УДК 004.056 **DOI: 10.14451/1.205.262**

ВЛИЯНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ТЕМПЫ ЭКОНОМИЧЕСКОГО РАЗВИТИЯ СТРАНЫ

© 2021 **Ганибаев Гаяз Рустемович**
аспирант кафедры экономической безопасности и налогообложения
Казанский (Приволжский) федеральный университет, Россия, Республика Татарстан, Казань
E-mail: mikkibaev@mail.ru

© 2021 **Хайруллин Рамиль Камилевич**
доктор экономических наук, доцент кафедры экономики и управления в спорте
Поволжский государственный университет физической культуры и спорта,
Россия, Республика Татарстан, Казань
E-mail: r.hayrullin@sportacadem.ru

© 2021 **Туфетулов Айдар Миралимович**
доктор экономических наук, профессор,
заведующий кафедрой экономической безопасности и налогообложения
Казанский (Приволжский) федеральный университет, Россия, Республика Татарстан, Казань
E-mail: ajdar-t@yandex.ru

© 2021 **Балабанова Юлия Николаевна**
старший преподаватель кафедры экономической безопасности и налогообложения
Казанский (Приволжский) федеральный университет, Россия, Республика Татарстан, Казань
E-mail: iylia_b@mail.ru

Настоящая статья посвящена исследованию зависимости направления и темпов развития информационной безопасности и кибербезопасности на территории Российской Федерации. Угрозы и атаки кибербезопасности влияют на формирование информационной безопасности на уровне личности и отдельных предприятий, регионов и государства в целом. Разработка и реализация комплексного подхода к формированию систем информационной безопасности позволит обеспечить за счет определяющих траекторию и темпы социально-экономического развития на различных уровнях.

Ключевые слова: информационная безопасность, кибербезопасность, угрозы информационной безопасности, кибератаки, показатели уровня информационной безопасности, цифровые технологии, цифровизация экономики, информационная среда.

Процессы виртуализации национального экономического пространства, включающие широкое внедрение информационно-коммуникационных технологий, облачных систем и переход к цифровым бизнес-моделям, приводят к возникновению качественно новых рискообразующих факторов информационной безопасности отдельных индивидов, предприятий и государственных образований в целом, что влечет за собой усиление уязвимости государства перед угрозами национальной безопасности. Повышение уровня информатизации факторов производства и технологий их использования обусловливает обострение внешних и внутренних рисков функционирования национальной экономики и входящих в ее состав регионов, управление которыми становится необходимой предпосылкой формирования траектории устойчивого развития и предупреждения негативного воздействия на объекты информационной инфраструктуры, банковские и финансовые институты, органы государственного управления и др. Одновременно происходит изменение субъектного состава преступного мира и модификация способов совершения преступлений, что вызывает необходимость введения в систему государственного регулирования качественно новых инструментов.

Применяемые в современном российском обществе меры, направленные на защиту информации, представляются необходимыми, но не достаточными. Повышение уровня инфор-

мационной безопасности предполагает реализацию комплексного подхода, включающего совершенствование нормативно-правовой базы, изменение организационной системы управления рисками, моделирование угроз, разработку системы пороговых значений показателей, усиление ответственности за принимаемые управленческие решения и контроля в сфере использования информационных технологий и др.

Кибербезопасность сформировалась всего несколько десятилетий назад, однако сейчас мы не представляем возможности передачи информации через системы криптографической защищенной связи. На сегодняшний день методы кибербезопасности перестали быть исключительно реактивными. Теперь кибербезопасность способна реагировать не только на произошедшие атаки, но и предотвращать угрозы до их начала, применяя различные технологии и накопленные знания.

Понятие «информационной безопасности» более широкое и многоплановое чем понятие «кибербезопасность», под кибербезопасностью следует понимать совокупность условий, при которых все составляющие киберпространства защищены от максимально возможного числа угроз и воздействии с нежелательными последствиями. Исходя из этого можно отметить, что кибербезопасность рассматривает и защищает от угроз в искусственно созданной и развивающейся цифровой информационной среде, а информационная безопасность рассматривает и защищает физическую и цифровую безопасность.

Согласно результатам опроса «Глобальное состояние информационной безопасности в 2018 году», проведенного компанией «PricewaterhouseCoopers» (PwC), в 48% российских предприятий отсутствуют программы обучения, направленные на повышение уровня осведомленности сотрудников в вопросах безопасности; процесс реагирования на инциденты информационной безопасности не регламентирован в 56% компаний; 48% респондентов отмечают, что цифровая трансформация бизнес-процессов увеличила расходы на информационную безопасность. Это подтверждает тезис об отсутствии в современной России комплексного подхода к формированию системы информационной безопасности при постепенном осознании значимости данной проблемы руководителями всех уровней. При этом растущий уровень поляризации национального экономического пространства выступает объективной предпосылкой формирования мезоэкономических систем безопасности [6].

