УДК 336.02

С.Н. Белоусова, Л.В. Афанасьева, В.Ю. Циклаури
Юго-Западный государственный университет, г. Курск, email: bsn275@mail.ru; valentina0209@mail.ru

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В РФ: СОВРЕМЕННОЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ ОБЕСПЕЧЕНИЯ

Ключевые слова: информационная безопасность, угрозы, система управления рисками информационной безопасности РФ.

Информационная безопасность предполагает высокую степень защищенности национальных интересов России в информационном пространстве. Стремительно развивающиеся информационные технологии и технологические возможности современных информационных систем могут оказывать различное влияние на политику, экономику и гражданское общество. Интернет-покупки, общение в социальных сетях, учебные курсы и деловые встречи в режиме онлайн становятся более популярными. Основной целью статьи является выявление угроз информационной безопасности и оценка степени их влияние на национальную безопасность страны и хозяйствующих субъектов и граждан. Сделаны выводы о том, что несанкционированный доступ к информационным данным с целью их похищения, искажение или фальсификация информации наносит серьезный материальный и моральный ущерб государству, хозяйствующим субъектам и физическим лицам. В современных условиях информационная безопасность становится важнейшим базовым элементом всей системы национальной безопасности российского государства, поскольку активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации.

S.N. Belousova, L.V. Afanasiev, V.Yu. Tsiklauri
Southwest State University, Kursk, email: bsn275@ mail.ru;valentina0209@mail.ru; brusentsevajulia@gmail.com

INFORMATION SECURITY IN THE RUSSIAN FEDERATION: CURRENT STATUS AND PROSPECTS FOR ENSURING

Keywords: information security, threats, information security risk management system of the Russian Federation.

Information security implies a high degree of protection of Russia's national interests in the information space. Rapidly developing information technologies and the technological capabilities of modern information systems can have various impacts on politics, economics and civil society. Online shopping, social networking, training courses and online business meetings are becoming more popular. The main purpose of the article is to identify threats to information security and assess the degree of their impact on the national security of the country and business entities and citizens. Conclusions are drawn that unauthorized access to information data for the purpose of their theft, distortion or falsification of information causes serious material and moral damage to the state, business entities and individuals. In modern conditions, information security is becoming the most important basic element of the entire system of national security of the Russian state, since it actively influences the state of the political, economic, defense and other components of the security of the Russian Federation.

Информатизация в современном мире является динамично развивающейся сферой, способной конкурировать по уровню рентабельности с топливно-энергетическим комплексом страны, автомобильной промышленностью, сельскохозяйственным производством, а также определяет наукоемкость промышленной продукции и ее конкурентоспособность на мировом рынке. На информационную безопасность оказывают влияние внешние угрозы, которые обусловлены конкурентным характером развития межгосударственных и международных отношений и внутренние.

Система информационных угроз существенно изменилась за последние годы – помимо хакерских атак и традиционно работающих иностранных разведывательных организаций, генерировать угрозы начали экстремистские организации и деструктивные секты, часто также направляемые службами разведки иностранных стран. Угрозы усилились, уча-

стились попытки перехвата управления объектами критической инфраструктуры, посягательства на государственные информационные ресурсы и сети. Самостоятельной проблемой стали действия, направленные на подрыв авторитета России на международном уровне.

Обеспечение информационной безопасности в различных сферах общественной жизни имеет свои особенности и в каждой сфере используются различные методы, в большей или меньшей степени эффективные. Перед специалистами по обеспечению информационной безопасности стоит задача оценить вероятные риски, эффективно им противодействовать и разрабатывать рекомендации по улучшению защитных мер.

Вопросы обеспечения информационной безопасности являются всегда актуальными и постоянно обсуждаются учеными и практиками [1-3].

Материалы и методы

Информация для аналитики представлена на сайте Федеральной службы государственной статистики РФ.

В статье применяются методы логического, системного, сравнительного анализа, методы обобщения, группировки и статистические методы.

Результаты и их обсуждение

Состояние безопасности информационной системы любого уровня предполагает, что она наименее восприимчива к вмешательству и нанесению ущерба со стороны.

В Концепции национальной безопасности РФ указаны угрозы в информационной сфере:

– стремление ряда стран к доминированию в мировом информационном пространстве;

– вытеснение государства с внутреннего и внешнего информационного рынка;

– разработка рядом государств концепции информационных войн;

– нарушение нормального функционирования информационных систем;

– нарушение сохранности информационных ресурсов, получение несанкционированного доступа к ним [4].

Данные угрозы реализуются посредством разведывательной деятельности зарубежных государств и информационно-технические воздействия со стороны не дружественных стран, направленные против интересов РФ.

