В Республике Беларусь в настоящее время при формировании цены используется сочетание двух методов – ресурсного и базисно-компенсационного. Накладные расходы распределяются на основании одного из выбранных на предприятии методов, при этом себестоимость продукции формируется исходя из требований Инструкции МАРТ, Минэкономики, Минфина и Минтруда и соцзащиты от 04.11.2022 № 71/15/50/68 [6].

Таким образом, обеспечение граждан, нуждающихся в улучшении жилищных условий, квадратными метрами жилья по цене ниже рыночной, остается не до конца решенным вопросом в Республике Беларусь. Это объясняется наличием неприемлемых интересов государства, гражданина и субъектов строительной отрасли. Для выравнивания вектора развития в однонаправленном движении государство используется механизмы регулирования цен. Главное, чтобы неизбежное вмешательство государство не пришло в противоречие с закономерности функционирования рыночной экономики, что может привезти к негативным последствиям. А для этого сам процесс выработки решения должен носить характер государственного компромисса всех заинтересованных лиц.

Список использованных источников

1. О ценообразовании : Закон Республики Беларусь, 10 мая 1999 г., № 255-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
2. О порядке регулирования цен : постановление Министерства архитектуры и строительства Республики Беларусь, 12 июля 2022 г., № 69 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
3. Об архитектурной, градостроительной и строительной деятельности в Республике Беларусь : Закон Республики Беларусь, 05 июля 2004 г., № 300-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
4. О регулирования цен : постановление Совета Министров Республики Беларусь, 06 июля 2022 г., № 447 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
5. О системе регулирования цен : постановление Совета Министров Республики Беларусь, 19 октября 2022 г., № 713 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.
6. Инструкция о порядке планирования и калькулирования себестоимости продукции для целей ценообразования : постановление МАРТ, Министерства экономики, Министерства финансов и Министерства труда и соцзащиты Респ. Беларусь, 04 ноября 2022 г., № 71/15/50/68 // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. – Минск, 2022.

Т. В. Филиппова, Е. А. Крачун
Брестский государственный технический университет

КИБЕРБЕЗОПАСНОСТЬ В РЕСПУБЛИКЕ БЕЛАРУСЬ

T. Filippova, K. Krachun
Brest State Technical University

CYBER SECURITY IN THE REPUBLIC OF BELARUS

Аннотация. Развитие информационного общества предполагает внедрение цифровых технологий во все сферы жизни, что одновременно создает условия для появления новых угроз безопасности – от утечек информации до кибертерроризма.

Annotation. The development of the information society involves the introduction of digital technologies in all spheres of life, which at the same time creates conditions for the emergence of new security threats- from information leaks to cyberterrorism.

Ключевые слова: КИБЕРБЕЗОПАСНОСТЬ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УТЕЧКА ДАННЫХ, КИБЕРАТАКА, КИБЕРТЕРРОРИЗМ, ВРЕДОНОСНОЕ ПО, ВИРУСЫ.

Keywords: CYBERSECURITY, INFORMATION SECURITY, DATA LEAKAGE, CYBERATTACK, CYBERTERRORISM, MALWARE, VIRUSES.

Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий.

Кибербезопасность — это процесс, который обеспечивает всем нам знакомые свойства конфиденциальности, целостности, доступности, но только в некоторых абстрактных рамках – киберпространстве. В свою очередь под киберпространством понимается комплексная виртуальная информационная среда, которая не имеет привычного нам физического воплощения.

В этом направлении можно выделить несколько основных категорий:

- Безопасность сетей – действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ.
- Безопасность приложений – защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.
- Безопасность информации – обеспечение целостности и приватности данных как во время хранения, так и при передаче.
- Операционная безопасность – обращение с информационными активами и их защита. К этой категории относится, например, управление разрешениями для доступа к сети или правилами, которые определяют, где и каким образом данные могут храниться и передаваться.
- Аварийное восстановление и непрерывность бизнеса – реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.
- Повышение осведомленности – обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства [1].