Согласно опросу PwC, в 2020 году показывает более половины (52%) российских компаний планируют повысить бюджет на кибербезопасность. Так, 96% руководителей крупных компаний изменили свою стратегию обеспечения кибербезопасности в связи с COVID-19. Пандемия повлияла на все сферы экономики, в том числе это связано с ускорением цифровизации, существенное влияние которой на характер управленческих решений признают 24% руководителей российских компаний и 40% руководителей зарубежных компаний.

Исходя из плановых показателей на 2021 год на основе Глобального исследования «Доверие к цифровым технологиям — 2021», согласно опросу руководителей российских компаний, можно сказать, что кибербезопасность стала одним из наиболее значимым аспектом бизнеса. Так согласно высказыванию директора по информационной безопасности Liberty Mutual «Нынешние экономические обстоятельства доказывают огромное давление на организацию безопасности, заставляя нас тщательно следить за тем, чтобы наши инвестиции приносили результат и высокую ценность». Таким образом, руководители российских и зарубежных компаний желают получить максимальную выгоду от каждого рубля, вложенного в кибербезопасность [5].

Наиболее распространенной угрозой информационной безопасности является атаки шифровальщиков, так в 2020 году средний ущерб от атак на организации составила около 4,44 миллиона долларов США, нанеся больше финансовый ущерб за счет дополнительного восстановлению данных, чем нанесенный ущерб после атак шифровальщиков.

Методы, используемые преступниками, также становятся все более сложными и изощренными. Все больше внимания уделяется вымогательским атакам, когда преступники крадут данные компании и шифруют их, чтобы те не смогли получить к ним доступ. После этого кибер-преступники начинают шантажировать компанию, угрожая обнародовать ее данные, если не будет выплачен выкуп. Ущерб от таких кибер-угроз существенен, учитывая компрометацию конфиденциальных данных и экономические последствия от выплаты выкупа.

В Российской Федерации, в основном, атаки

направлены на компрометацию компьютеров, серверов и сетевого оборудования, за первое полугодие 2021 году количество атак увеличилось на более чем 15% по сравнению с тем же периодом в 2020 году, чаще всего злоумышленники атаковали медицинские и государственные учреждения и промышленную отрасль. Данные о количестве кибератак в мире за период с 2019 по 2021 гг. по кварталам представлены на рисунке 1.

Согласно данным, приведенным в данные на основе исследований IT-компании Positive Technologies число кибератак в мире во втором квартале 2021 года, увеличилось на 0,3% по сравнению с первым кварталом года, при этом на 16% выросла доля связанных с получением финансовой выгоды атак на организации. Также стоит отметить, что доля атак на государственные учреждения выросла с 12% до 20% исходя из общего числа атак, нацеленных на организации, на торговые сети количество атак в 2021 году составила 59%, в то время за аналогичный период 2020 года количество атак составляло около 26%. Доля инцидентов, нацеленных на частных лиц в 2021 году составила около 12%, при этом, при атаках на частных лиц мошенники чаще руководствовались мотивом получения данных.

Рассмотрим количество кибератак на организации и частные лица. В атаках на частных лиц злоумышленники чаще руководствовались мотивом получения данных, при этом большая часть связана с похищением платежных данных. Что касается организаций, то в основном кибератаки связаны с получением конфиденциальных данных организации или получение финансовой выгоды. Данные по доле атак и мотивов злоумышленников на данные организаций и частных лиц за 2021 год представлены на рисунке 2.

Согласно данным представленными Positive Technologies, к одним из наиболее распространенных типов украденных данных в организациях являются персональные данные- 36% и учетные данные — 23%, меньшее количество атак на организации направлены на коммерческую тайну — 8%, медицинская информация — 3%, база данных клиентов — 3%, данные платежных документов — 2%, что касается частных лиц, то наибольшее количество украденных данных учетные данные — 55%, персональные данные — 17%, данные платежных карт 11%, личная переписка 11%, другая информация — 4%.

