Интернет-журнал «Отходы и ресурсы» https://resources.today
Russian Journal of Resources, Conservation and Recycling

2023, Том 10, № s1 / 2023, Vol. 10, Iss. s1 https://resources.today/issue-s1-2023.html

URL статьи: https://resources.today/PDF/01FAOR123.pdf

DOI: 10.15862/01FAOR123 (https://doi.org/10.15862/01FAOR123)

Ссылка для цитирования этой статьи:
Амонов, А. Х. Обеспечение информационной безопасности с целью сохранения национальных интересов России в начале 21-го века / А. Х. Амонов, А. Х. Ратник // Отходы и ресурсы. — 2023. — Т. 10. — № s1. — URL: https://resources.today/PDF/01FAOR123.pdf DOI: 10.15862/01FAOR123

For citation:
Amonov A.Kh., Ratnik A.Kh. Ensuring information security in order to preserve the national interests of Russia at the beginning of the 21st century. *Russian Journal of Resources, Conservation and Recycling*. 2023; 10(s1): 01FAOR123. Available at: https://resources.today/PDF/01FAOR123.pdf. (In Russ., abstract in Eng.) DOI: 10.15862/01FAOR123

УДК 338

Амонов Амир Хаетович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Военный учебный центр имени профессора, генерал-майора С.М. Ермакова
E-mail: Amonov99@yandex.ru

Ратник Анатолий Харитонович
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Военный учебный центр имени профессора, генерал-майора С.М. Ермакова
E-mail: anatolyarslong@gmail.com

Научный руководитель: **Ахметов Миннегалей Гизятович**
ФГОБУ ВО «Финансовый университет при Правительстве Российской Федерации», Москва, Россия
Военный учебный центр имени профессора, генерал-майора С.М. Ермакова
Доцент
Кандидат военных наук, член-корреспондент Российской академии военных наук
E-mail: mgahmetov@fa.ru

Обеспечение информационной безопасности с целью сохранения национальных интересов России в начале 21-го века

Аннотация. Целью данной статьи является анализ основных рисков информационной безопасности в России в новом тысячелетии и эффективности программ обеспечения информационной безопасности РФ. Объектом исследования выступает система обеспечения информационной безопасности РФ. В статье были выявлены основные риски информационной безопасности в России, такие как киберпреступность, нарушения правил обработки персональных данных, утечки конфиденциальной информации и другие. Авторы проанализировали распределение перечисленных видов угроз информационной безопасности компаний-клиентов ПАО Ростелеком за 2022 год. Акцентируется внимание на том, что низкая культура информационной безопасности среди военнослужащих и персонала, работающего на объектах Вооруженных сил, может привести к уязвимостям и рискам утечки данных важных стратегических объектов.

Были рассмотрены программы обеспечения информационной безопасности РФ, включая Федеральную целевую программу "Информационная Россия", Федеральный закон "О защите персональных данных" и другие. Авторами были выделены основные цели и показатели

таких национальных программ. Проведен анализ эффективности системы обеспечения информационной безопасности РФ и представлен прогноз ее развития. Государственные программы, направленные на развитие цифровой экономики, защиту критической информационной инфраструктуры, разработку механизмов борьбы с киберугрозами, а также создание современных технологий для Вооруженных Сил России и криптографии являются ключевыми направлениями работы России в этой области. Авторами также проанализирован прогноз развития рынка кибербезопасности России, а также глобальный прогноз развития технологий информационной безопасности. Сделаны выводы, что несмотря на меры, принимаемые Российской Федерацией для обеспечения информационной безопасности, система все еще остается уязвимой перед новыми угрозами. разработаны рекомендации по совершенствованию текущей системы обеспечения информационной безопасности в РФ.

Ключевые слова: информация; информационная безопасность; информационные технологии; защита информации; обеспечение информационной безопасности; криптография; кибератака; национальные интересы; цифровые платформы; государственное управление

Введение

Развитие информационной технологий в рамках научно-технического прогресса в Российской Федерации с целью сохранения национальных интересов в начале 21-го века, повлекло за собой создание уникальных технологий, появлений ИТ-направлений деятельности, внедрение цифровых платформ во все сферы жизнедеятельности населения ознаменовало формирование новых направлений национальных интересов страны как прогрессивного этапа в развитии обеспечении информационной безопасности страны.

