УДК 004
DOI 10.51691/2541-8327_2022_11_16

АСПЕКТЫ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ КОМПАНИИ

Журавлева В.В.
студент,
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Ткаченко А.Л.
к.т.н., доцент,
Калужский государственный университет им. К.Э. Циолковского,
Калуга, Россия

Исламгереева Я. С.
ассистент,
Чеченский государственный университет им А. А. Кадырова,
Грозный, Россия

Аннотация

Рассматривая экономическую безопасность компании и современную экономику можно сделать вывод сразу, что они неразрывно связаны. Те объемы данных, которые хранится в компаниях необходимо защищать от внешних посягательств. Высокая оценка уровня экономической безопасности за счет информационных технологий делает возможным сохранение коммерческой тайны компании. В данной статье рассматривается принцип работы экономической безопасности в компании, а также способы ее поддержки в современном мире.

Ключевые слова: экономическая безопасность, внутренние угрозы, внешние угрозы.

ASPECTS OF THE COMPANY'S ECONOMIC SECURITY

Zhuravleva V.V.
student,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Tkachenko A.L.
candidate of Technical Sciences,
Kaluga State University named after K. E. Tsiolkovsky,
Kaluga, Russia

Islamgereeva Ya .S.
assistant,
A. A. Kadyrov Chechen State University,
Grozny, Russia

Abstract
Considering the economic security of the company and the modern economy, we can immediately conclude that they are inextricably linked. The volumes of data that are stored in companies must be protected from external attacks. A high assessment of the level of economic security due to information technology makes it possible to preserve the company's trade secrets. This article discusses the principle of economic security at the enterprise, as well as ways to support it in the modern world.
Keywords: economic security, internal threats, external threats.

В нашем мире невозможно предотвратить или спрогнозировать различные случаи угроз экономической безопасности компании. Коллектив компании не может быть уверен, что все пройдет гладко и без происшествий. Внешние и внутренние изменения, которые затрагивают наше общество,

заставляют задуматься о безопасности отдельных аспектов нашей жизни. Это потребность в защищенности нашей личности, бюджета, семьи, предприятия, государства от негативных последствий со стороны изменения рыночной экономики. Всю жизнь физические и юридические лица сталкиваются с проблемами безопасности на производстве. В особенности это касается отрасли именно экономической. Не обеспечив экономической безопасности (ЭБ), нельзя надеяться на благополучное самостоятельное решение проблем.

Чтобы обеспечить плавное и устойчивое развитие предприятия без негативного влияния на работников и население в целом, специалистам необходимо организовать цепь внедрения обязательных мер против внутренних и внешних угроз безопасности. К таким относятся имущество, деньги и информация.

Под внутренними и внешними угрозами понимаются такие негативные факторы, которые имея свой характер и свою сферу деятельности влияют сначала на отдельные структуры предприятия и нарушают их порядок деятельности, а затем и на всю систему в целом, всей компании. Ко внешним факторам относят:

- Состояние рыночной экономики.
- ЧС техногенного характера.
- Снижение репутации.
- Снижение статистических данных.

Ко внутренним факторам относят:

- Утечку информации.
- Саботирование.
- Неисполнение прямых обязанностей.

Для наилучшей организации мероприятий по защите экономики на предприятии, необходимо в точности знать, что она из себя представляет. Таким образом, для ЭБ предприятия есть несколько основных определений:

1. ЭБ предприятия – определяется уровнем эффекта от использования ресурсов компании и функционалом развития в настоящее время и положительная статистика на будущее [1].

2. ЭБ компании – стабильность функционирования, благополучие с материальной стороны, а также обеспечение прибылью от выполнения поставленных задач и целей [2].

3. ЭБ предприятия – организация защиты от мировых угроз основных структур предприятия с помощью таких мер как право, экономика и информационные технологии [3].

Экономическая безопасность компании тесно связана с защитой информации в информационных системах предприятия, т.к. утечка данных, связанных с коммерческой тайно может подорвать потенциал компании.