Количество данных постоянно увеличивается: с 2010 по 2020 год объём информации вырос в 50 раз. Число серверов Google и Amazon исчисляется миллионами. Ценность информации стала сравнима с ценностью сырья. Особую важность информация приобретает в контексте её обработки с помощью машинного обучения и других современных технологий. Чем ценнее информация для бизнеса, тем выше необходимость её защиты.

Кибербезопасность относится к одной из отраслей информационной безопасности и охватывает защиту данных в сетях компаний и организаций, а также защиту приватной информации частных лиц. Специалистов по кибербезопасности готовят и высшие учебные заведения, и специализированные курсы.

Несколько раз в год случаются «мега-утечки», когда в открытый доступ попадают конфиденциальные данные десятков и сотен миллионов пользователей. Самая масштабная утечка информации произошла в 2019 г., когда в открытом доступе были опубликованы логины и пароли электронных почт 773 млн человек. Ранее в 2018 г. оказались скомпрометированы более 500 млн клиентов гостиничной сети Marriott, 440 млн пользователей программного обеспечения Veeam, 300 млн клиентов логистической компании SF Express.

Данные утекают не только через сеть. Нередко хакеры и инсайдеры получают ценные данные с помощью сменных носителей, голосовых сообщений, SMS, аудио- и видеоканалов связи, через бумажные документы и даже изучая содержимое мусорных корзин. Распространённой проблемой остаётся кража или утеря ноутбуков и других гаджетов.

В современном мире, где организации коммерческой, финансовой, медицинских, перерабатывающих и энергетических сфер, в том числе все правительственные структуры, организовывают сбор, хранение и обработку всей необходимой в работе информации, а также пер-

сональные данные сотрудников, пользователей, клиентов и посетителей. В основном вся эта информация требует защиты, так как является конфиденциальной, а возможные утечки ее, потери или хищения могут иметь непредсказуемые (негативные) последствия для людей и организаций (государств).

Разносторонней комплексной кибератаке с большей вероятностью подвергаются такие организации, которые непосредственно обеспечивают инфраструктуры целых городов, стран и мирового сообщества в целом. Такие организации или структуры называются критическими инфраструктурами (КИ). К КИ относятся: энерго и теплоснабжение, водо- и электроснабжение, системы переработки отходов и разнообразные транспортные структуры. В определенной мере каждая такая КИ взаимодействует с ЭВМ и безопасность всех взаимодействующих между собой инфраструктур необходима для полноценного их функционирования и нормальной жизнедеятельности общества. Критические инфраструктуры представляют собой сложные, пространственно-распределенные, многокомпонентные системы, устойчивая работа которых критически важна для функционирования экономики и жизнедеятельности людей [2].

В Республике Беларусь в настоящее время отсутствует Стратегия кибербезопасности, нет такого определения «кибербезопасность» в законодательстве, однако многие детальные положения, ее характеризующие, содержатся в различных нормативных документах.

Попробуем дать определение кибербезопасности как создание и реализация мероприятий по защите систем, сетей и различных приложений от компьютерных (цифровых) атак. Такие атаки обычно направлены на получение доступа к конфиденциальной информации, ее изменение и уничтожение, хищение денежных средств у банковских учреждений либо граждан.

В Республике Беларусь более устоявшимся термином является информационная безопасность.

От информационной безопасности банка зависят его репутация и конкурентоспособность. Высокий уровень обеспечения информационной безопасности кредитной организации позволяет минимизировать риски.

Система обеспечения информационной безопасности банка должна:

- быть адекватной внутренним и внешним угрозам;
- реализовывать комплексный подход к защите – включать все необходимые организационные меры и технические решения и защищать все компоненты ИС, включая системы ДБО;
- обеспечивать высокую производительность – обрабатывать значительные объемы информации без снижения быстродействия;
- быть надежной и отказоустойчивой благодаря применению инновационных технологий;
- иметь инструменты сбора, анализа данных об инцидентах и реагирования на инциденты информационной безопасности [3].

