УДК 338

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В ИГРОВОЙ ИНДУСТРИИ: АНАЛИЗ ПОНЯТИЙНОГО АППАРАТА

В.Т. ФИРСОВА
(Представлено: канд. экон. наук, доц. Е.Ю. АФАНАСЬЕВА)

В данной статье рассматриваются теоретические подходы к определению информационной безопасности и кибербезопасности в сфере игровой индустрии. Проведен анализ специфических угроз и уязвимостей современных компьютерных игр, а также обоснована необходимость применения комплексного подхода к защите пользовательских данных и игровой инфраструктуры.

Ключевые слова: *информационная безопасность, игровая индустрия, кибербезопасность, компьютерные игры, уязвимости и угрозы.*

Развитие цифровой экономики неразрывно связано с ростом индустрии развлечений, где игровая сфера занимает лидирующие позиции по объёму вовлечённого капитала и пользовательской аудитории.

По данным отраслевых отчётов в сфере кибербезопасности, игровая индустрия в последние годы демонстрирует взрывной рост числа кибератак с использованием методов социальной инженерии, фишинга и взлома учётных записей.

Исследователи «Лаборатории Касперского» представили годовые данные по кибератакам, связанным с более чем десятью разными популярными играми. За это время было зафиксировано более 4 миллионов попыток кибератак с «игровой тематикой». В абсолютном большинстве случаев целью становились игроки в Minecraft: больше 70% вредоносных программ были ассоциированы с этой игрой. На втором месте – игровая платформа Roblox (чуть больше 20%), далее следует Counter Strike: Global Offensive (4,78%) и PlayerUnknown's Battlegrounds (2,85%). На мобильных устройствах доля угроз, распространяющихся под видом модов и подобного контента для Minecraft, ещё выше – больше 90%.

Действия мошенников приводят не только к прямым финансовым потерям, таким как хищение виртуальных ценностей, но и к репутационному ущербу и оттоку пользователей, что ставит под угрозу экономическую состоятельность бизнеса. Как показал анализ, проведённый на основе изучения нормативных актов Российской Федерации и Республики Беларусь, в современной науке и практике сложились разные подходы к толкованию защиты: от узкой практики защиты компьютеров до широкого состояния защищенности национальных интересов. В связи с этим возрастает актуальность разграничения и определения роли ключевых понятий в системе противодействия этим угрозам.

Несмотря на наличие нормативно-правовой базы, у субъектов хозяйствования игровой индустрии отсутствует чёткое понимание понятийного аппарата в сфере безопасности. Анализ дефиниций, представленных в научной литературе, демонстрирует терминологическую разобщённость: кибербезопасность в равной мере трактуется и как практическая деятельность по защите от атак, и как способность сохранять функциональную устойчивость в киберпространстве, в то время как информационная безопасность смещается в сторону статичного состояния защищенности среды и интересов личности, общества и государства. При этом в ключевом для белорусской практики документе – Постановлении Совета Безопасности Республики Беларусь от 18 марта 2019 г. № 1 «О Концепции информационной безопасности Республики Беларусь» – встречаются оба понятия, однако не раскрыта их взаимосвязь, не определены сходства и принципиальные различия.

В связи с этим необходимо раскрыть экономическую сущность понятий «информационная безопасность» и «кибербезопасность», определить их роль в обеспечении экономической безопасности субъекта хозяйствования в игровой индустрии.

Следует отметить, что в литературных источниках существует множество различных подходов к дефиниции «кибербезопасность». Результаты исследования экономической сущности понятия «кибербезопасность», показали, что до настоящего времени не существует единого подхода к его трактовке.

На основе признаков, выделенных нами в процессе исследования, все рассмотренные определения понятия «кибербезопасность» были сгруппированы в четыре подхода.

Первая группа исследователей придерживается подхода, определяющего кибербезопасность как практическую деятельность, совокупность мер и методов защиты. Данной точки зрения придерживаются такие авторы, как Пол Тронкон и Карл Олбинг [1, с. 57], А. И. Белоус и В. А. Солодуха [2, с. 12], А. А. Аверкиев и А. Д. Камбулов [3, с. 567], А. В. Борисенко [4, с. 298], а также В. А. Артамонов и Е. В. Артамонова [5, с. 777]. Данная группа составляет 25% от общего числа рассмотренных определений.

На наш взгляд, преимуществом подхода является его ориентация на реальные, прикладные действия по отражению угроз, что превращает кибербезопасность из абстрактного идеала в непрерывный рабочий процесс компании.