Актуальность темы исследования обусловлена необходимостью адаптации системы обеспечения информационной безопасности государственного управления к сохранению национальных интересов России. Государство должно создать благоприятные условия и минимизировать барьеры для развития цифровизации, регулировать цифровые изменения в отраслях, где информационная безопасность необходима, чтобы добиться полной защиты информационных потоков внутри государства.

Успешное обеспечение информационной безопасности будет возможно только при согласованных, эффективных и своевременных действиях органов власти Российской Федерации.

Цель исследования заключается в разработке предложений и рекомендаций по совершенствованию системы обеспечения информационной безопасности Российской Федерации.

Объектом исследования является информационная безопасность Российской Федерации.

Предметом исследования являются совокупность мер по обеспечению информационной безопасности Российской Федерации.

1. Методы и материалы

При написании научной публикации авторами использовались следующие методы: сравнительный, статистический, математический анализы, анализ и обобщение нормативно-правовых актов и документов, научных исследований и статей, табличные и графические способы визуализации статистических данных.

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Для достижения данной цели в работе были поставлены следующие задачи:

- рассмотреть организационно-правовые основы развития и управления информационной безопасности в Российской Федерации;
- проанализировать угрозы информационной безопасности;
- определить стратегические направления совершенствования информационной безопасности в России.

Исследование основывается на теоретических и методологических положениях, разработанных отечественными авторами, нормативно-правовых документах стратегического планирования, предложениях, раскрывающих перспективы разработки и реализации цифровой экономики на региональном уровне.

Различные аспекты информационной безопасности (трактование понятия, свойства информационной безопасности, направления развития) рассмотрены в работах: Р.Н. Абалуева [1], А.О. Калашникова [2], А.С. Белова [3].

Вопросы государственного регулирования информационной безопасности при помощи информационного права исследованных в трудах Т.А. Поляковой [4], Г.Г. Фастович [5].

Проблемы информационной безопасности рассматривались такими авторами, как П.Д. Зегжда [6], З.И. Харисовой [7], Н.Н. Пронькина [8].

Информационной базой исследования послужили: постановления и распоряжения Правительства РФ, Федеральные законы РФ, нормативно-правовые документы по информационной безопасности, развитию цифровой экономики касающиеся стимулирования научно-технического прогресса, научные труды отечественных ученых, Интернет-ресурсы (официальные сайты).

2. Результаты и обсуждения

Как и любая другая организованная структура, Вооруженные силы России также сталкиваются с рисками информационной безопасности. Ввиду особой секретности данных, относящихся к Министерству Обороны РФ, привести точную статистику атак невозможно, однако можно рассмотреть общие данные компании-провайдера ИТ-услуг Министерства Обороны РФ — ПАО Ростелеком[1] (рис. 1) [9].

Которые по данным, приведенных в открытой печати включают:

Кибератаки. Вооруженные силы могут стать целью кибератак со стороны других государств или киберпреступников, что может привести к утечке конфиденциальных данных и повреждению систем управления вооружением. Например, атака на ГИС систему, что в итоге может мешать корректной работе координации войск в слаживании [10].

Кибершпионаж. Разведывательные службы других государств могут использовать кибершпионаж для получения доступа к конфиденциальной информации военных объектов и устройств, что может привести к утечке государственных секретов и важной технологической информации, что в конце может быть использовано для саботажной деятельности и подрыва деятельности государственного строя.

[1] ПАО Ростелеком URL: https://www.company.rt.ru (дата обращения 28.04.2023).

Кибертерроризм. Террористы могут использовать кибертерроризм для атак на военные объекты и критически важные системы вооруженных сил, что может привести к серьезным последствиям для национальной безопасности страны.

Фейковые новости и дезинформация. В интернете могут распространяться фейковые новости и дезинформация, которые могут нанести ущерб имиджу и доверию к Вооруженным силам, а также повлиять на политическую стабильность страны.

