Российский экономический интернет-журнал №4/2023

Научная статья
Original article
Шифр научной специальности 5.2.3
УДК 338

Взаимосвязь кибербезопасности и экономической безопасности на современном этапе развития

Микаева А.С., к.э.н., доцент, доцент кафедры «Финансовый учёт и контроль» Института кибербезопасности и цифровых технологий
МИРЭА - Российский технологический университет», Москва, Россия
Пенчукова Т.А., к.э.н., доцент, доцент кафедры «Финансовый учёт и контроль» Института кибербезопасности и цифровых технологий
МИРЭА - Российский технологический университет», Москва, Россия
Сенькина В.А., студент кафедры «Финансовый учёт и контроль» Института кибербезопасности и цифровых технологий
МИРЭА - Российский технологический университет», Москва, Россия

Аннотация. В статье был проведен анализ и оценка состояния кибербезопасности в Российской Федерации с целью выявления рисков и угроз в информационной инфраструктуре страны и их влияние на состояние экономической безопасности Российской Федерации, а также были определены необходимые меры для повышения уровня защиты кибербезопасности в системе экономической безопасности.

Ключевые слова: кибербезопасность, экономическая безопасность, киберпреступность, киберугрозы, кибератаки, информационная безопасность, защита критической информационной инфраструктуры.

The relationship between cybersecurity and economic security at the present stage of development

Mikaeva A.S., Ph.D., Associate Professor, Associate Professor of the Department of Financial Accounting and Control, Institute of Cybersecurity and Digital Technologies

MIREA – Russian Technological University, Moscow, Russia
Penchukova T.A., Ph.D., Associate Professor, Associate Professor of the Department of Financial Accounting and Control, Institute of Cybersecurity and Digital Technologies
MIREA – Russian Technological University, Moscow, Russia
Senkina V.A., student of the Department of Financial Accounting and Control, Institute of Cybersecurity and Digital Technologies
MIREA – Russian Technological University, Moscow, Russia

Annotation. The article analyzed and assessed the state of cybersecurity in the Russian Federation in order to identify risks and threats in the country's information infrastructure and their impact on the state of economic security of the Russian Federation, and also identified the necessary measures to increase the level of cybersecurity protection in the economic security system.

Key words: cybersecurity, economic security, cybercrime, cyberthreats, cyberattacks, information security, protection of critical information infrastructure.

В современном информационном обществе, где возрастает зависимость экономики от цифровых технологий, защита информационных систем и данных от киберугроз становится неотъемлемой частью обеспечения безопасности государства. В настоящее время взаимосвязь между кибербезопасностью и экономической безопасностью играет ключевую роль в обеспечении устойчивого развития страны и экономики в целом [4].

Под кибербезопасностью понимается защита информационных систем, сетей, программного обеспечения и данных от кибератак, вредоносных программ, взломов и других угроз. Обеспечение кибербезопасности позволяет предотвратить утечку конфиденциальной информации, нарушение работы информационных систем и потерю данных, что в свою очередь может предотвратить финансовые потери и ущерб в рамках обеспечения экономической безопасности на уровне хозяйствующего субъекта или страны в целом [10].

Экономическая безопасность определяется как способность экономики обеспечивать устойчивое развитие, противостоять внутренним и внешним угрозам, сохранять стабильность и обеспечивать рост благосостояния населения. Эффективное управление кибербезопасностью способствует обеспечению экономической безопасности, предотвращая возможные потери от кибератак и сохраняя стабильность информационных систем.

Становится очевидным, что в ближайшие годы сохранится положительная тенденция данного явления, требуя от государств и хозяйствующих субъектов непрерывного совершенствования мер по защите данных.

С учетом вышесказанного, следует отметить важное значение вопроса правового регулирования и международного сотрудничества в области кибербезопасности, которое помогает эффективно противостоять угрозам в данной сфере [1].

Создание правового фундамента для обеспечения кибербезопасности в Российской Федерации выступает одной из главных задач нормативного регулирования, которое направлено на защиту безопасности государства, хозяйствующих субъектов и всех граждан. В рамках этой задачи разрабатывается и принимается соответствующее законодательство, которое определяет обязанности и ответственность организаций и граждан в области обеспечения кибербезопасности, а также устанавливает механизмы контроля и наказания за совершение правонарушений и преступлений. Регулирование выполняется на различных уровнях – международном и государственном.

