УДК 004.056

УГРОЗЫ КИБЕРБЕЗОПАСНОСТИ ДЛЯ ЭКОНОМИКИ

Янбарцева А.А.

студентка,

Вятский государственный университет,

Киров, Россия

Суслов М.Д.

студент

Вятский государственный университет,

Киров, Россия

Логинов Д.А.

д.э.н., профессор,

Вятский государственный университет,

Киров, Россия

Аннотация. В данной статье рассматриваются угрозы кибербезопасности для экономики. В связи с растущей зависимостью от информационных технологий и цифровизацией многих сфер деятельности, киберпреступность становится все более актуальной проблемой. Исследуются различные виды киберугроз, анализируется их воздействие на экономику и предлагаются меры для обеспечения кибербезопасности.

Ключевые слова. Угрозы, кибербезопасность, киберпреступность, информационные технологии, цифровизация, меры безопасностбезопасности, цифровое пространство.

CYBERSECURITY THREATS TO THE ECONOMY

Yanbartseva A.A.

3rd year student, direction "Economic security",

Vyatka State University,

Kirov, Russia

Suslov M. D.

3rd year student, direction "Economic security",

Vyatka State University,

Kirov, Russia

Loginov D.A.

Doctor of Science: Doctor of Economic Sciences

Vyatka State University,

Kirov, Russia.

Annotation. This article examines the threats of cybersecurity to the economy. Due to the growing dependence on information technology and the digitalization of many fields of activity, cybercrime is becoming an increasingly urgent problem. Various types of cyber threats are investigated, their impact on the economy is analyzed, and measures to ensure cybersecurity are proposed.

Keywords. Threats, cybersecurity, cybercrime, information technology, digitalization, security measures, digital space.

В наше время, когда информационные технологии проникают во все сферы жизни и деятельности, безопасность в цифровом пространстве играет критическую роль для экономического благосостояния. Угрозы кибербезопасности становятся все более представительными и многообразными, поэтому оценка их влияния на экономику и разработка соответствующих мер безопасности являются важной задачей.

Одним из наиболее серьезных видов угроз кибербезопасности является киберпреступность. Киберпреступники постоянно развивают новые и все более сложные методы атак, направленные на корпорации, правительства и гражданские структуры. Их целью является получение конфиденциальной информации, манипуляция системами или просто нанесение ущерба целевым организациям, что может серьезно повлиять на экономическую стабильность и снизить доверие к цифровым технологиям. [1]

Растущая зависимость от информационных технологий также открывает новые уязвимости для экономики. Киберугрозы могут привести к краже интеллектуальной собственности, нарушению важных производственных процессов или даже вымогательству. Это может иметь серьезные последствия, такие как потеря конкурентоспособности, обваливание рыночной стоимости компании или даже ее полное разорение.

Для обеспечения кибербезопасности и минимизации угроз компании и государства должны принимать ряд мер. Прежде всего, это обновление устаревших систем и программ с целью устранения уязвимостей. Также важно проводить обучение сотрудников о безопасном поведении в онлайн-среде. Регулярное аудирование систем и применение современных методов шифрования также играют важную роль в защите данных. [4]

Для обеспечения кибербезопасности важно использовать комплексный подход, что включает не только технические меры, но и организационные и человеческие. Настройка угроз и обнаружение инцидентов также является важной частью эффективной кибербезопасности. Это позволяет оперативно реагировать на атаки и минимизировать негативные последствия. Сотрудничество между компаниями и государственными организациями также имеет большое значение, поскольку это позволяет обмениваться информацией об актуальных угрозах и разрабатывать совместные стратегии по борьбе с киберпреступностью.