Для решения задачи обеспечения информационной безопасности в настоящее время наиболее часто используются следующие программные комплексы: CRAMM, FRAP, Risk Watch, Microsoft Security Assessment Tool (MSAT), ГРИФ, CORAS. Все известные методики можно разделить на:

– методики, использующие оценку риска на качественном уровне (например, по шкале «высокий», «средний», «низкий»), к таким методикам, в частности, относится FRAP;

– количественные методики (риск оценивается через числовое значение, например, размер ожидаемых годовых потерь), к этому классу относится методика RiskWatch;

– методики, использующие смешанные оценки (такой подход используется в CRAMM, методике MSAT) [5].

Собственникам и руководителям организаций до принятия решения о внедрении той или иной методики управления рисками информационной безопасности следует убедиться, что она в полном объеме учитывает масштабы, интересы и потребности компаний по защите информационных данных.

В таблице 1 нами представлена динамика кибератак по ряду российских отраслей за 2019-2021 годы.

Анализ данных, представленный в таблице 1, показывает, что чаще всего атакам подвергаются компьютеры компаний и организаций, сетевое оборудование, ПО с целью получения определенных данных из этих систем. За период 2019-2021 гг. зафиксировано наибольшее количество атак на информационные системы государственных предприятий, предприятий промышленности, медицинских учреждений и финансовых организаций. Значительно увеличилось число атак на персональные компьютеры физических лиц.

Основная угроза для всех это утечка информации и потеря доступа к данным из-за кибератак. В большинстве случаев хакеров в отношении организаций интересуют учетные данные сайтов и организаций, данные категории «коммерческая тайна», база данных клиентов организации, информация платежных карт. В отношении физических лиц – персональные данные, данные с банковских карт и личная информация.

Таблица 1

Динамика киберинцидентов в РФ за 2019-2021 годы

Показатель		Госучреждения	Финансовые организации	Промышленность	Медицинские учреждения	Онлайн-сервисы	IT-компании	Торговля	Сфера услуг	Частные лица
2019 год										
Всего атак		241	92	125	93	47	63	49	51	292
Объект	Компьютеры, сервисы и сетевое оборудование	169	82	118	54	15	51	17	18	92
	Веб-сервисы	54	5	4	22	31	11	27	14	25
	Пользователи	15	2	3	17	1	1	1	1	91
Метод	Использование ВПО	154	78	112	47	5	34	19	31	169
	Социальная инженерия	130	74	105	47	2	20	15	9	184
	Хакинг	25	5	10	4	5	13	2	4	5
	Эксплуатация веб-уязвимостей	45	1	5	3	23	9	27	8	7
Мотив	Финансовая выгода	143	61	110	57	29	37	37	42	167
	Получение данных	51	28	12	35	3	21	9	7	109
	Хактивизм	39	3	2	1	15	5	3	2	16
2020 год										
Всего атак		359	126	239	178	70	115	124	93	325
Объект	Компьютеры, сервисы и сетевое оборудование	290	103	220	144	30	94	63	76	116
	Веб-сервисы	51	12	8	14	53	11	60	17	19
	Пользователи	230	77	178	118	5	51	40	60	225
Метод	Использование ВПО	255	82	212	121	9	75	52	68	191
	Социальная инженерия	230	77	178	118	6	51	40	62	225
	Хакинг	71	27	50	38	18	44	24	30	23
	Эксплуатация веб-уязвимостей	34	5	6	6	40	2	50	15	4
Мотив	Финансовая выгода	103	48	87	101	20	49	27	53	98
	Получение данных	210	89	200	112	49	77	111	65	234
	Хактивизм	58	10	7	9	10	17	5	5	22
2021 год										
Всего атак		322	113	209	227	75	150	76	103	349
Объект	Компьютеры, сервисы и сетевое оборудование	248	71	183	192	28	134	51	89	130
	Веб-сервисы	75	27	10	15	55	16	23	14	19
	Пользователи	165	68	116	154	7	50	35	61	308
Метод	Использование ВПО	119	51	160	147	11	89	44	71	201
	Социальная инженерия	165	68	116	154	7	50	35	61	308
	Хакинг	85	17	78	56	16	81	20	29	23
	Эксплуатация веб-уязвимостей	51	8	5	10	35	7	21	13	7
Мотив	Финансовая выгода	131	41	107	129	22	60	41	60	95
	Получение данных	194	70	138	154	46	95	53	71	268
	Хактивизм	37	37	12	3	13	20	4	6	18

Источник: составлено авторами [6].

