Краснодарский университет МВД России

МАТЕМАТИЧЕСКИЕ МЕТОДЫ И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА

Материалы
XIX Международной научно-практической конференции
(22 июня 2023 г.)

Краснодар
2023

УДК 004+50+51+53
ББК 22.1+32.81
М34

Одобрено
редакционно-издательским советом
Краснодарского университета
МВД России

Математические методы и информационно-технические средства М34 [Электронный ресурс] : материалы XIX Междунар. науч.-практ. конф. (22 июня 2023 г.) / редкол.: И. Н. Старостенко, Е. В. Михайленко, М. В. Шарпан и др. – Электрон. дан. – Краснодар : Краснодарский университет МВД России, 2023. – 1 электрон. опт. диск.

ISBN 978-5-9266-1914-7

В сборнике содержатся материалы XIX Международной научно-практической конференции «Математические методы и информационно-технические средства», состоявшейся в Краснодарском университете МВД России 22 июня 2023 г., посвященной математическим методам и моделированию, программному обеспечению и информационно-техническим средствам, информационным технологиям в борьбе с экстремизмом, терроризмом и организованной преступностью, информационным технологиям в образовании, проблемам информатизации и информационной безопасности.

Для профессорско-преподавательского состава, адъюнктов, курсантов, слушателей образовательных организаций МВД России и сотрудников органов внутренних дел Российской Федерации.

УДК 004+50+51+53
ББК 22.1+32.81

ISBN 978-5-9266-1914-7

СОДЕРЖАНИЕ

Акапьев Виктор Львович,
Савотченко Сергей Евгеньевич,
Ковалева Екатерина Геннадьевна

ТЕОРЕТИЧЕСКИЕ АСПЕКТЫ РЕГУЛЯРНОЙ АКТУАЛИЗАЦИИ ПОНЯТИЯ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Современный уровень развития информационных технологий и цифровизация российского пространства привели как к развитию новых форм преступности, так и к совершенствованию существовавших ранее. В настоящее время преступники нацелены на поиск наиболее благоприятных условий и среды совершения преступлений, в качестве которой все чаще выбирается Интернет. В результате сами информационно-телекоммуникационные технологии стали площадкой для преступности.

Развитое использование компьютеров и иных электронных систем в последние годы стало повсеместным, и это несет в себе как благоприятные, так и не благоприятные последствия в аспекте того, кто пользуется данными технологиями. Использование телекоммуникации субъектами криминального мира, их умысел и знание устройства кодовых систем создает благоприятные условия для совершения преступления. Знания таких субъектов больше, чем граждан, не имеющих таких познаний, что приводит к необходимости регулярной актуализации квалификации составов преступлений, заключенных в содержании статей Уголовного Кодекса РФ.

Преступления, которые совершаются путем использования информационных и телекоммуникационных технологий, являются высоколатентными, так как создание одноразовых кодов, использование незарегистрированных сотовых номеров и подобное, не дает возможности качественно и оперативно отрабатывать в сроки, установленные планом следственных действий по уголовному делу, в результате чего раскрытие преступлений в данной сфере становится затруднительным.

С каждым годом преступность с использованием информационно-телекоммуникационных технологий приобретает все более «изощренные» формы [1]. Происходит совершенствование способов совершения преступлений, появляются новые способы распространения вредоносных программ, способных нанести существенный ущерб нормальному функционированию и использованию информационно-телекоммуникационных технологий (ИТ). Большинство противоправных деяний уже являются преступными и наказуемыми с точки зрения Уголовного кодекса Российской Федерации.

Преступления, совершаемые с использованием ИТ, в условиях современной цифровой действительности стали занимать значительную долю среди всех совершенных преступлений. Актуальное значение приобретает проблема борьбы с этой группой преступлений. Стоит отметить, что ее нельзя объединить по объекту уголовно-правовой охраны, поскольку использование информационно-телекоммуникационных технологий при совершении преступления отражает лишь способ совершения преступления.

В научной литературе активно обсуждается вопрос о правовом закреплении понятия ИТ-преступления, или общественно опасного деяния с использованием сети Интернет, иных телекоммуникационных технологий, так как происходит стремительное мировое развитие всех существующих процессов жизнедеятельности общества. Законодательство не успевает подстраиваться под них, так как принятие норм занимает много времени, потому представляется необходимым обратиться к доктринальному толкованию данного понятия на сугубо теоретическом уровне. Поэтому важно регулярно актуализировать содержание понятия ИТ-преступления, его содержание и разновидности.

Прежде всего, предлагается обратить внимание, что преступления, совершенные с использованием информационно-телекоммуникационных технологий в юридической литературе именуются по-разному. Например, можно встретить такие названия как «компьютерные преступления», «информационные преступления», «киберпреступления», «интернет-

преступления» и др. Трактовки всех этих терминов обладают как общими чертами, так и различиями, в большинстве своем, незначительными. Разберем их на нескольких примерах далее более подробно.

Т.Г. Смирнова писала: «Под преступлениями в сфере компьютерной информации понимаются запрещенные уголовным законом общественно опасные виновные деяния, которые причиняют либо создают угрозу причинения вреда жизни, здоровью личности, правам и свободам человека и гражданина, государственной и общественной безопасности» [2]. Однако в условиях современности данное определение является совершенно несостоятельным. Это объясняется тем, что в настоящее время использование информационно-телекоммуникационных технологий является способом совершения преступлений, различных по своим уголовно-правовым характеристикам. К тому же, в настоящее время список средств, используемых для совершения преступлений в качестве информационно-телекоммуникационных технологий, не ограничивается одним компьютером или мобильным устройством.

Автор А.С. Унукович [3] выказывает наиболее современный взгляд на понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий. Автор обращает внимание, что использование информационно-телекоммуникационных технологий происходит в новой среде – в виртуальном пространстве. Основу виртуального пространства, за счет чего и происходит моделирование виртуальной среды, составляют информационно-телекоммуникационные технологии. В виртуальной среде смоделированы те элементы, которые имеют место в реальной действительности – это данные о лицах, предметах, фактах, определенных обстоятельствах [4]. Описывая технологическую сторону процесса воспроизведения сведений, данных из действительности в виртуальной среде, автор указывает, что они приобретают форму электрических сигналов, находящихся в непрерывном движении в информационно-телекоммуникационных сетях. Виртуальные

данные хранятся в устройствах памяти на физических носителях или в виртуальной форме.

Т.П. Кесареева [5] также предлагает отделить информационные преступления и компьютерные преступления. По мнению автора, компьютерные преступления являются лишь частью преступлений, совершенных с использованием ИТ. Автор также утверждает, что преступления, совершаемые в сети Интернет, являются составной частью компьютерной преступности, форма которой так актуальна для современного времени. Т.П. Кесареева ограничивается тем, что под преступлениями в информационной телекоммуникационной сети Интернет следует понимать запрещенные уголовным законом деяния, связанные с использованием сети Интернет и компьютерной техники.

По нашему мнению, преступления, совершаемые в сфере использования информационных и телекоммуникационных технологий, причиняют вред интересам и правам граждан, организаций и государству, охраняемым уголовным законодательством.

Некоторые авторы справедливо отмечают, что стремительное развитие преступности в информационно-коммуникационной среде и с использованием кибернетических технологий при совершении преступлений требует совершенствования национальной системы права. Например, по мнению Е.Д. Василькова [6], необходима разработка профильного нормативного правового акта, закрепляющего основополагающие понятия. Автор отмечает, что современный комплекс борьбы с преступностью с использованием информационно-телекоммуникационных технологий требует совершенствования не только частной криминалистической методики расследования соответствующей группы преступлений, но и разработки соответствующего правового фундамента, закрепляющего основополагающие понятия. Это утверждение справедливо относится к разработке на

законодательном уровне таких ключевых понятий как «компьютерная преступность», «киберпреступность» и др.

Следует отметить, что некоторые специалисты, казалось бы, традиционные квалификационные признаки преступлений, но при условии использования ИКТ, выделяют их в отдельные группы. В частности, по мнению М. Сазоновой [7], которая выделила 5 групп преступлений, совершаемых с помощью ИКТ, «ненадлежащее оказание медицинской помощи с применением телемедицинских технологий в зависимости от наступивших последствий вполне может быть квалифицировано как причинение смерти или тяжкого вреда здоровью по неосторожности».

В заключение следует отметить, что необходимо регулярно обновлять главу 28. УК РФ «Преступления в сфере информационных технологий», дополняя ее новыми составами в связи с постоянным появлением новых форм и преступлений в сфере компьютерной информации и способов их совершения, а также их бурным ростом.

Литература

1. Тимофеев С.В. Информационное обеспечение противодействия преступлениям, совершаемым с использованием информационно-коммуникационных технологий / С.В. Тимофеев. – Текст: электронный // Известия Тульского государственного университета. Экономические и юридические науки. – 2021. – С. 132-137.

2. Смирнова, Т. Г. Уголовно-правовая борьба с преступлениями в сфере компьютерной информации: Автореф. дис. канд. юрид. наук. – М., 1998. – 27 с.

3. Унукович, А.С. Понятие преступлений, совершаемых с использованием информационно-телекоммуникационных технологий // Государственная служба и кадры. – 2021. – № 4. – С. 278-280.

4. Архипов А. Цифровые объекты как предмет хищения // Уголовное право. – 2020. – N 6. – С. 16-23.

5. Кесареева, Т.П. Криминологическая характеристика и проблемы предупреждения преступности в российском сегменте сети Интернет: Автореф. дис. ... канд. юрид. наук. – М., 2002. – 25 с.

6. Васильков, Е.Д. Уголовно-правовая характеристика преступлений, совершенных с использованием информационных технологий // StudNet. – 2021. – № 6. – С. 1809-1823.

7. Сазонова М., Уголовно-правовые риски в условиях цифровизации: способы противодействия. Гарант.ру // URL: https://www.

Сведения об авторах

Савотченко Сергей Евгеньевич, доктор физико-математических наук, профессор кафедры информационно-компьютерных технологий в деятельности ОВД, доцент Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: savotchenkose@yandex.ru.

Акапьев Виктор Львович, кандидат педагогических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: akapevvl@yandex.ru.

Ковалева Екатерина Геннадьевна, кандидат технических наук, доцент кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: kovalevazchs@yandex.ru.

Алимжанова Жанна Муратбековна,
Ендыбайулы Ерлан

АНАЛИЗ СОВРЕМЕННЫХ АЛГОРИТМОВ ИДЕНТИФИКАЦИИ ПРЕСТУПЛЕНИЙ В СРЕДЕ ИНТЕРНЕТ

В настоящее время большой проблемой является развитие преступлений, совершаемых посредством информационных и телекоммуникационных технологий. Это явление сопряжено с распространением информационных технологий в повседневной жизнедеятельности, а также все большем охвате населения, в необходимом использовании интернет ресурсов при различных видах регистрации, а также при получении различных социальных услуг. Наиболее широкий скачок в количестве пользователей произошел в период пандемии, когда большинство населения работали и учились на удаленном режиме с применением информационных технологий и систем.

Те действия, попадающие под категорию киберпреступлений, как и в обычной социальной среде, могут быть различными по масштабу, урону для общества и тяжести последствий. В связи с этим исследования в направлении идентификаций различных видов преступлений могут позволить в той или иной мере проводить расследования, принимать решения по составлению доказательной базы и также максимально эффективно принимать профилактические меры по выявлению вредоносного контента в среде информационных технологий.

Для формирования общей классификации преступлений в информационной среде предлагается произвести ранжирование по различным уровням угроз и последствий – что позволит классифицировать и определять меры реагирования и иные мероприятия, исходя из особенностей преступления – что позволяет выстраивать оптимальную стратегию по розыску и формированию доказательной базы, а также по другим особенностям и специфике преступлений, позволяющее накопить успешный опыт проведения расследований и формирования доказательной базы.

Как известно, все алгоритмы взаимодействий между людьми или группами лиц, присутствующие в социальной среде общества, и сопутствующие им схемы правонарушений в настоящее время переносятся частично или полностью в среду информационных технологий. Для реализации своих целей существует множество алгоритмов и схем, имеющих в основе реализацию преступной деятельности. Также существуют особенности, связанные с процедурами передачи, хранения и обмена информацией, позволяющие классифицировать принципы работы в сети. Также особенностью является глобальность дислокации, что, во-первых, конкретизирует процесс реализации розыска, а во-вторых, ставит задачи по интеграции в международные организации по розыску, создание нормативно-правовой документации по сотрудничеству в правоохранительной деятельности. Сопутствующие сетевому обмену данными принципы также определяют возможности профилактически определять и влиять на динамику правонарушений, или методом других оперативных алгоритмов (при недостижимости оперативной реализации по цифровому следу) реализовывать розыскные мероприятия.

В традиционном понимании кибербезопасности принимают три основные категории киберпреступлений:

- индивидуальные;
- имущественные;
- государственные.

Также, очевидно, в связи со спецификой передачи информации, в интернет среде можно выделить дополнительный класс – комбинированные (т.е. категории, которые посредством традиционных методов одного вида могут осуществлять или перерастать в другой вид из вышеназванных).

Также классически рассматривают преступления на два типа: непосредственно на уничтожение оборудования (технологии) и преступления, применяемые для совершения преступной деятельности.

Согласно Будапештской конвенции 2014 года, как основополагающего документа в сфере борьбы с киберпреступностью, классификация представлена:

1. Правонарушения против конфиденциальности, целостности и доступности компьютерных данных и систем: незаконный доступ (взлом, обман и др.).

