- прозрачность: доступное описание работы искусственного интеллекта для ознакомления широких масс потребителей и разработчиков;
- технологический суверенитет: обеспечения материальной поддержки для создания отечественных технологий для разработки новых алгоритмов работы, основанные на ИИ;
- целостность инновационного цикла: обеспечение совместного взаимодействия научных исследований и аналитических секторов в области криминогенной обстановки страны;
- адаптация для отечественных государственных информационных систем.

Таким образом развитие и применение искусственного интеллекта в правоохранительной сфере произведет положительный эффект в борьбе с преступностью и противоправной деятельности. Для реализации полноценной его работы нужно учитывать все недостатки и разработать методику регулирования создания данной системы.

***

1. Указ Президента Российской Федерации от 10.10.2019 № 490 "О развитии искусственного интеллекта в Российской Федерации"
2. Баранов С.А., Голодков Ю.Э., Демаков В.И., Кургалеева Е.Е. Основы информационной безопасности. Учебное пособие. – Иркутск, ФГОУ ВПО ВСИ МВД России, 2015, С. 21
3. Ларина Е. С. Искусственный интеллект. Большие данные. Преступность / Е. С. Ларина, В. С. Овчинский. — М. : Кн. мир, 2018. — С.162-164
4. Суходолов А. П., Бычкова А. М. Искусственный интеллект в противодействии преступности, ее прогнозировании, предупреждении и эволюции // Всероссийский криминологический журнал. 2018. Т. 12, № 6. С. 753–766

Редников Д.В., Комарова М.А.

Проблемы формирования культуры кибербезопасности

*ФГБОУ ВО «Башкирский государственный университет»
(Россия, Уфа)*

doi: 10.18411/trnio-12-2021-102

Аннотация

В статье проанализированы основные проблемы кибербезопасности в современных российских реалиях, рассмотрена необходимость формирования информационной культуры граждан для предотвращения нарушения их материальных и нематериальных прав.

Ключевые слова: кибербезопасность, информационная безопасность, информационные технологии.

Abstract

The article analyzes the main problems of cybersecurity in modern Russian realities, considers the need to form an information culture of citizens to prevent violations of their material and non-material rights.

Keywords: cybersecurity, information security, information technology.

Информатизация населения, организаций и государственной сферы является неизбежным этапом общественного прогресса, который сейчас активно проходит в российском обществе. Однако по мере распространения информационных технологий увеличивается и количество правонарушений в этом поле, в связи с чем в Российской Федерации в 2016 году принимается Доктрина информационной безопасности Указом Президента РФ от 5.12.2016 №646 [8], где ей указаны основные представления государства в области кибербезопасности, в частности, само понятие «информационная безопасность»

выражается через определение «состояние защищенности...», а «информационная инфраструктура» как «объекты информатизации, сайты сети Интернет и сети связи» [8].

Стоит понимать, что современное общество все более становится информационно-ориентированным, а значит, в урбанизированной части общества уже невозможно представить действия экономические и юридические, которые могли бы не сопровождаться соприкосновением с информационными технологиями [1]. Исходя из этого, можно предположить, что информационной атаке подвергаются не только сами технологии, но также и сами информационные процессы, а ещё более – люди. Таким образом, вернее всего будет принимать меры по защите: объектов инфраструктуры, процессов обмена информации, а также самих людей. Причем в этом тройственном звене, при теоретическом абстрагировании можно представить идеальную защищенность объектов и процессов, однако не людей. Поэтому именно люди и человеческий фактор становится главной проблемой информационной безопасности: от простых граждан, не имеющих представления о процессах работы информационных программ и принципов безопасности работы в сети Интернет, до государственных служащих, намеренно или неосознанно нарушающих протоколы безопасности. Именно человеческий фактор чаще всего является основной нарушения информационной безопасности, и в то же время может стать ключом к качественному повышению кибербезопасности, при общем повышении грамотности в сфере информационных технологий.

В самой Доктрине информационной безопасности РФ впервые законодательно указывается проблема низкой культуры информационных технологий, но спустя 5 лет до сих пор не приняты серьезные шаги в системе образования [5], качественно решающие проблему неосведомленности граждан. Для координации государственной политики в области информационной безопасности 10 мая 2017 года была принята Стратегия развития информационного общества на 2017-2030 года. Одним из 9 целей (направлений) государственной политики (на последнем месте) стоит обеспечение информационной безопасности. Причем, в Задачах обозначается методология работы в двух видах: а) разрабатывать нормы международно-правового регулирования в области информационной безопасности; и второй вид - б) создать системы, обеспечивающие возможность устойчивого, безопасного и независимого функционирования российского сегмента сети "Интернет" [7]. Таким образом, Стратегия вновь касается инфраструктуры и косвенно информационных процессов (в законодательном аспекте), но упускается человеческий фактор в информационной безопасности.