Таблица 2

Показатели информационной безопасности в РФ за 2017-2021 гг., %

№	Наименование показателя	2017г.	2018г.	2019г.	2020г.	2021г.	Изменение 2021 к 2017 г.	
							абс.	отн.
1	Доля организаций, использовавших средства защиты информации, передаваемой по глобальным сетям, в общем числе обследованных организаций	87,2	89,3	89,5	87,3	89,6	2,4	102,7
2	Доля населения, не использующего сеть Интернет по соображениям безопасности, в общей численности населения	0,6	0,4	0,5	0,4	0,5	-0,1	83,3
3	Доля населения, использующего средства защиты информации, в общей численности населения, использующего сеть Интернет	83,4	83,4	78,5	82,7	85,6	2,2	102,8

Источник: составлено авторами по данным Федеральной службы государственной статистики [7]

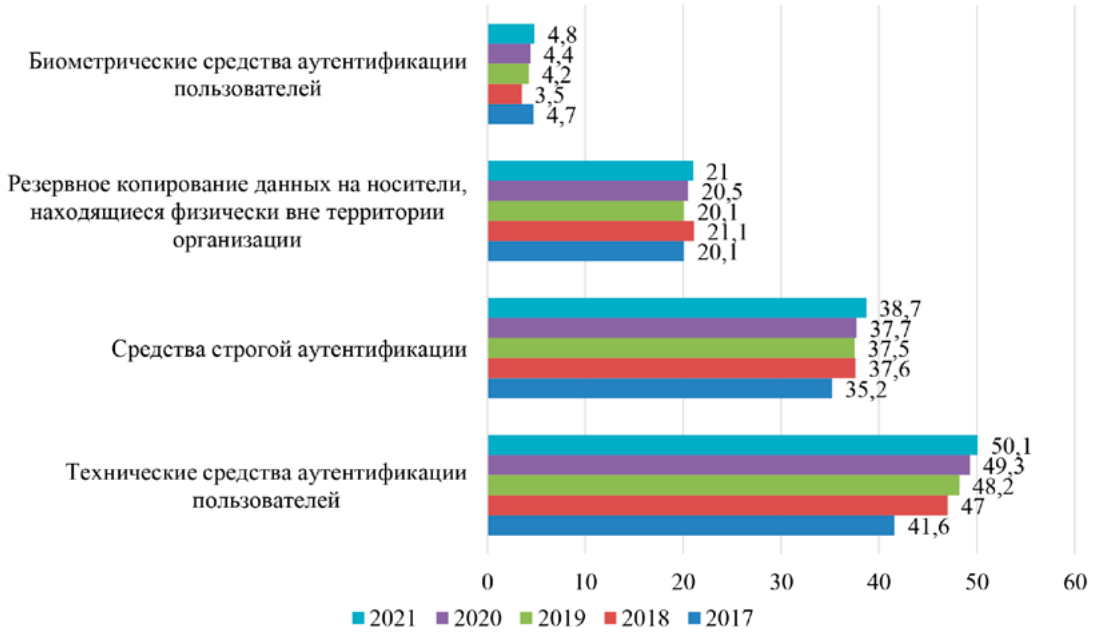

Рис. 1. Доля организаций, использующих средства информационной безопасности (в процентах от общего числа организаций)

В абсолютном большинстве случаев объектами для атаки выбирались компьютеры, серверы и сетевое оборудование – этот показатель зафиксировался в 75% всех кибератак. В остальных 25% в качестве объектов для атак выступали люди, веб-ресурсы, мобильные устройства, «интернет вещей» и др.

На фоне сложной геополитической обстановки необходимо признать, что количества атак будет увеличиваться как на информационные системы организаций, так и персональные гаджеты пользователей, поэтому главный акцент в обеспечении информационной безопасности сегодня должен быть сделан на обеспечении киберустойчивости.

Рис. 2. Последствия нападений на информационную сферу РФ

В последнее время множество независимых аналитических компаний пытаются оценить информационную безопасность по отдельным показателям.

В таблице 2 нами представлены показатели информационной безопасности в РФ, отражающие состояние защищенности информационных данных организаций и физических лиц.

Согласно данных таблицы 2 за период исследования происходит рост доли организаций и физических лиц, использующих средства защиты для своей информации.

Очень часто персональные компьютеры граждан подвергаются атакам из-за невнимательности и небрежности их хозяев – не установка лицензионных антивирусных программах, их отключение для получения доступа к другим ресурсам в сети Интернет. Вследствие этого домашние компьютеры являются привлекательной мишенью для киберпреступников, затратив незначительные усилия, мошенники могут раздобыть пароли доступа от банковских счетов и кредитных карт, украсть личные материалы для последующего шантажа, а также устроить массовую хакерскую атаку используя зараженные компьютеры.

Чаще всего для защиты информации используются антивирусные средства, антиспамовые фильтры, электронная цифровая подпись и средства шифрования.