На вопрос в чем состоит трудность определения экономической безопасности можно выдвинуть сразу несколько причин:

1. Цели и задачи, которые обеспечивают благополучное влияние на прибыль при их успешной реализации, должны учитываться как со стороны материальной, так и производственной, а также с оглядкой на потенциал с тех же сторон.

2. Наличие мировых угроз, а также затрачиваемые ресурсы на их нейтрализацию.

3. Развитие рыночных отношений и все большее влияние экономики на жизнь, повлекшее к изменению мер по защите экономики и их постоянному контролю.

Обеспечение экономической безопасности в организации – это состояние, при котором все экономически важные посредники находятся в тесной взаимосвязи и используют свои возможности для полной поддержки функционала компании на протяжении всего ее существования.

ЭБ всегда должна ориентироваться на данные цели:

- Сформировать меры для плавного развития предприятия.

- Обеспечение роста функционала предприятия.
- Нейтрализация мировых угроз.
- Исполнение важных целей компании.
- Ориентир на создание условий для дальнейшего роста организации.

Выполнение данных целей особенно важно при изменяющихся условиях экономического мира.

Экономическая сторона компании должна быть настроена на следующие условия формирования:

1. Придерживаться интересов национальной экономики, то есть увеличивать уровень ЭБ каждой фракции предприятия.
2. Подготовка каждой фракции к угрозам ЭБ.
3. Постоянный контроль предпринимательской деятельности за поиском и решением различных угроз.

Модернизация рыночной экономики приводит к росту необходимости в усовершенствовании мер по борьбе с экономическими угрозами безопасности на каждой подструктуре предприятия.

Если руководство способно защитить свою структуру экономики от мировых угроз, то уровень ЭБ предприятия считается высоким. Уровень может варьироваться от самого низкого до самого высокого в зависимости от способности контролировать экономическую безопасность предприятия и поддерживать ее на определенном уровне. Предугадать появление угроз практически невозможно, поэтому в этом и заключается вся сложность руководителя использовать логику и интуицию в решении различного вида опасностей на производстве.

Виды угроз ЭБ различают на основные и дополнительные. Основные связаны с финансово-экономической деятельностью, информационной, правовой, и экологической. А дополнительные с криминалом, управленческими и административными угрозами. Их называют составляющими ЭБ.

Рассмотрим более подробно аспекты информационной безопасности. У любых экономических информационных систем существуют так называемые «уязвимости» - недостатки системы, которые могут быть использованы для реализации угрозы. Чтобы понять, какими способами злоумышленники совершают компьютерные атаки следует рассмотреть основные типы атак:

- Инъекционные атаки;
- Нарушенная аутентификация;
- Незащищённость критичных данных;
- Нарушение контроля доступа;
- Небезопасная конфигурация;
- Небезопасная десериализация;
- Использование компонентов с известными уязвимостями;
- Неэффективный мониторинг.

Нарушенная аутентификация. Некорректная аутентификация – это нарушение процедуры проверки подлинности пользователя, такая уязвимость может позволить злоумышленнику попытаться получить контроль над любой учётной записью в системе возможно даже полный контроль над системой.

Разрешение пользователям использовать подбор комбинации логина и пароля так же является проблемой - злоумышленник пользуется известными ему логинами или подбирает их вручную и пытается получить доступ к аккаунту путем восстановления забытого пароля, и если система восстановления пароля на сайте реализована не безопасно, такие попытки могут оказаться успешными.

Незащищённость критичных данных. Многие приложения имеют доступ к данным пользователей, однако не все из них достаточно хорошо их защищают. Речь идёт в первую очередь о конфиденциальных данных, таких как:

- Финансовые данные;
- Медицинские данные

- Документы, удостоверяющие личность;
- Другие персональные данные.