Одним из главных принципов кибербезопасности является постоянная актуализация и обновление мер безопасности. Киберугрозы постоянно эволюционируют, поэтому необходимо постоянно мониторить и анализировать новые виды угроз и обновлять системы и программы с учетом этих изменений. Применение современных методов шифрования и аутентификации также помогает защитить данные от несанкционированного доступа. [3]

Обучение сотрудников безопасному поведению в онлайн-среде также является неотъемлемой частью эффективной кибербезопасности. Подготовленный и осведомленный персонал может быть первой линией защиты от фишинговых атак, социальной инженерии и других видов мошенничества. Проведение регулярных тренингов и обучающих программ помогает повысить осведомленность сотрудников и укрепить их навыки.

Одной из важных составляющих комплексного подхода к кибербезопасности является проведение регулярного аудита систем и программного обеспечения. Это позволяет выявлять уязвимости в инфраструктуре и предотвращать возможные атаки на ранних стадиях. Также важно вести постоянный мониторинг сетевой активности и анализировать необычное поведение, чтобы оперативно обнаруживать инциденты.

Еще одним важным аспектом кибербезопасности является защита персональных данных и конфиденциальной информации. Каждая организация или предприятие должны разработать и реализовать строгую политику доступа к данным, чтобы ограничить доступ только к нужным лицам. Это поможет предотвратить утечку информации и защитить компании от финансовых или репутационных потерь. [2] (рис.1)

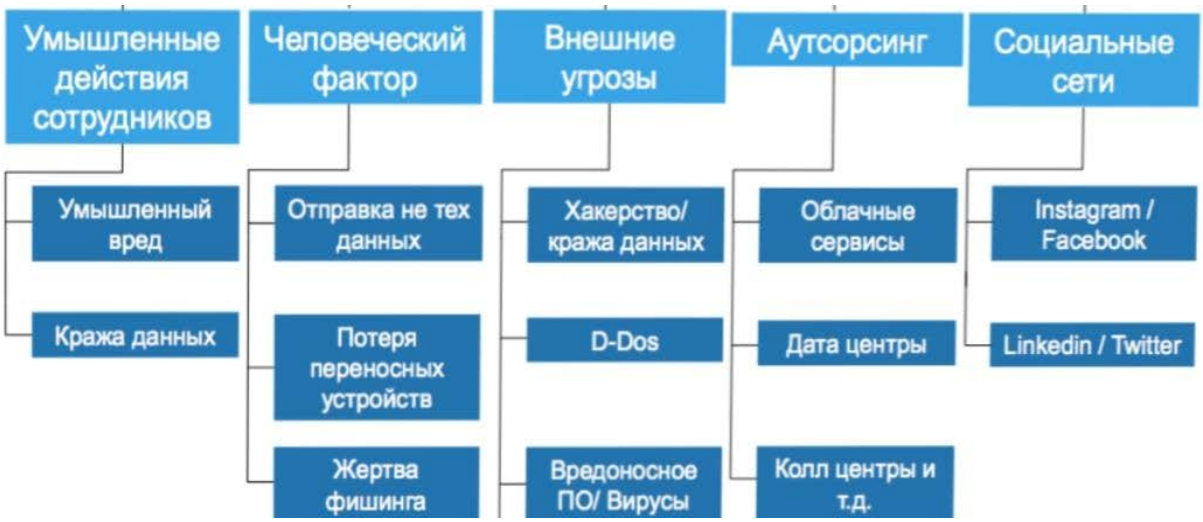

Рис. 1 – Виды экономических рисков и кибер – угроз

Компании должны иметь четкий план действий в случае возникновения кибератаки или другого инцидента. Это включает в себя определение ролей и ответственностей, настройку систем мониторинга и оповещения, а также проведение учений и симуляций, чтобы проверить эффективность плана. Следовательно, эффективная кибербезопасность требует постоянного внимания и усилий со всех участников системы. Только совместными усилиями компаний, правительственных организаций и общественности мы сможем создать надежную и безопасную цифровую среду. Постоянное обновление мер безопасности, обучение сотрудников и разработка новых технологий – все это необходимо для защиты от современных киберугроз и обеспечения безопасности в цифровой эпохе.