Вторая группа авторов трактует кибербезопасность как состояние или свойство защищенности, способность противостоять угрозам. К этой группе относятся А. С. Марков и В. Л. Цирлов [6, с. 29], авторы Концепции стратегии кибербезопасности Российской Федерации [5, с. 2], Концепции информационной безопасности Республики Беларусь [6], Национальный институт стандартов и технологий [7, с. 90], а также Ю. В. Бородакий, А. Ю. Добродеев и И. В. Бутусов [8, с. 6]. Данная группа также составляет 25%.

На наш взгляд, такой подход важен тем, что задаёт конечную, целевую характеристику системы безопасности, описывая не инструментарий, а желаемый результат усилий – состояние устойчивости и надёжности в киберпространстве.

Третья группа авторов рассматривает кибербезопасность через призму безопасности в определённой среде, акцентируя внимание на её локализации в киберпространстве или киберсфере. Данный подход разделяют Ю. В. Бородакий, А. Ю. Добродеев и И. В. Бутусов [8, с. 6], Н. Ш. Козлова и В. А. Довгаль [9, с. 91], а также О. Г. Ковалев [10, с. 5]. Данная группа авторов также составляет 25% от рассмотренных.

На наш взгляд, преимуществом данного подхода является чёткое очерчивание границ ответственности – фокус исключительно на цифровой природе активов, что крайне важно для распределения ресурсов в высокотехнологичных компаниях.

Четвёртая группа авторов сводит кибербезопасность к защите информации, данных и связанных с ними технологий, делая упор на объект защиты как таковой. Этой точки зрения придерживаются Н. Ш. Козлова и В. А. Довгаль [9, с. 91] в ряде своих определений. Данная группа составляет 25% и уравнивается в объёме с остальными.

На наш взгляд, ценность этого подхода в его предельной конкретности: он прямо указывает, что именно подлежит охране, облегчая идентификацию критических активов и инвентаризацию объектов защиты в игровой индустрии.

Проанализировав литературные источники, можно сделать вывод, что до настоящего времени не существует единого подхода также и к трактовке понятия «информационная безопасность».

На основе выделенных нами признаков все рассмотренные определения были сгруппированы в четыре подхода.

Первая группа исследователей придерживается подхода, определяющего информационную безопасность как состояние защищенности. Данной точки зрения придерживаются такие авторы и источники, как Федеральный закон «Об информации, информатизации и защите информации» [11, с. 20], В. В. Гафнер [11, с. 20], В. И. Ярочкин [11, с. 20], Е. В. Вострецова [12, с. 15], Закон Республики Казахстан [13], Закон РФ «Об участии в международном информационном обмене» [14], Закон РФ «О безопасности» [15], Концепция информационной безопасности Республики Беларусь [16], а также Н. Н. Карзаева [9, с. 90]. Данная группа составляет 55% и является самой многочисленной из приведённых.

На наш взгляд, преимуществом подхода является его нацеленность на фиксацию желаемого, стабильного результата – состояния полной защищённости, что особенно важно для оценки соответствия нормативным требованиям и стратегического планирования безопасности.

Вторая группа авторов представляет подход, трактующий информационную безопасность как защищенность информации и инфраструктуры от воздействий. К этой группе относятся В. Бетелин и В. Галатенко [17, с. 20], А. Н. Асаул [18], Д. В. Ковалев [9, с. 90]. Данная группа составляет 20%.

На наш взгляд, данный подход важен тем, что он смещает акцент с абстрактного «состояния среды» на конкретные объекты защиты – информацию и поддерживающую её инфраструктуру, что делает его удобным для выработки технических и организационных мер защиты в компаниях.

Третья группа авторов трактует информационную безопасность с позиций комплекса мер по обеспечению конфиденциальности, целостности и доступности информации. К этой группе относятся ГОСТ Р ИСО/МЭК 17799-2005 [19], Я. С. Гродзенский [19], В. В. Гафнер [11, с. 20]. Данная группа авторов составляет 15%.

На наш взгляд, преимуществом данного подхода является его практическая ориентация, что обеспечивает чёткие критерии для аудита и построения системы управления информационной безопасностью.

Четвертая группа авторов предлагает иные определения, указывающие на защиту от атак, выделяя специфические черты понятия, которые сложно однозначно отнести к трём вышеуказанным подходам. Этой точки зрения придерживаются Н. Ш. Козлова и В. А. Довгаль [9, с. 91] в ряде своих определений. Данная группа авторов составляет 10%.

Для комплексного понимания роли проанализированных дефиниций в обеспечении экономической безопасности субъекта хозяйствования игровой индустрии необходимо соотнести понятия «кибербезопасность» и «информационная безопасность», определив их синонимичность либо взаимосвязь, а также выявив принципиальные сходства и различия.

Проведённый сравнительный анализ позволил выделить ряд схожих черт между рассматриваемыми категориями.

1. Оба понятия в своей сущностной основе направлены на обеспечение конфиденциальности, целостности и доступности информации.

