УДК 65.011.56

1.10. Глобальные угрозы информационной безопасности для государства и общества

Евдокимов Д.С., н.с. ЦЭМИ РАН, Москва, Россия
Катасонова К.А., м.н.с. ЦЭМИ РАН, Москва, Россия
Комолов К.Ю., с.л. ЦЭМИ РАН, Москва, Россия

В статье исследуются современные тенденции в области информационной безопасности в условиях стремительной цифровизации общества с рассмотрением различных возрастных когорт. На основе актуальных данных доказывается, что увеличение доли интернет-пользователей до 5,56 млрд человек (67,9% населения мира) в 2025 году и их демографическое разнообразие напрямую ведут к росту количества и сложности киберугроз. Эмпирические данные по России подтверждают этот тезис: за первые три квартала 2024 года 56% россиян уже столкнулись с кибернападением, а число фишинговых атак за год выросло на 33%. В работе проведен анализ различных возрастных групп, которые формируют спрос на онлайн-сервисы и становятся мишенями злоумышленников, а также оценивается финансовый ущерб, превысивший 350 млрд руб. за последние три года.

Характерный пример влияния цифровой агрессии на государственные сервисы в масштабе страны можно рассмотреть на примере тотального сбоя в Южной Корее в 2025 году. Такая ситуация продемонстрировала, как хакерские атаки могут парализовать работу всех государственных органов управления и привести к гражданским потрясениям: мгновенная потеря доступа к экстренным службам, медицине, банковским операциям и росту социальной тревожности населения. В исследовании освещены современные технологии защиты использования ИИ и биометрии, а также сделан вывод, что кибербезопасность – это не только защита данных, а также инструмент социальной стабильности, требующий пристального внимания со стороны руководства страны.

Введение

Рост цифровизации общества и увеличение числа пользователей онлайн-сервисов привели к резкому скачку количества кибератак. Пандемия COVID-19 стала катализатором этого процесса, ускорив переход на удаленную работу и развитие цифровых экосистем. Ключевым фактором изменений в области информационной безопасности является демография: рост пользователей в цифровом пространстве, расширение «поколения Z» и «цифровых пенсионеров», а также массовое внедрение онлайн-сервисов в повседневную жизнь. Целью данной статьи является анализ современных киберугроз с позиции демографических сдвигов в обществе, а также оценка эффективности современных технологий защиты в условиях, когда цифровые риски становятся повседневностью для большинства населения.

За последние годы фиксируется стремительный рост цифровизации и создания онлайн сервисов для предоставления государственных услуг населению. По данным отчета Digital 2025: Global Overview Report, на начало 2025 года численность населения всего мира достигла 8,2 млрд человек, интернетом пользуются около 5,56 млрд человек, что составляет 67,9 % от общей численности населения мира. В России же уровень внедрения интернета в стране достиг 88%, а число пользователей цифровых сервисов продолжает увеличиваться[1]. Особенно важно отметить, что расширение цифровой повестки для населения сопровождается ростом атак на массовые сервисы. Так, по данным агентства «РИА Новости» в период с января по сентябрь 2024 года, уже 56% россиян столкнулись с тем или иным видом кибератак[2]. Это показывает, что киберугрозы становятся обыденностью для большинства граждан.

Одним из наиболее быстрорастущих направлений остается фишинг. Согласно исследованию, число фишинговых атак в 2024 году увеличилось на 33% по сравнению с 2023 годом и на 72% относительно 2022-го. При этом 84% таких атак происходят через электронную почту, что делает уязвимыми все возрастные группы, в том числе людей пожилого возраста, которые только начинают активно использовать цифровые сервисы. Также рост наблюдается и в массовых атаках на инфраструктуру. По данным RED Security SOC, в 2024 году количество зафиксированных ИБ-инцидентов в России выросло в 2,5 раза, почти достигнув 130 тысяч случаев[3]. Более 60% из них пришлись на критически важные отрасли – финансы, промышленность и телекоммуникации.

[1] Digital 2025: Global Overview Report // DataReportal URL: https://datareportal.com/reports/digital-2025-global-overview-report (дата обращения: 31.08.2025).