2. Правонарушения, связанные с компьютерами (подделка, мошенничество).

3. Правонарушения, связанные с содержанием информации (детская порнография, расизм, ксенофобия и др.).

4. Правонарушения, связанные с нарушением авторских и смежных прав.

Там же категорируется мотивация совершения преступлений:

- кибермошенничество с целью завладения средствами;

- кибермошенничество с целью завладения информацией;

- вмешательство в работу информационных систем с целью получения доступа (повреждение, ущерб конкурентам);

- иные [1, 2].

Также можно выделить в категорию незаконную реализацию (баз данных и др.), а также отмывание преступных доходов.

Далее, при ранжировании производится типизация киберпреступлений:

- мошенничество с использованием электронной почты и интернета;

- кража цифровой личности (хищение и использование личных данных);

- кража данных платежных карт и другой финансовой информации;

- хищение и перепродажа корпоративных данных;

- кибершантаж (вымогательство денег под угрозой атаки);

- атаки с использованием программ-вымогателей (одна из разновидностей кибершантажа);

- криптоджекинг (майнинг криптовалют с использованием чужих ресурсов);

- кибершпионаж (получение несанкционированного доступа к государственным или корпоративным данным);

- нарушение работы систем с целью компрометации сети;

- нарушение авторских прав;

- незаконное проведение азартных игр;

- онлайн-торговля запрещенными товарами;

- домогательства, изготовление или хранение детской порнографии.

Киберпреступление всегда подразумевает хотя бы одно из указанного:

- преступную деятельность с целью атаки на компьютеры с использованием вирусов или другого вредоносного ПО;

- использование компьютеров для совершения других преступлений [3].

В связи с растущим образованием населения в среде потребления и эксплуатации информационных и телекоммуникационных ресурсов неизбежно развиваются методики и схемы различных видов преступлений, позволяющих при наименьшем непосредственном контакте достигать своих целей (преимущественно в целях наживы и материального обогащения).

В этой категории наиболее распространенными являются следующие виды преступлений:

1) Мошенничество в сети Интернет, в частности:

- создание «финансовых пирамид» в сети Интернет;

- мошенничество при продаже товаров (услуг) через Интернет или на Интернет-аукционах;

- деятельность по созданию программных средств с целью хищения финансовой, коммерческой или персональной информации (создание фиктивных WEB-сайтов, распространение компьютерных вирусов и троянских программ, перехват трафика и т.п.).

2) Мошенничество в системах дистанционного банковского обслуживания (далее – ДБО), в частности:

- создание компьютерных вирусов и троянских программ для скрытого перехвата управления компьютером клиента с установленным программным обеспечением ДБО;

- открытие счетов, проведение несанкционированных операций и получение наличных средств в результате несанкционированных операций в системах ДБО;

- получение платежей от иностранных отправителей через международную систему SWIFT вследствие вмешательства в работу компьютеров и систем ДБО клиентов иностранных банковских учреждений.

3) Подделка платежных карт и банкоматное мошенничество, в частности:

- использование утраченных/похищенных/поддельных платежных карт;

- похищение реквизитов платежных карт, в том числе с применением технических средств их «клонирования»;

- скимминг – изготовление, сбыт и установка на банкоматы устройств считывания/копирования информации с магнитной полосы платежной карты и получение ПИН-кода к ней;

- использования «белого пластика» для «клонирования» (подделки) платежной карты и снятия наличных в банкоматах;

- Transaction Reversal Fraud – вмешательство в работу банкомата при осуществлении операций выдачи наличных, которое оставляет неизменным баланс карточного счета при фактическом получении наличных злоумышленником;

- Cash Trapping – заклеивание диспенсера для присвоения злоумышленником наличности, которая была списана с карточного счета законного держателя карты [1, 4].

Рассмотрим наиболее распространенные виды мошеннических схем, используемых посредством информационных и телекоммуникационных технологий, которые все-таки являются пассивными и зачастую не имеют явного состава преступления. Преимущественно устанавливается контакт с жертвой в

интернет - среде, социальных сетях и далее выходят на непосредственный контакт, с целью войти в доверие и получить определенную сумму денег:

- благотворительность;
- выигрыш;
- финансовая пирамида как заработок;
- блокировка аккаунта с целью получения данных электронного кошелька;
- хищение личных данных с целью взять кредит;
- вакансии;
- сайты знакомств;
- обучение и вебинары;
- фейковые организации или нелицензированные;
- интернет-торговля [5].

Особенности данных видов мошенничества – преимущественно в рассылке приглашений к контакту, которые ориентированы на самостоятельную реакцию и добровольный контакт со стороны жертвы.

Также существуют виды схем, принуждающих жертву к передаче денежных средств, персональных данных или данных банковских карт:

- вишинг: с использованием мессенджеров, телефона и др., а также социальной инженерии, например, банковского служащего или родственника в тяжелой ситуации, вымогают деньги или данные банковской карты, реже предлагают установить вирусную программу по краже данных;

- фишинг: преимущественно создают фальшивый сайт, например, Госуслуг, с целью получения данных интернет-банкинга;

- смишинг (СМС+фишинг): контакт через рассылку СМС, о выигрыше или о платной подписке с предложением отписаться на предлагаемом сайте.

Исходя из вышесказанного, стоит отметить, что те мошеннические схемы, которые происходят с применением живого контакта – социальной инженерии с жертвой (с учетом психологии и менталитета), как правило, имеют локальный характер. Это обуславливается знаниями особенностей пользования

традиционными ресурсами, языковым барьером, знаниями определенных данных о жертве.

Таблица 1. Классификация интернет мошеннических схем

№	Виды	Возможность быстрой реакции	Утрата персональных данных	Вероятность обращения или жалобы
1	Благотворительность	-	-	низкая
2	Выигрыш	-	+	средняя
3	Финансовая пирамида как заработок	-	-	высокая
4	Блокировка аккаунта с целью получения данных электронного кошелька	+	+	средняя
5	Хищение личных данных, с целью взять кредит	+	+	средняя
6	Вакансии	-	-	низкая
7	Сайты знакомств	-	-	низкая
8	Обучение и вебинары	-	-	низкая
9	Фейковые организации или нелицензированные	+	-	низкая
10	Интернет торговля	-	-	низкая
11	Вишинг	+	-	средняя
12	Фишинг	-	+	высокая
13	Смишинг	-	+	низкая

В заключение, хочется отметить, что при достижении сформированной системы ранжирования преступлений кибер-специфики возникнет возможность:

- разработки типовых алгоритмов по реагированию на возможные или уже совершенные преступления в кибер-среде;

- применения систем искусственного интеллекта, что позволит автоматизировать и ускорить методики принятия решений по обеспечению профилактики или реагирования на те или иные формы преступной деятельности.

Литература

1. Интернет-ресурс:https://www.kaspersky.ru/resource-center/threats/what-is-cybercrime; запрос 05.06.2023.

2. Интернет-ресурс: https://www.cloudav.ru/mediacenter/security/types-of-cybercrime/ запрос 05.06.2023.

3. Проект типологического исследования на тему «Киберпреступность и отмывание денег» Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма. Подразделение по борьбе с экономическими преступлениями, Совет Европы, Страсбург 2014г. 50 с.

4. Типологическое исследование «Криминальные денежные потоки в сети Интернет: методы, тенденции и взаимодействие между всеми основными участниками» Евразийская группа по противодействию легализации преступных доходов и финансированию терроризма. Подразделение по борьбе с экономическими преступлениями, Совет Европы, Страсбург, МАНИВЭЛ 2012 г. 147 с.

5. Интернет-ресурс:https://blog.avast.com/ru/7-samyh-rasprostranennyh-vidov-moshennichestva-v-sotssetyah запрос 05.06.2023.

6. Интернет-ресурс:https://www.sravni.ru/enciklopediya/info/vidy-moshennichestva/ запрос 05.06.2023.

Сведения об авторах

Алимжанова Жанна Муратбековна, кандидат физико-математических наук, профессор кафедры кибербезопасности и информационных технологий Алматинской академии МВД имени М. Есболатова; e-mail: zhannamen@mail.ru.

Ендыбайулы Ерлан, магистр технических наук, доцент кафедры кибербезопасности и информационных технологий Алматинской академии МВД имени М. Есболатова; e-mail: erlan.endybayuly@mail.ru.

Аршинов Георгий Александрович

ОЦЕНКА ДОПУСТИМЫХ РАЗМЕРОВ ПОДЗЕМНЫХ ПОЛОСТЕЙ-ХРАНИЛИЩ, СООРУЖАЕМЫХ В ТОЛЩАХ СОЛЯНЫХ ОТЛОЖЕНИЙ

Рассмотрим неоднородное по прочности тело объема V и пусть пределы прочности элементов тела задаются функцией распределения

$$F_v(\sigma_n) = 1 - [1 - F(\sigma_n)]^{nV}.$$

Здесь nV – число микронарушений структуры тела, в которых превышен предел прочности.

Предположим, что число nV>>1, т. е. велико, тогда имеем соотношения:

а) $F_v(\sigma\} = 0$ когда $\sigma \leq \sigma_n^0$, $F(\sigma)>0$, для $\sigma > \sigma_n^0$;

б) $\lim\limits_{\varepsilon \to 0} \dfrac{F_v(\sigma + \varepsilon)}{\varepsilon^{\alpha}} = c$,

в которых постоянные c >0 и α>0 , а ε > 0 – малая величина.

Если nV >>1, σ_n^0 – минимальная прочность дефектного элемента, то, переходя к пределу, получим

$$F_v(\sigma) = P = 1 - \exp[-cnV(\sigma - \sigma_n^0)^{\alpha}].$$

Применяя замену $cn = 1/V_0\sigma_c^{\alpha}$, приходим к равенству

$$P = 1 - \exp\left[\frac{V}{V_0}\left(\frac{\sigma - \sigma_n^0}{\sigma_c}\right)^{\alpha}\right].$$

Разобьем объем V на микрообъемы ΔV_k так, что в каждой точке любого микрообъема действует одинаковое напряжение, тогда вероятность прочности всего объема

$$P = 1 - \exp\left[-\frac{1}{V_0}\sum_K \Delta V_k\left(\frac{\bar{\sigma} - \sigma_n^0}{\sigma_c}\right)^{\alpha}\right].$$

Здесь суммирование выполняется по тем ΔV_k, где $\sigma \geq \sigma_n^0$, т.е. по области возможного разрушения.

Оценим допустимые размеры путем сравнения вероятностей разрушения проектируемой и эксплуатируемой полостей, применяя формулу

$$P = 1 - \exp\left[-\frac{1}{V_0} \int_{Vp} \left(\frac{\bar{\sigma} - \sigma_n^0}{\sigma_c} \right)^{\alpha} dV \right], \quad (1)$$

в которой интеграл вычисляется по области возможной потери прочности.

Приведенное напряжение для соляных пород определим по критерию Мора

$$\bar{G} = \frac{1}{1 - \sin\delta} [G_1 - G_3 - (G_1 + G_3)\sin\delta], \quad (2)$$

где δ – угол внутреннего трение соли, а главные напряжения – σ_1, σ_2 ($\sigma_1 > \sigma_3$).

Предполагается, что рассчитываемая полость будет устойчивой, если вероятность ее разрушения не превысит вероятности потери прочности полости, находящейся в эксплуатации, т. е.

$$P \le P_э. \quad (3)$$

Величина интегрального слагаемого в (1) определяется видом хранилища и пропорциональна квадрату или кубу его характерного размера.

Используя (1), (3), приходим к формуле, позволяющей найти отношение характерного размера L проектируемого хранилища к размеру $L_э$ емкости, находящейся в эксплуатации:

$$\frac{L}{L_э} = \left[\frac{\int_{Vp} \left(\frac{\bar{\sigma} - \sigma_n^0}{\sigma_c} \right)_э^{\alpha} dv}{\int_{Vp} \left(\frac{\bar{\sigma} - \sigma_n^0}{\sigma_c} \right)^{\alpha} dv} \right]^{1/n} \ (n = 2,3), \quad (4)$$

Экспериментальное исследование на прочность соляных пород показало, что для оценки их прочности применимы линейный критерий Мора (2) и нелинейный вида

$$\sigma_n = \frac{\sigma_1 + \sigma_3 \sigma_1'}{\sigma_1' + 1};$$

$$\tau_{nt} = \frac{(\sigma_1 - \sigma_3)(\sigma_1^{'})^{0,5}}{\sigma_1^{'} + 1};$$

$$\sigma_1^{'} = \frac{b\sigma_c^a}{a\sigma_p \sigma_1^{a-1}},$$

в котором $\sigma_1, \sigma_2, \sigma_3$ – главные напряжения; σ_c, σ_p – величины напряжения, при которых наблюдалось разрушение образцов, сжимаемых и растягиваемых в одноосных опытах; постоянные a =2, b =1 для пород каменной соли, а также соотношение

$$\bar{\sigma} = \chi[\sigma_И - \sigma_1] + \sigma_1, \qquad (5)$$

в котором σ_u – интенсивность напряжений, σ_1 – максимальное главное напряжение, χ – постоянная.

При использовании в расчетах метода конечных элементов интегрирование в (4) заменяется суммированием по конечным кольцевым элементам

$$\frac{L}{Lэ} = [\frac{\sum\limits_K \Delta V_k (\bar{\sigma} - \sigma_n^0)_э^{\alpha}}{\sum\limits_K V_k (\bar{\sigma} - \sigma_n^0)^{\alpha}}]^{\frac{1}{3}}.$$

Сетка конечных элементов аппроксимирует соляной массив с емкостью.