2. Единая цель – создание и поддержание состояния защищённости от угроз и минимизация потенциального ущерба.

3. Дефиниции определяются в научной литературе не только как сугубо технические категории, но и как совокупность организационных, правовых, политических мер и процессов, что подтверждает их комплексный характер.

4. В обеих группах дефиниций присутствует деятельностный подход, характеризующий данные понятия как непрерывную практику защиты, а не как статичный результат.

Вместе с тем между понятиями существуют и принципиальные различия, которые целесообразно рассмотреть по ряду критериев.

1. По предмету защиты. Кибербезопасность сфокусирована исключительно на защите информации и активов в цифровой (электронной) форме, в то время как информационная безопасность защищает информацию в любой форме её представления – не только цифровой, но и аналоговой, бумажной, вербальной, а также саму информационную среду общества.

2. По объекту и среде. Для кибербезопасности объектами выступают кибератривы – компьютеры, серверы, сети, мобильные устройства и программы, а средой является киберпространство. Объектами же информационной безопасности служат информационные ресурсы, системы и инфраструктура в целом, а также права субъектов информационной деятельности, а средой – информационная сфера общества.

3. По природе угроз. Кибербезопасность концентрируется преимущественно на умышленных, злонамеренных атаках – действиях хакеров, киберпреступности, кибертерроризме, информационном противоборстве. Информационная безопасность рассматривает более широкий спектр угроз, включая как преднамеренные, так и случайные воздействия естественного или искусственного характера, а также внутренние и внешние угрозы.

4. По характеристике состояния. Кибербезопасность часто определяется через активную, динамическую способность противостоять атакам и сохранять функциональную устойчивость в режиме реального времени. Информационная безопасность значительно чаще характеризуется как статичное «состояние защищённости» интересов, ресурсов и среды от угроз.

5. По масштабу защищаемых интересов. Кибербезопасность направлена в первую очередь на защиту собственно активов – систем, данных, их надёжности и функциональности. Информационная безопасность прямо и явно защищает интересы национального масштаба – личности, общества и государства.

На основании выявленных различий представляется возможным утверждать, что понятие «информационная безопасность» является более широким по отношению к понятию «кибербезопасность». Кибербезопасность выступает как специализированная, технологически ориентированная подсистема информационной безопасности, ограниченная цифровой средой направленная на оперативное противодействие киберугрозам. Информационная безопасность охватывает данный сегмент, дополнительно включая защиту нецифровых информационных активов, соблюдение прав субъектов и обеспечение национальных интересов в информационной сфере в целом.

Игровая индустрия как объект защиты обладает выраженной спецификой, существенно влияющей на выбор подходов к обеспечению экономической безопасности субъекта хозяйствования. Данная специфика заключается в двойственной природе игрового продукта: с одной стороны, это высокотехнологичная цифровая платформа, функционирующая в режиме реального времени и требующая непрерывной защиты от кибератак; с другой – это социально-экономическая экосистема, аккумулирующая колоссальные массивы персональных и платёжных данных, внутриигровые экономики, репутационные активы и объекты интеллектуальной собственности.

С учётом выявленной специфики представляется обоснованным следующий вывод о распределении ролей рассматриваемых понятий в обеспечении экономической безопасности субъекта хозяйствования игровой индустрии.

Методы кибербезопасности в игровой индустрии призваны выполнять оперативно-тактическую роль, обеспечивая защиту цифровой инфраструктуры в режиме реального времени. Их задача – противодействие DDoS-атакам на игровые серверы, предотвращение взлома клиентских приложений, нейтрализация читов и эксплойтов, защита сетевых протоколов и баз данных от несанкционированного доступа. Кибербезопасность обеспечивает ту самую функциональную устойчивость и надёжность систем в условиях информационного противоборства, без которой непрерывность игрового процесса и, следовательно, непрерывность получения выручки оказываются невозможными.

Методы информационной безопасности в игровой индустрии выполняют стратегическую роль, направленную на создание всеобъемлющего состояния защищённости информационной среды компании. В их сферу входят: защита персональных и платёжных данных пользователей от утечек и неправомерного доступа, обеспечение сохранности интеллектуальной собственности (исходного кода, дизайн-документов, ещё не анонсированного контента), противодействие инсайдерским угрозам, защита репутации бренда от дезинформации и атак с использованием методов социальной инженерии, а также обеспечение соответствия нормативным требованиям в области защиты информации. Информационная безопасность формирует ту

самую среду доверия пользователей и инвесторов, которая лежит в основе долгосрочной экономической состоятельности игрового бизнеса.