[2] Каждый второй россиянин столкнулся с кибератакой в 2024 году // РИА новости URL: https://ria.ru/20240929/kiberataki-1975391272.html (дата обращения: 31.08.2025).

[3] RED Security SOC: хакеры усилили давление на критическую информационную инфраструктуру России // redsecurity.ru URL: https://redsecurity.ru/news/red-security-soc-khakery-usilili-davlenie-na-kriticheskuyu-informatsionnuyu-infrastrukturu-rossii (дата обращения: 31.08.2025).

В ряде работ других исследователей подчеркивается, что человеческий фактор в настоящее время является одной из ключевых причин инцидентов информационной безопасности. Ошибки пользователей, недостаточный уровень цифровой грамотности, а также игнорирование базовых требований информационной безопасности нередко приводят к утечке данных, даже при наличии современных средств защиты [И.А. Горбунов, 2024]. При этом человек рассматривается не только как источник уязвимостей, но и как важнейший элемент системы обеспечения информационной безопасности, от которого во многом зависит эффективность защитных мер [А.Д. Майданский, 2023].

Защита персональных данных и личных кабинетов от цифровых сервисов становится ключевым фактором, определяющим новые тенденции в области информационной безопасности. Чем больше возрастных и социальных групп активно вовлекается в цифровую экосистему, тем более разнообразными становятся киберугрозы и повышаются требования к адаптивности систем защиты.

Уровень распространения интернет-сервисов в мире и связь с информационной безопасностью

Число пользователей интернета увеличилось на 136 миллионов (+2,5 процента) по сравнению с 2024 годом. В России же уровень использования интернета достиг 88%, а число пользователей цифровых сервисов продолжает увеличиваться[4]. Этот рост имеет общемировую демографическую специфику:

Таблица 1. Основные причины использования интернета разными возрастными группами

Возрастная группа 16-24	**Возрастная группа 25-34**	**Возрастная группа 35-44**	**Возрастная группа 45-54**	**Возрастная группа 55-64**
Поиск информации – 60,7%	Поиск информации – 58,7%	Поиск информации – 59,7%	Поиск информации – 62,1%	Поиск информации – 66,9%
Общение с друзьями и семьей – 59,2%	Общение с друзьями и семьей – 55,6%	Общение с друзьями и семьей – 55,7%	Общение с друзьями и семьей – 56,3%	Следить за новостями и событиями – 59,1%
Просмотр видео и шоу – 58,4%	Просмотр видео и шоу – 54,1%	Следить за новостями и событиями – 52,9%	Следить за новостями и событиями – 54,8%	Общение с друзьями и семьей – 56,3%
Прослушивание музыки – 54,8%	Следить за новостями и событиями – 49,4%	Просмотр видео и шоу – 51,7%	Узнать, как что-то делать – 49,2%	Узнать, как что-то делать – 51,4%
Образование и учеба – 53,0%	Узнать, как что-то делать – 47,7%	Узнать, как что-то делать – 48,9%	Просмотр видео и шоу – 48,8%	Просмотр видео и шоу – 43,0%
Узнать, как что-то делать – 51,1%	Прослушивание музыки – 46,6%	Прослушивание музыки – 42,6%	Провести свободное время / серфинг – 40,9%	Исследовать места и путешествия – 40,7%
Провести свободное время / серфинг – 48,3%	Провести свободное время / серфинг – 41,5%	Провести свободное время / серфинг – 41,1%	Прослушивание музыки – 39,4%	Исследование здоровья – 39,8%
Следить за новостями и событиями – 47,8%	Образование и учеба – 39,0%	Исследование мест и путешествия – 39,1%	Исследование мест и путешествия – 38,9%	Провести свободное время / серфинг – 38,9%

Источник: Составлено авторами на основе отчета DataReportal[5].

Исходя из таблицы можно сделать следующие выводы:

- Молодое поколение (до 30 лет) активно использует финтех, цифровую идентификацию и сервисы «умных городов»;
- Средний возрастной сегмент (30–55 лет) ориентирован на удаленную работу, госуслуги и облачные экосистемы;
- Старшие поколения вовлекаются в цифровую среду через телемедицину, онлайн-банкинг и биометрические сервисы.