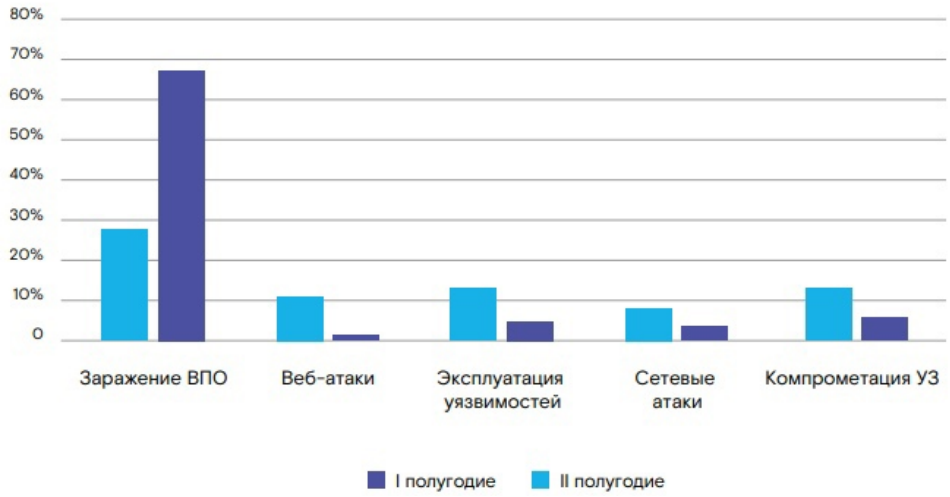

Рисунок 1. *Распределение видов угроз информационной безопасности компаний-клиентов ПАО Ростелеком за I и II кварталы 2022 года (составлено автором на основании данных официального сайта Ростелеком[2])*

Низкая культура информационной безопасности среди военнослужащих и персонала, работающего на объектах Вооруженных сил, может привести к уязвимостям и рискам утечки данных важных стратегических объектов.

Вооруженные силы России являются потенциальной мишенью для кибератак, кибершпионажа и кибертерроризма. Фейковые новости и дезинформация также могут быть использованы как способ воздействия на работу военных структур и политическую ситуацию в стране. Однако, при правильной организации информационной безопасности и повышении культуры информационной безопасности, можно уменьшить уязвимости и риски утечки данных, и тем самым обеспечить национальную безопасность России [11].

Программы обеспечения информационной безопасности РФ в 2023 году Россия продолжала работу по обеспечению информационной безопасности. Некоторые из программ, связанных с информационной безопасностью в РФ, включают в себя:

Государственная программа "Развитие цифровой экономики", которая направлена на развитие высокотехнологичных отраслей экономики России, включая сектор информационной безопасности (табл. 1).

Программа "Развитие информационной безопасности Российской Федерации на 2019–2025 годы", целью которой является создание современной системы защиты информации в России, включая развитие криптографических технологий, защиту критической информационной инфраструктуры, разработку механизмов борьбы с киберугрозами и т. д.

[2] Отчет об Кибератаках на российские компании в 2022 году URL: https://rt-solar.ru/upload/iblock/4a4/ghus61x9rd8cv5vczms5ig1svts4tlep/Otchet-o-kiberatakakh-na-rossiyskie-kompanii-v-2022-godu.pdf (дата обращения 28.04.2023).

Программа "Цифровая трансформация обороны", которая направлена на создание современных цифровых технологий для Вооруженных Сил России, включая информационную безопасность.

Программа "Развитие криптографии в Российской Федерации на 2020–2030 годы", которая направлена на развитие исследований и разработок в области криптографии, включая защиту критической информации от кибератак.

Это лишь некоторые из программ обеспечения информационной безопасности, которые были запущены или продолжены в РФ в 2021–2022 году.