Международное правовое регулирование кибербезопасности осуществляется через международные договоры и соглашения. Один из ключевых документов – это Всемирная конвенция об информационной безопасности (WCIS), принятая Генеральной Ассамблеей ООН в 2010 году. Конвенция предлагает ряд мер и принципов, включая защиту критической информационной инфраструктуры, борьбу с киберпреступностью и кооперацию между государствами [6].

Основными документами, определяющими подходы к обеспечению кибербезопасности в Российской Федерации, являются:

1. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» данный закон устанавливает основные принципы и подходы к обеспечению кибербезопасности в России [3].

2. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» предусматривает определения основных понятий, связанных с информацией, информационными технологиями и защитой информации, а также устанавливает правила и принципы организации, хранения, передачи, обработки и защиты информации [1].

3. Стратегия национальной безопасности Российской Федерации документ, который определяет цели и задачи в области кибербезопасности, а также основные направления развития киберинфраструктуры страны [7].

4. Доктрина информационной безопасности Российской Федерации устанавливает цель, основные принципы и задачи обеспечения информационной безопасности в стране [4].

5. Национальная стратегия развития киберинтеллекта Российской Федерации определяет основные цели и приоритеты развития киберинтеллектуальных возможностей. Ее основная задача заключается в обеспечении информационной безопасности и защите интересов государства в киберпространстве [5].

6. Национальная программа «Цифровая экономика Российской Федерации» представляет собой стратегический документ, разработанный с целью стимулирования развития цифровой экономики в России. Она определяет меры и задачи для достижения этой цели.

На основании проведенного анализа, можно выделить задачи кибербезопасности, которые включают в себя защиту государственных и коммерческих информационных систем от кибератак, предотвращение утечек

конфиденциальной информации, обеспечение надежности электронной коммерции и банковских операций, защиту критической инфраструктуры страны, включая энергетические системы, транспортную и коммуникационную инфраструктуру [2].

Для России, как одной из ведущих кибердержав мира, проблема кибербезопасности имеет стратегическое значение как фактор обеспечения суверенитета обороны и безопасности государства, а также эффективного развития экономической и социальной сферы. В этой связи необходимы постоянный мониторинг данных, о совершаемых правонарушениях в данной сфере и киберпреступлениях, и анализ событий с целью выявления потенциальных угроз.

Кибератаки могут нанести ущерб любой отрасли экономики, так как электронные системы используются повсеместно, но есть несколько секторов, которые обычно подвергаются им в большей степени (рис. 1):

- банки, финансовые учреждения и платежные системы;
- онлайн-магазины и другие компании, осуществляющие онлайн-торговлю, подвергаются атакам со стороны злоумышленников, целью которых является получение доступа к платежным данным клиентов или кража личной информации;
- кибератаки, нацеленные на производственные предприятия, стремятся нарушить процессы производства. Такие атаки могут привести к серьезным негативным последствиям, затронув производственные линии, дизайн продуктов и передовые технологии;
- телекоммуникационные компании подвергаются угрозам кибератак, так как они играют ключевую роль в передаче данных и связи между организациями и людьми;
- медицинские организации владеют большим количеством информации, включая медицинские записи и личные данные пациентов, что делает их привлекательными для хакеров;

- кибератаки на государственные учреждения могут иметь различные мотивы, начиная от кражи секретных данных до нарушения функционирования государственных систем.

