УДК 334.021.1

Голуб Владимир Андреевич,
студент 1 курса магистратуры,
факультет цифровой экономики и информационных технологий
Академия маркетинга и социально-информационных технологий - ИМСИТ,
Россия, г. Краснодар
e-mail: golub_info@mail.ru

Мадатова Оксана Владимировна,
кандидат экономических наук, доцент,
доцент кафедры бизнес-процессов и экономической безопасности,
Академия маркетинга и социально-информационных технологий - ИМСИТ,
Россия, г. Краснодар

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ БИЗНЕСА

Аннотация: *Сегодня проблема безопасности является одной из самых актуальных в мире бизнеса. Однако безопасность часто понимается только как физическая защита персонала и материальных ценностей, но таким способом можно защититься от криминала. А бизнес, вступивший в рыночное отношение, сталкивается с острой конкурентной борьбой, существующей на любом цивилизованном рынке, и такая борьба состоит из немалых опасностей для предприятия. Особенно если компания сильно выделилось, тогда любая информация о её работе будет ценной. Поэтому защита информации становится важнейшей частью современной системы безопасности бизнеса.*

Цель данной статьи рассмотреть сущность информационной безопасности в бизнесе и методы её защиты.

Ключевые слова: экономика, информационная безопасность, бизнес, информация, экономическая безопасность.

Golub Vladimir Andreevich,
1st year master student,
Faculty of Digital Economics and Information Technology
Academy of Marketing and Social Information Technologies - IMSIT,
Russia, Krasnodar
Madatova Oksana Vladimirovna,
candidate of economic sciences, associate professor,
associate professor of the department of business processes and economic Security
Academy of Marketing and Social Information Technologies - IMSIT,
Russia, Krasnodar

BUSINESS INFORMATION SECURITY

Abstract: *Today, the security problem is one of the most pressing in the world of business. However, security is often understood only as the physical protection of personnel and material assets, but in this way you can protect yourself from crime. And a business that has entered into a market economy is faced with intense competition that exists in any civilized market, and such a struggle consists of considerable dangers for the enterprise. Especially if the company stood out strongly, then any information about its work will be valuable. Therefore, information security is becoming an essential part of a modern business security system.*

The purpose of this article is to consider the essence of information security in business and how to protect it.

Key words: economics, information security, business, information, economic security.

Информационная безопасность — это состояние защищенности информации среды общества, обеспечивающее ее формирование, использование и развитие в интересах граждан, организаций, государств [1].

Важно понимать, что компании должны защищать не всю информацию, которой они владеют, а только ту информацию, которая используется третьими сторонами и может повлиять на бизнес компании. Определенная информация может быть раскрыта. Поэтому информация о ценах, которые будут защищены от конкурентов, не является полезной. Однако информация на сырье и материалы, приобретаемые предприятием, должна храниться в тайне. Чрезмерное закрытие информации компании приведет к тому, что потенциальные партнеры, клиенты и инвесторы будут негативно относиться к компании. Это особенно навредит компании, планирующая выпуск ценных бумаг. Чтобы предотвратить это, компания должна сначала определить информацию, которую должны быть раскрыты. В то же время вы можете сосредоточиться на западных стандартах раскрытия информации. Федеральная комиссия по рынку ценных бумаг устанавливает те же стандарты для компаний, выпускающих ценные бумаги [2, с. 37]. К информации, обязательной для раскрытия, относятся:

– годовые бухгалтерские отчеты (бухгалтерский баланс, отчет о прибылях и убытках, отчет о движении денежных средств);

– данные акционеров;

– данные о крупных сделках с капиталом.

Для нераскрытой информации организация должна классифицировать в соответствии со степенью конфиденциальности и разработать стандарты информационной безопасности для каждой категории.

Прежде всего информацию нужно защищать от конкурентов. Их действия несут наибольшую опасность для компании. Поскольку компания занимает часть рынка, она всегда является легкой добычей для конкурентов, и ущерб, вызванный потерей важной информации о новом продукте, может быть непоправимым.

