ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ЭЛЕМЕНТ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

И. С. Русакович, Т. А. Бокунович

Белорусский государственный университет, г. Минск;
mc3po4ki@gmail.com; happymahana@gmail.com;
науч. рук. – Н. И. Шандора

В статье обосновывается актуальность создания качественной системы информационной безопасности, а также обозначается её роль в создании условий экономической безопасности. Приведена классификация угроз информационной безопасности. Рассмотрены существующие мероприятия по защите информации и раскрываются наиболее частые причины её утечки.

Ключевые слова: информационная безопасность; экономическая безопасность; угрозы информационной безопасности; защита информации; причины утечки информации.

Одним из ключевых качественных отличий современного этапа развития общества и экономики можно назвать всеобщую информатизацию. Благодаря значительной для успешного функционирования и развития предприятия роли накопления, обработки и использования информации, она стала одним из ключевых управленческих ресурсов. Возникает необходимость защиты источников информации, методик её обработки и самих ресурсов от несанкционированного доступа к ним и их изменению. Защищённая информация создаёт условия для заключения более выгодных контрактов с контрагентами, позволяет предприятию иметь значительно более высокий уровень конкурентоспособности и повысить уровень доходов [1]. Это устанавливает и подтверждает роль грамотной системы информационной безопасности в создании условий экономической безопасности предприятия [2].

На данный момент не существует общепризнанного определения понятий «экономическая безопасность» и «информационная безопасность». Критерии их определения зависят от социально-экономических факторов, в среде которых проводится анализ с их использованием. При выделении общих черт всевозможных определений этих понятий можно представить их следующим образом:

- экономическая безопасность – состояние среды деятельности предприятия, в котором она защищена от негативных дестабилизирующих факторов внешней и внутренней среды, способных повлиять на осуществление его социально-экономических функций и интересов;
- информационная безопасность – состояние информационной среды предприятия, в котором она защищена от негативных

дестабилизирующих факторов внешней и внутренней среды, способных каким-либо образом повлиять на сохранность основных свойств имеющейся информации [3].

Объективная необходимость в создании состояния информационной безопасности возникает в результате ряда факторов. Первым фактором, упомянутым ранее, является возросшая роль информации в деятельности предприятия. В условиях информационного общества информационные технологии нашли широкое использование в производстве, например, в постепенном переходе от бумажного документооборота к цифровому. Быстрое развитие информационных технологий привело к повсеместности компьютерных средств и объединению их в сети, что в разы облегчает задачи обработки, обмена и доступа к информации. Важно заметить, что простота доступа распространяется также на рыночных конкурентов и других лиц, которые могут использовать информацию предприятия в противоправных целях. Информация получила экономическую роль – стала ресурсом, товаром и услугой. Возник сектор производства информации, в котором задачи информационной безопасности имеют ещё большее значение. Эти факторы обусловили значительный рост заинтересованности организаций в создании комплексных систем информационной безопасности.

При неграмотной организации условий информационной безопасности создаётся среда для появления её угроз – событий, действий, процессов и явлений, которые могут привести к утрате конфиденциальности, целостности и/или доступности информации. Угрозы информационной безопасности можно классифицировать в зависимости от задействованного аспекта информационной безопасности, задействованной части информационной системы, преднамеренности возникновения угроз и других, менее часто используемых, признаков (табл.) [2].

Непреднамеренные угрозы достаточно хорошо изучены и методы их предотвращения и минимизации ущерба в случае их возникновения тщательно разработаны, но при этом их возникновение всё равно влечет за собой значительные потери. Преднамеренные угрозы постоянно увеличиваются в числе и качественном составе, что связано с динамичностью информационной среды предприятий [2].

Защитой информации называется комплекс мероприятий, направленный на обеспечение целостности, доступности и конфиденциальности информации и инструментов работы с ней. Грамотно построенная система информационной безопасности позволяет минимизировать ущерб от появления угроз информационной безопасности, а также решает задачи защиты информации, т.е. позволяет предотвратить появление угроз, связанных с человеческим фактором, а также оперативно реаги-

ровать на появление новых видов умышленных угроз. Системы защиты информации затрагивают саму информацию, средства работы с ней и сотрудников, использующих эти средства работы.

Таблица

Классификация угроз информационной безопасности

В зависимости от задействованного аспекта информационной безопасности			В зависимости от задействованной части информационной системы			В зависимости от преднамеренности возникновения	
Угрозы конфиденциальности (утечки информации)	Угрозы целостности	Угрозы доступности	Угрозы коммуниканта	Угрозы коммуникационного канала	Угрозы реципиента	Непреднамеренные (случайные)	Преднамеренные (умышленные)
Угрозы, в результате которых лица, не имеющие права доступа к информации, могут каким-либо образом получить это право.	Угрозы, в результате которых информация имеет возможность каким-либо образом измениться.	Угрозы, в результате которых доступ к информации может быть временно или перманентно затруднён или недоступен.	Угрозы, связанные с отправителем информации, которым может быть человек или другая информационная система.	Угрозы, связанные с уязвимостью в линии связи, по которой информация движется между коммуникантом и реципиентом.	Угрозы, связанные с получателем информации.	Угрозы, не связанные с преднамеренными действиями каких-либо лиц.	Угрозы, происходящие в результате преднамеренных действий злоумышленников.

Примечание: собственная разработка

Мероприятия по защите информации зачастую являются многогранными и затрагивают сразу несколько типов угроз информационной безопасности. К таким мероприятиям относятся:

- шифрование информации;
- использование антивирусного ПО;
- использование систем многофакторной аутентификации, минимизирующих вероятность несанкционированного доступа к аккаунтам;
- использование услуг «белых хакеров»;
- проведение проверок и стресс-тестов различных компонентов информационных систем;
- обучение персонала основным методам и понятиям информационной безопасности и работы с информационными

системами, что позволяет предотвратить возможные человеческие ошибки и атаки коммуниканта-реципиента [4].

Согласно исследованию ITRC (Identity Theft Resource Center), проведённому в 2019 году, частыми причинами утечек информации являлись атаки хакеров и получение несанкционированного доступа к системе, что является доказательством необходимости защиты системы в первую очередь от преднамеренных угроз конфиденциальности [5] (рис.).

Рис. 1. Наиболее частые причины утечки информации, 2018 (в процентах)

Таким образом, создание комплексной системы информационной безопасности является ключевым фактором обеспечения экономической безопасности предприятия.

Библиографические ссылки

1. Введение в информационную безопасность: учеб. пособие / А.А. Малюк [и др.]. Москва: Горячая линия, 2011. 288 с.
2. *Гатчин Ю.А., Сухостат В.В.* Теория информационной безопасности и методология защиты информации: учеб. пособие. СПб: СПбГУ ИТМО, 2010. 98 с.
3. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 3. Гарантийные требования безопасности: СТБ 34.101.3-2014 (ИСО/МЭК 15408-3:2008). Взамен СТБ 34.101.3-2004 (ИСО/МЭК 15408-3:1999); введ. 01.09.2014. Минск: Госстандарт, Минск: Бел-ГИСС, 2014. 131 с. (Государственный стандарт Республики Беларусь).
4. *Коломойцев В.С.* Задачи и средства обеспечения безопасности информационных систем в условиях цифровой экономики // Технико-технологические проблемы сервиса. 2017. №4. С. 50-55.
5. ITRC 2018 End-of-Year Data Breach Report // Identity Theft Resource Center [Электронный ресурс]. – 2019. – Режим доступа: https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf. Дата доступа: 26.04.2020.