Кулагина Ирина Ивановна
канд. экон. наук, доцент
Волгоградский институт управления (филиал)
ФГБОУ ВО «Российская академия народного хозяйства
и государственной службы при Президенте РФ»
г. Волгоград, Волгоградская область

ИНФОРМАЦИОННЫЕ РИСКИ В ОБЕСПЕЧЕНИИ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Аннотация*: раскрыта сущность понятий «экономическая безопасность» и «информационная безопасность». Дан обзор актуальных проблем управления информационными рисками в сфере обеспечения экономической безопасности предприятия. Рассмотрены источники угроз информационной безопасности.*

Ключевые слова*: экономическая безопасность предприятия, информационные риски, утечка информации, информационная безопасность.*

Понятие «экономическая безопасность» чаще всего связывают с возможностью организации противостоять неблагоприятным воздействиям внешней среды. В экономической литературе понятие «экономическая безопасность предприятия» определяется, как такое состояние всех имеющихся ресурсов, которое способно обеспечивать эффективное их использование и стабильное функционирование для непрерывного производственного и социального развития предприятия, а также достижения его поставленных стратегических задач [4, с. 11].

Влияния информационных рисков на экономическую безопасность предприятия становится все более актуальным с каждым годом. Это связано с тем, что происходит непрерывное развитие цифровизации экономики, к примеру предприятия, переходят на электронный документооборот, используют облачные технологии, различное программное обеспечение, компьютеры и другие электронные устройства постоянно подключены к Интернету, предоставление услуг осуществляется с применением электронных ресурсов, хранение информации происходит в базах данных, в том числе распределенных.

Изменения в макро и микроокружении предприятия требуют постоянного пересмотра и дополнения элементов экономической безопасности, так как новые уязвимости могут представлять угрозу для предприятий. Сегодня информационная безопасность играет ключевую роль в управлении предприятием и его экономической безопасностью. Очевидна необходимость разработки системы управления рисками в системе обеспечения информационной безопасности, как неотъемлемой части экономической безопасности предприятия.

Регулирование деятельности в сфере информационной безопасности в Российской Федерации исполняется на основании стандарта ГОСТ Р ИСО/МЭК 27001–2021, который был образован в соответствии с международным стандартом системы управления информационной безопасностью ISO/IEC 27 000. Указанный стандарт определяет информационную безопасность как, состояние, при котором возможно обеспечение конфиденциальности, доступности и целостности информации [2].

Очевидно, что эффективность деятельности предприятий все больше находится в зависимости от безопасности их информационных систем. Вся система информационного обеспечения безопасности включает в себя подходы, которые являются ее составляющими: финансовый, административный, производственный. Данная система функционирует как единый элемент в создании бизнес-среды на предприятии, а также в управлении качеством бизнеса и его персонала. В ней содержится информация о планах, характеристика материальных и финансовых потоков, контрактных обязательствах, данных управленческого и финансового учета. Именно эти сведения могут иметь решающее значение для интересов предприятия. Данная информация требует защиты от несанкционированного доступа, изменения, раскрытия и обеспечения своевременного изъятия.

Последствия атак на информационные ресурсы предприятия достаточно разнообразны. Влияния атак злоумышленников может варьироваться в масштабе от вреда конкретному человеку до подрыва функциональных возможностей целой отрасли экономики или региона. Соответственно, если на предприятии недостаточно обеспечивается информационная безопасность, то под влиянием

информационных рисков возможно возникновение угрозы полного прекращения деятельности экономического субъекта.

Количество атак на предприятия выросло в 2022 г более чем в 2 раза по сравнению с 2019 года. Пик количества киберугроз пришелся на сентябрь 2021 года. Однако в целом в 2021 году отмечается незначительный рост атак по сравнению с 2020 годом, в результате адаптации к условиям работы на фоне коронавирусной пандемии [1]. Рост количества атак в 2022 г эксперты связывают не только со сложившейся международной ситуацией, но и с приостановкой деятельности в РФ иностранных поставщиков корпоративных средств информационной безопасности [3]. На основе докладов компании Positive Technologies за 2020–2022 гг. составлена таблица 1.

Таблица 1

Среднее число атак на организацию в мире

Год/Квартал	1	2	3	4
2019	347	357	379	425
2020	521	567	583	600
2021	607	609	580	622
2022	714	754		

Источники угроз информационной безопасности принято разделять на внешние и внутренние. Если говорить об источниках угроз, которые влияют на предприятие из вне, то основными субъектами являются:

– конкуренты;

– контрагенты;

– преступные группировки;

– хакеры;

– другие лица, заинтересованные в информации, находящейся во владении предприятия.

Внутренние же угрозы исходят не только от сотрудников предприятия и могут быть вызваны:

– человеческим фактором (например, умышленное или небрежное раскрытие информации руководством предприятия, сотрудниками, в том числе IT-специалистами, ее утечка или несанкционированный доступ к источникам);

– техническими средствами, используемыми на предприятии (программное обеспечение, электронная почта, другие средства связи).

Степень опасности несанкционированного владения информацией, согласно данным портала информационной безопасности Content Security [5] можно представить в следующем виде (таблица 2).