Вот несколько примеров того, что может случиться при раскрытии конфиденциальных данных:

1. Данные кредитных карт обычно шифруются автоматически в самом приложении, но при получении эти данные расшифровываются, что позволяет злоумышленнику, получившему доступ к устройству пользователя или приложению, в котором производится оплата, получить всю информацию по платежу в доступном для понимания виде.

2. Пароли и логины пользователей хранятся в базе данных ресурса и должны быть защищены шифрованием. С помощью расшифровки базы данных злоумышленник может получить базу данных паролей пользователей, и зная логин просто подобрать пароль из имеющейся базы и получить доступ к данным пользователя.

За последние годы утечка конфиденциальных данных стала очень распространенной проблемой во всём мире. Воспользоваться этой уязвимостью системы не так просто, однако в случае успеха, злоумышленники могут похитить или изменить эти данные, а затем осуществить мошеннические действия.

Нарушение контроля доступа. Данная уязвимость представляет собой некорректный контроль за действиями, разрешенными аутентифицированным пользователям – пользователям, вошедшим в систему используя логин и пароль.

Если такая уязвимость существует на том или ином web-ресурсе, то злоумышленник может получить доступ к аккаунтам других пользователей и соответственно, к информации, содержащейся в их профиле, а также может изменить данные для входа в систему – «взломать аккаунт».

Использование компонентов с известными уязвимостями. Приложения имеют в своем составе множество компонентов – библиотеки, программные модули и другие системы. Некоторые компоненты имеют уязвимости,

известные злоумышленникам. Таким образом, приложение становится уязвимым, и злоумышленнику остается узнать, какой компонент с известной уязвимостью входит в состав системы и провести атаку.

Так же, данный тип уязвимости появляется в том случае, когда компоненты не обновляются или обновляются несвоевременно, так как в обновлениях выходят поправки, которые позволяют устранить найденную разработчиками уязвимость.

Неэффективный мониторинг. Мониторинг – это проверка событий, происходящих в системе, он позволяет отслеживать попытки несанкционированного доступа к ресурсам, попытки взлома учетных записей и многое другое.

Собственно, недостатки мониторинга позволяют злоумышленнику остаться незамеченным, и проникнуть глубоко в систему, украсть из нее данные или уничтожить их [4].

Так как экономическая безопасность организации должна быть учтена в комплексе со всеми структурами предприятия, а также действовать против угроз безопасности необходимо в комплекте со всеми частями ЭБ, то можно выдвинуть экономическую безопасность компании как систему. В системе сформированы комплексные группы, которые за счет некоторых принципов ЭБ обеспечивают порядок регулирования экономической безопасности в целом.

Отсюда появляется еще одно определение ЭБ – это система мероприятий по поддержке устойчивой конкурентоспособности и постоянство статистики, минуя негативные последствия на жизнь населения.

Обеспечение ЭБ на предприятии проходит в 3 этапа:

1. Разработка плана по уничтожению угроз.
2. Обнаружение и нейтрализация угроз.
3. Процедуры по защите от угроз в дальнейшем.

Защита от угроз экономической безопасности поддерживается за счет:

- Службы безопасности.

- Охраны доступа.
- Внутреннего контроля.
- Контроль управления персоналом.

С вышеописанными мерами возможно проводить программу противодействия угрозам ЭБ, которая проходит в 4 этапа:

1. Предотвращение.
2. Выявление
3. Расследование.
4. Привлечение к ответственности.

В крупных компаниях для подтверждения угроз безопасности существуют аналитические службы. Но ее существование не означает, что безопасность будет точно соблюдена. Поэтому для крупных организаций приемлемо наличие внешних фирм, контролирующих ЭБ.

Кроме аналитических служб в организации действуют экономические и производственные отделы. Которые обосновывают решения на своем уровне, а служба экономической безопасности принимает решения по устранению и избавлению от рисков. Существует также контролирующий орган, который проводит проверку на обоснованность отчетности предприятия.

В настоящее время для обеспечения экономической безопасности в целом государство имеет такие цели:

- Обеспечение роста экономического суверенитета Российской Федерации.
- Закаливание к внешним и внутренним угрозам ЭБ.
- Экономический рост.
- Рост качества жизни населения.