Что касается заинтересованности партнерства в информации о вашей компании, оно может быть активировано из соображений нашей безопасности. Поэтому необходимо создать среду, позволяющую им получать информацию о компании, которая не превышает необходимую структуру для плодотворного сотрудничества. Для этого нужно точно определить какую информацию предоставлять своевременно и в полном объёме, а к какой ограничить доступ.

Информация, которую будет получать клиент, очень конкретна. Это общая информация о компании и ее продуктах, данные о надежности компании и информация о ценах [3, с. 70].

Для клиентов важно обеспечить максимальную доступность такой информации. Когда речь заходит о защите информации, следует понимать, что нежелательным был бы “вынос сора из избы”. Однако, это же касается и партнёров. Поэтому необходимо определить, какая внутренняя информация не может быть раскрыта.

Отношения компании с налоговыми и контролирующими органами являются специфическими. Эти организации предъявляют особые требования к предоставлению информации. Отношения с ними очень важны, необходимо полностью соблюдать их требования и своевременно предоставлять информацию в необходимом количестве, но не превышающем это количество. В этом случае недостаточная и избыточная предоставленная информация

приведет к самым нежелательным последствиям.

Следующий важный вопрос - понять, какую информацию следует защищать. Вредные действия, которые могут быть выполнены с использованием секретной для организации информации: уничтожение важной информации, уничтожение публичной информации, хранение конфиденциальной информации, копирование конфиденциальной электронной информации, закрытие или ограничение доступа к информации, требуемой компанией, несанкционированный доступ и доступ к информации. ограничено.

Прежде чем рассматривать меры защиты информации, сначала подумайте, какие инструменты и методы можно использовать для получения необходимой информации о компании. Существуют две основные группы средств и методов бизнес-аналитики или промышленного шпионажа:

– методы сбора информации с применением специальной техники;

– методы фрагментарного сбора информации.

Промышленный шпионаж, связанный с использованием специального оборудования, включает:

– прослушивание телефонных разговоров;

– прослушивание помещений;

– телевизионное наблюдение;

– слежка;

– вторжение в компьютерную сеть;

– считывание информации с мониторов.

Все эти методы очень трудоемки и дороги, и могут использоваться только крупными конкурентами и правоохранительными органами. Только профессионалы могут выполнять такие действия, что делает их гораздо опаснее. К фрагментарному сбору информации относятся:

– Вы можете получить много информации о компании по телефону, сделав несколько разумных оправданий (например, установление деловых контактов или проведение статистических обследований).

– Конкуренты могут представиться, как ваши потенциальные клиенты или партнеры, и в ходе предварительных переговоров, если вы не проведёте проверку и будете слишком открыты по отношению к ним, они получат много интересной информации. Также различные выставки являются особенно благодатной почвой для получения такой информации.

– Иногда переманивая специалистов конкуретной организации к себе на работу даёт очень много узнать о конкурентной компании.

– Внедрение своего сотрудника в конкурентную компанию для шпионажа за организацией.

В целом, обеспечение безопасности корпоративной информации делится на две основные задачи. Прежде всего, для обеспечения целостности и безопасности информации. А во-вторых, защитите вашу информацию от несанкционированного доступа.

Рассмотреть способы обеспечения целостности и безопасности информации. Бумажные и электронные носители используются для хранения информации.

На бумаге они хранятся в виде документов. Копии документов в ограниченном количестве и часто существует в одном экземпляре. Тогда их потеря нанесёт большой вред компании. Чтобы избежать этого, все документы должны быть строго записаны, храниться в соответствующих условиях и должен быть обеспечен контроль доступа. По возможности, вы должны иметь копию информации и хранить ее в специально оборудованном месте. В то же время важно также хранить оригиналы и копии в отдельных комнатах. Кроме того, рекомендуется по возможности использовать копию и хранить оригинал в секретном хранилище. Это особенно важно в случае непредвиденных обстоятельств, как огонь или воровство.