Перемещения $u(\rho, z)$ в точках конечных элементов определяются зависимостью

$$\bar{\upsilon}(\rho, z) = \sum_{e=1}^{E} q_N^{(e)} (a_N + b_N \rho + c_N z),$$

где количество треугольных элементов в аппроксимации равно E, и матрица перемещений вершин е-го треугольника

$$\mathrm{q}_{\mathrm{N}}^{(\mathrm{e})} = \begin{bmatrix} \mathrm{u}_{\mathrm{N}} \\ \mathrm{v}_{\mathrm{N}} \end{bmatrix} \ (\mathrm{N} = 1,2,3) \cdot$$

Константы a_N, b_N, c_N, подлежащие определению, находятся по координатам вершин конечных элементов.

Матрица деформаций элемента строится по соотношениям Коши

$$\varepsilon_{(e)} = \begin{bmatrix} \varepsilon_\rho \\ \varepsilon_z \\ \varepsilon_\theta \end{bmatrix} = B_{(e)} q_{(e)}, \tag{6}$$

$$B_{(e)} = [B_1 B_2 B_3]; \quad B_i = \begin{bmatrix} b_i & 0 \\ 0 & c_i \\ \dfrac{a_i}{\rho} + b_i + \dfrac{c_i z}{\rho} & 0 \\ c_i & b_i \end{bmatrix}, \; i=1,2,3, \text{ а } q_{(e)} = \begin{bmatrix} q_1^{(e)} \\ q_2^{(e)} \\ q_3^{(e)} \end{bmatrix}.$$

Напряжения в е-ом конечном элементе являются компонентами матрицы

$$\sigma_{(e)} = DE(e). \tag{7}$$

Для решения смешанной краевой задачи минимизируется функционал

$$J(u) = 2\pi\left(\int_V \frac{1}{2}\varepsilon^{|}\sigma\rho d\rho dz - \int_s u^{|} p ds\right). \tag{8}$$

Используя (6) и (7), получаем приближение

$$J(\bar{\upsilon}) = \sum_{e=1}^{E} \frac{1}{2} q_{(e)}^{|} k_{(e)} q_{(e)} - 2\pi \sum_{e=1}^{E} q_{(e)}^{|} \int_{s_{(e)}} A_{(e)}^{|} \rho ds, \tag{9}$$

$$k_{(e)} = 2\pi \int_{v_{(e)}} B_{(e)}^{|} D B_{(e)} \rho d\rho dz,$$

$$A_{(e)} = [A_1 A_2 A_3]; \quad A_i = \begin{bmatrix} a_i + b_i\rho + c_i z & 0 \\ 0 & a_i + b_i\rho + c_i z \end{bmatrix}.$$

Далее используются матрицы $C_{(e)}$ с размерами $6 \times 2G$, элементы которых принимают значения 0 или 1. Компоненты матриц $C_{(e)2m\text{-}1,2i\text{-}1}$, $C_{(e)2m\text{-}1,2i}$, $C_{(e)2m,2i\text{-}1}$, $C_{(e)2m,2i}$ равны единице для любой m-ой вершины е-го конечного элемента, которая совпадает с i-ой вершиной в общей нумерации вершин конечно-элементной аппроксимации.

После прохождения всех конечных элементов аппроксимации и приравнивания к 1 соответствующих элементов матрицы $C_{(e)}$, оставшиеся ее элементы полагаются равными 0.

Если $\upsilon = [u_1, v_1 ... u_G, v_G]'$ – матрица перемещений узлов в соответствие

глобальной нумерацией вершин аппроксимации, то

$$q_{(e)}=C_{(e)}\upsilon. \qquad (10)$$

После применения (9), (10) получаем

$$J(\upsilon)=\frac{1}{2}\upsilon^{|}(\sum_{e=1}^{E}C_{(e)}^{|}K_{(e)}C_{(e)}\upsilon-2\pi\sum_{e=1}^{E_1}C_{(e)}^{|}\int_{s_{(e)}}A_{(e)}^{|}\rho ds)$$

или

$$J(\upsilon)=\frac{1}{2}\upsilon^{|}K\upsilon-\upsilon^{|}F\ .$$

Минимум J определяется условиями

$$\frac{\partial J}{\partial \upsilon_i}=0\ ;\ \ \upsilon_i=\begin{bmatrix}u_i\\ v_i\end{bmatrix};\ \ i=1,2,\ldots,\sigma,$$

приводящими к системе линейных алгебраических уравнений

$$K\upsilon=F\ .$$

Решение этой системы позволяет найти неизвестные компоненты перемещений матрицы υ, позволяющие вычислить деформации и напряжения в точках соляного массива в окрестности полости.

Список литературы

1. Аршинов Г.А. Исследование размеров, обеспечивающих устойчивость подземных полостей в вязкоупругих горных породах / Г.А. Аршинов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2004. – №02(004). С. 27 – 37. – IDA [article ID]: 0040402003. – Режим доступа: http://ej.kubagro.ru/2004/02/pdf/03.pdf, 0,688 у.п.л.

Сведения об авторе

Аршинов Георгий Александрович, доктор технических наук, доцент, профессор кафедры комьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина; e-mail: arshinov_kts@mail.ru.

Бакулин Василий Михайлович

ИСПОЛЬЗОВАНИЕ КОМПЬЮТЕРНЫХ ОБУЧАЮЩИХ ПРОГРАММ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Компьютерные обучающие программы стали неотъемлемой частью современного образования и широко используются в школах и университетах. Они представляют собой специальное программное обеспечение, которое предназначено для получения знаний и навыков обучающимися в различных предметных областях. Обучающие программы могут быть использованы как независимое средство обучения или в качестве дополнения к традиционным методам обучения.

Основная цель компьютерных обучающих программ – это повышение эффективности обучения путем нахождения оптимальной траектории усвоения учебного материала. С помощью таких программ учебный процесс становится более наглядным и простым для восприятия, а также обеспечивается возможность создания обратной связи с обучающимся и организация коллективного обучения.

Одним из основных преимуществ компьютерных обучающих программ является их способность к моделированию различных ситуаций, процессов и явлений, что позволяет обучаемым взаимодействовать с информацией более динамично и эффективно.

Области применения компьютерных обучающих программ могут включать [1]:

Онлайн-курсы и дистанционное обучение. Создание и использование виртуальных классов и онлайн платформ облегчает процесс удаленного обучения, позволяет интегрировать электронные материалы и учебные задания и симуляции в интернет-среду.

Интерактивные учебники и материалы. Данная область применения включает в себя интерактивные мультимедийные учебные материалы с

использованием графики, анимации, видео, интерактивных правил, инструкций и таблиц, а также различные варианты проверки знаний в режиме реального времени.

Симуляторы и виртуальные лаборатории. Использование компьютерных симуляторов и графического моделирования облегчает получение практических навыков в случаях, когда проведение прямых натурных занятий является затруднительным или чрезмерно затратным.

Системы мониторинга и контроля. Компьютерные обучающие программы для проведения мониторинга и контроля эффективности в изучении учебных дисциплин позволяют проводить тестирование, оценивать уровень знаний обучающихся, просматривать и анализировать статистические данные результатов обучения.

Стоит также отметить основные преимущества применения компьютерных обучающих программ:

Увеличение доступности образования. Данные программы позволяют обучающимся брать на себя большую долю ответственности за свое обучение и не зависеть от времени и места проведения учебных занятий.

Увеличение гибкости учебного процесса. Некоторые компьютерные обучающие программы позволяют настраивать и адаптировать уроки, задания и материал по индивидуальным потребностям обучающихся, под темп обучения в соответствии с их индивидуальными уровнями знаний и навыков. Правда стоит отметить, что процесс разработки подобных программ достаточно сложен и трудоемок, поэтому далеко не все обучающие программы обладают указанными возможностями.

Ускорение процесса обучения. Компьютерные обучающие программы позволяют работать в удобном темпе, повторять материал до полного усвоения, выполнять практические задания и задачи по несколько раз до достижения нужного результата.

Увеличение мотивации студентов. Подобные программы часто содержат элементы игры, что увеличивает потенциальную заинтересованность обучающихся и их мотивацию в процессе обучения.

Улучшение качества обучения. Обучающие программы позволяют использовать инновационные методы обучения и быстро адаптировать контент к актуальным требованиям и новшествам в различных сферах.

Увеличение эффективности работы преподавателей. Компьютерные обучающие программы предоставляют преподавателям возможности составления тестов, проверок, проведения автоматического подсчета результатов по отдельным темам, разделам и дисциплинам.

Сокращение времени на подготовку обучающих материалов. Компьютерные обучающие программы предлагают обширный контент и библиотеки, которые часто содержат пошаговые инструкции, готовые примеры и материалы, что делает подготовку учебных материалов для обучения более быстрой и эффективной.

Таким образом, общее эффективное использование компьютерных обучающих программ может значительно улучшить качество образовательного процесса.

Хотя компьютерные обучающие программы могут иметь множество преимуществ и применений, но все же они не могут заменить весь учебный процесс и некоторые виды обучения в определенных сферах, например, практические занятия в лабораториях, которые требуют прямого взаимодействия обучающихся с оборудованием, материалами и веществами.

Для того, чтобы компьютерные обучающие программы были полезны, они должны обладать соответствующими функциональными возможностями, а также быть правильно разработаны с учетом педагогических целей и методик подачи учебного материала.

При создании компьютерных обучающих программ необходимо начинать с четкого определения педагогических целей обучения. Только после этого

можно приступать к разработке концепции, методики и способа взаимодействия обучаемого с компьютером. Но для этого необходимы глубокие педагогические знания в соответствующей предметной области.

С другой стороны, создание компьютерных обучающих программ также требует определенных технических знаний и умений в области программирования и разработки программного обеспечения. Педагогические работники часто не обладают достаточной квалификацией в этой области, что может затруднять процесс создания программы и обеспечения ее необходимой функциональностью.

Создание компьютерных обучающих программ является сложным и многопрофильным процессом, который учитывает как педагогические, так и технические аспекты. Нехватка квалифицированных специалистов, которые бы могли одинаково свободно ориентироваться в обеих областях, может привести к серьезным трудностям в создании качественных и востребованных обучающих компьютерных программ.

И здесь возникает вопрос о роли преподавателя в создании компьютерных обучающих программ [2]. Качественные компьютерные обучающие программы должны быть разработаны с учетом не только технических аспектов, но и педагогических потребностей и методик. Педагогические работники обладают необходимым комплексом знаний в области педагогики и понимают, какими методиками и приемами эффективнее проводить обучение. Разработчики программного обеспечения, в свою очередь, имеют навыки и знания, необходимые для создания высококачественного программного продукта.

Тесное взаимодействие педагогических работников и профессиональных разработчиков программного обеспечения позволяет объединить эти знания и опыт и создать компьютерные обучающие программы, наилучшим образом соответствующие требованиям и потребностям обучающихся.

Сотрудничество в области разработки обучающих программ позволяет создавать программы с оптимальным сочетанием педагогических и

технологических решений. Такие решения позволяют создать индивидуальную траекторию обучения, улучшить его интерактивность, а также повысить мотивацию обучающихся.

Таким образом, можно сказать, что только тесное взаимодействие педагогических работников и профессиональных разработчиков программного обеспечения способствует созданию уникальных и эффективных обучающих решений, которые могут существенно повысить качество образовательного процесса.

Литература

1. Бакулин В.М. К вопросу об использовании обучающих компьютерных программ в образовательном процессе / В.М. Бакулин, Д.Л. Еськин // Опыт и традиции подготовки полицейских кадров: Сборник научных трудов международной научно-практической конференции, Волгоград, 02–03 октября 2020 года. Том Выпуск 4. – Волгоград: Волгоградская академия Министерства внутренних дел Российской Федерации, 2021. – С. 30-35.

2. Еськин Д.Л. Преподаватель как субъект разработки обучающих компьютерных программ / Д.Л. Еськин, В.М. Бакулин // Учебно-воспитательный процесс в образовательном учреждении МВД России: традиции и инновации. – Волгоград: Волгоградская академия МВД РФ, 2017. – С. 41-45.

Сведения об авторе

Бакулин Василий Михайлович, кандидат физико-математических наук, доцент кафедры информатики и математики Волгоградской академии МВД России; e-mail: bvm@volgodom.ru.

Барсукова Виктория Юрьевна,
Василенко Вера Викторовна,
Кутюков Алексей Александрович

ОБ ОПТИМИЗАЦИИ ПРОЦЕДУР ЦИФРОВОЙ ОБРАБОТКИ МОНОХРОМНЫХ ИЗОБРАЖЕНИЙ

Цифровые технологии являются неотъемлемой частью существования современного общества. При этом наращивание информационного трафика требует совершенствования имеющихся способов обработки информации. Вполне естественно, что технологии и методы разрабатываются не только от постановки задач, но и исходя из природы начальных данных, которые условно можно разделить на определенные классы – допустим на: символьную (текстовую) информацию, графическую, мультимедиа и т.п. Отдельного внимания заслуживает класс изображений – он существует и сам по себе, и может быть рассмотрен как элемент медийного контента.