Таблица 1

Цели, целевые и дополнительные показатели национальной программы

N п/п	Цель, целевой показатель, дополнительный показатель	Уровень контроля	Базовое значение		Период, год		
			значение	дата	2022	2023	2024
1	Увеличение внутренних затрат на развитие цифровой экономики за счет всех источников (по доле в валовом внутреннем продукте страны) не менее чем в три раза по сравнению с 2017 годом	Совет					
1.1	Внутренние затраты на развитие цифровой экономики за счет всех источников по доле в валовом внутреннем продукте страны, проценты	президиум Совета	1,7	31 декабря 2017 г.	3,6	4,3	5,1
2	Создание устойчивой и безопасной информационно-телекоммуникационной инфраструктуры высокоскоростной передачи, обработки и хранения больших объемов данных, доступной для всех организаций и домохозяйств	Совет					
2.1	Доля домохозяйств, имеющих широкополосный доступ к сети "Интернет", проценты	президиум Совета	72,6	31 декабря 2017 г.	92	95	97
2.2	Доля социально значимых объектов инфраструктуры, имеющих возможность подключения к широкополосному доступу к сети "Интернет", проценты	президиум Совета	30,3	31 декабря 2017 г.	83,7	91,9	100
2.3	Наличие опорных центров обработки данных в федеральных округах, количество	президиум Совета	-		6	7	8
2.4	Доля Российской Федерации в мировом объеме оказания услуг по хранению и обработке данных, проценты	президиум Совета	0,9	31 июля 2018 г.	3	4	5
2.5	Средний срок простоя государственных информационных систем в результате компьютерных атак, часов	президиум Совета	-	-	12	6	1
3	Использование преимущественно отечественного программного обеспечения государственными органами, органами местного самоуправления и организациями	Совет					
3.1	Стоимостная доля закупаемого и (или) арендуемого федеральными органами исполнительной власти, органами исполнительной власти субъектов и иными органами государственной власти отечественного программного обеспечения, проценты	президиум Совета		31 декабря 2016 г.	> 80	> 85	> 90
3.2	Стоимостная доля закупаемого и (или) арендуемого государственными корпорациями, компаниями с государственным участием отечественного программного обеспечения, проценты	президиум Совета	-	31 декабря 2016 г.	> 60	> 65	> 70

Составлено автором

Издательство «Мир науки» \ Publishing company «World of science» http://izd-mn.com

Россия продолжает работу по обеспечению информационной безопасности и разработке современных технологий в этой области. Государственные программы, направленные на развитие цифровой экономики, защиту критической информационной инфраструктуры, разработку механизмов борьбы с киберугрозами, а также создание современных технологий для Вооруженных Сил России и криптографии являются ключевыми направлениями работы России в этой области. Это свидетельствует о стремлении государства обеспечить свою национальную безопасность и защитить критически важную информацию от киберугроз [12].

Оценить эффективность системы обеспечения информационной безопасности РФ можно как с положительной, так и с отрицательной стороны. С одной стороны, РФ активно разрабатывает и внедряет различные меры по обеспечению информационной безопасности, такие как законы, регулирующие сбор и обработку персональных данных, усиление защиты критически важных объектов и информационных систем, разработка криптографических методов защиты, укрепление кадрового потенциала и др. [13].

С другой стороны, система обеспечения информационной безопасности РФ все еще сталкивается с множеством проблем, таких как недостаточный контроль за использованием средств связи и информационных технологий, несовершенство законодательства, проблемы в обучении персонала, слабая координация между различными органами государственной власти и др. [14].

Но все же важно понимать, что консенсус-прогноз экспертов заключается в том, что рынок кибербезопасности РФ будет неуклонно расти (рис. 2).

