К вопросу об обеспечении информационной безопасности бизнеса при использовании систем электронной бухгалтерской отчетности

УДК 004.056.53

Максим Кобрин[1]

Харьковский национальный университет радиоэлектронники,
[1]kobrin.law@gmail.com

Для обмена электронными документами бухгалтерской отчетности, предприятия используют сертифицированные онлайн-сервисы. С помощью этих сервисов происходит подача бухгалтерской отчетности в органы государственной налоговой службы и обмен первичными документами между контрагентами. Например, в Украине большое распространение получили такие сервисы как, iFin, Арт-звит, Соната, Медок. Каждый из перечисленных сервисов является частью информационной системы (ИС) компании и дает функциональный ответ на функциональный запрос ИС (Рисунок 1). Каждый сервис имеет свои ограничения, достоинства и недостатки.

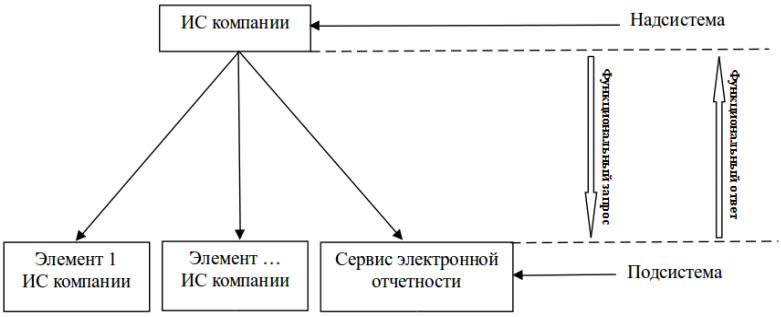

Рис. 1. ИС компании

Система электронной бухгалтерской отчетности (СЭБО) имеет доступ к критической информации компании. С другой стороны, СЭБО является частью ИС контролирующих органов и взаимодействующих с ней контрагентов. Компрометация системы может нанести ущерб всем пересекающимся ИС. На примере вирусных атак 2017 года (май – июнь) видно, что доверенные сервисы могут стать причиной компрометации и значительных повреждений информационных активов (ИА) компании.

Обеспечение безопасности ИА, как правило, носит приоритетный характер в управлении безопасностью предприятия.

Высокий уровень развития информационных технологий позволяет злоумышленникам находить уязвимости в процедуре работы СЭБО и использовать их для совершения преступлений в этой системе.

Для минимизации рисков при использовании СЭБО и обеспечения безопасности ИА, необходимо адаптировать систему информационной безопасности (СИБ) компании, с учетом новых факторов. СИБ должна быть оптимизирована на защиту от проникновения и работу инструментов

злоумышленника в информационной системе компании-жертвы. Классификация видов вредоносного воздействия приведена на рисунке 2.

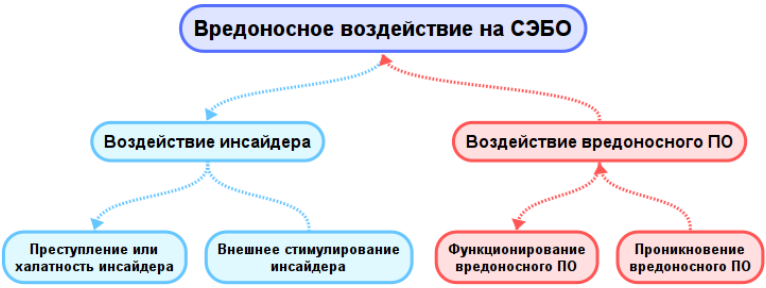

Рис. 2. Классификация видов вредоносного воздействия на СЭБО

С помощью метода системологического анализа было проведено исследование факторов, влияющих на управление информационной безопасностью (ИБ) предприятия, при условии пересечения ИС предприятия, контролирующих органов (государственной налоговой службы) и контрагентов предприятия. В связи с тем, что СЭБО присвоен статус доверенного процесса и нет возможности обеспечить на достаточном уровне ИБ системы, необходимо ограничить возможность влияния СЭБО на ИС предприятия. На основе результатов исследования был разработан ряд практических мер, направленных на оптимизацию СИБ компании, а именно, мер, обеспечивающих снижение вероятности реализации рисков при работе в СЭБО: 1) Объединение устройств СЭБО в отдельную сеть; 2) Использование ОС Linux; 3) Использование надежного антивирусного ПО с обновленными сигнатурами; 4) Использование учетной записи пользователя с ограниченными возможностями.

Предложенный в данной работе комплекс мер, был реализован на практике в системе менеджмента информационной безопасности восьми торговых компаний в Украине, в период реализации атак вируса «Petya» в 2017 г.

Таким образом, можно сделать следующие выводы: 1) Действия злоумышленников в СЭБО – это реальная угроза для юридических и физических лиц. Реализация угроз может привести к остановке основного бизнес-процесса компании; 2) Для снижения вероятности реализации угрозы необходимо использовать системный подход. Система СЭБО является подсистемой ИС организации; 3) Классификация вредоносного воздействия на СЭБО позволяет определить основные направления обеспечения ее безопасности и на их основе разработать практических меры, направленные на снижение вероятности возникновения инцидентов ИБ; 4) Предложенные меры легко реализуемы, не требуют значительных инвестиций, обеспечивают приемлемый уровень безопасности ИС организации и способствуют повышению конкурентоспособности компании.