Обработка изображений с помощью современных IT-технологий уже в силу своей специфики сформировала отдельные прикладные направления, в которых рассматриваются задачи сжатия, идентификации изображений, восстановления оригиналов по некачественным исходным данным и т.п. Подобные задачи имеют важное значение как в медицине, промышленности, так и в системах, обеспечивающих безопасность. И, хотя современные алгоритмы гарантируют заявленные показатели процедур цифровой обработки, выявление новых свойств оцифрованных данных имеет весомый потенциал оптимизации уже известных методов.

Например, рассмотрим метод ортогонализации Шмидта. В [3] были получены результаты, доказавшие его эффективность при решении задач обработки фотоизображений. Любое монохромное (в частности, чёрно-белое) изображение по сути – это прямоугольная матрица с целочисленными элементами, отвечающими за интенсивность белого цвета пикселя [6]. Однако картинка, представляющая собою исходный, достаточно объёмный массив

данных, часто влечет несопоставимые энергозатраты вычислительного процесса и по времени, и по оперативной памяти.

Идея улучшения показателей эффективности метода Шмидта является основой центральной гипотезы данной работы: применения параллельных блоковых ортогонализаций матрицы-изображения для повышения эффективности процедур цифровой обработки высококачественной графики. Проверка гипотезы проводится методами экспериментального исследования по подбору коэффициентов блочного разбиения исходной матрицы, а также созданием и реализацией программного кода с наперед заданной погрешностью и прогнозом быстродействия программы. Как наиболее гибкий инструмент программирования, для решения поставленной задачи был выбран язык Python [5] (версия 3.8).

Далее приведем кратко этапы проверки выдвинутой гипотезы и исследование полученных тестовых результатов. Рассмотрим основные математические методы:

1. Метод ортогонализации Шмидта. Будем рассматривать евклидово пространство V, с выбранным в нем базисом. Тогда если $b = (\overrightarrow{e_1}, \overrightarrow{e_2}, \dots, \overrightarrow{e_n})$ - базис пространства V, то для любых $\vec{x}, \vec{y} \in V$ будет выполняться следующее представление:

$$\vec{x} = x_1\overrightarrow{e_1} + \cdots + x_n\overrightarrow{e_n} = (\overrightarrow{e_1}, \dots, \overrightarrow{e_n}) \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}$$

$$\vec{y} = y_1\overrightarrow{e_1} + \cdots + y_n\overrightarrow{e_n} = (\overrightarrow{e_1}, \dots, \overrightarrow{e_n}) \begin{pmatrix} y_1 \\ \cdots \\ y_n \end{pmatrix}$$

$$(\vec{x}, \vec{y}) = \sum_{i,j=1}^{n} x_i y_j (\overrightarrow{e_i}, \overrightarrow{e_j}) = (x_1 \dots x_n) \begin{pmatrix} \overrightarrow{e_1}\overrightarrow{e_1} \dots \overrightarrow{e_1}\overrightarrow{e_n} \\ \cdots \\ \overrightarrow{e_n}\overrightarrow{e_1} \dots \overrightarrow{e_n}\overrightarrow{e_n} \end{pmatrix} \begin{pmatrix} y_1 \\ \cdots \\ y_n \end{pmatrix},$$

где $\begin{pmatrix} \overrightarrow{e_1}\overrightarrow{e_2} \dots \overrightarrow{e_1}\overrightarrow{e_n} \\ \cdots \\ \overrightarrow{e_n}\overrightarrow{e_1} \dots \overrightarrow{e_n}\overrightarrow{e_n} \end{pmatrix}$ – матрица Грамма, обозначаемая $\mathrm{G}(\overrightarrow{e_1}, \overrightarrow{e_2}, \dots, \overrightarrow{e_n})$. Тогда

$$(\vec{x}, \vec{y}) = [x]_b^T \, \mathrm{G}(\overrightarrow{e_1}, \overrightarrow{e_2}, \dots, \overrightarrow{e_n}) \, [y],$$

где b – нормированный базис.

Определим длину произвольного ненулевого вектора $\vec{x} \in V$:

$$|\vec{x}| = \sqrt{(\vec{x}, \vec{x})},$$

а базис из единичных векторов назовём нормированным.

Ортогональность пары векторов $\vec{x}, \vec{y} \in V$ обеспечивает свойство:

$$(\vec{x}, \vec{y}) = 0.$$

Введенные понятия позволяют задавать базис, состоящий из нормированных попарно ортогональных векторов, который называется ортонормированным. То есть, вектор $b = (\overrightarrow{e_1}, \overrightarrow{e_2}, \dots, \overrightarrow{e_n})$ является ортонормированным тогда, когда $G(\overrightarrow{e_1}, \overrightarrow{e_2}, \dots, \overrightarrow{e_n})$ есть единичная матрица.

Для такого случая справедливо равенство:

$(\vec{x}, \vec{y}) = [x]_b^T [y]$, где b – ортонормированный базис.

Любое подпространство $V' \subseteq V$ евклидова пространства V обладает ортонормированным базисом [1]. Алгоритм получения ортонормированного базиса определим следующим образом:

1.1 Строим ортогональный базис. Пусть $b = (\overrightarrow{f_1}, \overrightarrow{f_2}, \dots, \overrightarrow{f_n})$ – базис пространства $V' \subseteq V$. Положим $\overrightarrow{e_1} = \overrightarrow{f_1}$. Тогда если $\overrightarrow{e_1}, \dots, \overrightarrow{e_{k-1}}$ построены (уже попарно ортогональны), то строим

$$\overrightarrow{e_k} = \overrightarrow{f_k} + \lambda_1 \overrightarrow{e_1} + \cdots + \lambda_{k-1} \overrightarrow{e_{k-1}}$$

так, чтобы $(\overrightarrow{e_k}, \overrightarrow{e_i}) = 0$ для $i = 1, \dots, k-1$. То есть,

$$(\overrightarrow{e_k}, \overrightarrow{e_i}) = (\overrightarrow{f_k}, \overrightarrow{e_i}) + \lambda_1 (\overrightarrow{e_1}, \overrightarrow{e_i}) + \cdots + \lambda_{k-1} (\overrightarrow{e_{k-1}}, \overrightarrow{e_i}).$$

Отсюда следует, что

$$0 = (\overrightarrow{e_k}, \overrightarrow{e_i}) = (\overrightarrow{f_k}, \overrightarrow{e_i}) + \lambda_i (\overrightarrow{e_i}, \overrightarrow{e_i})$$

$$\text{и } \lambda_i = -\frac{(\overrightarrow{f_k}, \overrightarrow{e_i})}{(\overrightarrow{e_i}, \overrightarrow{e_i})}.$$

Получается

$$\overrightarrow{e_k} = \overrightarrow{f_k} - \sum_{i=1}^{k-1} \frac{(\overrightarrow{f_k}, \overrightarrow{e_i})}{(\overrightarrow{e_i}, \overrightarrow{e_i})} \overrightarrow{e_i}.$$

1.2 Ортонормированный базис построим с помощью нормировки векторов

$$b_0 = (\vec{e}_1^0, \dots, \vec{e}_n^0), \text{ где } \vec{e}_i^0 = \frac{1}{|\overrightarrow{e_i}|} \overrightarrow{e_i}.$$

2. Сингулярное разложение матрицы. Сингулярное разложение является удобным методом при работе с матрицами, используется при решении самых разных задач — от приближения методом наименьших квадратов и решения систем уравнений до сжатия изображений. Важно отметить, что сингулярное разложение (Singular Value Decomposition, SVD - преобразование) можно рассматривать как декомпозицию вещественной матрицы с целью ее приведения к каноническому виду. Для данной процедуры введем следующие определения:

Определение 1. Сингулярными числами вещественной $(m \times n)$ – матрицы A называются арифметические квадратные корни из собственных чисел $\lambda_1, \lambda_2, \dots, \lambda_k$ матриц $A^T A$ и AA^T, где $k = \min\{m, n\}$. Обозначаются сингулярные числа: $\sigma_1 \geq \sigma_2 \geq \cdots \geq \sigma_k \ (\geq 0)$.

Определение 2. Представление вещественной $(m \times n)$ – матрицы A в виде:

$$A = U\Sigma V,$$

где Σ – диагональная $(m \times n)$ – матрица с диагональю из невозрастающих сингулярных чисел $\sigma_1, \sigma_2, \dots, \sigma_k$, а U и V – ортогональные, соответственно, $(m \times m)$ – и $(n \times n)$ – матрицы, называется сингулярным разложением матрицы A или, иначе, SVD-разложением.

Исходя из справедливости следующих теоретических результатов – теоремы и утверждения:

Теорема. Если A – вещественная $(m \times n)$ – матрица, то существуют ортогональные матрицы

$$U = [u_1, \dots, u_m] \in R^{m \times m} \text{ и } V = [v_1, \dots, v_n] \in R^{n \times n},$$

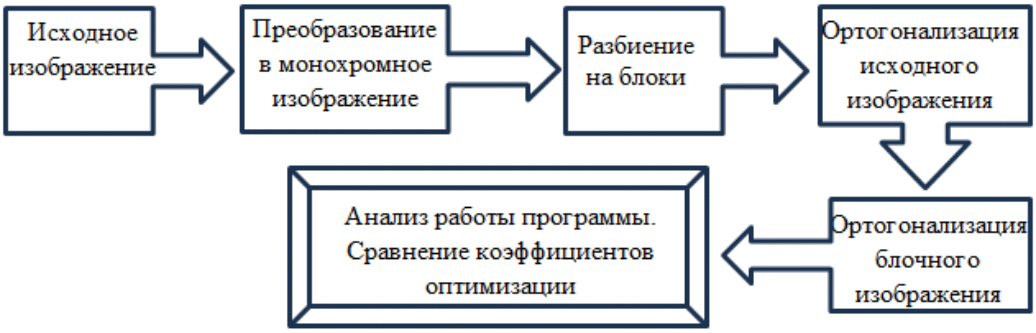
такие, что

$$U^T A V = \Sigma;$$

Утверждение. Всякая вещественная матрица имеет вещественное сингулярное разложение.

Проведены численные эксперименты.

Процесс реализации программного кода на основании приведенных математических методов может быть представлен следующей схемой:



В реализации на Pyton используются подключенные библиотеки:

– NumPy – обеспечивающая поддержку работы на многомерных массивах;

– CV2 – для перевода изображения в цифровую матрицу (bit-map);

– Multiprocessing – обеспечивает возможность распараллеливания вычислительных процессов на множество ядер процессора или на несколько машин в сети.

Результаты вычислительных экспериментов подтверждают выдвинутую гипотезу и предложенные методы – при приемлемом качестве повышается быстродействие алгоритма. Для сравнения в Таблице 1 приведены итоги выполнения программы на некоторых тестовых изображениях.

Таблица 1. Сравнение показателей применения метода Шмидта

Размер изображения	Количество блоков	Скорость ортогонализации исходного изображения	Скорость ортогонализации блочного изображения	Скорость ортогонализации блочного изображения при распараллеливании	Относительная погрешность сингулярных чисел
1920x1080		12.124 с	23.705 с	11.637 с	
		20.773 с	8.355 с		
		20.659 с	10.572 с		
2048x1152		16.107 с	26.845 с	16.106 с	
		25.528 с	10.239 с		
		26.213 с	13.152 с		
3840x2160		5 с	222.558 с	169.187 с	
		132.849 с	53.414 с		
		134.221 с	67.11с		

Результаты вычислительных экспериментов подтверждают основную гипотезу – при приемлемом качестве повышается быстродействие программы.

Продолжением данной работы может быть оптимизация построенных функций в современных методах цифровой обработки информации, в том числе и для обучения нейронных сетей процессам распознавания и принятия решений.

Литература

1. Беклемишев Д.В. Курс аналитической геометрии и линейной алгебры: учебник – Москва: Физматлит, 2011 – с. 223.
2. Вержбицкий В.М. Вычислительная линейная алгебра: учебное пособие для вузов – Москва; Берлин: Директ-Медиа, 2021. – с. 229 – 232.
3. Василенко В.В. Математические алгоритмы анализа цифровых изображений: Дис. канд. физ.-мат.наук: 05.13.18 Ставрополь, 2006 112с. РГБ ОД, 61:06–1/1061.
4. Голуб Дж., Ван Лоун Ч. Матричные вычисления. – М.: Мир, 1999 – с. 74.
5. Sebastian Raschka, Vahid Mirjalili «Python Machine Learning. Машинное обучение Python – третье издание: на англ. яз.»: книга – Packt Publishing, 2019.
6. Гонсалес Р., Вудс Р. Цифровая обработка изображений – 3 издание, 2012.

Сведения об авторах

Барсукова Виктория Юрьевна, кандидат физико-математических наук, доцент, заведующая кафедрой функционального анализа и алгебры Факультета математики и компьютерных наук Кубанского государственного университета; e-mail: barsukova.v.y@gmail.com.

Василенко Вера Викторовна, кандидат физико-математических наук, доцент кафедры функционального анализа и алгебры Факультета математики и компьютерных наук Кубанского государственного университета; e-mail: t9288487681@gmail.com.

Кутюков Алексей Александрович, факультет математики и компьютерных наук Кубанского государственного университета; e-mail: Kutyukova76@mail.ru.

Борисенко Александр Васильевич

ОСОБЕННОСТИ ИСПОЛЬЗОВАНИЯ ПРОГРАММНОГО ИНТЕРФЕЙСА ПРИЛОЖЕНИЯ

В данной статье приводится краткий обзор безопасности программного интерфейса приложения (API). Рассматриваются особенности использования интерфейса API разработчиками и конечными. Описываются основные методы и приемы, необходимые для обеспечения безопасности программной среды. Поднимаются вопросы защиты организациями используемых API от потенциальных угроз и уязвимостей.