Признание информационной безопасности в качестве фактора конкурентоспособности предприятия, национальной экономики в целом в входящих в ее состав регионов сочетается с отсутствием в экономической науке единых представлений о содержании ключевых категорий, отражающих существенные аспекты системы управления информационной безопасностью. Это не позволяет получить целостное представление о содержании мер по обеспечению безопасности бизнес-процессов и уровне их эффективности. Развитие и усложнение информационной среды, превращение инструментов

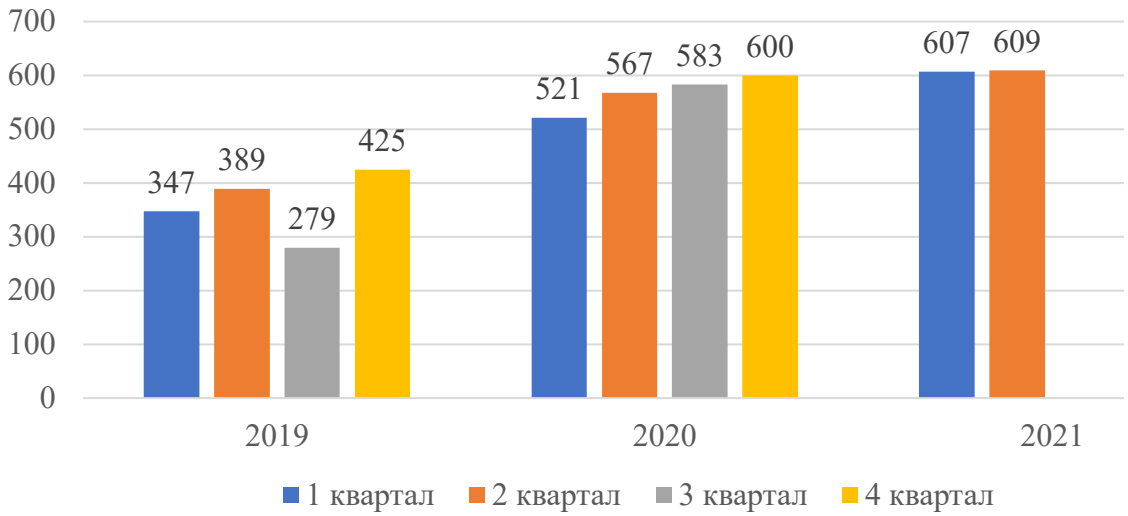

Рис. 1. **Количество атак за период с 2019 по 2021 гг. (по кварталам)**
Источник: Составлено автором на основе данных Positive Technologies — Режим доступа: https://www.ptsecurity.com/

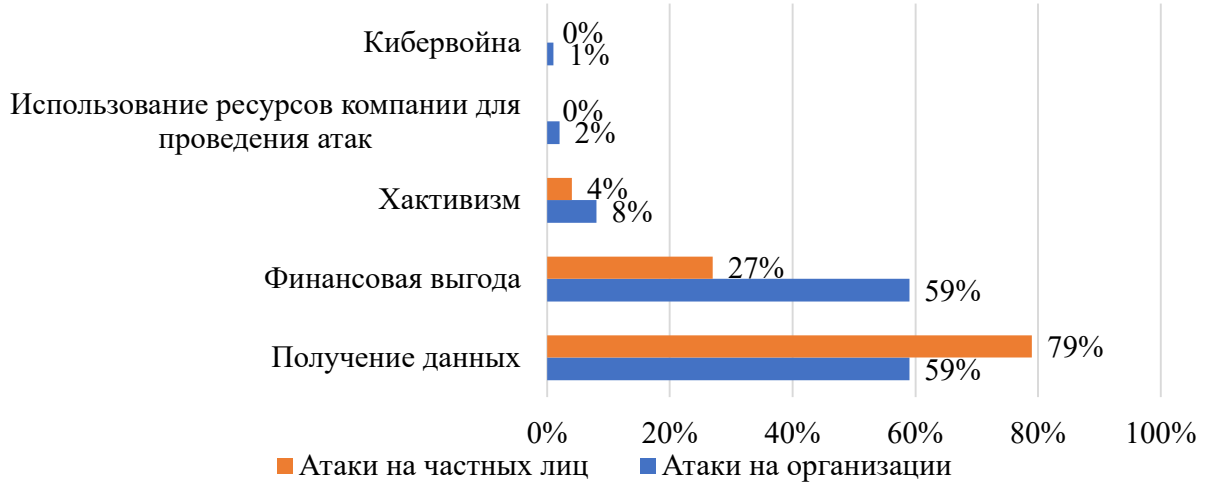

Рис. 2. **Доля атак на организации и частные лица в 2021 году**
Источник: Составлено автором на основе данных Positive Technologies — Режим доступа: https://www.ptsecurity.com/

управления информационными рисками в необходимый элемент управления предприятием и национальной экономикой в целом, формирование потребности в оперативном устранении источника угроз — все это требует разработки качественно новых подходов к содержанию технологий обеспечения информационной безопасности на микро- мезо- и макроуровнях.

