок представляет собой ценность для любого бизнеса. Если бывший сотрудник передаст эту информацию конкурентам или она попадет в сеть из-за действий злоумышленника – это может привести к финансовым убыткам и негативно отразиться на репутации компании. Кроме того, существует риск получения штрафов со стороны государства. Важно знать меры, которые компании могут принять для обеспечения информационной безопасности и предотвращения финансовых потерь, ущерба репутации и штрафов со стороны государства.

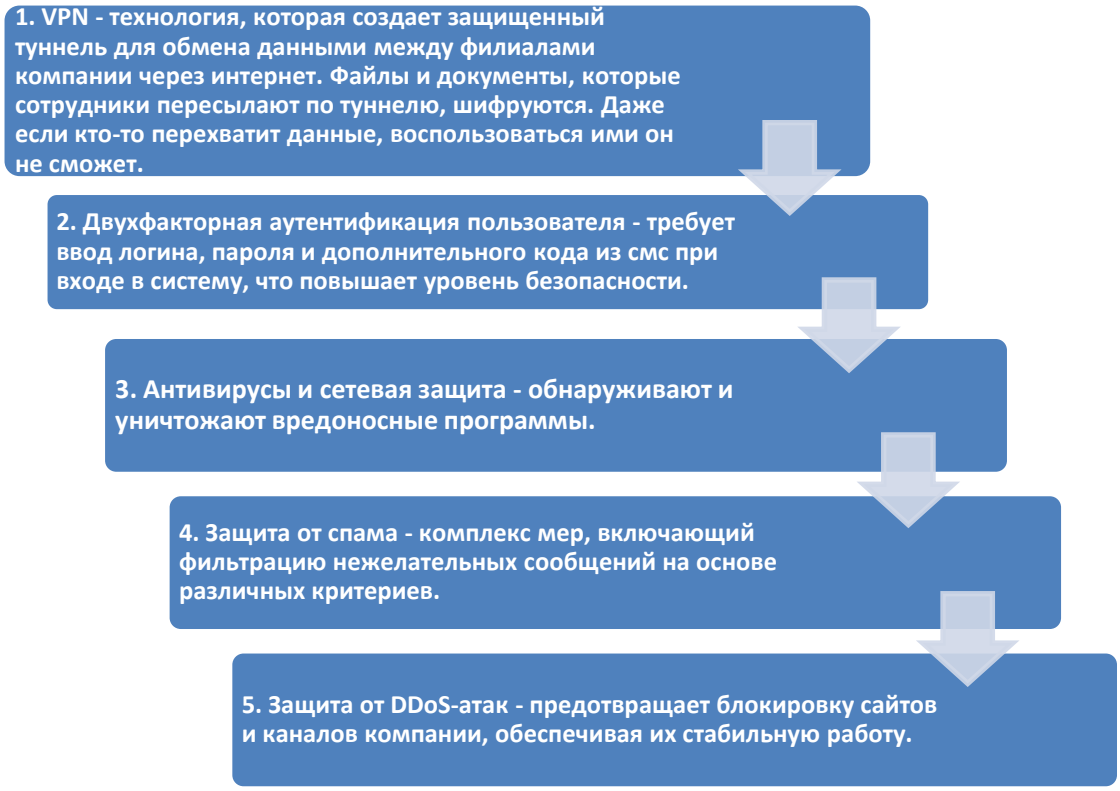
Существуют внешние и внутренние информационные угрозы. Внешние исходят от роботов, мошенников (фишинг и социальная инженерия), хакеров, вредоносного программного обеспечения (ПО), к которым относятся вирусы, троянские программы, шпионское ПО. Самый распространенный пример внешней угрозы – DDoS-атака (от англ. *Distributed Denial of Service*). DDoS-атака выглядит так, как будто бизнес-сайт одновременно пытаются открыть тысячи пользователей. Из-за большого количества запросов сервер, на котором хранятся файлы сайта, не успевает обрабатывать их и периодически выходит из строя. DDoS-атаки могут привести к отказу в обслуживании сайта и потере доходов. DDoS-атаки могут иметь различные цели: конкуренты могут использовать их для отключения сайта, мошенники – для вымогательства выкупа у владельцев ресурсов.

Внутренние угрозы могут быть:

- случайными (из-за ошибок сотрудников);
- намеренными (когда сотрудники намеренно нарушают безопасность, забирая с собой после увольнения часть клиентской базы или продавая ее конкурентам).

Так, информационная безопасность предприятия включает в себя защиту файлов, систем, программ и хранилищ от несанкционированного доступа. Ее цель – предотвратить хищение данных, заражение вирусами и уничтожение информации на серверах. Информационная безопасность требует комплексного подхода, включающего программы, технологии и их настройки, а не только установку антивируса.

Способы защиты, которые используются для защиты от внешних угроз (на рисунке):



Способы защиты от внешних угроз

Однако каждая компания использует собственный комплекс мер. Например, чтобы защититься от угроз со стороны сотрудников, применяют:

- Разграничение доступа: каждому сотруднику в офисе присваивают определенную роль. Доступ к работе с файлом открывается, если это входит в задачи сотрудника. То же самое касается программ. Сотрудники пользуются ими, если это необходимо для работы.

- DLP-система. Это программа, которая отслеживает и блокирует попытки передать файлы офисных систем третьим лицам. Допустим, сотрудник пытается переслать архив с корпоративной почты на личную. DLP-система заметит это и заблокирует отправку. Программу можно настроить так, чтобы она реагировала на любые подозрительные действия.

Конфиденциальность важна для любой организации. Иногда последствия хищения данных могут быть катастрофическими. Каким организациям особенно важна информационная безопасность: финансовым учреждениям, дата-центрам, интернет-магазинам, разработчикам программного обеспечения, хранилищам финансовых данных клиентов и операторам персональных данных. Шаги для обеспечения безопасности информации на предприятии включают наличие специалиста по информационной безопасности, выбор средств защиты и проведение инструктажа среди сотрудников. Однако, чем крупнее компания, тем сложнее задачи и выше требования к информационной безопасности.

Библиографические ссылки

1. Зонин Н. А., Кашпаров Д. В. Система управления моделью повышения конкурентоспособности малого предпринимательства / Молодой ученый. 2014. №7-1 (66). 10 с.

2. Гринберг Дж., Бэйрон Р. Организационное поведение: от теории к практике / Пер. с англ. О.В. Бредихина, В.Д. Соколова. М.: ООО «Вершина», 2004. 912.