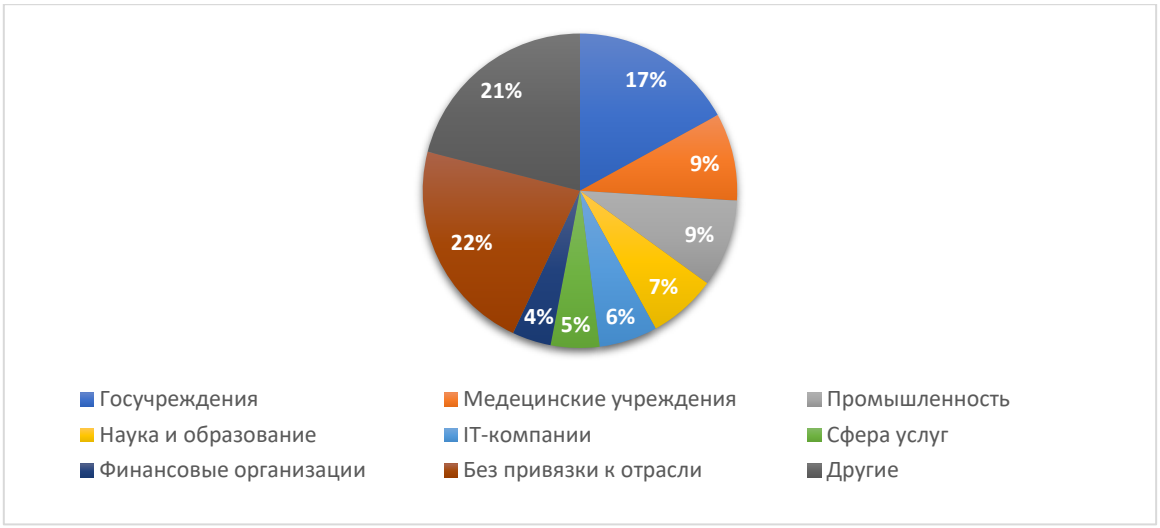

Рис. 1 – Киберпреступления по отраслям экономики

На расширенном заседании коллегии МВД, было извещено о том, что в 2021 году преступления, связанные с ИТ-сферой, составили 25 % от общего числа уголовных правонарушений в России, и выросли до полумиллиона. Отмечено главой государства, что приоритетом в деятельности МВД России является борьба с преступностью, включающая применение информационных технологий (рис. 2) [12].

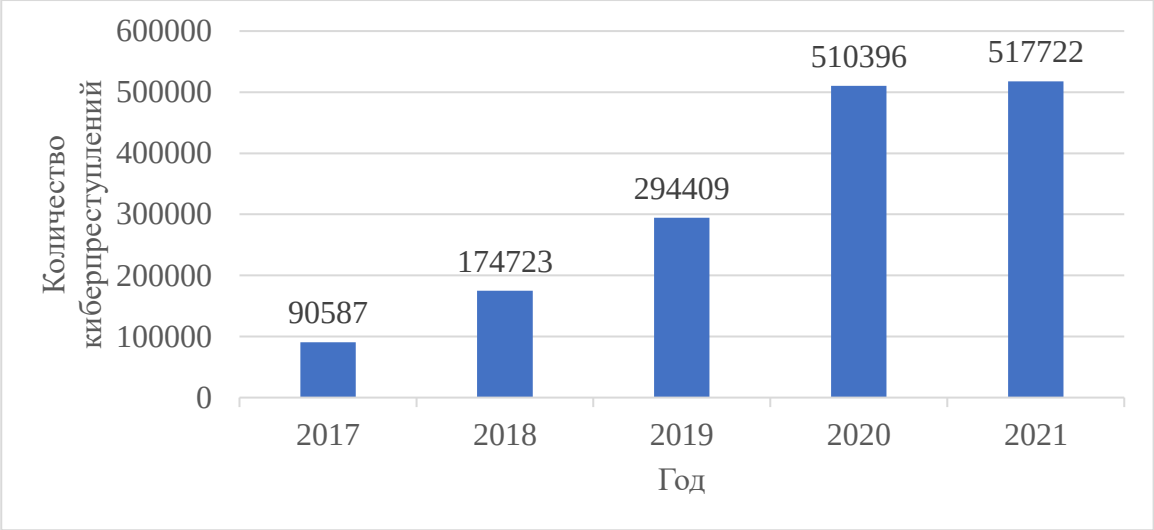

Рис. 2 - Динамика киберпреступлений 2017-2021 гг.

В 2021 году правоохранительные органы России провели расследование и выявили около 10 тыс. лиц, которые совершали мошенничества в сети Интернет или используя мобильную связь. Это число является значительным, так как оно увеличилось на 45% по сравнению с предыдущим годом.

Согласно статистическим данным, в 2021 году количество преступлений, связанных с использованием информационных технологий (ИТ), достигло отметки в 517 722 случая. Это число на 1,44% превышает показатель предыдущего года, когда было зарегистрировано 510 396 преступлений. Тем не менее, стоит отметить, что оно практически вдвое превышает результаты 2019 года, где было зафиксировано лишь 294 409 преступлений [13].

Хищения в онлайн-пространстве отличаются высокой латентностью и низким уровнем раскрываемости, из-за возможности совершения этих преступлений на расстоянии [14]. Общий процент разоблаченных дел в данной категории составляет 20%, в 2021 году было раскрыто 94 942 дела.

Финансовые потери от киберпреступности в России сложно точно определить, так как многие случаи несанкционированного доступа к данным или взлома систем остаются незарегистрированными или незамеченными. Они огромны и составляют миллиарды долларов ежегодно. С увеличением количества случаев кибератак и совершенствованием методов их применения, финансовые потери растут пропорционально (рис. 3).