Таким образом, для игровой индустрии категоричный выбор в пользу только одного из двух понятий является ошибочным. Обеспечение экономической безопасности субъекта хозяйствования в данной сфере требует неразрывного единства двух подходов: кибербезопасность обеспечивает тактическую защиту цифровых систем в момент атаки, а информационная безопасность задаёт стратегический контур защиты всех информационных активов и интересов компании от всего спектра угроз.

ЛИТЕРАТУРА

1. Bash и кибербезопасность: атака, защита и анализ из командной строки Linux. – СПб.: Питер, 2020. – 288 с. – (Серия «Для профессионалов»).
2. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения / А. И. Белоус, В. А. Солодуха. – М.: Техносфера, 2021. – 482 с.
3. Кибербезопасность: виды и методы [Электронный ресурс] // StudNet. – 2022. – № 1. – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-vidy-i-metody/viewer. – Дата доступа: 28.09.2026.
4. Информационная безопасность или кибербезопасность [Электронный ресурс] // eLIBRARY.RU. – Режим доступа: https://elibrary.ru/download/elibrary_49926303_86695229.pdf. – Дата доступа: 28.09.2026.
5. Кибербезопасность в условиях цифровой трансформации социума [Электронный ресурс] // StudNet. – 2025. – № 9-2. – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-v-usloviyah-tsifrovoy-transformatsii-sotsiuma/viewer. – Дата доступа: 28.09.2026.
6. Семь безопасных информационных технологий / под ред. А. С. Маркова. – М.: ДМК Пресс, 2017. – 224 с.: ил.
7. Кибербезопасность и информационная безопасность: сходства и отличия [Электронный ресурс] // Вестник Адыгейского государственного университета. Сер. 1: Регионоведение: философия, история, социология, юриспруденция, политология, культурология. – 2021. – Вып. 3(286). – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-i-informatsionnaya-bezopasnost-shodstva-i-otlichiya/viewer. – Дата доступа: 28.09.2026.
8. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1) [Электронный ресурс] // КиберЛенинка. – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-kak-osnovnoy-faktor-natsionalnoy-i-mezhdunarodnoy-bezopasnosti-hh-veka-chast-1/viewer. – Дата доступа: 28.09.2026.
9. Кибербезопасность и информационная безопасность: сходства и отличия [Электронный ресурс] // КиберЛенинка. – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-i-informatsionnaya-bezopasnost-shodstva-i-otlichiya/viewer. – Дата доступа: 28.09.2026.
10. Кибербезопасность современной России: теоретические и организационно-правовые аспекты [Электронный ресурс] // КиберЛенинка. – Режим доступа: https://cyberleninka.ru/article/n/kiberbezopasnost-sovremennoy-rossii-teoreticheskie-i-organizatsionno-pravovye-aspekty/viewer. – Дата доступа: 28.09.2026.
11. Информационная безопасность [Электронный ресурс]. – Режим доступа: https://jasulib.org/kg/wp-content/uploads/2024/02/uch00029.pdf. – Дата доступа: 28.09.2026.
12. Гродзенский, Я. С. Информационная безопасность: учебное пособие [Электронный ресурс]. – Режим доступа: https://jasulib.org/kg/wp-content/uploads/2024/02/Grodzenskiy_Ya_S_Informatsionnaya_bezopasnost_Uchebnoe_posobie_2020.pdf. – Дата доступа: 28.09.2026.
13. Об информатизации [Электронный ресурс]. – Режим доступа: https://kodeksy-kz.com/ka/ob_informatizatsii/1.htm. – Дата доступа: 28.09.2026.
14. Литература по информационной безопасности [Электронный ресурс]. – Режим доступа: https://clipr.cc/5TJp1. – Дата доступа: 28.09.2026.
15. Литература по кибербезопасности [Электронный ресурс]. – Режим доступа: https://clipr.cc/bBW8z. – Дата доступа: 28.09.2026.
16. Нормативно-правовой документ [Электронный ресурс] // Национальный правовой Интернет-портал Республики Беларусь. – Режим доступа: https://pravo.by/document/?guid=3871&p0=P2190001. – Дата доступа: 28.09.2026.
17. Информационная безопасность [Электронный ресурс]. – Режим доступа: https://jasulib.org/kg/wp-content/uploads/2024/02/uch00029.pdf. – Дата доступа: 28.09.2026.
18. Информационная безопасность [Электронный ресурс]. – Режим доступа: http://www.aup.ru/books/m6/8_4.htm. – Дата доступа: 28.09.2026.
19. Гродзенский, Я. С. Информационная безопасность: учебное пособие [Электронный ресурс]. – Режим доступа: https://jasulib.org/kg/wp-content/uploads/2024/02/Grodzenskiy_Ya_S_Informatsionnaya_bezopasnost_Uchebnoe_posobie_2020.pdf. – Дата доступа: 28.09.2026.