УДК 338

КИБЕРНЕТИЧЕСКАЯ ЭКОНОМИЧЕСКАЯ БЕЗОПАСНОСТЬ: КЛЮЧЕВЫЕ ТРЕНДЫ И ХАРАКТЕРИСТИКИ

Н.А. Герасимова
Белгород, Россия
Белгородский государственный национальный исследовательский университет
Н.М. Шевцова
г. Воронеж, Россия
Воронежский государственный аграрный университет имени императора Петра I

Аннотация. *В современном мире, где технологии играют ключевую роль, кибербезопасность стала чрезвычайно важной проблемой. В статье представлены базовые тренды кибернетической экономической безопасности.*

Ключевые слова: *экономическая безопасность, кибернетическая экономическая безопасность, киберпространство, угрозы, информация.*

CYBER ECONOMIC SECURITY: KEY TRENDS AND CHARACTERISTICS

N.A. Gerasimova
Belgorod, Russia
Belgorod State National Research University
N.M. Shevtsova
Voronezh, Russia
Voronezh State Agrarian University named after Emperor Peter the Great

Annotation. *In today's world, where technology plays a key role, cybersecurity has become an extremely important issue. The article presents the basic trends of cybernetic economic security.*

Keywords: *economic security, cybernetic economic security, cyberspace, threats, information.*

В условиях цифровой трансформации предприятие функционирует в киберпространстве. Киберпространство относится к виртуальному миру, который создается компьютерной сетью. Это место, где люди, устройства и компьютерные системы общаются и обмениваются информацией.

Киберпространство включает в себя интернет, социальные сети, веб-сайты, мобильные приложения и многое другое. В современном цифровом мире кибербезопасность чрезвычайно важна. Одним из важнейших аспектов киберпространства является безопасность. По мере развития технологий появляются и новые угрозы, такие как киберпреступность, кража личных данных или хакерские атаки. Вот почему так важно защищать свои данные и быть осторожными в сети. По мере того, как технологии развиваются все быстрее и быстрее, угрозы киберпреступности развиваются. Кибератака может привести к краже конфиденциальных данных, таких как личные данные, финансовые данные или коммерческая информация. Украденные данные могут быть использованы для различных целей, таких как кража личных данных, финансовое мошенничество или шантаж. Атака на компьютерную систему может привести к нарушению конфиденциальности пользователей. Хакеры могут получить доступ к личным сообщениям, фотографиям или другой конфиденциальной информации, что может привести к серьезным последствиям для жертв.

Кибератака может привести к перебоям в работе информационных систем, что, следовательно, приведет к сбоям в работе компании. Эти перерывы могут быть дорогостоящими и привести к потере клиентов и репутации компании.

Кибератака может так же представлять угрозу для критической инфраструктуры, такой как электростанции, электрические сети или транспортные системы. Атака на эти системы может привести к серьезным последствиям для общества, таким как перебои в подаче электроэнергии или сбои в транспортировке.

Характерные элементы и составные части кибербезопасности приведены на рисунке 1.

1. Защита каналов передачи данных.
2. Защита телекоммуникационной инфраструктуры.
3. Защита Интернет-сети.
4. Защита компьютерных устройств.
5. Защита приложений.
6. Защита данных.
7. Защита основных услуг.
8. Защита личности граждан.
9. Защита государственных интересов.
10. Защита национальных интересов..
11. Защита региональных интересов.
12. Защита международных интересов.

Рисунок 1 – Характерные элементы и составные части кибербезопасности

Угрозы информационной безопасности РФ, в том числе и в кибернетическом пространстве, подразделяются на следующие виды (рисунок 2).