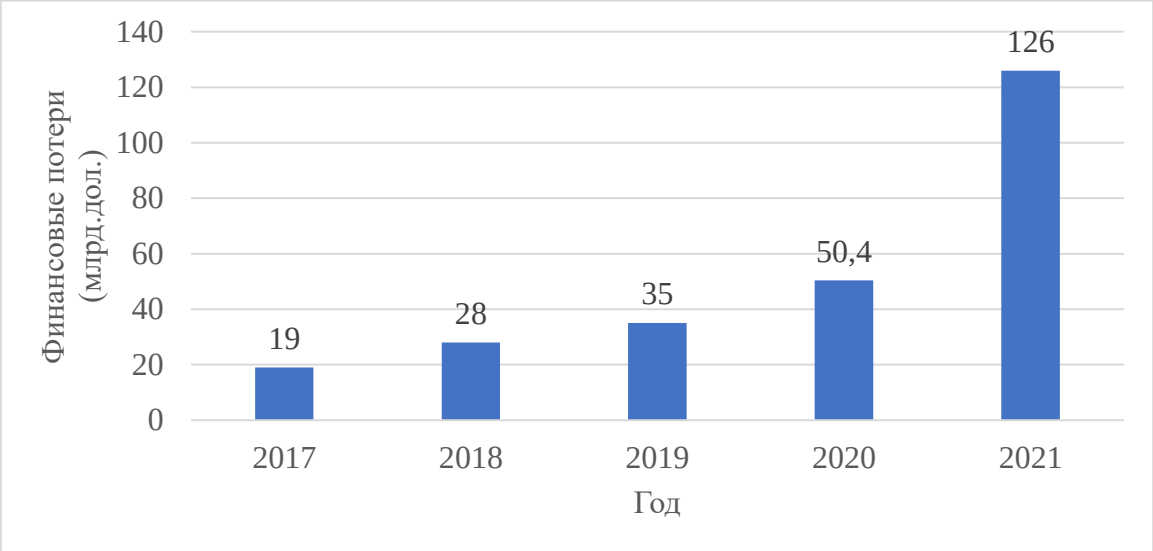

Рис. 3 – Финансовые потери в России от киберпреступности

Важно отметить, что киберпреступность несет не только финансовые потери, но и многочисленные иные негативные последствия. К ним можно отнести и репутационный ущерб, влияющий на доверие к компаниям и государству, а также потерю личных данных и нарушение приватности граждан. Все приведенные аспекты вместе создают серьезные проблемы для экономики и общества в целом [8].

Под угрозой кибербезопасности понимается потенциальное событие или действие, которое направленно на нанесение ущерба информационным системам, компьютерам, сетям или данным. Угрозы кибербезопасности могут иметь различные цели, такие как кража личной информации, вымогательство, разрушение, шпионаж, саботаж и т. д. Существует ряд угроз, которые могут негативно повлиять на экономическую безопасность [9]:

1. Финансовые мошенничества – преступные действия, которые направлены на получение незаконной выгоды или обман других людей в финансовых операциях. Одним из наиболее распространенных видов мошенничества является фишинг. Под видом официальных сайтов и электронных писем, злоумышленники получают доступ к личным данным, банковским счетам и кредитным картам.

2. Распространение вредоносного программного обеспечения. Злонамеренное программное обеспечение, такое как вирусы или троянские программы, может заражать компьютерные системы и сети, вызывая выход из строя важных инфраструктурных систем, таких как электросети или транспортные системы. Возможные последствия данной ситуации включают серьезные финансовые убытки и нарушение бизнес-процессов.

3. Кибершпионаж – это процесс взлома компьютерных систем или сетей с целью получения информации, которая может быть использована для различных целей, таких как получение конфиденциальной информации, торговых секретов, политическое подрывательство или хищение интеллектуальной собственности.

4. Социальная инженерия – приём влияния на поведение и мышление людей с целью незаконного доступа к конфиденциальным информационным ресурсам или получения неправомерных выгод. В социальной инженерии используются методы манипуляции и обмана, часто прибегают к использованию психологических техник, чтобы убедить лицо предоставить доступ к информации, паролям или выполнить конкретные действия.

5. Кибертерроризм является серьёзной угрозой для экономических систем и правопорядка. Данное явление может включать в себя атаки на критическую инфраструктуру, такую как электросети или финансовые системы.