Современные научные исследования показывают, что трансформация киберугроз в условиях цифровизации связана не только с развитием технологий, но и с расширением круга пользователей цифровых сервисов, уровень подготовки которых существенно различается [R. Anderson, 2020]. В связи с чем

[4] Digital 2025: Global Overview Report // DataReportal URL: https://datareportal.com/reports/digital-2025-global-overview-report (дата обращения: 31.08.2025).

[5] Digital 2024: Global Overview Report // DataReportal URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения: 31.08.2025).

наблюдается смещение акцента к угрозам, основанным на эксплуатации человеческого фактора, включая социальную инженерию, фишинг [M. A. Sasse, 2001].

Становится ясно, что разница осведомленности пользователей разных возрастов напрямую влияет на картину сетевых атак, делая их более разнообразными и массовыми. При этом важно понимать, что интересующий людей контент в интернете разнообразен и обширен, а большинство возрастных групп уязвимы перед различными типами киберугроз, поэтому меры защиты должны быть дифференцированы. Как можно увидеть на рисунке 1 распространение интернета происходит стремительно, но последовательно. С каждым годом растет число пользователей инфосферы, а вместе с этим число утечек и нарушений.

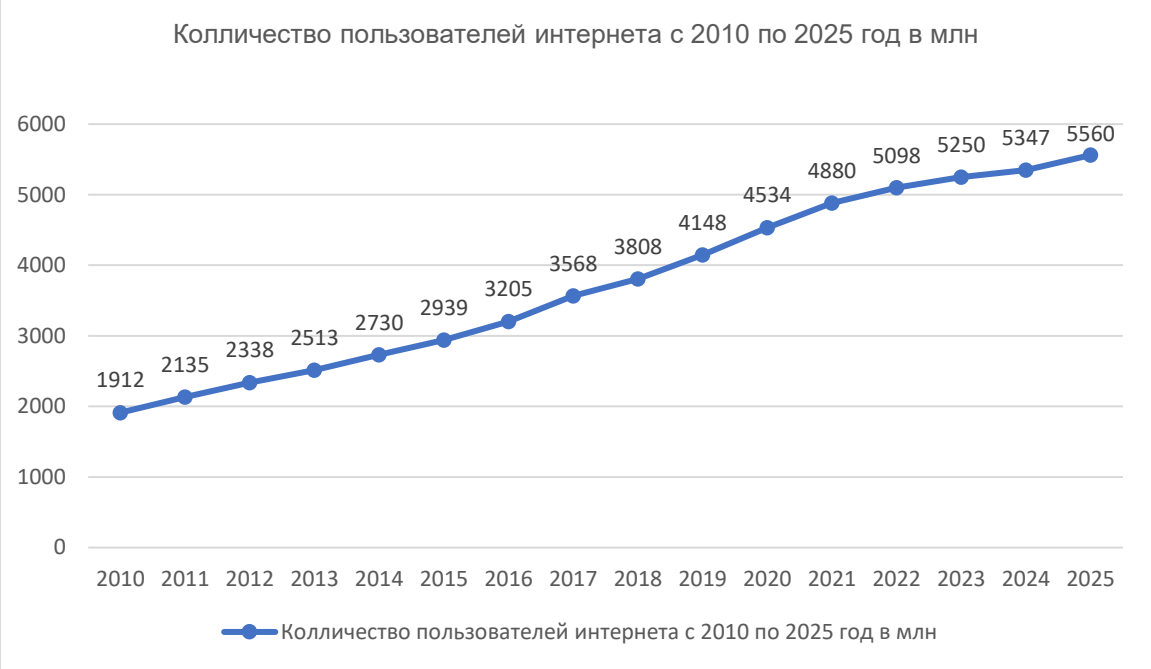

Рис.1 Количество пользователей интернета с 2010 по 2025 год в млн
Источник: Составлено авторами на основе отчета DataReportal[6].

Несмотря на широкое распространение, доступ остается неравномерным. Согласно актуальным данным, глобальный цифровой разрыв остается значительным: более 2,7 млрд человек (свыше трети мирового населения) не имеют доступа к интернету. На Индию приходится 680 млн из этого числа.