В рамках обеспечения информационной безопасности необходимо выполнение действий не только по защите информационного пространства от внешнего информационного воздействия, но и обучение государственных служащих, занимающихся вопросами коммуникации, на уровне предприятий постоянное обучение сотрудников в сфере информационной безопасности и на уровне личности постоянно повышать свою грамотность в информационном пространстве.

Одним из основных направлений в обеспечении информационной безопасности страны является обеспечение нормативно-правового регулирования в сфере обеспечения информационного суверенитета страны за счет формирования концепции развития сектора безопасности и обороны России. Это позволит предотвратить информационное воздействие на создание негативного международного имиджа, дестабилизации внутренней общественно политической обстановки [4].

Информационная безопасность и до начала пандемии имела большое значение в обеспечении национальной безопасности и национальных интересов, но в 2021 году она по праву считается ключевым фактором изменений социально-экономических процессов. Это связано с тем, что в настоящее время именно информационные технологии помогают преодолевать массу негативных явлений в экономике, возвращаться к намеченной стратегии развития РФ [3].

Информационная среда, представляя собой системообразующий фактор для всех сфер национальной безопасности, оказывает активное влияние на политическую, экономическую, оборонную и другие составляющие национальной безопасности. В рамках проведенного исследования разработан методический подход к оценке уровня информационной безопасности в российских регионах и федеральных округах.

Таким образом, можно констатировать, что в современных условиях для национальной безопасности страны и ее регионов необходимы достаточные уровни обеспечения информационной инфраструктуры и информационной безопасности, являющейся одним из важнейших факторов обеспечения ключевых интересов регионов Российской Федерации. В качестве одного из существенных факторов, определяющих траекторию и темпы социально-экономического развития, выступают информационно-коммуникационные технологии и состояние системы информационной безопасности. Для достижения необходимого уровня обеспечения информационной безопасности страны возможно за счет управления рисками кибербезопасности и информационной безопасности на микро- мезо- и макроуровнях.

Библиографический список

1. *Ахметьянова А.И., Кузнецова А. Р.* Проблемы обеспечения информационной безопасности в России и ее регионах / А. И. Ахметьянова, А. Р. Кузнецова // Фундаментальные исследования. 2016. № 8–1. С. 82–86.
2. *Зундэ В.В., Уточкина Я. Е.* Информационная безопасность России в 2021 году: трактование, особенности и роль в обеспечении национальной экономической безопасности / В. В. Зундэ, Я. Е. Уточкина // Сборник статей Международной научно-практической конференции «Инновационное развитие современной науки: актуальные вопросы теории и практики. — Наука и просвещение, 2021. — С. 86–88.
3. *Тарасова Н. В., Дорошкин С. Е.* Влияние информационных технологий на экономическую безопасность / Н. В. Тарасова, С. Е. Дорошкин // Экономика и бизнес: теория и практика. 2020. № 2–2. (60). С. 128–133.
4. «Глобальное исследование «Доверие цифровым технологиям» 2021 — Кибербезопасность вступает в пору зрелости // Официальный сайт PricewaterhouseCoopers в России [Электронный ресурс] — Режим доступа: https://www.pwc.ru/dti2021. Дата обращения: 5.12.2021.
5. Глобальное состояние информационной безопасности в 2018 году» // Официальный сайт PricewaterhouseCoopers в России [Электронный ресурс] — Режим доступа: Режим доступа: https://www.pwc.ru. Дата обращения: 5.12.2021
6. Исследование: количество кибератак в мире выросло на 0,3% во II квартале 2021 года // Официальный сайт ТАСС [Электронный ресурс] — Режим доступа: https://tass.ru/ekonomika/12250541 Дата обращения: 5.12.2021.
7. Официальный сайт Министерства цифрового развития, связи и массовых коммуникаций Российской Федерации за 2016 год. [Электронный ресурс] — Режим доступа: http://minsvyaz.ru/ru/activity/directions/783/ Дата обращения: 5.12.2021.
8. Официальный сайт ПАО «Группа Позититв» (Positive Technologies) [Электронный ресурс] — Режим доступа: https://www.ptsecurity.com/ Дата обращения: 5.12.2021.