Вышеприведенные угрозы являются одними из основных угроз кибербезопасности, и список является неполным, так как эта область постоянно меняется и развивается. Все эти угрозы могут привести к серьезным экономическим потерям, потере доверия и нарушению бизнес-процессов. Следовательно, обеспечение кибербезопасности становится жизненно важной задачей для гарантирования экономической стабильности.

Анализ киберугроз свидетельствует о том, что данное явление является серьезной проблемой для международной и национальной экономической безопасности. Постоянное развитие технических средств, используемых злоумышленниками для осуществления атак, обусловливает необходимость активного и комплексного подхода в реализации защитных мер для обеспечения стойкости и безопасности информационной инфраструктуры [11].

В целях обеспечения кибербезопасности в России существуют соответствующие государственные органы и структуры, можно выделить следующие: Федеральная служба безопасности (ФСБ), Министерство внутренних дел (МВД), Министерство цифрового развития, связи и массовых коммуникаций (Минцифры), Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор), Центр по противодействию киберпреступности и другие. Кроме того, разрабатывается и активно применяется законодательство, направленное на обеспечение безопасности в киберпространстве.

Помимо принятия внутренних мер, Россия активно взаимодействует с другими странами и международными организациями в области обеспечения кибербезопасности. В рамках такого сотрудничества обмениваются информацией об угрозах, разрабатываются совместные механизмы реагирования на кибератаки и проводятся совместные тренировки и учения [1].

Противодействие угрозам кибербезопасности на уровне государства включает в себя ряд мероприятий, которые направлены на предотвращение, обнаружение и реагирование на возможные атаки в Сети. Можно выделить следующие ключевые меры:

- разработка национальной стратегии кибербезопасности, в которой следует рассмотреть цели, принципы и меры по защите критической информационной инфраструктуры;
- создание центра управления кибербезопасностью, ответственного за координацию и мониторинг кибербезопасности на уровне государства;
- установка обязательных требований к защите критической информационной инфраструктуры для организаций, владеющих или эксплуатирующих такую систему;
- развитие национальной системы обнаружения и реагирования на кибератаки направленные на государственные системы;
- повышение профессиональной компетентности и расширение образования в области кибербезопасности;
- ужесточение мер наказания за киберпреступления, чтобы повысить их сдерживающий эффект и предотвратить новые атаки;
- международное сотрудничество на международном уровне для обмена информацией об угрозах и координации действий при обнаружении и реагировании на кибератаки;
- пропаганда безопасного поведения в сети Интернет. Проведение информационно-просветительских мероприятий и кампаний, направленных на

повышение осведомленности населения о киберугрозах и методах их предотвращения;

- разработка и внедрение инновационных технических решений для обеспечения безопасности, необходимо способствовать разработке и внедрению новых технологий и технических средств защиты, которые помогают предотвращать и реагировать на кибератаки;
- анализ и обмен информацией о киберугрозах с другими странами и хозяйствующими субъектами, чтобы улучшить меры противодействия внутри страны.

Подводя итог можно сказать, что существует тесная связь между кибербезопасностью и экономической безопасностью. Недостаточный уровень обеспечения кибербезопасности может серьезно повлиять на экономическую стабильность и безопасность хозяйствующих субъектов и государства.

В современном информационном обществе практически все экономические субъекты зависят от применения информационных систем и сети Интернет, постоянно сталкиваются с угрозами кибератак и другими преступными действиями посредствам Сети. Эффективное управление кибербезопасностью становится неотъемлемым условием для обеспечения стабильности и устойчивого экономического роста, создает благоприятную экономическую среду, способствует привлечению инвестиций и способствует развитию цифровых технологий.

Библиографический список:

1. Федеральный закон от 27.07.2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Собрание законодательства Российской Федерации, 2006 г., № 31, ст. 3448.

2. Федеральный закон от 28.12.2010 г. № 390-ФЗ «О безопасности», Собрание законодательства Российской Федерации, 2010 г., № 1, ст. 2

3. Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», Собрание законодательства Российской Федерации, 2017 г., № 31, ст. 4736.

4. Указ Президента РФ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации», Собрание законодательства Российской Федерации, 2016 г., № 50, ст. 7074.

5. Указ Президента РФ от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации», Собрание законодательства Российской Федерации, 2019 г., № 41, ст. 5700.

6. Указ Президента РФ от 12.04.2021 № 213 «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности», Собрание законодательства Российской Федерации, 2021 г., №16, ст. 2746.

7. Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации», Собрание законодательства Российской Федерации, 2021 г., № 27, ст. 5351.