Кибербезопасность борется с тремя видами угроз:

- Киберпреступление – действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
- Кибератака – действия, нацеленные на сбор информации, в основном политического характера.
- Кибертерроризм – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

Как злоумышленникам удается получить контроль над компьютерными системами? Они используют различные инструменты и приемы:

- Вредоносное ПО.

Название говорит само за себя. Программное обеспечение, которое наносит вред, – самый распространенный инструмент киберпреступников. Они создают его сами, чтобы с его помощью повредить компьютер пользователя и данные на нем или вывести его из строя. Вредоносное ПО часто распространяется под видом безобидных файлов или почтовых вложений. Киберпреступники используют его, чтобы заработать или провести атаку по политическим мотивам.

Вредоносное ПО может быть самым разным, вот некоторые распространенные виды:

- Вирусы – программы, которые заражают файлы вредоносным кодом. Чтобы распространяться внутри системы компьютера, они копируют сами себя.

• Троянцы – вредоносы, которые прячутся под маской легального ПО. Киберпреступники обманом вынуждают пользователей загрузить троянца на свой компьютер, а потом собирают данные или повреждают их.

• Шпионское ПО – программы, которые втайне следят за действиями пользователя и собирают информацию (к примеру, данные кредитных карт). Затем киберпреступники могут использовать ее в своих целях.

• Программы-вымогатели шифруют файлы и данные. Затем преступники требуют выкуп за восстановление, утверждая, что иначе пользователь потеряет данные.

• Рекламное ПО – программы рекламного характера, с помощью которых может распространяться вредоносное ПО.

• Ботнеты – сети компьютеров, зараженных вредоносным ПО, которые киберпреступники используют в своих целях.

• SQL-инъекция

Этот вид кибератак используется для кражи информации из баз данных. Киберпреступники используют уязвимости в приложениях, управляемых данными, чтобы распространить вредоносный код на языке управления базами данных (SQL).

• Фишинг-атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь официальной организацией.

• Атаки Man-in-the-Middle («человек посередине»).

Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.

• DoS-атаки (атаки типа «отказ в обслуживании»).

Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так, злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность организации.

Как защититься от атак: полезные советы по кибербезопасности:

Предлагаем вам советы о том, как оградить компанию и ее сотрудников от киберугроз.

1. Обновите программное обеспечение и операционную систему. Используя новое ПО, вы получаете свежие исправления безопасности.

2. Используйте антивирусные программы. Защитные решения, такие как Kaspersky Total Security, помогут выявить и устранить угрозы. Для максимальной безопасности регулярно обновляйте программное обеспечение.

3. Используйте надежные пароли. Не применяйте комбинации, которые легко подобрать или угадать.

4. Не открывайте почтовые вложения от неизвестных отправителей – они могут быть заражены вредоносным ПО.

5. Не переходите по ссылкам, полученным по почте от неизвестных отправителей или неизвестных веб-сайтов – это один из стандартных путей распространения вредоносного ПО.

6. Избегайте незащищенных сетей Wi-Fi в общественных местах – в них вы уязвимы для атак Man-in-the-Middle.

Список использованных источников

1. Что такое кибербезопасность? [Электронный ресурс]. – Режим доступа: https://www.kaspersky.ru/resource-center/definitions/what-is-cyber-security. – Дата доступа: 03.11.2022.

2. Важность обеспечения кибербезопасности [Электронный ресурс]. – Режим доступа: https://spravochnick.ru/informacionnaya_bezopasnost/kiberbezopasnost_i_informacionnaya_bezopasnost/ . – Дата доступа: 03.11.2022.

3. Кибербезопасность [Электронный ресурс]. – Режим доступа: http://digitalbusiness.by/napravleniya-sotrudnichestva/natsionalnyj-bank-respubliki-belarus/kiberbezopasnost. – Дата доступа: 03.11.2022.