Хотя уровень проникновения интернета превысил 25% во всех регионах мира, в Центральной Африке он по-прежнему ниже 50%. Рост подключений в Южной Азии, обусловленный в основном Индией, позволил региону преодолеть 50-процентный рубеж.

В рейтингах по интернетизации последние места занимают страны с тотальными ограничениями (КНДР) и низким уровнем развития инфраструктуры. 7 из 10 государств с наихудшими показателями расположены в Африке, причем в ЦАР охват лишь немногим превышает 10%[7].

IBM провела исследование кибернарушений среди тысяч своих клиентов в более чем 130 странах. Оно показало, что главной опасностью остается человеческий фактор, который являлся основной причиной (95%) всех нарушений[8]. Атаки, основанные на социальном факторе, используют манипуляции, обман и психологическое воздействие, и полностью предотвратить их с помощью одних лишь программных средств невозможно. Единственная эффективная защита – это регулярное обучение сотрудников и повышение их осведомленности о подобных угрозах.

Современные кибератаки становятся не только массовыми, но и более сложными, требующими междисциплинарного подхода к их анализу и предотвращению. Компании и государственные структуры вынуждены адаптировать системы защиты, чтобы противостоять угрозам.

Одним из ключевых инструментов анализа угроз стало имитационное моделирование кибератак. Оно позволяет изучать потенциальные векторы атак и тестировать защитные меры без реальных

[6] Digital 2024: Global Overview Report // DataReportal URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения: 31.08.2025).
[7] Digital 2024: Global Overview Report // DataReportal URL: https://datareportal.com/reports/digital-2024-global-overview-report (дата обращения: 31.08.2025).
[8] Why Human Error is #1 Cyber Security Threat to Businesses in 2021 // The Hacker News URL: https://thehackernews.com/2021/02/why-human-error-is-1-cyber-security.html (дата обращения: 31.08.2025).

рисков. Например, системы мониторинга на основе ИИ, такие как Darktrace[9], используют самообучающиеся алгоритмы для обнаружения и реагирования на киберугрозы в режиме реального времени. Подобные решения помогают минимизировать последствия атак и повышают уровень безопасности в критически важных секторах.

Таким образом, современное состояние информационной безопасности определяется не только технологическим прогрессом, но и демографическими особенностями цифрового общества. Распространенность интернета, разнообразие пользователей и их различный уровень цифровой грамотности формируют среду, в которой ИБ-решения должны быть адаптированы не только под спектр угроз, но и под особенности поведения людей. Тем самым создавая новые вызовы и тренды в области информационной безопасности, указывая на важность адаптации существующих и создания новых решений.

Современные тенденции в области информационной безопасности

Особую значимость приобретает понимание основных тенденций, появившихся в сфере информационной безопасности (ИБ), в следствии активного роста числа и сложности ИТ-сервисов. Рассмотрение этих тенденций позволяет выявить направления, по которым будут эволюционировать защитные технологии и организационные подходы в ближайшие годы.

Анализ тенденций 2024 г. показывает, что в сфере ИБ можно выделить несколько ключевых трендов[10]:

1) Более широкое использование многофакторной аутентификации[11].

На данный момент большинство компаний перешло на использование многофакторной аутентификации. Так как простые пароли стали не столь эффективны с использованием современных программных средств, хакеры легко подбирают или крадут их. Поэтому все больше компаний и сервисов добавляют второй уровень защиты, например код из SMS или код с привязанной почты.

2) Продолжающееся развитие искусственного интеллекта[12].

Искусственный интеллект (ИИ) уже сейчас нашел себе применение в области кибербезопасности, он помогает находить вирусы, предсказывать атаки и защищать данные. Он способен работать круглосуточно, замечать подозрительную активность быстрее человека. Примеры подобных систем уже разработаны и отлично функционируют. Например, Microsoft Security Copilot:

- ИИ анализирует сетевой трафик и поведение пользователей, чтобы выявлять необычную активность;
- если, система фиксирует, что сотрудник компании вдруг начал скачивать гигабайты данных ночью или подключается из необычного региона, то она предупредит службу безопасности;
- также он помогает анализировать сложные кибератаки, подсказывая специалистам, какие шаги нужно предпринять.