В современном мире рассматривается четкая тенденция к увеличению использования электронных средств массовой информации. Во многих компаниях весь процесс документирования выполняется в электронном виде. Электронные СМИ также хранят аудио и видео информацию. В последние годы

оплата производится в электронном виде, и информация об оплате хранится в банках. Даже информация о валютах и её курсе содержится в электронном виде. В то же время, с точки зрения уничтожения, наиболее уязвимой является цифровая информация. Дело в том, что электронные носители не очень долговечны, а неправильное использование оборудования может привести к случайному удалению информации. Другая серьезная опасность - компьютерные вирусы, которые в последнее время становятся все больше и больше. Меры, обычно используемые для защиты электронной информации от повреждения и удаления:

– Резервное копирование информации выполняется каждый день, и предоставляет возможность восстановить информацию.

– Наличие резервного сервера в локальной сети поможет в работе, если у основного сервера начнется сбои.

– Использование источника бесперебойного питания защитит компьютерную сеть компании от потери информации, связанной со сбоями в электрической сети.

– Архивировать информацию. Вся наиболее важная информация архивируется, записывается на съемный носитель и хранится в специально оборудованном помещении.

– Чтобы эффективно защитить компьютерную сеть от вирусных атак, вы должны отслеживать все файлы извне. Наибольшая вирусная опасность связана с использованием Интернета, поэтому необходимо, чтобы все файлы, проходящие через Интернет, проходили проверку и нужна ежедневная профилактическая проверка перед резервным копированием.

– Чтобы не произошло случайное уничтожение нужной информации или программного обеспечения, необходимо ограничивать права доступа для каждого сотрудника, который использует локальную сеть компании ту информацию, которая ему не нужна.

Рассмотрим способы по обеспечению защиты информации от несанкционированного доступа.

Наиболее важным способом решения проблемы утечки информации является работа с сотрудниками. При найме работника, компании не только следует обращать внимание на деловые и профессиональные качества заявителя, но также в первую очередь следует обращать внимание на его личностные качества - порядочные, честные и лояльные [4, с. 53]. После трудоустройства необходимо время от времени проводить тайный надзор за деятельностью сотрудников, чтобы предотвратить возможную утечку информации. Это поможет контролировать сотрудника от соблазна продажи секретной информации предприятия.

Самый эффективный способ защитить информацию от ненужного доступа - разделить ее. Принцип заключается в том, что любой сотрудник должен иметь информацию только о своей сфере деятельности. Поэтому любая информация будет распространяться среди сотрудников.

Чтобы использовать технические средства для предотвращения промышленного шпионажа, необходимо использовать специальные средства. Важно регулярно проводить соответствующие проверки и постоянно отслеживать уязвимости. Если ваш сайт оснащен отлаженной системой контроля доступа, вероятность использования технического шпионажа для атаки на вас значительно уменьшается.

Основными методами защиты цифровой информации является:

– Каждый сотрудник должен использовать только ту информацию, которая ему необходима для выполнения своих обязанностей в локальной сети.

– Чтобы предотвратить утечку информации необходимо установить в сети компьютеры, у которых не будет дисководов и параллельных портов.

– Чтобы уменьшить вероятность несанкционированного доступа, рекомендуется подключать к локальной сети только те компьютеры, которые выполняют одинаковые процессы.

– Шифрование информации.

– Необходимо разделить внутреннюю сеть предприятия и Интернет.

Ни одна из описанных мер по защите информации не может применяться

отдельно друг от друга. Для обеспечения эффективной защиты информации необходимо разработать корпоративные системы защиты данных. Каждая организация должна иметь собственную структуру системы информационной безопасности по своей сфере работы. Правильность ее выбора зависит от профессионального уровня сотрудников и руководителей компаний, занимающихся этим вопросом. Никогда не бывает слишком много защиты, но не забывайте, что основной целью системы безопасности является обеспечение надежной и бесперебойной работы организации.

Список литературы:

1. Федеральный закон «Об участии в международном информационном обмене» от 04.07.1996 № 85-ФЗ (последняя редакция) // Справочно-правовая система «Консультант-Плюс».

2. Мадатова О.В. Экономическая безопасность: Учебное пособие. М.: ООО «НЭЦПО КК», 2018. 27 с.

3. Гришина Н.В. Информационная безопасность предприятия: Учебное пособие. М.: Форум, 2018. 118 с.

4. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие. М.: Форум, 2017. 159 с.