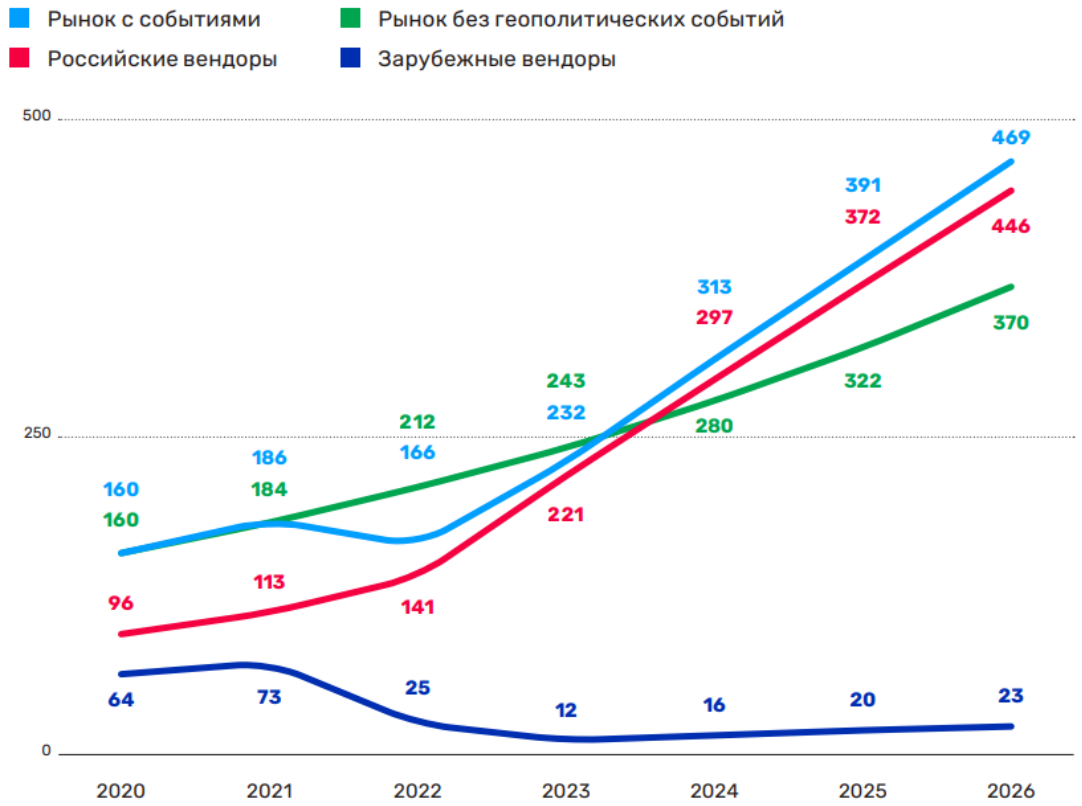

Рисунок 2. *Прогноз развития рынка кибербезопасности в России (составлено автором)*

График демонстрирует, что геополитическая ситуация, складывающаяся в настоящее время, приведет к понижению объема рынка в 2022–2023 годах, но национальные вендоры останутся не затронутыми. В целом, рынок кибербезопасности России преодолеет тренд снижения, связанный с уменьшением доли зарубежных вендоров, достигнув прогнозируемых

объемов (голубая линия на графике — рисунок 2) к 2023 году, после чего продолжит стремительный рост.

Прогнозы развития системы обеспечения информационной безопасности РФ сильно зависят от динамики мирового развития и технологических изменений (табл. 2).

В целом, можно ожидать, что информационные угрозы будут сохранять свою актуальность и эскалироваться в будущем, а РФ будет продолжать совершенствовать свои меры по обеспечению информационной безопасности, включая укрепление законодательства, развитие кадрового потенциала, совершенствование технологий защиты, улучшение координации между органами государственной власти и т. д.

Таблица 2

Глобальный прогноз развития технологий информационной безопасности от IDC за 2022 год

Год	Прогноз
2024	35 % компаний перейдут к использованию концепции стратегически встроенной приватности в ИТ-системы, процессы и продукты.
	30 % организаций будут использовать технологии конфиденциальных вычислений для объединения и улучшения важной информации при условии сохранения приватности.
	65 % крупных компаний будут требовать от своих поставщиков облачных услуг контроля над суверенитетом данных, чтобы соблюдать нормативные требования по защите и обеспечению конфиденциальности важной информации.
	30 % компаний усовершенствуют показатели ESG и эффективность управления данными, превышая возможности стандартной отчетности, для обеспечения эффективного управления затратами и получения конкурентных преимуществ.
	75 % крупных компаний будут использовать специализированное программное обеспечение для управления данными ESG и отчетности, чтобы соответствовать новому законодательству и растущим требованиям заинтересованных сторон.
2025	Публичные компании должны обновлять свою оценку ежегодно на основе данной методики.
	45 % руководителей компаний, которые не хотят тратить деньги на системы безопасности, не имеющие ясной окупаемости, начнут требовать от профильных отделов информацию о показателях эффективности использования инструментов защиты данных и предотвращения утечек.
2026	30 % корпораций перейдут на автономные центры управления безопасностью, где распределенные команды могут быстро реагировать на инциденты и эффективно решать проблемы.
2027	Дополнительно к ежегодным аудитам безопасности, 60 % компаний из списка Global 2000 (2000 крупнейших публичных компаний мира) будут производить непрерывную оценку рисков.