3) Более широкое внедрение инструментов и технологий проактивной безопасности[13].

Как правило, раньше компании просто реагировали на уже случившиеся атаки. Теперь внедряются инструменты, которые заранее ищут уязвимости и устраняют их. Благодаря проактивной безопасности организации смогут заранее узнать, на что лучше всего потратить бюджет компании для получения максимального результата.

4) Практики беспарольного доступа (биометрия)[14].

Разговоры про возможность полного отказа от паролей ведутся уже давно. Пароли часто забывают, теряют или используют слишком простые комбинации. Биометрия имеет ряд преимуществ и является уже привычным и широко распространенным вариантом аутентификации, поскольку уже годами сканирование отпечатков пальцев и лица используется во всех современных смартфонах и ноутбуках.

Современный подход к информационной безопасности не ограничивается простыми антивирусами и паролями. Внедряется все больше новых решений, например ИИ, биометрия и проактивные методы защиты. Эти технологии делают цифровой мир безопаснее, но одновременно ставят новые вопросы о конфиденциальности и контроле. Главная задача – найти баланс между удобством, защитой и правами пользователей.

В поисках этого баланса компании и разработчики все чаще обращаются к технологиям биометрической аутентификации. Отпечатки пальцев, распознавание лиц и другие методы идентификации становятся не просто удобными, но и все более безопасными. Эти технологии, начав свой путь в мобильных

[9] Официальный сайт компании Darktrace. URL: https://darktrace.com/ (дата обращения: 31.08.2025).

[10] Официальный сайт информационного портала SecurityLab.ru / 9 тенденций в области кибербезопасности на 2024 год URL: https://www.securitylab.ru/analytics/544688.php (дата обращения: 31.08.2025).

[11] 11 развивающихся тенденций информационной безопасности в 2021 году // SecurityLab.ru URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/350574.php (дата обращения: 31.08.2025).

[12] 11 развивающихся тенденций информационной безопасности в 2021 году // SecurityLab.ru URL: https://www.securitylab.ru/blog/company/PandaSecurityRus/350574.php (дата обращения: 31.08.2025).

[13] 9 тенденций в области кибербезопасности на 2024 год // SecurityLab.ru URL: https://www.securitylab.ru/analytics/544688.php (дата обращения: 31.08.2025).

[14] 9 тенденций в области кибербезопасности на 2024 год // SecurityLab.ru URL: https://www.securitylab.ru/analytics/544688.php (дата обращения: 31.08.2025).

устройствах, постепенно внедряются в повседневную жизнь, включая финансовые операции и системы доступа.

Впервые массово реализовывать технологии разблокировки по отпечатку пальца в смартфонах начали с выходом модели Apple iPhone 5s, которую представили в сентябре 2013 г. Технология распознавания лиц начала активно внедряться в смартфоны с выходом Apple iPhone X в сентябре 2017 г. Этот телефон представил функцию Face ID, которая использовала сложные алгоритмы и датчики для распознавания лица пользователя.

Эти изменения и тенденции оказывают огромное влияние на людей не только в информационной среде, они также затрагивают реальную жизнь. Например, в России с 2021 г. начала функционировать и развиваться система оплаты с помощью биометрии. Система начала действовать в метрополитене, и с 2024 г. ей пользуются тысячи людей, а Сбербанк реализовал ее для оплаты обычных покупок. Использование биометрии для оплаты – лишь одно из направлений ее развития. Технологии распознавания лиц давно вышли за рамки личных устройств и финансовых сервисов, становясь инструментом для обеспечения безопасности и контроля в общественных местах.