Экономическая безопасность предприятия – это основная часть функционала любой организации. Без внедрения различных мер по выявлению, нейтрализации и защите компании от внешних и внутренних угроз невозможно

развиваться в дальнейшем. Так как рыночная экономика изменчива и на протяжении многих лет она будет существовать и меняться. Важно знать и уметь противостоять этой изменчивости путем внедрения совершенно новых способов защиты от опасностей.

На основе проведенного исследования были выработаны рекомендации по экономической безопасности информации компании:

- Пользователям следует использовать многофазовую аутентификацию – подтверждение личности минимум двумя способами, например ввод данных учетной записи и одноразового кода из смс, если у web-ресурса есть поддержка такой функции, так же следует использовать максимально сложные пароли и регулярно их менять, по возможности следует избегать функции автозаполнения пароля, и вводить логин и пароль по памяти, так как если ваши логины и пароли не хранятся - их нельзя украсть, безопаснее хранить эти данные на бумажном носителе, который храниться в месте, доступном только для вас .
- В данных, украденных злоумышленником, могут быть так же данные банковских карт и документов, удостоверяющих личность. Имея такие данные, злоумышленники могут связываться с клиентами банка, на который была совершена успешная атака и представляться сотрудниками банка, пытаясь таким образом получить ваш пароль от карты, трехзначный код на обороте карты, ответ на секретный вопрос, который клиенты указывают в анкете при оформлении карты, чтобы получить доступ к денежным средствам, хранящимся на вашем счету. При получении подобных звонков или смс ни в коем случае нельзя сообщать никакой информации, лучше при первой возможности обратиться в ближайшее отделение вашего банка для выяснения всех обстоятельств.

- Пользователям не следует устанавливать «пиратские» приложения, игры, программное обеспечение и тем более операционные системы, так как в них могут содержаться вредоносные файлы, позволяющие злоумышленникам получить доступ к персональным данным пользователя. Так же не следует устанавливать «дополнительные» или «взломанные» приложения, позволяющие получать платный контент бесплатно или дающие другие дополнительные возможности.
- Пользователям необходимо регулярно обновлять приложения и программное обеспечение, так как обновления исправляют существующие ошибки и устраняют обнаруженные уязвимости, что позволяет повышать уровень защищенности используемых приложений.
- Пользователям следует понимать, что большая часть вредоносных файлов появляется на их персональных компьютерах посредством скачивания этих файлов или приложений, содержащих эти файлы, самими пользователями.
- Пользователям не следует переходить по неизвестным ссылкам, особенно если они получены от неизвестного им адресата по электронной почте или в сообщениях в социальных сетях.

Библиографический список:

1. Комплексная система обеспечения экономической безопасности предприятия : учеб. пособие / И. А. Сергеева, А. Ю. Сергеев. – Пенза : Изд-во ПГУ, 2017. – 124 с.
2. Герасимов, К.Б. Экономическая безопасность: учеб. Пособие К.Б. Герасимов, Г.Ф. Несоленов. – Самара: Изд-во Самарского гос. аэрокосм. ун-та, 2011. – 80 с.

3. Организация и управление экономической безопасностью предприятий: учебник / Федеральное государственное бюджетное образовательное учреждение высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации», СевероЗападный ин-т упр. -СПб.: ИПЦ СЗИУ -фил. РАНХиГС, 2016. – 332 с.
4. Иванец, М. Э. Анализ угроз информационной безопасности для коммерческой организации / М. Э. Иванец, А. Л. Ткаченко // Цифровая трансформация промышленности: тенденции и перспективы : Сборник научных трудов по материалам 2-й Всероссийской научно-практической конференции, Москва, 11 ноября 2021 года. – Москва: Общество с ограниченной ответственностью "Русайнс", 2022. – С. 364-370. – EDN RWMZDO.

Оригинальность 82%