В настоящее время именно среднестатистические пользователи нуждаются в базовых знаниях в области кибербезопасности для повседневной жизни [3]. И этот вопрос касается не только опасности для отдельно взятых людей, чьи материальные и не материальные права могут быть нарушены в ходе хищения информации, но также и в целом и всего общества, когда повседневные носители информации и их средства связи могут быть заражены вредоносными программами, способными на широкое распространение как эпидемия или пандемия, что может привести в целом к обрушению всех информационных процессов и инфраструктур [9]. В связи с этим необходимы координированные действия не только государственной органов, но также и частного сектора и общественных организаций, заинтересованных в улучшении культуры кибербезопасности. В этом аспекте кибербезопасность становится вопросом защитой интересов человека (не только пользователя), всего общества и государства, а также всех информационных и не информационных активов, которые могут пострадать при соприкосновении с киберпространством.

Изучая зарубежный положительный опыт становления культуры информационной безопасности [4], а также представления органов РФ из области правовой и экономической безопасности [2], можно смоделировать 4 основные сферы культуры кибербезопасности: технологии, общие ценности, анонимные запреты и знания.

Под технологиями в культуре кибербезопасности можно определять существующие механизмы и инфраструктуры безопасности, которые вольно или невольно работают на устройстве среднестатистического пользователя, организации или государственного органа.

Под общими ценностями можно принимать стратегии, концепции, принципы политики организации или государства в области кибербезопасности, принятые законодательные акты, протоколы, инструкции.

Под анонимными запретами (законами) предполагается понимать традиции, обычаи пользователей и сотрудников, коллективные бессознательные правила и запреты, соблюдаемые на уровне интуиции.

Под знаниями в области кибербезопасности логично выводить осознанные правила поведения при применении информационных технологий, рационально понимаемые пользователями действия при выполнении повседневных задач, бизнес-сделок, взаимодействиях с властью.

Эта попытка структурировать информационную культуру не может быть полностью раскрыта в рамках статьи или доклада, и каждый компонент требует отдельного исследования как в области более конкретного раскрытия и обоснования понятия, так и в области субъектов, способных и должных развивать данные компоненты информационной культуры. Однако можно выделить, что технологии, ценности и знания исходят сверху вниз, от организаций и государства к обществу, в то время как анонимные запреты формируются снизу в самих коллективах, и является основным регулятором поведения людей (пользователей, сотрудников, должностных лиц). Именно на развитие анонимных запретов, их самообновлении при возникновении новых угроз должны быть направлены остальные компоненты, поскольку логично предположить, что среднестатистический пользователь не сможет физически усвоить все знания, ценности и технологии. Примечательным примером развития анонимных запретов является объявление, играющая в громкоговорителях на общественных остановках в г. Уфа о запрете сообщения иным лицам CCV кода банковских карт, что обыгрывается в ролевой диалоговой форме между мужчиной и женщиной.

Делая обобщающий вывод, можно сказать, что внедрение информационных технологий в жизнь общества, коммерческих организаций и государственных структур открыло множество полезных последствий, как экономия времени, улучшение качества услуг, увеличение удобства в процессе повседневных необходимых действий и т.д. Но вместе с тем выросли потенциальные риски и угрозы, к которым киберобщество не было готово. Поэтому на современном этапе необходимо качественно повышать культуру общества в области кибербезопасности, особенно расширять количество анонимных запретов, усваиваемых среднестатистическим пользователем, запустить процесс самообновления данных запретов по мере возникновения новых угроз. Доктрина и Стратегия РФ в компоненте информационной безопасности упускается человеческий фактор и людей как основной источник угроз, поэтому для достижения целей необходимо изменить парадигма понимания информационной безопасности в области государственной политики до того момента, как непосредственно появится угроза на национальном уровне.

***

1. Абдусаламов Р.А. К вопросу о совершенствовании доктринальных положений в области обеспечения информационной безопасности // Юридический вестник Дагестанского государственного университета, 2017. [Электронный ресурс] – URL: <https://cyberleninka.ru/article/n/k-voprosu-o-sovershenstvovanii-doktrinalnyh-polozheniy-v-oblasti-obespecheniya-informatsionnoy-bezopasnosti> (дата обращения: 22.11.2021).
2. Гриценко В.В. Доктрина информационной безопасности как политико-правовой документ стратегического планирования в сфере обеспечения национальной безопасности России // Правовая политика и правовая жизнь, 2017. [Электронный ресурс] – URL: <https://cyberleninka.ru/article/n/doktrina-informatsionnoy-bezopasnosti-kak-politiko-pravovoy-dokument-strategicheskogo-planirovaniya-v-sfere-obespecheniya> (дата обращения: 22.11.2021).
3. Козырева А. А. Современное состояние государственной политики в сфере информационной безопасности // Вестник Воронежского института МВД России, 2018. [Электронный ресурс] – URL:

<https://cyberleninka.ru/article/n/sovremennoe-sostoyanie-gosudarstvennoy-politiki-v-sfere-informatsionnoy-bezopasnosti> (дата обращения: 22.11.2021).

4. Лариса В. М. Международные стандарты в области развития глобального информационного общества // Закон и право, 2019. [Электронный ресурс] – URL: <https://cyberleninka.ru/article/n/mezhdunarodnye-standarty-v-oblasti-razvitiya-globalnogo-informatsionnogo-obschestva> (дата обращения: 22.11.2021).
5. Морозов А. В. Проблемы педагогической деятельности в сфере информационного права и информационной безопасности: пути их решения // Международная конференция «Динамика институтов информационной безопасности. Правовые проблемы». М.: ИГП РАН, 2017.
6. Навальный С.В. Информационная безопасность в России: пути обеспечения // Правовая политика и правовая жизнь, 2015. [Электронный ресурс] – URL: <https://cyberleninka.ru/article/n/informatsionnaya-bezopasnost-v-rossii-puti-obespecheniya> (дата обращения: 22.11.2021).
7. О Стратегии развития информационного общества в Российской Федерации на 2017-2030 годы: указ Президента Рос. Федерации от 9 мая 2017 г. № 203 // Собр. законодательства Рос. Федерации. 2017. № 20.
8. Об утверждении Доктрины информационной безопасности Российской Федерации: указ Президента Рос. Федерации от 5 дек. 2016 г. № 646 // Собр. законодательства Рос. Федерации. 2016. № 50.
9. Чеботарева А.А. Обеспечение информационной безопасности личности: роль международной информационной безопасности и стратегического партнерства // Вестник Академии права и управления. 2016. № 42. С. 48-51.

Салтыкова Н.В.¹, Смирнов В.В.¹, Хохлова А.В.²

Разработка информационных систем для медицинских учреждений

¹Калужский государственный университет им. К. Э. Циолковского

²МКОУ "Шайковская средняя общеобразовательная школа №1"

(Россия, Калуга)

doi: 10.18411/trnio-12-2021-103

Аннотация

В статье рассматриваются вопросы информатизации системы здравоохранения, акцент сделан на изучении особенностей разработки и проектирования информационных систем для медицинских учреждений.

Ключевые слова: информационная система, разработка, здравоохранение.

Abstract

The article discusses the issues of informatization of the healthcare system, the emphasis is on the study of the features of the development and design of information systems for medical institutions.

Keywords: information system, development, healthcare.

С каждым годом современный мир всё больше погружается в цифровую среду: разрабатываются новые приложения для различных сфер профессиональной деятельности, сервисы, которые помогают в повседневной жизни. Новые технологии — это не только усложнение информационных процессов, но и облегчение работы, комфорт и удобство. Автоматизация и цифровизация позволяют облегчить труд сотрудников, повысить удобство и качество обслуживания в целом. Изменения в области информатизации коснулись и таких традиционных сторон общества как образование и медицина.

В медицине цифровые технологии применяются неравнозначно. С одной стороны, цифровые методы обследования и обработки результатов применяются с 80-х годов. С другой — автоматизированные информационные системы (далее - АИС) и медицинские информационные системы (далее - МИС) активно внедряются только последние несколько лет

В статьях К.А. Мызровой, В.С. Русовой, А. Г. Васина, А. В. Гусева рассмотрена перспективность цифровизации здравоохранения и результаты, которые уже удалось достичь в этом направлении. [2]