8. Белоус А. И., Солодуха В. А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. — Москва: ТЕХНОСФЕРА, 2021. — 482 с.

9. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения: учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва: Издательство Юрайт, 2023. — 342 с. — (Профессиональное образование).

10. Козырь, Н.С. Экономические аспекты информационной безопасности: учебник и практикум для вузов / Н. С. Козырь, Л. Л. Оганесян. — Москва: Издательство Юрайт, 2023. — 131 с. — (Высшее образование).

11. Мамаева Л.Н., Бехер В.В. Угрозы кибербезопасности в цифровом пространстве // Вестник Саратовского государственного социально-экономического университета. 2019. № 4 (78). С. 68-70.

12. Отчет Генеральной прокуратуры Российской Федерации о преступлениях, совершенных с использованием современных информационно-коммуникационных технологий / Официальный сайт Генпрокуратуры РФ. URL: https://epp.genproc.gov.ru/web/proc_cfo/mass-media/news/archive?item=84860550

13. Состояние преступности // МВД РФ [Электронный ресурс]. URL: https://мвд.рф/reports (дата обращения: 13.10.2023).

14. Микаева А.С., Пенчукова Т.А., Совершение мошеннических действий в сети Интернет и их влияние на экономическую безопасность / Российский экономический интернет-журнал. – 2022. – № 1.

References:

1. Federal Law of July 27, 2006 № 149-FZ «On information, information technologies and information protection», Collection of Legislation of the Russian Federation, 2006, № 31, Art. 3448.

2. Federal Law of December 28, 2010 № 390-FZ «On Security», Collection of Legislation of the Russian Federation, 2010, № 1, Art. 2

3. Federal Law of July 26, 2017 № 187-FZ «On the security of critical information infrastructure of the Russian Federation», Collection of Legislation of the Russian Federation, 2017, № 31, Art. 4736.

4. Decree of the President of the Russian Federation of December 5, 2016 № 646 «On approval of the Doctrine of Information Security of the Russian Federation», Collection of Legislation of the Russian Federation, 2016, № 50, Art. 7074.

5. Decree of the President of the Russian Federation dated October 10, 2019 № 490 «On the development of artificial intelligence in the Russian Federation», Collection of Legislation of the Russian Federation, 2019, № 41, Art. 5700.

6. Decree of the President of the Russian Federation dated April 12, 2021 № 213 «On approval of the Fundamentals of State Policy of the Russian Federation in the field of international information security», Collection of Legislation of the Russian Federation, 2021, № 16, Art. 2746.

7. Decree of the President of the Russian Federation dated July 2, 2021 № 400 «On the National Security Strategy of the Russian Federation», Collection of Legislation of the Russian Federation, 2021, № 27, Art. 5351.

8. Belous A.I., Solodukha V.A. Fundamentals of cybersecurity. Standards, concepts, methods and means of support. – Moscow: TECHNOSPHERE, 2021. – 482 p.

9. Kazarin, O.V. Fundamentals of information security: reliability and security of software: a textbook for secondary vocational education / O.V. Kazarin, I.B. Shubinsky. – Moscow: Yurayt Publishing House, 2023. – 342 p. – (Professional education).

10. Kozyr, N.S. Economic aspects of information security: textbook and workshop for universities / N.S. Kozyr, L.L. Oganesyan. – Moscow: Yurayt Publishing House, 2023. – 131 p. – (Higher education).

11. Mamaeva L.N., Bekher V.V. Cybersecurity threats in the digital space // Bulletin of the Saratov State Socio-Economic University. 2019. № 4 (78). pp. 68-70.

12. Report of the Prosecutor General's Office of the Russian Federation on crimes committed using modern information and communication technologies / Official website of the Prosecutor General's Office of the Russian Federation. URL: https://epp.genproc.gov.ru/web/proc_cfo/mass-media/news/archive?item=84860550

13. State of crime // Ministry of Internal Affairs of the Russian Federation [Electronic resource]. URL: https://Ministry of Internal Affairs.rf/reports (access date: 10/13/2023).

14. Mikaeva A.S., Penchukova T.A., Committing fraudulent actions on the Internet and their impact on economic security / Russian Economic Internet Journal. – 2022. – №1.

Для цитирования: Микаева А.С., Взаимосвязь кибербезопасности и экономической безопасности на современном этапе развития / Микаева А.С., Пенчукова Т.А., Сенькина В.А. // Российский экономический интернет-журнал. – 2023. – № 4. URL: