Информационная безопасность как элемент экономической безопасности

Елизавета Евгеньевна Ершова
Аспирантка 3 курса
Российская академия народного хозяйства и государственной службы
Москва, Россия
elizavetaersh909@yandex.ru
0000-0000-0000-0000

Поступила в редакцию 25.04.2022
Принята 11.05.2022
Опубликована 20.06.2022

10.25726/v8343-7232-2832-p

Аннотация

В статье рассмотрена и обосновывается необходимость создания и функционирования качественной системы информационной безопасности современного предприятия, осуществляющего свою деятельность в самых различных направлениях (промышленность, энергетика, гуманитарная сфера и проч.). Также здесь анализируется её роль, которая она играет в ходе создания условий экономической безопасности самой организации и государства в целом. В работе отображена существующая классификация угроз информационной безопасности. Еще проанализированы мероприятия, направленные на защиту информации в современном мире, а также приводится пример наиболее распространённых на сегодняшний день причин её утечки.

Ключевые слова

информационная безопасность, экономическая безопасность предприятия, защита информации, угрозы и риски информационной безопасности, искусственный интеллект.

Введение

На современном этапе развития человеческого общества одним из основных качественных его отличий от предыдущих периодов является его всеобщая информатизация. Именно благодаря качественному накоплению, обработке и использованию различной информации, предприятие может полноценно существовать и развиваться. При этом информатизация выступает одним из важнейших управленческих ресурсов, позволяющая развиваться предприятию в различных направлениях (Русакович, 2020).

Поэтому, из-за ее большой важности, возникает потребность защищать источники информации, методики ее обработки и сами ресурсы от несанкционированных взломов и попыток хищения. И это не случайно, потому что защищенная информация (например, от конкурентов), помогает предприятию заключать более выгодные сделки и контракты, а сама организация остается более долгое время конкурентоспособной, стабильной и с финансово прибыльной. Безусловно, все вышесказанное только подтверждает высокую роль качественной системы информационной безопасности, внедренной на предприятии, при создании максимально хороших условий для его экономической безопасности.

Материалы и методы исследования

Разбирая данный вопрос, нужно отметить, что сегодня нет общепризнанного определения понятий «экономическая безопасность» и «информационная безопасность». Критерии их определения рассматривали многие отечественные и зарубежные исследователи – Р.Ф. Абдеев, А.В. Бузгалин, С.А. Дятлов, Ю.Н. Коломин, А.И. Ракитов, Р. Хонтель и др.

Однако было отмечено, что критерии их определения определяют социально-экономические факторы, среди которых анализируются особенности с их использования. Существуют такие определения:

– экономическая безопасность – это особенности деятельности какого-либо предприятия, когда оно защищено внешних и внутренних негативных (дестабилизирующих) факторов, какие могут негативным образом повлиять (влиять) на его социально-экономическое развитие;

– информационная безопасность – это такое состояние информационного развития предприятия, когда оно защищено различных внешних и внутренних факторов, способных негативно влиять на его деятельность посредством «утечки» информации, которая может быть «повернута» против него самого (Коломойцев, 2017).

В тоже время, единственный официальный документ, в котором содержится определение информационной безопасности – это Указ Президента Российской Федерации от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». Читаем такое: «информационная безопасность российского государства – это состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства (Указ Президента РФ, 2016).

Результаты и обсуждение

Поэтому информационная безопасность является определенным состоянием защищенности общества и государства от внешних и внутренних угроз. И устойчивое развитие информационной безопасности в мире и в России в частности приобретает все более глобальный характер. Из здесь можно проследить то, что общий уровень экономической безопасности предприятия напрямую зависит от того, насколько хорошо она защищена от различных негативных или опасных информационных ресурсов (Кипкеева, 2020).

В свою очередь, экономическая безопасность предприятия позволяет ему получать постоянный стабильный доход не только на сегодня, но о оставаться рентабельным в будущем. Поэтому, чтобы оставаться как можно дольше «на плаву», противостоять «агрессивной» политике конкурентов, применяющейся во многих отраслях хозяйства, фирма обязательно должна грамотно составить, разработать и внедрить систему собственной экономической безопасности, что обеспечит ей защиту информации.

Не стоит забывать, что экономическая безопасность предприятия – это многоструктурное понятие, включающее в себя многочисленные компоненты. И именно информационная составляющая сегодня является одной из важнейших частей. Это не случайно, т. к. на данный момент невооруженным взглядом видно, что сейчас начинается эра информационного общества, где информация выступает важнейшим ресурсом, который должен полноценно развиваться у предприятия, дополняя собой существующие производственные, финансовые и экономические и ресурсы.

Информационная безопасность, будучи важной структурной составной частью экономической безопасности предприятия, включает в себя такие направления:

1) организация разрабатывает и реализовывает на практике такие программы, какие смогут обеспечить безопасность всех имеющихся у нее информационных ресурсов;

2) система технологической защиты информации, состоящая на «вооружении» у предприятия, должна способствовать полной защите информации от внешних и внутренних посягательств (Осипова, 2020).

Информация на предприятии должна постоянно собираться, обрабатываться и храниться в полной безопасности, что позволит ему качественно развиваться. Это приводит к тому, что на современном предприятии возникает необходимость организовывать обеспечение защищенности информационной составляющей, в т. ч. и экономической безопасности.

Как следствие, сегодня защита информационной безопасности в каждой организации должна организовываться и проводиться системно. Поэтому, она должна проводиться в определенном комплексе, что позволит исключить утечку важной информации. То есть, предприятие должно внедрять в жизнь такие мероприятия, которые позволят обеспечить надежную сохранность информации, что позитивно будет сказываться на будущих направлениях работы.

Руководителям всегда нужно помнить о том, что при неграмотной организации информационной безопасности на их предприятии (организации), могут быть похищены важные данные, использование которых их конкурентами самым негативным образом отобразиться на развитии их фирмы. Еще важно понимать, что угрозы информационных безопасности бывают разные. Однако они имеют свою собственную определенную классификацию, какую нужно знать, чтобы качественно противостоять им (табл. 1) (Русакович, 2020):

Таблица 1. Классификация угроз информационной безопасности

В зависимости от того, какой аспект информационной безопасности задействован			В зависимости от того, какая информационная часть задействована			Учитывая преднамеренность возникновения	
Преднамеренность возникновения	Угроза целостности	Угроза доступности	Угроза коммуникации	Угрозы канала коммуникации	Угроза реципиента	Непреднамеренные	Преднамеренные
Лица, у каких нет прав доступа к информ., могут как-либо получить такое право	Состоит в том, что информация может как-то измениться	При ней доступ к информ. может быть временно заблокирован или недоступен	Связанные с отправителем информации (человек или система)	Заключается в возможной уязвимости лини связи передачи информ.	Они связаны с поучателем информации	Угрозы, что не связаны с преднамеренными действиями каких-нибудь лиц	Они происходят в резуль-тате предна-меренных дейтвий злоумышленников

Следует сказать, что в рамках современного этапа развития организаций и фирм набольшее количество угроз информационной безопасности (по статистике) исходит от сотрудников организации и сторонних лиц, что говорит о преобладании здесь человеческого фактора (рис. 1) (Попкова, 2015).

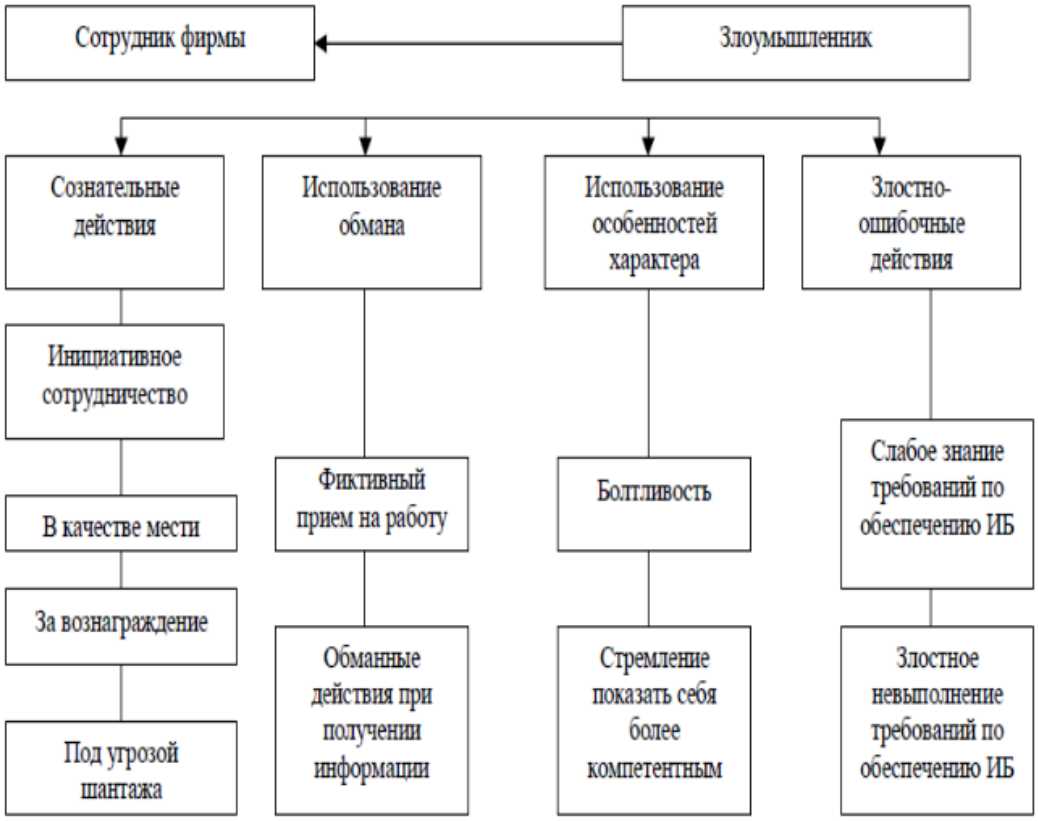

Рисунок 1. Действия сотрудников, какие могут нарушить информационную безопасность предприятия

Следующая угроза информационной безопасности предприятия – это DDoS-атаки. От тих на сегодняшний день не защищены любые предприятия – от крупнейших конгломератов и транснациональных компаний – до небольших фирм и организаций. Причем незащищёнными выступают предприятиях во всех сферах экономической жизни страны.

Поэтому предприятию нужно выстроить качественную систему обеспечения своей информационной безопасности, которая, безусловно, станет важной составной частью его экономической безопасности. И как основные направления по обеспечению такого направления следует сделать следующее:

– информационные ресурсы фирмы должны быть надежно защищены, что исключит несанкционированный доступ к ним;

– конфиденциальная информация не должна никоим образом искажаться, пропадать или становиться общедоступной;

– программные комплексы по защите информации должны работать без сбоев, поэтому их деятельность обязательно следует постоянно анализировать и совершенствовать;

– применяемое оборудование должно обеспечивать максимальную защиту информации (Палагин, 2019).

Еще нужно отметить, что система, обеспечивающая защиту информационной безопасности предприятия, может быть разработана как внутренними IT-специалистами, так и специально приглашёнными для этого специалистами из вне. Компания сама выбирает, кто будет обеспечивать разработку соответствующего программного обеспечения. Главное, из имеющего большого количества таких специалистов, предприятие должно найти и выбрать того, кто сделает свою работу максимально качественно. И такая задача сегодня ложиться на плечи менеджеров, отвечающих за такое направление работы.

Главное, нужно помнить, что, если предприятие захочет воспользоваться услугами соответствующих компаний, нужно проверить у последних наличие лицензий Федеральной Службы Безопасности (ФСБ), Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ), Государственной технической комиссии и др. специализированных организаций, деятельность которых которые обеспечивает защиту информации отечественных предприятий. Еще лучше изучить эффективность внедренных ими схожих проектов на подобную тематику (Камскова, 2014).

Заключение

Можно подытожить, что для большей части предприятий сегодня защита от взломов систем и несанкционированного доступа к данным и информации высочайший приоритет при обеспечении экономической безопасности. Поэтому они должны обеспечивать выстраивание комплексной системы информационной безопасности, учитывая всевозможные факторы, которые могут негативно на нее повлиять.

Как видим, информационная безопасность очень важна для нормальной деятельности любого современного предприятия. Как следствие, создав комплексную системы информационной безопасности, предприятие сможет обеспечить в будущем свою экономическую безопасность. Поэтому очень важно при обеспечении экономической безопасности учитывать все существующие риски в данном направлении, вовремя их устранять и не допуская утечки информации.

Список литературы

1. Камскова И.Д. Информационная безопасность как элемент экономической безопасности субъектов предпринимательства // Перспективы развития информационных технологий. 2014. № 18. С. 169–172.
2. Кипкеева А.М., Урусов А.А. Информационная безопасность – важнейший элемент обеспечения экономической безопасности организации // Вестник Академии знаний. 2020. № 40 (5). С. 157–161.
3. Коломойцев В.С. Задачи и средства обеспечения безопасности информационных систем в условиях цифровой экономики // Технико-технологические проблемы сервиса. 2017. № 4. С. 50–55.
4. Осипова В.А. Информационная безопасность как элемент экономической безопасности // Вектор экономики. 2020. № 3 (45). С. 47–53.
5. Палагин Р.А. Информационная безопасность в системе обеспечения экономической и национальной безопасности России // Мировая наука. 2019. № 5 (26). С. 551–556.
6. Попкова Е.Г., Островская В.Н. Экономическая безопасность современной России: проблемы и перспективы // Дайджест-финансы. 2015. № 4. С. 53–63.
7. Русакович И.С., Бокунович Т.А. Информационная безопасность как элемент экономической безопасности предприятия // Общественные науки. Экономика и экономические науки: 77-я научная конференция студентов и аспирантов Белорусского государственного университета: материалы конференции. В 3 ч. Ч. 2, г. Минск, 11–22 мая 2020 г. / Редкол.: В.Г. Сафонов (гл. ред.). Минск: БГУ, 2020. С. 375–378.
8. Указ Президента РФ от 05.12.2016 № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». https://www.consultant.ru/document/cons_doc_LAW_208191/

Information security as an element of economic security

Elizaveta E. Ershova
3rd year postgraduate student
Russian Academy of National Economy and Public Administration
Moscow, Russia
elizavetaersh909@yandex.ru
0000-0000-0000-0000

Received 25.04.2022
Accepted 11.05.2022
Published 20.06.2022

10.25726/v8343-7232-2832-p

Abstract

The article considers and substantiates the need to create and operate a high-quality information security system of a modern enterprise operating in a variety of areas (industry, energy, humanitarian sphere, etc.). It also analyzes its role, which it plays in the course of creating conditions for the economic security of the organization itself and the state as a whole. The paper shows the existing classification of information security threats. The measures aimed at protecting information in the modern world are also analyzed, and an example of the most common reasons for its leakage today is given.

Keywords

information security, economic security of the enterprise, information protection, threats and risks of information security, artificial intelligence.

References

1. Kamskova I.D. Informacionnaja bezopasnost' kak jelement jekonomicheskoj bezopasnosti sub#ektov predprinimatel'stva // Perspektivy razvitija informacionnyh tehnologij. 2014. № 18. S. 169–172.
2. Kipkeeva A.M., Urusov A.A. Informacionnaja bezopasnost' – vazhnejshij jelement obespechenija jekonomicheskoj bezopasnosti organizacii // Vestnik Akademii znanij. 2020. № 40 (5). S. 157–161.
3. Kolomojcev V.S. Zadachi i sredstva obespechenija bezopasnosti informacionnyh sistem v uslovijah cifrovoj jekonomiki // Tehniko-tehnologicheskie problemy servisa. 2017. № 4. S. 50–55.
4. Osipova V.A. Informacionnaja bezopasnost' kak jelement jekonomicheskoj bezopasnosti // Vektor jekonomiki. 2020. № 3 (45). S. 47–53.
5. Palagin R.A. Informacionnaja bezopasnost' v sisteme obespechenija jekonomicheskoj i nacional'noj bezopasnosti Rossii // Mirovaja nauka. 2019. № 5 (26). S. 551–556.
6. Popkova E.G., Ostrovskaja V.N. Jekonomicheskaja bezopasnost' sovremennoj Rossii: problemy i perspektivy // Dajdzhest-finansy. 2015. № 4. S. 53–63.
7. Rusakovich I.S., Bokunovich T.A. Informacionnaja bezopasnost' kak jelement jekonomicheskoj bezopasnosti predprijatija // Obshhestvennye nauki. Jekonomika i jekonomicheskie nauki: 77-ja nauchnaja konferencija studentov i aspirantov Belorusskogo gosudarstvennogo universiteta: materialy konferencii. V 3 ch. Ch. 2, g. Minsk, 11–22 maja 2020 g. / Redkol.: V.G. Safonov (gl. red.). Minsk: BGU, 2020. S. 375–378.
8. Ukaz Prezidenta RF ot 05.12.2016 № 646 «Ob utverzhdenii Doktriny informacionnoj bezopasnosti Rossijskoj Federacii». https://www.consultant.ru/document/cons_doc_LAW_208191/