УДК 334

ОЦЕНКА ЭФФЕКТИВНОСТИ СРЕДСТВ И МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ КОМПАНИЙ

Я. О. Азарко

студент экономического факультета, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: karachun@bsu.by

Научный руководитель: **И. А. Карачун**

кандидат экономических наук, доцент, заведующий кафедрой цифровой экономики, Белорусский государственный университет, г. Минск, Республика Беларусь, e-mail: karachun@bsu.by

В статье изучены современные задачи, методы и средства защиты информации; политики и стандарты безопасности информационных систем, а также проведен их сравнительный анализ; оценена эффективность применяемых мер по обеспечению информационной безопасности на предприятии; разработаны и рекомендованы мероприятия по совершенствованию.

Ключевые слова: информационная безопасность; защита информационных ресурсов; угрозы.

EVALUATION OF THE EFFICIENCY OF MEANS AND METHODS FOR COMPANIES INFORMATION PROTECTION

Ya. O. Azarco

student of the faculty of economics, Belarusian State University, Minsk, Republic of Belarus, e-mail: karachun@bsu.by

Academic supervisor: **I. A. Karachun**

PhD, associate professor, head of the department of digital economy, Belarusian State University, Minsk, Republic of Belarus, e-mail: karachun@bsu.by

The article studies modern tasks, methods and means of information protection; information systems security policies and standards, as well as their comparative analysis; the effectiveness of the measures taken to ensure information security at the enterprise was evaluated; measures for improvement are developed and recommended.

Keywords: information security; protection of information resources; threats.

С каждым годом фиксируется всё больше случаев угроз и атак. Это является важным признаком растущей значимости кибер- и информационной безопасности для организаций и граждан во всем мире. Следовательно, существование подобных угроз и атак показывает потребность в улучшении осведомленности и понимания информационной безопасности и поиска пути к более эффективному обеспечению безопасности, смягчению последствий и повышению устойчивости к угрозам. Также актуальной темой является разработка и внедрение новшеств, которые могут поспособствовать улучшению и

повышению уровня защищенности пользователей, а также различных организаций, которые тем или иным способом связаны с киберпространством.

Информационная безопасность относится к процессам и методологиям, которые разработаны и реализованы для защиты печатной, электронной или любой другой формы частной и конфиденциальной информации или данных от несанкционированного доступа, неправильного использования, раскрытия, уничтожения, изменения или нарушения. Информационная безопасность защищает конкретного пользователя и его личную информацию [1]. Проведя анализ уровня информационной безопасности предприятия УП «Агробизнесконсалт» был сделан вывод о том, что уровень защищенности информации является средним. На данное заключение повлиял проведенный анализ информационных активов предприятия и анализ уязвимости и угроз. Специфика работы компании подразумевает высокий уровень информационной безопасности вследствие работы с клиентами. Разработанные организационные меры и внедряемые программно-аппаратные средства обеспечения информационной безопасности на предприятии УП «Агробизнесконсалт» [2] являются эффективными и несут за собой как финансовую, так и репутационную выгоду. Суммарное значение ресурса, выделяемого на защиту информации исходя из расчетов, составляет 56 734 белорусских рублей. Данная стоимость включает в себя следующий перечень организационных и инженерно-технических мероприятий: закупка утвержденных руководством средств обеспечения информационной безопасности; монтаж и установка аппаратных и программных средств защиты; разработка, настройка и отладка установленных средств информационной безопасности; проведение занятий по обучению и использованию данных средств защиты информации с сотрудниками отдела; контроль и мониторинг работоспособности системы защиты; организация специального делопроизводства для конфиденциальной информации, устанавливающего порядок подготовки, использования, хранения, уничтожения и учета документированной информации; расходные материалы; выполнение плановых мероприятий администратора; физическая охрана помещений, где установлены системы защиты информации; своевременное обслуживание программных и аппаратных средств защиты информации.

Несмотря на срок окупаемости в 6,67 лет, рассмотренные мероприятия позволят в значительной степени минимизировать риски и угрозы информационной безопасности, и в дальнейшем предприятие сможет избежать потери клиентов и ухудшения собственной репутации по причине возможных инцидентов. В свою очередь, установка системы защиты информации по стандарту ISO/IEC-27014 [3] позволит упростить бизнес-процессы с иностранными лицами, инициирует обеспечение информационной безопасности в масштабах всей организации, внедрит риск-ориентированный подход в процесс принятия решений, поможет предприятию определить направления инвестиционных решений, обеспечит соответствие внутренних и внешних требований, сформирует культуру, обеспечивающую безопасность, что в свою очередь поспособствует увеличению клиентской базы.

Библиографические ссылки

1. Alsmadi Izzat M., Karabatis G. Information Fusion for Cybersecurity Analytics. – New York; Crown Business, 2017. – 379 p.

2. Белагротур: отдых в Беларуси [Электронный ресурс]. – URL: https://belagrotur.by/ (дата обращения: 10.09.2022).

3. Prasad R. Cyber Security the Lifeline of Information and Communication Technology. – New York: Aalborg University Ctr for TeleInFrastruktur, 2019. – 295 p.