Программный интерфейс приложения (API) – это механизмы, использующие набор определенных протоколов и позволяющие двум программам устанавливать связи между собой [1]. Тогда под данное определение подходит любое программное обеспечение (ПО), взаимодействующее друг с другом посредством запросов и ответов. API содержит информацию о том, как разработчики должны структурировать эти запросы и ответы. Для понимания процесса работы API можно привести взаимодействия по типу «клиент-сервер» [2]. Приложение, отправляющее запрос, называется клиентом, а приложение, отправляющее ответ, называется сервером.

Использование интерфейса прикладного программирования (API) резко возросло в последние годы. Увеличение числа взаимодействий между приложениями и большая потребность в данных привели к значительному росту трафика API [3,4].

Результаты исследований, проведенных международной фирмой «Гартнер» в 2022 году, говорят о том, что кибератаки на протоколы API стали наиболее частым вектором атак, используемым злоумышленниками. Несмотря на свою растущую популярность, API особенно уязвимы, если программные интерфейсы приложений должным образом не защищены. По данным компании «Group-IB» тремя основными типами уязвимостей API в организациях были:

неправильная настройка безопасности, чрезмерное раскрытие данных и инъекции [7,8].

Одной из наиболее распространенных уязвимостей API становится проблема неправильной настройки системы безопасности, связанной с общим доступом к ресурсам между источниками, а также неправильной политикой безопасности используемого контента [5].

Эти функции при внедрении довольно сложно правильно настроить, поэтому разработчики в целях экономии времени не уделяют должного внимания этому аспекту. В большинстве случаев эти уязвимости остаются незамеченными, однако в некоторых случаях могут иметь серьезные последствия.

Проблема чрезмерного раскрытия данных остается главным аспектом кибербезопасности программного обеспечения, объектом неотъемлемого риска получения нарушителем конфиденциальных данных вследствие плохой настройки API. В результате чего программа возвращает больше информации, чем необходимо для конкретного запроса. Уязвимости, связанные с инъекциями, такие как SQL, SMTP, HTML/XSS продолжают создавать значительные риски для безопасности информации.

Эти уязвимости позволяют злоумышленникам манипулировать поведением приложения, вставлять вредоносный контент, выполнять вредоносные запросы или команды. За последние годы разработчики добились значительного прогресса в устранении уязвимостей этого типа. Однако важно, чтобы они сохраняли бдительность и далее. Чтобы эффективно защитить свои API, разработчики должны оценить большое количество проблем. Вот краткое изложение некоторых из наиболее насущных проблем, которые могут возникнуть на этапе разработки: проверка ввода, аутентификация, авторизация, логические уязвимости, знание API.

API-ключи и токены часто утекают из-за халатности технического персонала организации. Многие разработчики хранят учетные данные в

исходном коде или файлах конфигурации либо в виде открытого текста, либо с использованием слабых типов шифрования. Это часто приводит к утечкам и несанкционированному использованию. Мобильные приложения также могут способствовать утечке ключей API. Разработчики должны помнить, что злоумышленники могут декомпилировать исходный код мобильных приложений в поисках конфиденциальной информации.

Кибербезопасность напрямую связана с рисками и вероятностями. Вот почему защитные механизмы должны иметь многоуровневый подход. Многофакторная аутентификация может обеспечить дополнительный уровень защиты, который может помочь предотвратить утечку данных [6]. Компаниям необходимо разрабатывать алгоритм обнаружения и реагирования на инциденты безопасности. Организация должна предугадать: где, как и кем предполагается использовать полученный токен. Таким образом, в случае злоупотребления им нарушителем организация сможет его выявить и принять меры по предотвращению его использования.

Защита от уязвимостей API должна быть важным аспектом стратегии безопасности любой компании. Безопасность API требует комплексного подхода, включающего оценку ключевых доменов, таких как аутентификация, авторизация, проверка ввода и логические уязвимости. В этой статье были описаны некоторые передовые методы, которые должны применять как разработчики, так и третьи стороны, чтобы устранить некоторые недостатки, которые могут возникнуть в случае неправильной настройки API. API-интерфейсы по-прежнему будут основной целью киберпреступников, и успешные атаки могут иметь разрушительные последствия, будь то нарушение работы, службы или кража конфиденциальных данных. Крайне важно подчеркнуть, что безопасность API – это круглосуточный процесс, требующий постоянного внимания и усилий. Организации должны следить за тем, чтобы их собственные или сторонние разработчики знали о важности безопасности API, а также иметь все необходимые ресурсы для создания безопасных API.

Литература

1. Баранова Е.К., Бабаш А.В. Основы информационной безопасности: учебник / Е.К. Баранова, А.В. Бабаш. – Москва: РИОР: ИНФРА-М, 2022. – 202с.

2. Белоус, А.И. Кибероружие и кибербезопасность. О сложных вещах простыми словами / А.И. Белоус, В.А. Солодуха. – Москва; Вологда: Инфра-Инженерия, 2020. – 692 с.

3. Диогенес Ю., Озкайя Э. Кибербезопасность: стратегии атак и обороны / пер. с анг. Д. А. Беликова. – М.: ДМК Пресс, 2020. – 326 с.

4. Ищейнов, В. Я. Информационная безопасность и защита информации: теория и практика: учебное пособие / В.Я. Ищейнов. – Москва; Берлин: Директ-Медиа, 2020. – 270 с.

5. Шаньгин В.Ф. Информационная безопасность и защита информации. – М.: ДМК Пресс, 2017. – 702 с.

6. URL: https://мвд.рф – Официальный сайт МВД России.

7. URL: https://www.kaspersky.ru – Официальный сайт компании «Лаборатория Касперского».

8. URL: https://mko-systems.ru/mobile-kriminalist – Официальный сайт компании «Мобильный криминалист».

Сведения об авторе

Борисенко Александр Васильевич, преподаватель кафедры информационно-компьютерных технологий в деятельности ОВД Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: Borisenko02.94@mail.ru.

Добровольская Наталья Юрьевна

ТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ НАУЧНЫХ СТАТЕЙ НА ОСНОВЕ АЛГОРИТМА BERT

Тематическое моделирование используется для автоматического извлечения информации из больших наборов данных, например, таких, как научные статьи, для классификации этих статей по темам. Актуальность цифровизации алгоритмов тематического моделирования определяется необходимостью исследователей в быстром поиске требуемой информации в больших объемах данных [1]. Подобные сервисы позволят классифицировать научные статьи, группировать их по основным тегам. Научные статьи часто сопровождаются списком ключевых слов, однако, такие наборы не всегда соответствуют контенту статьи, не упорядочены по значимости или вовсе отсутствуют.

Существует несколько подходов к построению ключевых слов: методы автоматического извлечения наиболее важных слов или фраз из текстового документа. Они используются для упрощения и ускорения процесса анализа больших объемов информации, а также для повышения эффективности поиска и категоризации документов. Выделим несколько основных типов алгоритмов построения ключевых слов, включая статистические методы, машинное обучение и методы на основе лингвистических правил: TF-IDF (term frequency-inverse document frequency), TextRank, RAKE (Rapid Automatic Keyword Extraction) и KEA (Keyphrase Extraction Algorithm). TF-IDF использует статистические методы для определения важности слов в документе, основываясь на частоте их встречаемости в документе и обратной частоте их встречаемости во всей коллекции документов. TextRank применяет аналогичный подход, но основывается на графовой модели текста. RAKE и KEA используют методы машинного обучения и на основе лингвистических правил соответственно. Выбор конкретного алгоритма зависит от целей и требований

конкретного проекта, а также от типа и объема данных, которые необходимо обработать.

Для определения ключевых тематик научных статей нами использован алгоритм BERT (Bidirectional Encoder Representations from Transformers). Это алгоритм глубокого обучения, предназначенный для обработки естественного языка. Его основное назначение - определение контекста и связей между словами в предложении, что дает ему преимущество по сравнению с традиционными методами обработки естественного языка. Разработчики BERT помимо англоязычной модели обучили также мультиязычную модель, в которую входит русский язык. Компания «Сбер» предоставила открытый доступ к модели ruBERT, позволяющей обрабатывать русский язык.

Использование модели ruBERT для задачи тематического моделирования включает следующие этапы: выделение эмбеддингов; кластеризация; выделение тематик. Под эмбеддингом понимают процесс преобразования слов или фраз в векторы чисел, которые в дальнейшем обрабатываются программно. На первом этапе использовалась мультиязычная модель BERT. Получившиеся вектора имеют большую размерность, так как учитывается контекст как до, так и после слова. Стоит обратить внимание, что слишком низкая размерность приводит к потере информации, а слишком высокая ухудшит результаты кластеризации. Для уменьшения размерности воспользуемся пакетом UMAP. Он хорошо справляется с этой задачей, при этом сохраняя значительную часть многомерной локальной структуры в меньшей размерности. После уменьшения размерности проведена кластеризация с помощью алгоритма HDBSCAN. HDBSCAN – алгоритм кластеризации данных, который основан на плотностной оценке иерархических структур данных. Он использует идею минимальной плотности, чтобы определить границы кластеров и их размеры, что позволяет ему эффективно обрабатывать данные с выбросами и шумом.

Для того чтобы извлечь темы необходимо понять, чем один кластер отличается от другого, какими наиболее подходящими ключевыми словами

представлен каждый кластер. Для решения этой задачи использована предложенная в 2020 году Мартеном Грутендорстом метрика c-tf-idf. Метрика tf-idf вычисляется, отталкиваясь не от одного документа, а от всех документов одного кластера, объединив документы кластера в один и посчитав метрики tf-idf для каждого слова. Таким образом, по величине метрики можно будет оценивать, насколько то или иное ключевое слово представляет тему, значимо в ней.

Метрика c-tf-idf вычисляется по следующей формуле:

$$c\_tf\_idf_i = \frac{t_i}{w_i} * log\frac{m}{\sum_j^n t_j},$$

где i – номер класса, t_i – частота слова t в классе i, w_i – общее количество слов в классе i, m – общее количество документов.

Для формирования тематики выделено десять наиболее значимых слов. На рисунке 1 приведен результат обработка научной статьи про Node.js.

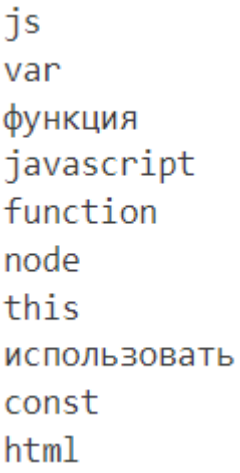


Рис. 1. Обработка текста с использованием модели BERT

Выявленные слова располагаются с учетов вероятности возникновения и первые несколько слов отражают собственно тематику статьи.

На основе модели BERT спроектировано и реализовано серверное приложение с пользовательским интерфейсом, позволяющие легко загрузить файл с научным текстом и получить набор тематик. Модель способна

эффективно выделять тематики текста, что позволяет оценить содержание статьи без её прочтения.

Модели и алгоритмы тематического моделирования позволяют не только определять список ключевых слов, но и выявлять особенности контента социальных сетей. Тематическое моделирование подписок пользователей позволяет выявить их интересы [2]. Расширение набора тематических моделей является перспективным вектором продолжения исследования.

Литература

1. Бабкина Н.С., Нугуманова А.Б., Оскорбин Н.М., Половикова О.Н., Смолякова Л.Л. Машинные методы тематического моделирования коллекции учебных текстов на естественном языке // Известия АлтГУ. 2020. №1 (111). С. 68-71.

2. Сысоев А.С., Добровольская Н.Ю. Анализ контента социальных сетей на основе графовых моделей // Прикладная математика: современные проблемы математики, информатики и моделирования. Материалы IV Всероссийской научно-практической конференции молодых ученых. 2022. С. 374-378.

Сведения об авторе

Добровольская Наталья Юрьевна, кандидат педагогических наук, доцент кафедры информационных технологий Кубанского государственного университета; e-mail: dnu10@mail.ru.

Дырма Сергей Валерьевич

К ВОПРОСУ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО БОРЬБЕ С IT-ПРЕСТУПЛЕНИЯМИ

Со времен зарождения государственности по настоящее время преступность, как деструктивное социальное явление, выступает серьезным дестабилизирующим фактором развития общественных институтов. Различные формы преступных проявлений причиняют материальный, нравственный и духовный ущерб как отдельным гражданам, так и обществу в целом.

В эпоху активного развития информационно-коммуникационных технологий, современное общество сталкивается с новейшими формами проявления преступной активности, при которых телекоммуникационные средства межличностного взаимодействия используются для совершения преступлений против личности, собственности, здоровья населения и общественной нравственности и других общественных отношений.

Безусловно, развивающиеся современные информационно-коммуникационные технологии способствуют ускорению межличностной коммуникации, обеспечивают быстрый и комфортный доступ граждан к своим электронным банковским счетам, значительно упрощают и оптимизируют развитие производства, общественных отношений, а также экономики в целом. Вместе с тем, информационно-коммуникационные технологии все активнее используются злоумышленниками для совершения различных преступлений.

Отличительными особенностями преступлений, совершаемых с использованием информационно-коммуникационных технологий, является дистанционный способ совершения, экстерриториальность, использование программных средств, позволяющих оставаться анонимными при использовании сети Интернет, динамичное многообразие способов совершения, а в отдельных случаях существенный уровень латентности.