Внедрять системы распознавания лиц через уличные камеры начали еще раньше, но дальше всех в плане создания единой системы распознавания лиц на государственном уровне продвинулся Китай. Реализация этой программы началась еще в 2013 г. и с тех пор активно развивается. Так в 2023 г., по оценке CBS News, в Китае таких камер насчитывается 400 млн[15]. Работы по их установке начали в связи с идеей внедрить «систему социального рейтинга», которая на данный момент еще до конца не реализована, но продолжается тестироваться в 12 крупных городах. В зависимости от конкретной системы используется балльная шкала (от 0 до 1000) или буквенная шкала (от A до D). Рейтинг формируется на основе данных из официальных источников (налоговые и правоохранительные органы, правительственные учреждения, ЗАГСы, образовательные организации, компании), а также цифровых следов (поисковые запросы, онлайн-покупки, активность в соцсетях). Дополнительно учитываются данные с камер видеонаблюдения и систем распознавания лиц. Система оценки представлена в таблице 2**.**

Таблица 2. Категории социального рейтинга граждан Китая

Система	Диапазон оценки	Описание категории	Последствия
Zhima Credit (Sesame Credit)	350–950 баллов	Индивидуальная кредитная оценка, основанная на покупках, платежах, соцактивности	Высокий балл: аренда без залога, скидки, ускоренные визы; низкий балл: ограничения в кредитовании
Муниципальный социальный рейтинг	A – образцовый гражданин	Высокий уровень доверия, активное участие в общественной жизни	Доступ к льготам, приоритет при поступлении в университеты и на госслужбу
	B – благонадежный гражданин	Нет серьезных нарушений, стабильное выполнение обязательств	Стандартные права, без бонусов и ограничений
	C – гражданин группы риска	Замечены нарушения (задержки по платежам, штрафы), но без серьезных инцидентов	Могут возникнуть сложности с кредитами и госуслугами
	D –неблагонадежный гражданин	Систематические нарушения, долги, административные наказания	Ограничения на покупку билетов на самолеты и поезда, запрет на определенные работы

Источник: Составлено авторами на основе открытых источников.

Китайский опыт демонстрирует, к чему может привести тотальное внедрение биометрических технологий без четких правовых рамок. Реализация «Системы социального рейтинга» является ярким примером слияния цифрового наблюдения с социальным управлением. Граждане получают оценки на основе их поведения (финансового, социального, онлайн-активности), которые напрямую влияют на их доступ к услугам и ресурсам, что формирует серьезные риски для приватности граждан и создает инструмент для массового контроля, выходящего далеко за рамки борьбы с киберпреступностью.

Рост влияния биометрических технологий и систем слежения ставит перед обществом сложный вопрос: где та грань, за которой обеспечение безопасности превращается в тотальную слежку? Как и в реальном мире, где биометрия помогает выявлять риски, в киберпространстве развиваются модели, позволяющие прогнозировать атаки, но их внедрение требует баланса между безопасностью и правами человека.

Теневые риски в кибербезопасности

Помимо классический угроз, современная кибербезопасность сталкивается со скрытыми, теневыми рисками, связанными с манипуляцией данными. Злоумышленники могут тайно внедрять ложные записи или «отравленные» данные в критические ИТ-системы, создавая основу для дальнейшего вторжения без явного признака взлома. Так, описывают «data poisoning» атаки, когда в обучающие датасеты моделей ИИ или корпоративные базы внедряются ошибочные или предвзятые точки данных, что позволяет

[15] China's buildup of the surveillance state – "Intelligence Matters" // CBS News URL: https://www.cbsnews.com/news/chinas-buildup-of-the-surveillance-state-intelligence-matters/ (дата обращения: 31.08.2025).

незаметно или радикально изменить поведение систем и алгоритмов[16]. В таких случаях система продолжает функционировать, как будто все в порядке, но ее выводы становятся далёкими от истины, и порой просто вымышленными. Это делает подмену особенно опасной – реальные последствия могут оставаться незамеченными до катастрофы. По мнению экспертов, скрытый саботаж данных способен подорвать доверие к информационным ресурсам и вывести из строя множество гражданских или военных объектов[17]. Подобные атаки очень опасны и как правило приводят к тяжелым последствиям.

Примером такой цифровой агрессии может послужить вирус Stuxnet, с помощью которого была произведена атака против ядерной программы Ирана. Он стал наиболее известным из подобный инцидентов, продемонстрировав опасность и серьезность возможных последствий. При атаке на иранские центрифуги он воспроизводил оператору ранее записанные успокаивающие ложные данные вместо реальных показаний датчиков, скрывая настоящую аварийную ситуацию[18]. Аналогичные приемы в государственных системах могли бы заставить доверять вредоносно искаженной статистике или разведданным: принятые на их основе решения окажутся ложными. Опасность кроется в сложности обнаружения подобных вмешательств, поскольку при мониторинге систем изменений заметно не будет, так как станут использоваться уже поддельные данные, выдаваемые за реальные. В результате последствия могут оказаться катастрофическими, вплоть до уничтожения или паралича критической инфраструктуры государства.

Последствия глобального нарушения работы государственных сервисов в условиях тотальной цифровизации Южной Кореи

Наглядным примером уязвимости критической инфраструктуры стал пожар в Национальной службе информационных ресурсов в Южной Корее 26 сентября 2025 года. По данным SecPost, это одна из самых масштабных технологических катастроф последних лет, произошедшая из-за возгорания литий-ионных батарей в серверных. В результате инцидента оказались парализованы 709 государственных сервисов, от портала для граждан до систем экстренного реагирования. А также было уничтожено облачное хранилище G-Drive, которым пользовались около 750 тысяч госслужащих, в нем хранилось порядка 858 терабайтов данных, которые были безвозвратно утеряны[19].

Последствия пожара были ощутимы для всей страны. Наиболее популярные сервисы, такие как: правительственный портал, банковские и почтовые системы, экстренные службы – перестали работать или функционировали с перебоями. К середине октября удалось восстановить лишь около 27% систем, в том числе за счет переброски архивов с локальных машин сотрудников и бумажных копий[20]. В данной ситуации президент Ли Чжэ Мен лично выступил с извинениями за сбои и признал, что отсутствие резервных копий в подобных системах недопустимо.

Социальные последствия оказались значительными. Массовый сбой вызвал своего рода цифровой коллапс – жители Южной Кореи ощутили острый дефицит обычных услуг, повысилась тревожность и недовольство населения. Министр безопасности Юн Ходжон предупредил об «усиленных сбоях в повседневной жизни» до полного восстановления сервисов[21]. Этот инцидент демонстрирует, что отказ ключевой инфраструктуры мгновенно оборачивается цифровым локдауном для общества, нарушая привычный образ жизни миллионов людей и несет с собой серьезные социальные проблемы, создавая новые вызовы в области информационной безопасности.

Благодарности

Работа выполнена при поддержке Министерства науки и высшего образования Российской Федерации в рамках проекта № 075-15-2024-525 от 23.04.2024

Литература

1. Горбунов И. А. Информационная безопасность: сущность и современное состояние в системе национальной безопасности России // Образование и право. 2024. № 4. URL: https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-suschnost-i-sovremennoe-sostoyanie-v-sisteme-natsionalnoy-bezopasnosti-rossii (дата обращения: 18.01.2026).

[16]Официальный сайт компании IBM // What is data poisoning? URL: https://www.ibm.com/think/topics/data-poisoning (дата обращения: 21.11.2025).

[17]Big Data as a National Security Issue // The University of Chicago URL: https://legal-forum.uchicago.edu/print-archive/big-data-national-security-issue (дата обращения: 21.11.2025).

[18]Stuxnet Facts Report // NATO Cooperative Cyber Defence Centre of Excellence URL: https://ccdcoe.org/uploads/2018/10/Falco2012_StuxnetFactsReport.pdf (дата обращения: 21.11.2025).

[19]Кибер-катастрофа в Южной Корее. Какие ИБ-уроки можно извлечь из пожара в главном ЦОДе страны // SecPost URL: https://secpost.ru/kiber-katastrofa-v-yuzhnoj-koree-kakie-ib-uroki-mozhno-izvlech-iz-pozhara-v-glavnom-czode-strany/ (дата обращения: 21.11.2025).

[20]Кибер-катастрофа в Южной Корее. Какие ИБ-уроки можно извлечь из пожара в главном ЦОДе страны // SecPost URL: https://secpost.ru/kiber-katastrofa-v-yuzhnoj-koree-kakie-ib-uroki-mozhno-izvlech-iz-pozhara-v-glavnom-czode-strany/ (дата обращения: 21.11.2025).