Еще одним важным аспектом кибербезопасности является постоянное обновление мер безопасности и защитных систем. Киберугрозы постоянно эволюционируют, искусные хакеры находят новые способы атаки, поэтому необходимо быть на шаг впереди и постоянно адаптироваться к новым угрозам. Это включает в себя регулярные обновления программного обеспечения, патчи безопасности, а также улучшение систем обнаружения и

предотвращения атак. Компании должны также следить за последними трендами в области кибербезопасности и принимать меры для защиты от наиболее актуальных угроз. [2]

Важным аспектом эффективной кибербезопасности является также обучение сотрудников. Человеческий фактор может быть слабым звеном в системе безопасности, поэтому необходимо обеспечить обучение и повысить осведомленность сотрудников о наиболее распространенных угрозах, методах фишинга и способах защиты от них. Это включает проведение тренингов, организацию семинаров и распространение информационных материалов о безопасности информации. Чем лучше подготовлены сотрудники, тем меньше вероятность успешной атаки изнутри компании.

Кроме того, создание партнерств и сотрудничество между компаниями, правительственными организациями и общественными структурами является неотъемлемой частью эффективной кибербезопасности. Киберугрозы не заботятся о границах и отраслевых различиях, поэтому важно совместно работать над разработкой общих стандартов безопасности, обменом информацией о новых угрозах и лучшими практиками. Компании и правительственные организации могут также сотрудничать в области обмена экспертами и разработки новых технологий для более эффективной защиты от киберугроз.

Таким образом, эффективная кибербезопасность требует комплексного подхода и включает в себя проведение аудита систем и программного обеспечения, защиту персональных данных и конфиденциальной информации, разработку стратегии реагирования на инциденты, постоянное обновление мер безопасности, обучение сотрудников и сотрудничество между компаниями и организациями.

Кроме того, компании должны уделить особое внимание обеспечению защиты от внутренних угроз. Даже самые сильные и надежные меры безопасности могут быть обойдены, если злоумышленник получит доступ к

внутренним системам или намеренно нарушит правила. Для борьбы с этими угрозами необходимо устанавливать строгие политики доступа, проводить регулярные проверки систем и мониторинг активности сотрудников. Технические решения, такие как системы обнаружения утечек данных и внутренних атак, также могут помочь выявить и предотвратить потенциальную угрозу изнутри.

В заключение можно сказать, что эффективная кибербезопасность требует постоянного внимания и принятия всеобъемлющих мер. Она включает в себя не только технические аспекты, такие как обновление систем и программного обеспечения, но и развитие «культуры безопасности», обучение сотрудников, контроль внутренних угроз и сотрудничество между различными участниками сектора. Только совместными усилиями можно создать безопасную среду в цифровом пространстве и эффективно противостоять современным киберугрозам.

Библиографический список

1. Бальтасаров А.В. Киберугрозы и методы их обнаружения / А.В. Бальтасаров // Кибербезопасность: образование, наука, технологии. – 2019. – Т. 5, № 4. – С. 26-33.

2. Вязовский В.И. Взаимодействие информационной безопасности с деятельностью предприятия [Электронный ресурс] / В.И. Вязовский // Вестник Московского университета [Сайт]. – 2015. – № 2. – С. 24-31. – Режим доступа: https://vestnik.msu.ru/media/magazines/10_170_2015_2/1678/1678.pdf

3. Гросул В.П. Профессиональная подготовка специалистов по кибербезопасности в высшей школе: проблемы и перспективы / В.П. Гросул, О.В. Клочко // Труды БГТУ. – 2019. – Т. 8, № 2. – С. 111-118.

4. Данилова С.В. Актуальные проблемы кибербезопасности в сфере электроэнергетики / С.В. Данилова, А.В. Качур // Вестник НГТУ. – 2018. – Т. 26, № 2. – С. 113-119.

5. Еремин И.К. Проектирование системы обработки информации при разработке стандартов информационной безопасности / И.К. Еремин // Кибербезопасность: образование, наука, технологии. – 2017. – Т. 3, № 3. – С. 11-19.

Оригинальность 80%