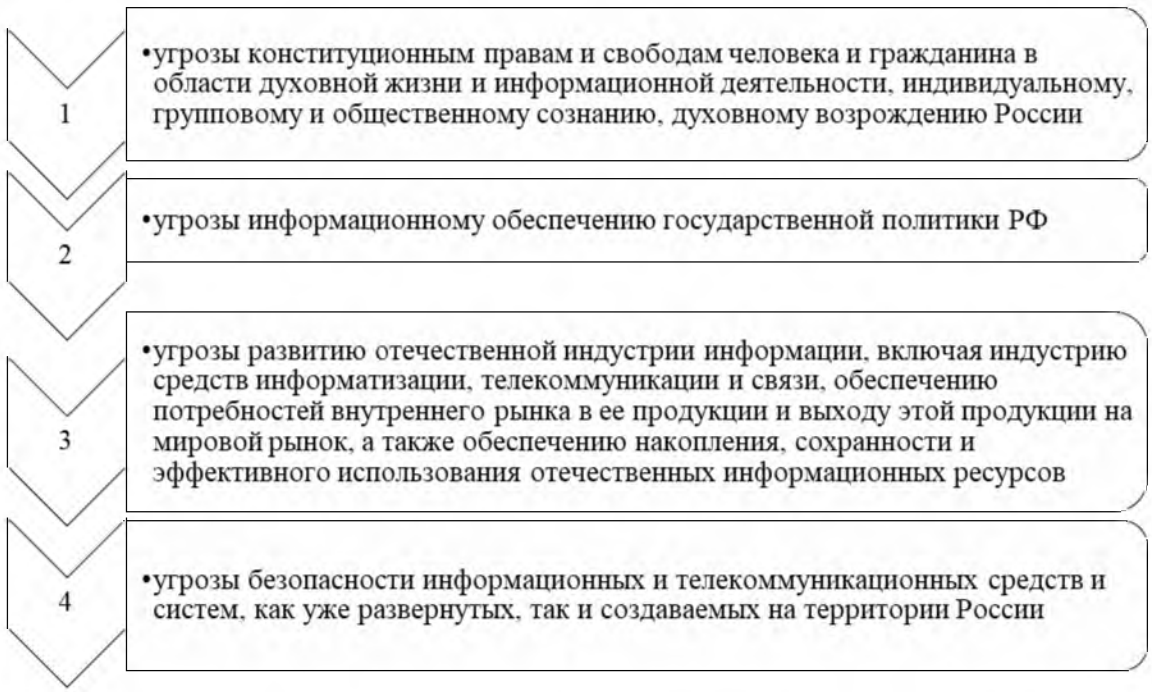

Рисунок 2 – Угрозы информационной безопасности РФ

Дадим более подробную характеристику угроз. Вымогатели – одна из самых серьезных угроз в киберпространстве. Это включает в себя блокировку доступа к данным или устройству, а затем запрос выкупа в обмен на их разблокировку. Это серьезная угроза, которая может привести к потере ценной информации.

Фишинг – это метод, используемый киберпреступниками для получения конфиденциальной информации, такой как пароли или данные кредитной карты. Злоумышленники выдают себя за доверенные учреждения или отдельных лиц, отправляя поддельные электронные письма или текстовые сообщения.

Вредоносное ПО – это программное обеспечение, которое может заразить рабочие устройства; под его воздействием могут производиться различные вредоносные действия: кража данных, мониторинг активности пользователя, повреждение операционной системы.

Важным шагом в обеспечении кибербезопасности предприятия является понимание и принятие угроз, связанных с хранением, обработкой и обменом информацией. Предприятия должны осознавать, какая информация наиболее ценна для достижения целей, в том числе и финансовых, какие риски могут возникнуть при ее обработке и хранении, вырабатывать стратегии управления кибербезопасностью. Так же важным является внедрение следующих мероприятий, как:

1. Регулярное обновление программного обеспечения, реализация данного процесса имеет решающее значение для обеспечения безопасности системы.
2. Использование надежных, уникальных паролей важно, чтобы хакерам было труднее получить доступ к учетным записям. Пароли должны быть длинными, содержать комбинацию букв, цифр и специальных символов.
3. Установка и регулярное обновление антивирусного программного обеспечения может помочь вам обнаружить и заблокировать вредоносное программное обеспечение.
4. Сотрудники должны получать возможность проходить специальное обучение, повышать свою квалификацию, с точки зрения появления у них компетенций, помогающих реализации процесса распознавания потенциальных угроз и умения быстро реагировать и принимать своевременные действия снижения негативного влияния угроз..