На рисунке 1 нами отражена динамика организаций в РФ, использующих еще и дополнительные средства защиты информационных данных.

Таким образом, данные рисунка 1 отражают, что дополнительные меры защиты информации, такие как резервное копирование данных на носители, находящиеся физически вне территории организации используют 20% организаций, биометрические средства аутентификации 4,8% организаций. Более 50% предприятий в нашей стране. Применяют технические средства аутентификации пользователей.

Жертвой кибератаки может стать любая организация, и последствия этой атаки будут напрямую зависеть от того, какие меры по защите информации были приняты.

Усиление внешнеполитической нестабильности и противостояние на Украине спровоцировали небывалый рост информационных атак на российские веб-ресурсы. Распределенные атаки типа «отказ в обслуживании» стали самой распространенной угрозой информационной безопасности России. С начала 2022 года их жертвами стали сайты Центризбиркома РФ, Президента РФ, «Госуслуг», Россельхознадзора, Роспотребнадзора и десятков региональных СМИ; сервисы РЖД, «1С», Сбербанка; информационные ресурсы Петербургского международного экономического форума и видеохостинг Rutube; сети Росавиации и агрохолдинга «Мираторг»; ряд российских систем электронного документооборота (ЭДО); платежная система «Мир» и Национальная система платежных карт (НСПК). При этом атаки стали масштабнее не только по охвату, но также по силе и по длительности [8].

Последствия нападений на информационную сферу представлены на рисунке 2.

Президентом РФ 1 мая 2022 г. подписан указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» направленный на обеспечение информационной безопасности ряда ключевых компаний России. К таким компаниям относятся органы власти, предприятия с государственным участием, субъекты критической информационной инфраструктуры, стратегические и системообразующие организации российской экономики [9]. Госструктуры должны предоставлять органам ФСБ беспрепятственный доступ, в том числе удаленный, к принадлежащим или используемым ими ресурсам для мониторинга и выполнять их указания по его результатам.

Кроме того, указ запрещает с 1 января 2025 года госорганам и вышеуказанным организациям использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия, либо производителями которых являются организации, находящиеся под юрисдикцией таких иностранных государств, прямо или косвенно подконтрольные им либо аффилированные с ними.

Выводы

В целях повышения уровня информационной безопасности в РФ необходимо:

– переходить на российское программное обеспечение, перечень которого представлен на сайте «Реестр программного обеспечения». Хозяйствующие субъекты малого и среднего бизнеса могут приобрести отечественное программное обеспечение со скидкой 50%, в соответствии с федеральной Программой поддержки цифровизации малого и среднего бизнеса. В рамках программы реализуются 98 программных продуктов от 32 российских правообладателей;

– юридическим и физическим лицам в сегодняшних условиях необходимо обеспечить безопасность информационных систем, за счет ограничения удаленного доступа к информационным ресурсам и ужесточения политики безопасности паролей – чаще их менять, и делать сложнее.

Статья выполнена в рамках государственного задания Юго-Западного государственного университета, код проекта 0851-2020-0034.

Библиографический список

1. Исаева М.Ф. О внутренних угрозах информационной безопасности // Международный научно-исследовательский журнал. 2019. № 5-1 (83). С. 26-28.

2. Белоусова С.Н., Афанасьева Л.В., Ткачева Т.Ю. и др. Организационно-экономический механизм противодействия органами внутренних дел экономическим преступлениям в системе обеспечения экономической безопасности региона: монография. Курск, 2019. 139 с.

3. Евдокимов О.Г., Гавдан Г.П., Резниченко С.А. Подход к оценке эффективности системы обеспечения информационной безопасности распределенной системы передачи данных // Безопасность информационных технологий. 2022. Т. 29. № 2. С. 57-70.

4. Стратегия национальной безопасности Российской Федерации. Утверждена Указом Президента РФ от 2 июля 2021 г. № 400.

5. Профессиональные средства для защиты компании от разглашения конфиденциальной информации. [Электронный ресурс]. URL: https://www.staffcop.ru/articles/top-7-programm-po-obespecheniyu-informacionnoj-bezopasnosti (дата обращения 24.10.2022).

6. Актуальные киберугрозы. [Электронный ресурс]. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения 24.10.2022).

7. Официальный сервер Федеральной службы государственной статистики. [Электронный ресурс]. URL: https://rosstat.gov.ru/ (дата обращения 24.10.2022).

8. Пережить кибершторм: главные угрозы информационной безопасности в 2022. [Электронный ресурс]. URL: https://eternalhost.net/blog/bezopasnost-v-internete/ugrozy-informatsionnoj-bezopasnosti (дата обращения 24.10.2022).

9. Указ Президента Российской Федерации от 1 мая 2022 г. N 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации».