Секция «9.6 Цифровизация общества: траектории трансформации, управленческие вызовы и социальные последствия»

Формирование региональной системы кибербезопасности как управленческий вызов цифровой трансформации (на примере Владимирской области)

Научный руководитель – Солодилов Анатолий Васильевич

Паточнова Александра Максимовна
Студент (бакалавр)
Государственный университет просвещения, Москва, Россия
E-mail: patochnova@inbox.ru

Цифровая трансформация государственного и муниципального управления, которая является стратегическим приоритетом развития Российской Федерации, сопровождается не только расширением доступности и качества услуг, но и беспрецедентным ростом киберугроз. Как справедливо отмечает министр цифрового развития Владимирской области Александр Белоусов, «цифровизация открыла безграничные возможности... Но за прогрессом следуют и угрозы — кибератаки, утечки данных, цифровое мошенничество. Эти вызовы не просто нарушают работу систем, они ставят под удар доверие граждан, стабильность экономики и безопасность региона». В этих условиях формирование эффективной региональной системы кибербезопасности перестаёт быть сугубо технической задачей и превращается в комплексный управленческий вызов, требующий координации усилий органов власти, бизнеса и институтов гражданского общества.
В 2024 году в структуре Министерства цифрового развития Владимирской области создан специализированный отдел информационной безопасности госструктур, в функции которого входит защита официальных сайтов и каналов от кибер-атак. В рамках региональной системы кибербезопасности развернуты две профильные группы: группа обнаружения инцидентов и группа реагирования, осуществляющие тренировки в реальных условиях по защите серверной инфраструктуры.
Цель исследования – выявить управленческие механизмы формирования региональной системы кибербезопасности в условиях цифровой трансформации Владимирской области, оценить их эффективность, а также разработать рекомендации по совершенствованию управления кибербезопасностью в регионе.
В докладе освещены такие вопросы как:

- Нормативно-правовые и организационные основы обеспечения кибербезопасности на региональном уровне.
- Ключевые угрозы информационной безопасности, характерные для Владимирской области.
- Реализация мероприятий по защите региональных информационных систем и противодействию киберугрозам.
- Роль межведомственного взаимодействия и общественных инициатив в формировании региональной системы кибербезопасности.
- Рекомендации по совершенствованию управления кибербезопасностью во Владимирской области.

Объект исследования – региональная система обеспечения кибербезопасности Владимирской области.
Предмет исследования – управленческие механизмы, организационные формы и социальные практики формирования системы кибербезопасности в регионе.

Методология исследования включает в себя: анализ документов - изучение нормативно-правовых актов Владимирской области в сфере цифровой трансформации и информационной безопасности; анализ статистических данных - обработка официальных данных о киберпреступности, предоставленных УМВД по Владимирской области; метод тематического кодирования экспертных интервью, взятых из официальных новостных источниках региона для систематизации выявленных проблем и предложений.
Сочетание количественных (статистический анализ) и качественных (анализ документов) методов позволяет обеспечить надежность выводов. Анализ официальной статистики дает объективную картину масштаба киберугроз, а экспертные интервью позволяют понять управленческую логику принятия решений и выявить латентные проблемы, не отражаемые в отчетности.
Управленческий механизм - совокупность организационных структур, нормативно-правовых инструментов, процедур взаимодействия и ресурсного обеспечения, направленных на реализацию государственной политики в сфере защиты информационных систем и данных на уровне субъекта Российской Федерации.
Эффективность региональной системы кибербезопасности - способность системы достигать установленных целей защиты информационной инфраструктуры и граждан от киберугроз при оптимальном использовании имеющихся ресурсов.
Уникальной особенностью Владимирской области является развитие добровольческого движения «КиберПатруль», слет которого состоялся в декабре 2025 года. Активисты движения выполняют функции мониторинга интернет-ресурсов, выявления контента экстремистской направленности, информации о незаконном обороте наркотических средств, а также противодействуют фишинговым и мошенническим схемам.
Более 1000 волонтёров состоят в общественном формировании «КиберПатруль» во Владимирской области по состоянию на 2025 год . В 2023 году численность движения составляла чуть более 100 человек . За два года количество участников увеличилось в 10 раз, что свидетельствует о значительном расширении движения и росте общественной активности молодежи в сфере кибербезопасности. Штабы «КиберПатруля» действуют во всех муниципальных образованиях Владимирской области. По данным МВД России, в 2024 году был ограничен доступ к 42 000 ресурсов с радикальным контентом (в общероссийском масштабе). Как подчеркивает координатор партийного проекта «Цифровая Россия» во Владимирской области Максим Байрак, деятельность цифровых волонтеров является важным социальным институтом в построении безопасной цифровой среды, способствующим формированию устойчивости граждан к кибер угрозам. Данная практика коррелирует с европейскими подходами, где подчеркивается необходимость развития цифровой грамотности среди граждан через обучение на протяжении всей жизни и общественные инициативы.

В 2025 году количество краж с банковских карт, взломов личных кабинетов и дистанционных мошенничеств в регионе сократилось на 15%. Одновременно уровень раскрываемости таких преступлений вырос на 17%. Общее число раскрытых тяжких и особо тяжких преступлений в области увеличилось на 12%, а количество раскрытых «глухарей» (преступлений прошлых лет) возросло на 11%. Однако, несмотря на положительную годовую динамику, оперативные сводки фиксируют сохранение высокой активности аферистов. Только за одну неделю 2026 года в органы внутренних дел поступило 36 сообщений о дистанционных кражах, а общая сумма похищенных средств превысила 15 миллионов рублей.
Характерные мошеннические схемы:

- *Схема «декларирования сбережений»* — 78-летняя жительница Владимира передала прибывшему курьеру почти 3 миллиона рублей после убеждения в необходимости

срочного «декларирования» накоплений.

- *Схема «выгодных инвестиций»* — 50-летняя жительница Владимира перевела мошенникам 2,6 млн рублей, потеряв личные сбережения и кредитные средства.
- *Схема фиктивной продажи автомобилей* — житель Коврова перевел 1,45 млн рублей «менеджеру» из мессенджера для покупки BMW, после чего канал был удален.

В ходе исследования был сделан ряд выводов, в целом были выделены следующие направления для совершенствоания региональной системы кибербезопасности:

- Расширение программ цифровой грамотности для наиболее уязвимых категорий граждан (пенсионеры, социально незащищённые слои).
- Углубление интеграции с образовательными программами вузов и колледжей для подготовки кадров в сфере кибербезопасности.
- Развитие механизмов обратной связи с населением для оперативного выявления новых мошеннических схем.

Источники и литература

1) Владимирская полиция стала на 17% эффективнее ловить интернет-аферистов // Progorod33. – 2026. – 30 января. – URL: https://progorod33.ru (дата обращения: 02.03.2026).
2) Банных Г.А., Туктарев П.В. Управленческие практики реализации государственной политики обеспечения безопасности критической информационной инфраструктуры в субъекте РФ – 2025. – Т. 8, № 3. – С. 266-282.
3) Туктарёв П.В. Реализация государственной политики обеспечения безопасности критической информационной инфраструктуры: анализ управленческих практик : магистерская диссертация / Уральский федеральный университет. – Екатеринбург, 2025. – 115 с.
4) Яковлева Н.В. Безопасность цифровой экономики России и ее регионов // Управленческий учет. – 2025. – № 8.
5) Хубулури Е.И. Кибербезопасность в органах местного самоуправления: системный обзор и анализ основных проблем // Государственное и муниципальное управление. Ученые записки. – 2025. – № 4. – С. 218-224.
6) Киберпатруль Владимирской области - https://avo.ru/-/-kiberpatrul-na-straze-bezopasnogo-interneta-vo-vladimirskoj-oblasti (Дата обращения: 02.03.2026)