IT-преступность, как особый вид общественно-опасных отношений, достаточно динамична. Злоумышленниками совершенствуются как подходы к

использованию технических и программных средств, позволяющих остаться анонимными при использовании сети Интернет или средств мобильной связи, так и методы психологического воздействия на граждан, с помощью которых возможно быстро и эффективно получить доступ к конфиденциальной информации.

Проведенный анализ преступлений, зарегистрированных на территории Российской Федерации в период с 2018 по 2022 год, показал, что при снижении регистрации всех преступлений на 0,1% (с 1 991 532 в 2018 году до 1 966 795 в 2022 году) [5], количество зарегистрированных IT-преступлений увеличилось на 199% (с 174 674 до 522 065) [6].

Согласно официальной статистической отчетности из 522 065 выявленных в 2022 году IT-преступлений 70,7 % (369 270 преступлений) составляют преступления против собственности (кражи – 21,8%, мошенничества – 47,9%, вымогательства – 1%) [6], которые характеризуются существенным многообразием способов совершения, а также использованием методик социальной инженерии, позволяющих злоумышленникам получать от граждан конфиденциальную информацию, необходимую для совершения хищений денежных средств с банковских счетов. Например, посредством телефонного звонка злоумышленник, представившись сотрудником банка, убеждает собеседника в угрозе безопасности денежных средств, хранящихся на банковском счёте последнего, после чего предлагает срочно снять все имеющиеся денежные средства и перевести их на другой «безопасный» счёт.

Структура IT-преступности в отдельных субъектах Российской Федерации с учетом региональной специфики может быть различна. Например, согласно анализу официальных статистических сведений по итогам 2022 года доля IT-преступлений против собственности, совершенных на территории Республики Крым составила 74,6%, Краснодарского края – 77,1%, г. Севастополь – 81,2% [6].

Решением коллегии МВД России от 01.11.2019 № 3 км в 2019 году в Центральном аппарате и территориальных органах внутренних дел на районном

уровне в структуре подразделений по контролю за оборотом наркотиков, противодействия экстремизму, уголовного розыска, экономической безопасности и противодействия коррупции, следственных подразделениях, подразделениях дознания и специальных технических мероприятий, созданы подразделения, специализирующиеся на противодействии преступлениям, совершаемым с использованием IT-технологий.

Приказом МВД России от 31 октября 2022 г. № 812 «О внесении изменений в приказ МВД России от 30 апреля 2011 г. № 333 «О некоторых организационных вопросах и структурном построении территориальных органов МВД России» определено создание в структуре территориальных органов МВД России на районном уровне подразделений по борьбе с противоправным использованием информационно-коммуникационных технологий [1].

Применительно к рассматриваемой теме отметим, что приказом МВД России от 1 февраля 2018 года № 50 «Об утверждении Порядка организации прохождения службы в органах внутренних дел Российской Федерации» определены общие квалификационные требования к сотрудниками, выполняющим обязанности, связанные с раскрытием или расследованием уголовных дел (например, преимущественное наличие высшего юридического образования), общие требования к стажу службы в органах внутренних дел и стажу (опыту) работы по специальности, а также уровню профессиональных знаний [3,с.27]. Специальные квалификационные требования к сотрудникам, специализирующимся на раскрытии и расследовании IT-преступлений, отсутствуют.

Вышеизложенное, по нашему мнению, определяет необходимость системного подхода со стороны органов внутренних дел не только к вопросам выявления, предупреждения, пресечения и раскрытия различных форм киберпреступности, но и необходимость совершенствования деятельности по

подготовке сотрудников подразделений, специализирующихся на противодействии IT-преступлениям.

Динамичный рост IT-преступности, уникальная специфика и многообразие способов совершения отдельных видов преступлений определяют необходимость не только особых требований к сотрудникам соответствующих специализированных подразделений, но и необходимость совершенствования методик подготовки специалистов в сфере борьбы с киберпреступностью.

Подготовка специалистов в сфере противодействия IT-преступности, а также повышение уровня их профессиональной квалификации, по нашему мнению, не должны сводиться к прохождению отдельных исключительно теоретических обучающих курсов.

Знаменитому русскому полководцу Александру Васильевичу Суворову нередко приписывают следующее выражение «Теория без практики мертва, практика без теории слепа» [4].

Проецируя глубокий смысл данного изречения на возможные пути совершенствования деятельности органов внутренних дел по подготовке квалифицированных специалистов в области противодействия IT-преступности, с учетом многогранности и динамичности данного вида преступности, мы приходим к очевидной необходимости непрерывной взаимосвязи теории и практики противодействия киберпреступности.

Практически ежегодно появляются все новые и новые способы совершения IT-преступлений, совершенствуются и создаются новые программные продукты, используемые злоумышленниками, а также оттачиваются криминальные техники социальной инженерии. Кроме этого, IT-преступность в тех или иных регионах имеет свою уникальную структуру и специфику. Правоприменительная практика противодействия отдельным видам IT-преступлений в различных субъектах Российской Федерации также не столь однообразна, о чем может свидетельствовать отсутствие единого подхода к определению критериев малозначительности при решении вопроса о

возбуждении уголовного дела по пункту «г» части 3 статьи 158 Уголовного кодекса Российской Федерации.

Руководствуясь изложенным, по нашему мнению, системный подход в вопросе подготовки специалистов органов внутренних дел в сфере борьбы с IT-преступлениями должен включать следующие основные элементы:

1. Выявление положительного регионального опыта противодействия отдельным видам и способам совершения IT-преступлений, в том числе организованных форм преступности.

2. Своевременное обобщение и анализ выявленного положительного опыта.

3. Совершенствование методического обеспечения в области противодействия IT-преступности на основе изученного положительного опыта.

4. Внедрение выявленного положительного опыта в правоприменительную деятельность.

5. Организация обучения сотрудников на основе постоянно дорабатываемой методической базы в области противодействия IT-преступности.

Литература

1. О внесении изменений в приказ МВД России от 30 апреля 2011 г. № 333 «О некоторых организационных вопросах и структурном построении территориальных органов МВД России»: приказ МВД России от 31 октября 2022 г. № 812.

2. Об утверждении Порядка организации прохождения службы в органах внутренних дел Российской Федерации: приказ МВД России от 1 февраля 2018 г. № 50.

3. Сенафонкин П.С., Дырма С.В. Особенности подбора персонала для подразделений по противодействию преступлениям, совершаемым в сфере информационно-телекоммуникационных технологий. Актуальные проблемы борьбы с преступлениями и иными правонарушениями: материалы

девятнадцатой международной научно-практической конференции / под ред. Д.Л. Проказина. – Барнаул: Барнаульский юридический институт МВД России, 2021. ч.1. С. 27-28.

4. URL: https://eksmo.ru/interview/15-aforizmov-aleksandra-suvorova-ID3934366 (дата обращения: 13.06.2023).

5. URL: http://crimestat.ru/offenses_chart (дата обращения: 12.06.2023).

6. Статистическая отчетность формы федерального статистического наблюдения № 4-ЕГС «Сведения о состоянии преступности и результатах расследования преступлений» // ЦСИ ФКУ «ГИАЦ МВД России» (10.5.0.16/csi).

Сведения об авторе

Дырма Сергей Валерьевич, преподаватель кафедры гуманитарных и социально-экономических дисциплин Крымского филиала Краснодарского университета МВД России; e-mail: s.dyrma@mail.ru.

Иванов Игорь Петрович,
Епифанцева Виктория Александровна

ЦИФРОВОЕ ОБРАЗОВАНИЕ: ОТ ПЕРСПЕКТИВНЫХ ТЕХНОЛОГИЙ К УЛУЧШЕНИЮ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Распространение цифровых технологий (ЦТ) ведет общество к качественным изменениям не только в политике, индустрии, экономике, но и социальной сфере. Современный мир стремительно меняется, и вместе с ним регулярно изменяется образовательный процесс. Проникновение ЦТ во все сферы жизни требует от массового работника нового качества образования. Базовой грамотности, которую формирует сложившаяся система образования, стало недостаточно.

Революционные преобразования общества невозможны без перехода от всеобщего массового образования к качественному образованию и всестороннему развитию личности. При этом быстрое развитие технологий не только ставит перед образованием новые задачи, но также предлагает инструменты для их решения.

Недавно мы столкнулись с новым форматом образования – дистанционное обучение. Преподаватели стали более активными и вовлеченными в процесс обучения, используя интерактивные методы и технологии. Это позволило им лучше понять потребности курсантов и слушателей и адаптировать учебный процесс к их индивидуальным потребностям. Преподаватели много усилий вкладывают в изменение формы преподавания, уходя от проведения классических занятий.

Инновационные образовательные технологии приобретают популярность, так как они позволяют обучающимся получать новые знания и навыки, на основе развития критического мышления и используя творческий подход к решению профессиональных задач.

Необходимо уходить от количественного показателя обучения к качественному и творческому восприятию материала.

Одна из ключевых функций цифровой трансформации обучения – это персонализация. Такой подход позволяет организовать более гибкий образовательный процесс для каждого студента. Не секрет, что разным людям нужно разное количество часов для освоения учебного материала и разный формат подачи информации. Это позволит обучающимся самостоятельно формировать свой учебный день, график изучения отдельных дисциплин, выбирать наиболее оптимальное время для выполнения заданий.

Например, курсантам, которые испытывают трудности с определенной концепцией, могут быть предоставлены дополнительные ресурсы и виртуальные помощники, которые помогут им в освоении материала. Это не только позволит обучающимся освоить предмет, но и повысит их уверенность в себе, а также мотивацию к обучению.

В России до сих пор многие скептически относятся к применению информационных технологий в обучении, в то время как в зарубежных странах, согласно статистике, около 76% студентов проходили онлайн-курсы, причём большинство опрошенных считают, что дистанционный формат не снижает эффективность занятий, а наоборот приносит новые качественные результаты.

Цифровая трансформация обучения подразумевает под собой не только онлайн-уроки, но также электронные библиотеки, электронные журналы и дневники, онлайн-тесты, дистанционную аттестацию, возможности отправки домашних заданий при помощи электронной почты или специальных платформ, возможность консультации с преподавателем не только в рамках занятия, но и дополнительно.

Использование информационных технологий в образовании имеет множество преимуществ. Одним из преимуществ является то, что качественные изменения проявляются в процесс обучения как у обучаемых, так и у преподавателей. Использование интерактивных досок во время занятий позволяет преподавателям разрабатывать современные увлекательные занятия, основанные на мультимедийных элементах. Применяемые мультимедийные

технологии помогают развивать интерес к новым видам подачи учебного материала и способствуют вовлеченности курсантов в интерактивное общение. Онлайн-инструменты, с технологиями виртуальной и дополненной реальности, могут быть использованы для закрепления концепций и выработки у обучающихся профессиональных практических навыков.

В настоящее время в образовательных учреждениях используются различные передовые методы информационных технологий, такие как:

- облачные технологии, которые предоставляют доступ к учебным материалам и ресурсам через интернет, что позволяет учащимся получать доступ к материалам из любой точки мира и в любое удобное для обучения время. Облачные технологии предоставляют возможность создания интерактивной учебной среды преподавателю и обучающимся совместно;
- системы дистанционного обучения позволяют обучающимся и преподавателям интерактивно общаться на расстоянии, обучаться, обмениваться информацией. Данное общение возможно при использовании образовательных платформ, онлайн курсов или программного обеспечения для видеоконференций;
- современные технологии искусственного интеллекта позволяют создавать персонализированные программы обучения, адаптированные к индивидуальным профессиональным потребностям;
- технология блокчейн позволяет создавать безопасные и прозрачные системы для обмена данными между учебными заведениями и обучающимися;
- технологии виртуальной и дополненной реальности могут быть использованы для проектирования инновационных и интерактивных образовательных сред, погружающих обучающихся в виртуальные миры для обеспечения более глубокого и продуктивного понимания изучаемого материала;

- применение мобильной техники и разработанных приложений для планшетов или смартфонов позволит обучаться в транспорте (электрички, метро, наземный транспорт);
- использование игровых элементов позволяет повысить мотивацию обучения и обеспечить вовлеченность при изучении учебного материала.

Наряду с большим количеством положительных примеров использования информационных технологий в образовательных организациях, существуют и недостатки. Например:

- недостаточная квалификация преподавателей и обучающихся к использованию инновационных технологий в учебной деятельности;
- отсутствие необходимой технической или программной инфраструктуры в учебных заведениях, зависимость от качества интернет-соединения или отсутствия современных технологических ресурсов;
- ограниченность доступа к современным образовательным технологиям и платформам, а также к источникам других образовательных организаций;
- длительная работа с компьютерной техникой может привести к проблемам со здоровьем;
- уход в мир компьютера приводит к нарушению межличностного общения и приобретения навыков командной и управленческой работы.

В заключение можно сказать, что цифровое образование имеет свои преимущества и недостатки. Однако, при правильном использовании информационных технологий и методов обучения, оно может стать эффективным инструментом для получения качественного профессионального образования. Важно помнить, что каждый обучающийся уникален, и подход к его обучению должен быть индивидуальным. Баланс использования компьютерных технологий и других методов обучения позволит создать оптимальную образовательную среду.

Литература

1. Иванов И.П. Некоторые аспекты цифровой трансформации традиционного образования в образовательных организациях МВД России / И.П. Иванов // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей IX Всероссийской научно-практической конференции. – Белгород: Белгородский юридический институт Министерства внутренних дел Российской Федерации им. И.Д. Путилина. 2022. С. 51-55.