Таким образом, цифровая трансформация предприятий, все связанные с ней технологические преобразования произошедшие в последние годы, открывают ряд новых возможностей для предприятий. С новыми возможностями появляются и новые угрозы. охватывать такие темы, как фишинг, пароли и безопасное использование сети.

Кибератаки оказывают серьезное влияние на безопасность данных, бизнес-деятельность и общество в целом. Для защиты от этих атак важно использовать соответствующие меры безопасности, такие как обновление программного обеспечения, надежные пароли, антивирусная защита и обучение сотрудников. Только так можно минимизировать риск кибератак и защитить наши данные и инфраструктуру.

К возникающим в ходе реализации трансформационных процессов, вопросам кибербезопасности следует относиться с особым вниманием, так как их игнорирование приводит к очень негативным последствиям. Политика создания безопасной и устойчивой среды информационной предприятия должна быть включена в корпоративную цифровую стратегию.

ЛИТЕРАТУРА

1. Герасимова, Н.А. Кибернетические риски социально-экономических систем, возникающие в процессе цифровой трансформации / Н. А. Герасимова // Актуальные проблемы развития экономических, финансовых и кредитных систем : Сборник материалов XI Международной научно-практической конференции, Белгород, 14–15

сентября 2023 года. – Белгород: Белгородский государственный национальный исследовательский университет, 2023. – С. 185-188. – EDN QAXGIU.

2. Нежурина, Д.О. Оценка рисков в системе экономической безопасности предприятия / Д. О. Нежурина, Н. А. Герасимова // Экономическая безопасность социально-экономических систем: вызовы и возможности : Сборник трудов V Международной научно-практической конференции, Белгород, 28 апреля 2023 года / Отв. редакторы Е.А. Стрябкова, Н.А. Герасимова. – Белгород: Общество с ограниченной ответственностью Эпицентр, 2023. – С. 284-287. – EDN JDYTSP.

3. Указ Президента от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности РФ» // СПС «Консультант Плюс».

4. Управление киберрисками. Как определить главные угрозы для компании Электронный ресурс, режим доступа: https://m.hightech.plus/2023/05/22/upravlenie-kiberriskami-kak-opredelit-glavnie-ugrozi-dlya-kompanii (дата обращения 30.09.2023).

5. Цхададзе, Н. В. Кибербезопасность в Российской Федерации / Н. В. Цхададзе, А. З. Калмыкова // Проблемы информационной безопасности социально-экономических систем : Труды IX Международной научно-практической конференции, Гурзуф, 02–04 марта 2023 года / Под редакцией О.В. Бойченко. – Симферополь: Крымский федеральный университет им. В.И. Вернадского, 2023. – С. 153-156. – EDN DESLGL.

УДК 338

ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ХОЗЯЙСТВУЮЩИХ СУБЪЕКТОВ РФ В СФЕРЕ ПОД/ФТ И ФРОМУ

Т.Н. Добродомова
г. Белгород, Россия
Белгородский государственный национальный исследовательский университет
И.В. Савенкова
г. Ростов-на-Дону, Россия
Управление Федерального казначейства по Ростовской области

Аннотация. В статье рассматриваются вопросы, связанные с правовым обеспечением экономической безопасности хозяйствующих субъектов, а именно в сфере противодействия отмыванию денег, финансированию терроризма, распространению оружия массового уничтожения. Анализируются нормативные акты, регулирующие деятельность государств в рамках эффективной борьбы с этими явлениями.

Ключевые слова: *правовое обеспечение, экономическая безопасность, противодействие, отмывание денег.*

LEGAL SUPPORT OF ECONOMIC SECURITY OF ECONOMIC ENTITIES OF THE RF IN THE FIELD OF POD/FT AND FROMU

T.N. Dobrodomova
Belgorod, Russia
Belgorod State National Research University
I.V. Savenkova
Rostov-on-Don, Russia
Federal Treasury Department for the Rostov region

Annotation. The article discusses issues related to the legal provision of economic security of business entities, namely in the field of combating money laundering, the financing of