Составлено автором

Однако, эффективность этих мер будет зависеть от множества факторов, включая уровень технологического развития, международную конъюнктуру, экономическую обстановку и др.

На основе анализа основных рисков информационной безопасности РФ в новом тысячелетии можно сделать следующие выводы и выработать рекомендации по совершенствованию текущей системы обеспечения информационной безопасности РФ:

Необходимо усилить контроль за использованием средств связи и информационных технологий, особенно в отношении критически важных объектов и информационных систем.

Необходимо совершенствовать законодательство в области информационной безопасности, учитывая новые вызовы и угрозы, а также обеспечивая международную совместимость.

Необходимо улучшить обучение персонала по вопросам информационной безопасности, включая не только специалистов, но и обычных пользователей.

Необходимо укрепить кадровый потенциал, в том числе за счет увеличения численности квалифицированных специалистов, а также обеспечение надлежащего качества образования.

Необходимо совершенствовать технологии защиты, в том числе за счет разработки и внедрения новых криптографических методов, средств защиты от хакерских атак и др.

Необходимо улучшить координацию между различными органами государственной власти, а также между государственными и частными организациями по вопросам информационной безопасности.

Необходимо учитывать международные требования и стандарты в области информационной безопасности и стремиться к их соблюдению.

Необходимо увеличивать финансирование системы обеспечения информационной безопасности РФ и обеспечивать его эффективное использование.

Выводы

Реализация представленных рекомендаций позволит совершенствовать систему обеспечения информационной безопасности РФ и повышать уровень ее эффективности. Информационная безопасность является комплексной задачей, требующей участия всех участников информационного пространства, включая не только государственные организации, но и частные компании и обычных пользователей. Поэтому необходимо проводить информационную работу и пропаганду в этой области, а также стимулировать внедрение современных технологических решений для защиты информации. Только совместными усилиями государства и общества можно создать надежную систему обеспечения информационной безопасности в РФ.

ЛИТЕРАТУРА

1. Абалуев Р.Н., Крумкаченко А.А. Обзор современных подходов к обеспечению информационной безопасности при создании инфраструктуры интернета вещей в агропромышленном комплексе // Наука и образование. 2019. — № 2. — С. 289.
2. Калашников А.О., Сердечный А.Л., Остапенко А.Г. Картографический подход в библиометрическом исследовании отечественных научных школ, сложившихся в области защиты информации и обеспечения информационной безопасности // Информация и безопасность. 2019. — № 4 — С. 455–484.
3. Белов А.С., Добрышин М.М., Борзова Н.Ю. Формирование модели угроз информационной безопасности на среднесрочный период // Приборы и системы. Управление, контроль, диагностика. 2021. — № 7 — С. 41–48.
4. Полякова Т.А. Цифровизация и синергия правового обеспечения информационной безопасности // Информационное право. 2019. — № 2 — С. 4–7.
5. Фастович Г.Г., Кудашова И.В. Информационные технологии в системе повышения эффективности деятельности органов государственной власти: теоретико-правовой аспект // Право и практика. — 2020. — № 2. — С. 18–22.