2. Иванов И.П. Цифровой вызов традиционному образованию/ И.П. Иванов // Математические методы и информационно-технические средства [Электронный ресурс]: материалы XVIII Междунар. науч.-практ. конф. (17 июня 2022 г.) / редкол.: И. Н. Старостенко, Е. В. Михайленко, А. В. Еськов и др. – Электрон. дан. – Краснодар: Краснодарский университет МВД России, 2022. – 1 электрон. опт. диск. 2022. С. 67-70.

3. Концепция развития единой информационной образовательной среды в российской федерации. 2013. [Электронный ресурс, 5.05.2023]. URL: https://minobr.gov-murman.ru/files/koncepciya_eios.pdf.

4. Путин В.В. Послание Президента Федеральному Собранию. 1 марта 2018. [Электронный ресурс, 5.05.2023]. URL: http://kremlin.ru/events/president/news/56957.

5. Уваров А.Ю. Образование в мире цифровых технологий: на пути к цифровой трансформации. Изд. дом ГУ-ВШЭ, М.: 2018. - 168 с.

Сведения об авторах

Епифанцева Виктория Александровна, преподаватель кафедры информатики и математики Краснодарского университета МВД России; e-mail: torohova_viktori@ma.

Иванов Игорь Петрович, кандидат педагогических наук, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: iv_on_off@mail.ru.

Еськин Дмитрий Леонтьевич

ТЕХНОЛОГИЯ ДОПОЛНЕННОЙ РЕАЛЬНОСТИ НА СЛУЖБЕ ПОЛИЦИИ: НОВЫЕ ВОЗМОЖНОСТИ И ПЕРСПЕКТИВЫ

В современном мире развитие информационных технологий происходит с огромной скоростью. Ежегодно появляется множество различных новых устройств и технических разработок, которые позволяют упростить жизнь человека и сделать ее более комфортной, повысить эффективность его труда благодаря автоматизации рутинных действий и возникновению ранее недоступных возможностей в различных сферах деятельности.

Сегодня новые технологии являются весьма важным инструментом, позволяющим повысить эффективность правоохранительной деятельности. Изначально они использовались для организации базовых систем учета и обработки информации, но с развитием информационных технологий, возможности применения средств вычислительной техники существенно расширились. Одним из достаточно перспективных направлений применения информационных технологий в правоохранительной деятельности является использование технологии дополненной реальности.

Дополненная реальность (англ. Augmented Reality, AR) – это технология, которая позволяет объединить виртуальный мир с реальным. Принцип работы AR заключается в следующем. С помощью цифровой камеры осуществляется захват изображения окружающего мира, затем в режиме реального времени на полученное изображение добавляется дополнительная информация, после чего дополненное цифровыми объектами изображение транслируется на экран устройства дополненной реальности. В результате создается иллюзия того, что цифровые объекты находятся в окружающем мире, что позволяет пользователям взаимодействовать с ними в режиме реального времени. Дополненная реальность может применяться как на мобильных устройствах, так и на специализированных устройствах, например, очках или шлемах дополненной реальности. Основное отличие дополненной реальности от виртуальной заключается в том, что пользователь не выходит за пределы реального мира, а

остается в нем, однако получает возможность взаимодействовать с цифровыми объектами.

Можно выделить два главных принципа построения дополненной реальности: на основе использования специальных маркеров и на основе координат местоположения пользователя (безмаркерные) [1].

Технология дополненной реальности маркерного типа для определения местоположения виртуальных объектов использует маркеры, представляющие собой заранее заданные изображения или паттерны. В качестве таких маркеров могут выступать как QR-коды и специальные графические символы, так и схематичные или фотографические изображения реальных физических объектов. Когда такой маркер попадает в объектив камеры, то он распознается устройством и выступает в качестве точки отсчета, относительно которой осуществляется размещение элементов дополненной реальности в реальное окружение. Технология дополненной реальности безмаркерного типа основана на определении точных координат устройства в пространстве, для чего могут использоваться данные, получаемые от специальных датчиков устройства, например датчика системы спутниковой навигации, компаса, гироскопа, акселерометра, а также от камеры устройства для получения информации о расположении окружающих физических объектов в пространстве.

Несмотря на свою относительную новизну, технология дополненной реальности уже успела завоевать популярность в самых разных сферах человеческой деятельности. Так в развлекательной индустрии разрабатываются игровые и иные развлекательные проекты, прежде всего для мобильных устройств, в которых пользователь взаимодействует с виртуальными объектами и игровыми персонажами, отражаемыми в реальном мире.

Технологии дополненной реальности все чаще применяются в экспозициях галерей, выставок и музеев для внесения в экспозиции элемента интерактивности, тем самым способствуя погружению посетителей и улучшению восприятия информации в целом [2].

В образовании находят применение интерактивные учебники, позволяющие рассматривать трехмерные модели изучаемых объектов, наблюдать за динамикой каких-либо изучаемых процессов, что позволяет добиться более глубокого понимания изучаемого материала благодаря наглядности.

Коммерческие организации используют технологию дополненной реальности для проведения интерактивных рекламных кампаний, позволяющих потенциальным покупателям или потребителям взаимодействовать с продуктами или услугами до того, как они решат их приобрести [3].

В медицине дополненная реальность используется для построения моделей органов человека, визуализации хода предстоящего хирургического вмешательства, в психотерапевтических целях [4].

Дополненная реальность позволяет дизайнерам и архитекторам визуализировать проекты в режиме реального времени, создавать трехмерные модели зданий и помещений, изменять масштаб и форму объектов, а также оценивать их функциональность.

Возможности технологии дополненной реальности могут быть использованы для повышения эффективности выполнения различных задач, стоящих перед сотрудниками полиции. Технология дополненной реальности может оказать существенную помощь сотрудникам полиции, несущим службу по охране общественного порядка. Так на экран мобильного устройства или специальных очков может выводиться дополнительная информация при наведении камеры на объекты окружающего пространства. Например, отображаться интерактивная карта местности, содержащая сведения о наиболее значимых объектах, требующих повышенного внимания, местах, в которых ранее уже были совершены преступления и административные правонарушения, расположение соседних нарядов и т.д. Это может помочь полицейским быстро ориентироваться в новых локациях. Системы дополненной реальности могут осуществлять распознавание подозрительного поведения и сигнализировать сотруднику полиции в случае обнаружения потенциальной опасности.

Интеграция технологии дополненной реальности с системами распознавания образов и базами данных предоставляет полицейским еще больше возможностей для эффективного выполнения своих задач. Так интеграция с системой распознавания лиц позволит в автоматизированном режиме осуществлять идентификацию людей, попадающих в кадр камеры, и в случае выявления потенциально опасных лиц и лиц, находящихся в розыске, выделять их на экране устройства полицейского и выводить дополнительную информацию о них. Интеграция с системой распознавания государственных регистрационных знаков автотранспортных средств позволит выявлять среди попавших в объектив камеры автомобилей те, которые числятся в угоне или розыске, получать сведения о владельцах транспортных средств, совершении ими административных правонарушений в области дорожного движения.

С помощью технологий дополненной реальности можно осуществлять проверку документов на наличие признаков, указывающих на подделку, осуществлять сверку отраженной в документе информации с данными, содержащимися в специализированных базах данных.

Дополненную реальность можно применять при обучении сотрудников полиции. В этих целях можно использовать различные визуальные тренажеры для симуляции ситуаций, которые могут возникать в повседневной деятельности сотрудника полиции, что позволит обучаться в условиях, максимально приближенных к реальным, тем самым способствуя повышению качества подготовки полицейских. Например, такие тренажеры могут быть использованы для развития умений и навыков оказания первой помощи, огневой подготовки, проведения обыска помещений, обучения тактике действий при пресечении массовых беспорядков и т.д.

С помощью приложений дополненной реальности можно создавать трехмерные модели мест происшествий, размещать на них виртуальные отметки и комментарии, например, обнаруженные следы, которые будут видны все сотрудникам.

Таким образом, технология дополненной реальности представляет собой мощный инструмент, находящий применение в различных сферах человеческой деятельности, в том числе и правоохранительной. В полиции технология дополненной реальности может значительно повысить эффективность работы сотрудников. Она предоставляет им дополнительную информацию об окружающей среде, помогая лучше ориентироваться в новых местах, распознавать подозрительное поведение и обнаруживать потенциальные угрозы, автоматизировать процессы идентификации лиц, поиска угнанных автомобилей, проверки документов и других задач, стоящих перед сотрудниками полиции. Вместе с тем, внедрение технологии дополненной реальности в правоохранительную деятельность сопряжено с рядом проблем. Некоторые из них связаны с трудностями сугубо технологического характера, другие связаны с опасениями нарушения прав человека на конфиденциальность и неприкосновенность частной жизни. Тем не менее, при правильном подходе к организации использования технологии дополненной реальности все возникающие проблемы могут быть успешно решены, а ее преимущества могут значительно перевесить все недостатки.

Литература

1. Маслова Ю.А., Белов Ю.С. Технологии дополненной реальности // E-Scio. 2022. №2 (65). С. 313–322.

2. Соловьева А.А. Технологии дополненной реальности в музейном пространстве // Наука без границ. 2020. №1 (41). С. 48–53.

3. Аминова Г.Г., Козырева Л.К. технологии виртуальной и дополненной реальности в дизайне рекламы // Ноэма. 2021. №2 (7). С. 178-188.

4. Намиот Е.Д. Дополненная реальность в медицине // International Journal of Open Information Technologies. 2019. № 11. С. 94–99.

Сведения об авторе

Еськин Дмитрий Леонтьевич, кандидат физико-математических наук, заместитель начальника кафедры информатики и математики Волгоградской академии МВД России; e-mail: deskin2@mvd.ru.

Ефремов Сергей Константинович

АНАЛИЗ ФАКТОРОВ, ВЛИЯЮЩИХ НА ТОЧНОСТЬ ПРОГНОЗА УСПЕВАЕМОСТИ КУРСАНТОВ С ПОМОЩЬЮ ИСКУССТВЕННОЙ НЕЙРОННОЙ СЕТИ

Каждый абитуриент при поступлении в университет несет, с одной стороны, определенный набор способностей к освоению программы специальности, на обучение по которой он поступает, и, с другой стороны, определенный уровень знаний по предыдущему обучению, которые необходимы для освоения этой программы. То и другое имеет описание конкретными показателями, которые для каждого абитуриента имеют конкретную количественную оценку.

Исследователи выделяют показатели [3, 4], влияющие на будущую успеваемость, основными из которых являются:

- данные из аттестата о среднем образовании и результаты ЕГЭ;
- декларируемые цели обучения (достижение уровня специалиста в выбранной специальности, получение диплома о высшем образовании и т.п.);
- трудовой стаж до поступления в университет;
- внеучебные увлечения абитуриента (спорт, музыка, живопись);
- уровень доходов семьи и т.д.

В значениях данных показателей заложены оценочные сведения о потенциальных уровнях освоения дисциплин выбранной абитуриентом специальности. Специалиста формируют практически все дисциплины учебного плана специальности. И разные показатели в разной степени влияют на способность освоения каждой отдельной дисциплины. Поэтому для интегральной оценки уровня подготовки будущего специалиста необходим учет большого числа показателей.

С другой стороны, потенциальный уровень подготовки специалиста может быть определен наиболее вероятными оценками обучающегося по дисциплинам учебного плана. В итоге, задача прогнозирования уровня будущей подготовки

специалиста (ныне абитуриента) приобретает черты задачи прогноза с большим числом входных и выходных параметров, с которой достаточно хорошо справляются искусственные нейронные сети [2].

В описанном направлении исследований проделана работа [1], в которой в качестве входных параметров использованы оценки абитуриентов по основным предметам обучения в школе, а в качестве выходных – экзаменационные оценки первого и второго семестра обучения курсантов по направлению подготовки 40.03.02 Обеспечение законности и правопорядка. Полученные результаты позволили сделать выводы:

1) в отечественном образовании используется достаточно грубая система 5-балльной (а реально в аттестатах о среднем образовании 3-балльной) оценки знаний. В результате реальные уровни знаний 3,52 и 4,48 (разница практически в один балл из трех в используемой шкале) оценивается одинаково – 4;

2) проявляется высокая степень субъективизма в выставлении оценок в школе, на которую практически не повлияло введение ЕГЭ.

Обработка результатов исследований показала, что полученное в эксперименте среднее значение модуля ошибки прогноза (модуль разности между спрогнозированной и реально полученной оценкой) составила 0,55 балла. В это значение большой вклад вносят проблемы образования, описанные выше. Такая точность оценок явно недостаточна для практического использования.

На втором этапе исследований планируется использовать в качестве входных параметров не оценки школьного аттестата, а результаты психо-физиологических исследований абитуриентов, проводимых в форме тестирования. Преимущества этого направления:

1) измерения проводятся для всех абитуриентов в одинаковых условиях;

2) количественные оценки результатов тестирования выставляются тестирующими программами автоматически (нет субъективизма);

3) тестирование проводится непосредственно перед началом обучения в университете (в противоположность этому оценки в школьном аттестате накапливаются в течение нескольких последних лет обучения в школе).

