А. С. ТРУБЧИК
(г. Гомель, Белорусский торгово-экономический
университет потребительской кооперации)
Науч. рук. **Н. В. Яцевич**,
канд. экон. наук, доц.

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В БИЗНЕСЕ

Актуальность исследования информационной безопасности организации обусловлена тем фактом, что именно информация является одним из наиболее важных активов любой организации или фирмы, которая требует высокого уровня защиты. В работе любой организации участвует определенное количество конфиденциальной информации, которая в любой момент может подвергнуться изменению или удалению от рук злоумышленника, что окажет существенное влияние на эффективность бизнес-процессов. Информационная безопасность предприятия объединяет системы безопасности, операций и внутреннего контроля для обеспечения доступности, целостности и конфиденциальности данных и различных процедур работы в организации. Эти факторы должны быть обеспечены в совокупности, например, если информация является целостной и конфиденциальной, однако недоступной для авторизованных пользователей, то она считается бесполезной. Потому на сегодняшний день мы можем наблюдать, что интерес к обеспечению информационной безопасности не только не снижается, но и ежедневно растёт как среди обычных пользователей, так и среди специалистов компаний.

Таким образом, информационная безопасность – это сохранение и защита информации, а также ее важнейших элементов, в том числе системы и оборудование, предназначенные для использования, сбережения и передачи этой информации. Из данного определения следует и главная цель информационной безопасности – обеспечение и поддержание защиты всех информационных данных для предотвращения возможных попыток завладеть информацией со стороны злоумышленников, которые могут стать причиной потери данных или же внезапного их изменения, что может стать причиной негативных последствий [1].

Итак, существует три главных принципа, которым должна соответствовать любая информационная система:

1 Конфиденциальность. Под этим термином понимают реализацию контроля для обеспечения высокого уровня безопасности данных, ресурсов и информации компании на различных этапах бизнес-операций, чтобы предотвратить нежелательное или несанкционированное раскрытие. Конфиденциальность должна иметь регулярный характер как в самой организации, защищающей данную информацию, так и во время транзита через сторонние организации, независимо от вида данной информации.

2 Целостность. Целостность отвечает за обеспечение зависимости в структуре формирования информации для гарантии предотвращения её искажения.

3 Доступность. Обеспечение надежного и эффективного доступа к авторизованной информации гарантирует данный принцип. Сетевая среда должна вести себя предсказуемым образом, чтобы при необходимости безо всяких проблем получить полный доступ к интересующей информации или же данным. Любая система не идеальна и всегда имеется шанс сбоя её работы, таким образом, восстановление системы после подобной ситуации – крайне важный фактор в отношении доступности информации. Потому при подобной проблеме именно доступность должна обеспечить быстрый и удобный доступ к информации уполномоченных лиц.

Естественно, просто знать данные принципы и придерживаться их – недостаточно. Для полноты картины нужно знать конкретные виды угроз в сторону информационной безопасности, что даст возможность выбрать инструмент для борьбы с возникающими опасными ситуациями и обеспечить достаточный уровень защиты. На данный момент поэтапный подход к построению системы защиты информации является наиболее корректным. Состоит он из трёх этапов [2]:

Этап 1 позволяет определить основные требования по информационной безопасности для вашей организации через детальное изучение инфраструктуры.

В самом начале, чтобы добраться до точки информационной безопасности, требуется разобраться с тем, где хранится наиболее важная информация, какова структура сети компании, с каким программным обеспечением ведётся работа, и какие онлайн-ресурсы использует персонал компании. Невозможно обеспечить достаточный уровень информационный безопасности, не имея никаких сведений о том, что конкретно предстоит защищать и в какую сторону могут быть направлены атаки со стороны злоумышленников.

Этап 2 фокусируется на обеспечении основных требований безопасности и обучении персонала основам информационной безопасности, поскольку чаще всего работа сотрудников состоит в использовании или редактировании данных и информации.

Сотрудники – наиболее важная часть любого предприятия, ведь в большинстве случаев их работа связана непосредственно с информацией. Защита информации не может быть обеспечена исключительно за счёт программного обеспечения, обучение работников поможет системам организации работать с минимальными рисками потери данных и вывода систем из строя. На этом этапе сотрудников стоит обучить, желательно, не только основам информационной безопасности, но и углублённым знаниям о возможных угрозах и методах борьбы с ними, включая работу с прикладными программными средствами, отвечающими за защиту систем от внешних атак. Никогда не стоит пренебрегать антивирусным программным обеспечением, сэкономив время или же средства на их установке можно потерять значительно больше.

Этап 3 состоит в подготовке организации к всевозможным инцидентам в сфере информационной безопасности, ведь угрозы могут иметь глобальный характер и без своевременного реагирования вся деятельность организации будет поставлена под удар.

После создания прочного фундамента информационной безопасности необходимо подумать о механизмах реагирования на инциденты. Как бороться с инцидентами и что делать после? Вот главная цель данного этапа, ответ на который – резервные копии. Резервная копия поможет восстановить работоспособность всех систем и вернуть все утерянные, случайно или намеренно, данные. Многие не думают о данном аспекте, иг- норируя его, однако никогда нельзя быть защищённым в полной мере и именно на этот случай полноценная копия системы будет спасательным кругом для любой организации.

Итак, безопасность информационных систем организаций является очень актуаль- ной проблемой на сегодняшний день. Существует множество угроз и средств борьбы с ними, однако не всё можно решить одним только программным обеспечением. В обес- печении безопасности информационным системам стоит уделить внимание всей ин- фраструктуре организации, уровню подготовки персонала в критичных ситуациях, а также наличию системы резервного копирования всех данных на случай утери данных.

Список использованной литературы

1 Информационная безопасность [Электронный ресурс]. – 2020. – Режим доступа: https://pirit.biz/reshenija/informacionnaja-bezopasnost. – Дата доступа: 05.02.2020.

2 Рекомендации по информационной безопасности для малого и среднего бизнеса [Электронный ресурс]. – 2020. – Режим доступа: https://habr.com/ru/post/348892/. – Дата доступа: 05.02.2020.