6. Зегжда П.Д., Анисимов В.Г., Анисимов Е.Г., Сауренко Т.Н. Модель оптимального комплексирования мероприятий обеспечения информационной безопасности // Проблемы информационной безопасности. Компьютерные системы. 2020. — № 2. — С. 9–15.
7. Харисова З.И. О некоторых проблемах обеспечения информационной безопасности государства и общества от современных киберугроз // Актуальные проблемы права и государства в XXI веке. 2019. — № 1 — С. 387–391.
8. Пронькин Н.Н. Условия решения проблем обеспечения информационной безопасности московского мегаполиса // Экономические исследования и разработки. 2019. — № 8 — С. 121–124.
9. Зегжда П.Д., Зегжда Д.П., Анисимов В.Г., Анисимов Е.Г., Сауренко Т.Н. Модель формирования программы развития системы обеспечения информационной безопасности организации // Проблемы информационной безопасности. Компьютерные системы. 2021. — № 2 — С. 109–117.
10. Добринская Д.Е. Социологическое осмысление Интернета: теоретические подходы к исследованию сети (окончание) // Вестник Московского университета. Серия 18. Социология и политология. — 2016. — Т. 22. — № 4. — С. 43–64.
11. Гончарова Ю.А. Вопросы обеспечения внутренней информационной безопасности военнослужащих ВС РФ // Актуальные проблемы защиты и безопасности Труды XXII Всероссийской научно-практической конференции РАРАН. Том 7. 2019. С. 73–76.
12. Павлюкова А.В., Гришина Е.Е. Экономическая безопасность России // Тенденции развития науки и образования. — 2017. — № 32–1. — С. 19–22.
13. Молоканова А.А. Особенности обеспечения информационной безопасности сотрудника органов внутренних дел как компонент профессиональной культуры // Совершенствование профессиональной и нравственной культуры курсантов и слушателей в образовательных организациях системы МВД России: сборник научных трудов межвузовской конференции и всероссийского семинара. 2018. С. 34–36.
14. Полякова Т.А., Минбалеев А.В., Кротков Н.В. Развитие науки информационного права и правового обеспечения информационной безопасности: формирование научной школы информационного права (прошлое и будущее) // Государство и право. 2021. — № 12 — С. 97–108.

Amonov Amir Khaetovich
Financial University under the Government of the Russian Federation, Moscow, Russia
Military Training Center named after Professor, Major General S.M. Ermakova
E-mail: Amonov99@yandex.ru

Ratnik Anatoly Kharitonovich
Financial University under the Government of the Russian Federation, Moscow, Russia
Military Training Center named after Professor, Major General S.M. Ermakova
E-mail: anatolyarslong@gmail.com

Academic adviser: **Akhmetov Minnegaley Gizyatovich**
Financial University under the Government of the Russian Federation, Moscow, Russia
Military Training Center named after Professor, Major General S.M. Ermakova
E-mail: mgahmetov@fa.ru

Ensuring information security in order to preserve the national interests of Russia at the beginning of the 21st century

Abstract. The purpose of this article is to analyze the main risks of information security in Russia in the new millennium and the effectiveness of information security programs in the Russian Federation. The object of the study is the information security system of the Russian Federation. The article identified the main risks of information security in Russia, such as cybercrime, violations of the rules for processing personal data, leaks of confidential information, and others. The authors analyzed the distribution of the listed types of threats to information security of Rostelecom's client companies for 2022. Attention is focused on the fact that a low culture of information security among military personnel and personnel working at the facilities of the Armed Forces can lead to vulnerabilities and risks of data leakage of important strategic facilities.

The programs for ensuring information security of the Russian Federation were considered, including the Federal Target Program "Information Russia", the Federal Law "On the Protection of Personal Data" and others. The authors identified the main goals and indicators of such national programs. An analysis of the effectiveness of the information security system of the Russian Federation is carried out and a forecast of its development is presented. State programs aimed at developing the digital economy, protecting critical information infrastructure, developing mechanisms to combat cyber threats, as well as creating modern technologies for the Russian Armed Forces and cryptography are the key areas of Russia's work in this area. The authors also analyzed the forecast for the development of the Russian cybersecurity market, as well as the global forecast for the development of information security technologies. It is concluded that despite the measures taken by the Russian Federation to ensure information security, the system is still vulnerable to new threats. recommendations were developed to improve the current information security system in the Russian Federation.

Keywords: information; Information Security; information Technology; data protection; ensuring information security; cryptography; cyber-attack; national interests; digital platforms; public administration