[21]South Korea scrambles to restore digital services after server fire // Reuters URL: https://www.reuters.com/world/asia-pacific/south-korea-restores-46-services-after-data-centre-fire-safety-minister-says-2025-09-29/ (дата обращения: 21.11.2025).

2. Майданский А. Д. Основные механизмы получения информации при использовании социальной инжененнрии // E-Scio. 2023. №3 (78). URL: https://cyberleninka.ru/article/n/osnovnye-mehanizmy-polucheniya-informatsii-pri-ispolzovanii-sotsialnoy-inzhenerii (дата обращения: 18.01.2026).
3. Anderson R. Security Engineering: A Guide to Building Dependable Distributed Systems. 3rd ed. Chichester: Wiley, 2020. URL: https://www.google.ru/books/edition/Security_Engineering/GNIHEAAAQBAJ (дата обращения: 18.01.2026).
4. Stephan P.B. Big Data as a National Security Issue // The University of Chicago Legal Forum – 2024. URL: https://legal-forum.uchicago.edu/print-archive/big-data-national-security-issue (дата обращения: 21.11.2025).
5. Sasse M.A., Brostoff S., Weirich D. Transforming the “weakest link”: A human–computer interaction approach to usable and effective security // BT Technology Journal. 2001. URL: https://discovery.ucl.ac.uk/id/eprint/144215/1/BTTJSECv5.pdf (дата обращения: 18.01.2026).

References in Cyrillics

1. Gorbunov I. A. Information Security: Essence and Current State in the System of National Security of Russia // *Education and Law*. 2024. No. 4.
2. Majdanskij A.D. Osnovnye mekhanizmy polucheniya informacii pri ispol’zovanii social’noj inzhenerii // E-Scio. 2023. №3 (78).

Евдокимов Дмитрий Сергеевич, научный сотрудник ЦЭМИ РАН (dimaevd15@gmail.com)
ORCID 0000-0001-8304-9448

Катасонова Кристина Александровна, младший научный сотрудник ЦЭМИ РАН (kkristinjour@gmail.com) ORCID 0000-0002-8349-8451

Комолов Клим Юрьевич, старший лаборант ЦЭМИ РАН (komolov.klim@mail.ru) ORCID 0009-0009-6557-5706

Ключевые слова
Информационная безопасность, киберугрозы, цифровизация общества, искусственный интеллект, многофакторная аутентификация, биометрия, проактивная защита, цифровая грамотность населения.

Dmitry Evdokimov, Kristina Katasonova, Klim Komolov. Global threats to information security for a government and society

Keywords
Information security, cyber threats, digitalization of society, artificial intelligence, multi-factor authentication, biometrics, proactive defense, digital literacy of the population.

DOI: 10.34706/DE-2026-01-10
JEL classification: L86 – Информационные и интернет-услуги • Компьютерные программы, N20 — Общая, международная и сравнительная информация

Abstract
The article examines current trends in the field of information security in the context of the rapid digitalization of society, considering various age cohorts. Based on current data, it is proved that the increase in the share of Internet users to 5.56 billion people (67.9% of the world's population) in 2025 and their demographic diversity directly lead to an increase in the number and complexity of cyber threats. Empirical data on Russia confirms this thesis: in the first three quarters of 2024, 56% of Russians have already experienced a cyber attack, and the number of phishing attacks has increased by 33% over the year. The paper analyzes various age groups that generate demand for online services and become targets of intruders, as well as estimates of financial damage that has exceeded 350 billion rubles over the past three years.

A typical example of the impact of digital aggression on government services nationwide can be seen in the example of the total disruption in South Korea in 2025. This situation has demonstrated how hacker attacks can paralyze the work of all government agencies and lead to civil unrest: instant loss of access to emergency services, medicine, banking operations and an increase in social anxiety among the population. The study highlights modern technologies for protecting the use of AI and biometrics, and concludes that cybersecurity is not only data protection, but also a tool for social stability that requires close attention from the country's leadership.