Таблица 2

Степень опасности внутренних и внешних угроз информационной безопасности предприятия

Наименование угрозы	Степень угрозы
Разглашение сотрудниками конфиденциальной информации	32%
Склонение сотрудников конкурентами к разглашению информации	24%
Отсутствие достаточного контроля и условий обеспечения для ИБ	14%
Обмен производственным опытом между компаниями	12%
Бесконтрольное использование информационных ресурсов сотрудниками	10%
Некорректная кадровая политика	8%

Соотношение между внутренними и внешними угрозами составляет примерно 80 к 20 процентов, что говорит о том, наибольшего внимания в области обеспечения информационной безопасности требуют сотрудники экономического субъекта. Необходимо постоянное внимание к уровню компетентности и лояльности сотрудников.

Ежегодно экспертно-аналитический центр InfoWatch [6] проводит анализ динамики утечек данных из коммерческих, некоммерческих (государственных, муниципальных) организаций России.

В соответствии с представленным отчетом прослеживается динамика снижения количества утечек данных в организациях с 2019 года по 2021 год. Так в 2021 году число утечек меньше на 40%, чем в 2020 году, и на 46% меньше, чем в 2019 году. Но все же, данные цифры не являются утешительными. Число утечек в 2020 году может быть связано с тем, что в период пандемии COVID-19

большинство предприятий перевело сотрудников на удаленный режим работы, вследствие чего, произошло ослабление контроля за сотрудниками, и эти факторы дали новые возможности для злоумышленников. Многие инциденты могли оказаться не обнаруженными.

Даже одна утечка конфиденциальных данных наносит ущерб всей деятельности предприятия, его размер зависит от критичности информации, которая была скомпрометирована. Так, например, если компания конкурент узнала секретные технологии производства или получила конфиденциальные бухгалтерские документы, то безусловно, это скажется на экономической безопасности предприятия. Иногда, когда предприятие находится не в лучшем положении, то конкурентам и злоумышленникам выгодно получить данные, утечка которых сможет довести даже до банкротства.

По данным экспертно-аналитического центра InfoWatch, в первом полугодии 2022 года произошло рекордное количество утечек данных в российских компаниях таких, как: образовательный портал GeekBrains, авиакомпания «Аэрофлот», «Гемотест», «Почта России», «Ростелеком» и «Билайн», «РИА Новости», информационный портал Ykt.ru, ресурс Pikabu, экосистема «Яндекс», Delivery Club, школа «Сколково» [7].

Непременно, любое распространение конфиденциальной информации может серьезно навредить репутации предприятия, вследствие чего, уровень доверия у клиентов к компании снизится, и соответственно, возможен риск недополучения прибыли.

Можно сделать вывод, что возникновение информационных рисков на предприятии приводят к нанесению ущерба. Управление информационными рисками является одним из главных направлений из всех проблем обеспечения экономической безопасности организации. На многих предприятиях, даже на крупных, система информационной безопасности налажена не лучшим образом, что становится риском утечки информации, и приводит к негативным последствиям для успешной работы предприятия.

Сотрудники остаются основным звеном в обеспечении информационной безопасности предприятия. Необходимо проводить регулярные обучения и тренинги по правилам безопасного обращения с информацией, а также усиливать контроль за доступом к конфиденциальным данным. Важно внедрять современные технологии защиты информации, чтобы минимизировать риски утечки данных.

Таким образом, очевидна важность всех усилий по созданию эффективной системы информационной безопасности на предприятии, для чего необходимо выявлять существующие внутренние и внешние угрозы, осуществлять их постоянный мониторинг и принимать меры по предотвращению утечки информации или несанкционированного доступа к ней, например, расширенные системы обнаружения и реагирования на сложные кибератаки класса XDR (Extended Detection and Response).

Список литературы

1. Актуальные киберугрозы: I квартал 2022 года [Электронный ресурс]. – Режим доступа: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/

2. ГОСТ Р ИСО/МЭК 27001-2021. Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования: издание официальное: утвержден и введен в действие Приказом Федерального агентства по техническому регулированию и метрологии от 30 ноября 2021 г. №1653-ст: дата введения 2022–01–01 / разработан ФСТЭК России. – М.: ФГБУ «РСТ», 2021. – V, 3 с.

3. «Лаборатория Касперского» фиксирует рост сложных кибератак на российские компании [Электронный ресурс]. – Режим доступа: https://habr.com/ru/news/657473/

4. Сергеев А.А. Экономическая безопасность предприятия / А.А. Сергеев. – М.: Юрайт, 2022. – 275 с. EDN NFWCSU

5. Утечки информации: экономические эффекты. Корпоративный менеджмент [Электронный ресурс]. – Режим доступа: https://www.cfin.ru/appraisal/info_leakage.shtml

6. Infowatch: ИТ-компания [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/analytics/utechki-informatsii

7. Отчёт об утечках данных за 1 полугодие 2022 года. Infowatch [Электронный ресурс]. – Режим доступа: https://www.infowatch.ru/sites/default/files/analytics/files/otchyot-ob-utechkakh-dannykh-za-1-polugodie-2022-goda_0.pdf