Качественный многоплановый анализ психофизиологических параметров абитуриентов подразумевает использование нескольких тестов, каждый из которых выдает от нескольких до десяти и более выходных параметров. Не все они ощутимо влияют на качество освоения дисциплин высшего образования. Поэтому встает задача отбора более значимых параметров для дальнейшего их использования в прогнозировании успеваемости курсантов.

Степень взаимосвязи входных параметров и оценок по отдельным дисциплинам может быть оценена в значениях коэффициентов корреляции (психофизиологические параметры и оценки по вузовским дисциплинам при этом считаются случайными величинами). Для апробирования такого подхода использованы данные из первого этапа исследований, здесь вместо психофизиологических параметров – результаты обучения в школе. При оценке использовались 111 примеров (данные по 111 курсантам), что позволяет оценивать результаты как достаточно адекватные. Взяты их оценки по 14 предметам обучения в школе и по 9 предметам вузовского обучения. Получены значения 126 коэффициентов корреляции.

Результаты оценки коэффициентов корреляции приведены в табл.1.

Некоторые выводы из анализа результатов:

1. Максимальное значение коэффициента корреляции – 0,51 – между школьной и вузовской информатикой.

2. Коэффициент корреляции между школьной физической культурой и вузовской физической подготовкой – 0,08, т.е. близок к нулю.

3. Оценки по школьному и вузовскому русскому языку коррелированы на уровне 0,37.

Таблица 1. Значения коэффициентов корреляции

	ИИТПД	Философия	Административное право	Русский язык в деловой документации (КР)	Физическая подготовка	Иностранный язык	Профессиональная этика и служебный этикет	Гражданское право	Криминалистика
Русский язык	0,4	0,36	0,34	0,37	0,13	0,33	0,17	0,21	0,18
Русская литература	0,36	0,3	0,27	0,24	0,11	0,26	0,11	0,16	0,24
Иностранный язык	0,31	0,33	0,23	0,21	0,1	0,27	0,2	0,18	0,14
Алгебра и начала анализа	0,28	0,27	0,26	0,17	0,05	0,24	0,14	0,12	0,15
Геометрия	0,29	0,29	0,25	0,18	0,11	0,27	0,2	0,17	0,15
История	0,25	0,3	0,28	0,2	0,06	0,25	0,1	0,18	0,18
География	0,32	0,14	0,18	0,22	0,06	0,2	0,13	0,11	0,05
Физика	0,25	0,22	0,26	0,19	0,01	0,2	0,07	0,18	0,15
Химия	0,36	0,31	0,33	0,19	0,09	0,27	0,25	0,22	0,18
Биология	0,36	0,34	0,31	0,26	0,01	0,33	0,29	0,21	0,38
ОБЖ	0,24	0,13	0,2	0,16	0,05	0,12	0,17	0,09	0,09
Информатика и ИКТ	0,51	0,25	0,2	0,2	0,13	0,12	0,28	0,2	0,06
Физическая культура	0,24	0,15	0,07	-0	0,08	0,11	0,17	0,06	-0
Обществознание	0,4	0,36	0,34	0,37	0,13	0,33	0,17	0,21	0,18

Выводы:

1. Оценки школьных аттестатов характеризуются низкой информативностью, недостаточно адекватно отражают реальный уровень учеников.

2. Рассмотренный в статье подход позволит по значениям коэффициентов корреляции выделить из всего списка психофизиологических параметров наиболее значимые, имеющие наибольшие значения коэффициентов, для

использования на втором этапе исследований – прогнозирование вузовской успеваемости по значениям психофизиологических параметров абитуриентов.

Литература

1. Ефремов С.К., Михайленко Е.В. О возможности использования нейронной сети в индивидуализации приема и обучения студентов. // Проблемы современного педагогического образования. – Сборник научных трудов. – Ялта: РИО ГПА, 2019. – Вып. 65. – Ч. 1, с. 114-117.

2. Иванов, В.М. Интеллектуальные системы: учебное пособие / В.М. Иванов. – Екатеринбург: Изд-во Урал. ун-та, 2015. – 92 с.

3. Ильин Е.П. Дифференциальная психология профессиональной деятельности. – СПб.: Питер, 2011. – 432 с.

4. Крылова А.Г. Успеваемость студентов экономических специальностей и статистическая оценка факторов, на нее влияющих. // Современные научные исследования и инновации. 2012. № 6 [Электронный ресурс]. URL: http://web.snauka.ru/issues/2012/06/14688 (дата обращения: 29.09.2017).

Сведения об авторе

Ефремов Сергей Константинович, кандидат технических наук, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: efremovsk@yandex.ru.

Жмурко Даниил Юрьевич,
Кунгбала Моконзикуа Нарцисс Сильвер

ЭКСТРЕМИСТСКИЕ И ТЕРРОРИСТИЧЕСКИЕ МАТЕРИАЛЫ В СЕТИ ИНТЕРНЕТ: ОПРЕДЕЛЕНИЕ, КРИТЕРИИ И КЛАССИФИКАЦИЯ

В данной статье рассматривается определение экстремистских и террористических материалов в сети Интернет. Представлены критерии определения таких материалов. А также рассматривается классификация экстремистских и террористических материалов в сети Интернет. Описываются примеры таких материалов и предлагаются методы их обнаружения и противодействия на основе российского, африканского и международного опыта.

Введение

В современном мире интернет является одним из основных источников информации, однако, к сожалению, он также служит площадкой для распространения экстремистских и террористических материалов. В связи с этим возникает необходимость разработки критериев, методов определения и классификации таких материалов для их блокирования и предотвращения пропаганды насилия и терроризма.

Определение экстремистских и террористических материалов

Экстремистские материалы – это информация, размещенная в сети Интернет, которая призывает к насилию, неприязни или дискриминации по признакам расы, национальности, религии, пола или другим основаниям, а также пропагандирующая идеи экстремизма [3].

Террористические материалы – это информация, содержащая призывы к совершению террористических актов, оправдание терроризма или пропаганду террористической деятельности, а также информация о методах и тактике осуществления террористических актов [3].

Критерии определения экстремистских и террористических материалов:

1. Наличие призывов к насилию, террористическим актам или подстрекательства к неприязни и дискриминации.

2. Размещение символики, связанной с экстремистскими или террористическими организациями.

3. Пропаганда идеологии экстремизма или терроризма, в том числе публикация материалов, воспевающих лидеров экстремистских или террористических организаций и их деятельность.

4. Обучение методам и тактике совершения террористических актов или другим противоправным действиям.

5. Финансирование или поддержка экстремистских или террористических организаций через интернет-ресурсы [4].

Примеры практического использования критериев определения экстремистских и террористических материалов в ЦАР

В ЦАР было предпринято несколько практических мер для определения и пресечения экстремистских и террористических материалов в интернете:

А. Мониторинг интернет-ресурсов. Правоохранительные органы и специализированные государственные структуры ЦАР осуществляют мониторинг интернет-ресурсов с целью выявления экстремистских и террористических материалов [4]. Мониторинг включает в себя анализ сайтов, блогов, форумов, социальных сетей и других платформ для определения контента, соответствующего критериям экстремистских и террористических материалов.

Б. Сотрудничество с интернет-провайдерами и платформами. ЦАР активно сотрудничает с интернет-провайдерами и администрациями платформ для блокировки доступа к экстремистским и террористическим материалам. В рамках этого сотрудничества правоохранительные органы информируют провайдеров и администрацию платформ о выявленных материалах, а провайдеры и администрация платформ, в свою очередь, обязаны принять меры для блокировки доступа к таким материалам [9].

В. Привлечение к ответственности лиц, распространяющих экстремистские и террористические материалы. На основе результатов мониторинга и сотрудничества с интернет-провайдерами и платформами, правоохранительные органы ЦАР привлекают к ответственности лиц, распространяющих экстремистские и террористические материалы. Это может включать уголовное преследование, административные взыскания и другие меры [10].

Российский и международный опыт

1. Российский опыт

В России существует федеральный список экстремистских материалов, который регулярно обновляется и включает произведения, признанные судом экстремистскими [5]. Кроме того, в 2012 г. был принят закон «О противодействии экстремистской деятельности», который устанавливает основные принципы и меры по борьбе с экстремизмом [12].

2. Африканский опыт

В Африке существуют различные меры по борьбе с экстремизмом и терроризмом. Например, Африканский союз принял Конвенцию о предотвращении и борьбе с терроризмом в 1999 г., которая определяет основные принципы и меры противодействия терроризму на континенте [1]. Кроме того, в ряде африканских стран приняты национальные законы и программы по борьбе с экстремизмом и терроризмом [14].

2.1. Законодательная база ЦАР в области борьбы с экстремизмом и терроризмом

ЦАР реализует меры по борьбе с экстремизмом и терроризмом в рамках национального законодательства. Законодательство страны включает уголовные нормы, направленные на предотвращение и пресечение экстремистской и террористической деятельности, а также на наказание лиц, совершающих такие преступления [3].

3. Международный опыт

На международном уровне существуют различные международные инструменты по борьбе с экстремизмом и терроризмом, такие как резолюции Совета Безопасности ООН [8]. Кроме того, международные организации, такие как Европейский союз, Организация по безопасности и сотрудничеству в Европе [ОБСЕ] и Организация американских государств [ОАГ], также имеют свои стратегии и программы по борьбе с экстремизмом и терроризмом [2, 6, 7].

Методы классификации экстремистских и террористических материалов в интернете

Экстремизм и терроризм представляют собой серьезные угрозы для общества и безопасности. В интернете распространение экстремистских и террористических материалов особенно опасно, так как это облегчает вербовку сторонников и координацию действий.

Методы классификации:

1. *Анализ содержания.* Классификация экстремистских и террористических материалов часто начинается с анализа содержания, которое затем сравнивается с возможными мерками для определения его степени радикализма [20]. Анализ содержания включает оценку текстовых и визуальных элементов материалов, таких как язык, символы, изображения и видео.

2. *Сетевой анализ* используется для определения структуры и взаимосвязей между участниками онлайн-сообществ, связанных с экстремизмом и терроризмом [22]. Этот метод классификации помогает определить ключевых участников, передающих экстремистские и террористические материалы, и может способствовать разработке стратегий борьбы с распространением такого контента в интернете.

3. *Анализ социальных медиа* показывает взаимосвязь между пользователями и распространением экстремистских и террористических материалов [9]. Методы анализа могут включать сбор и анализ данных об аккаунтах, хештегах, геотегах, упоминаниях и репостах, чтобы определить роли пользователей и их влияние на распространение такого контента.

4. *Автоматизированные методы классификации.* С развитием технологий искусственного интеллекта и машинного обучения появились автоматизированные методы для классификации экстремистских и террористических материалов [4]. Эти методы используют алгоритмы классификации, основанные на наличии определенных признаков, таких как ключевые слова или фразы, видео- или аудиохарактеристики, и проводят анализ больших объемов данных для определения степени риска таких материалов.

5. *Кросс-культурная классификация* подразумевает сравнение экстремистских и террористических материалов из разных культур и контекстов, чтобы понять общие и уникальные характеристики, а также основания для сотрудничества между группами [10]. Этот метод способствует развитию культурно-специфичных подходов к борьбе с экстремизмом и терроризмом в интернете.

6. *Анализ поведения пользователей*, занимающихся распространением экстремистских и террористических материалов, также является ценным методом классификации [15]. Этот подход может включать наблюдение за активностью пользователей в социальных сетях, анализ их комментариев и мотивов, а также определение частоты и типов контента, которым они делятся.

7. *Коллаборативная фильтрация* – это метод классификации, который опирается на оценки пользователей и их мнения о том, что является экстремистским или террористическим материалом [17]. Он позволяет анализировать информацию, полученную от пользователей, и создавать интеллектуальные системы для автоматического обнаружения экстремистских и террористических материалов на основе предпочтений и решений пользователей.

8. *Методы исследования трафика.* Анализ трафика – это метод исследования активности пользователей в сети интернет и их взаимодействия с экстремистскими и террористическими материалами [13]. Это может включать мониторинг сетевого трафика для определения основных источников и путей

распространения экстремистских и террористических материалов, а также определение подозрительного поведения с целью предотвращения новых случаев экстремизма и терроризма.

9. *Интегрированные подходы* к классификации экстремистских и террористических материалов в сети интернет объединяют различные методы и технологии с целью создания максимально точной и эффективной системы обнаружения [14]. Такие подходы могут включать использование машинного обучения, анализа социальных медиа, сетевого анализа и других методов, а также разработку совместных международных стандартов и практик для борьбы с экстремистскими и террористическими материалами в интернете.

10. *Юридическая классификация* заключается в определении того, является ли определенный материал незаконным с учетом законодательства о борьбе с экстремизмом и терроризмом [15]. Это может включать анализ нарушений законодательства разных стран, а также национальных и международных норм.

11. *Геоинформационный анализ* используется для определения географического распространения экстремистских и террористических материалов и их аудитории [16]. Этот метод классификации помогает определить географические особенности и зоны повышенного риска распространения экстремистских и террористических материалов, что облегчает разработку мер по ограничению их распространения.

12. *Психологические методы* экстремизма и терроризма оценивают влияние экстремистских и террористических материалов на мышление и поведение человека [18]. Эти методы классификации дают представление о том, как восприимчивы пользователи к экстремистским и террористическим идеям и к каким изменениям в поведении эти материалы могут привести.

13. *Этнографические методы* дают глубокое понимание образа жизни и культуры в определенных сообществах и группах, связанных с экстремизмом и терроризмом [19]. Применение этнографических методов может помочь

исследователям выявить основные ценности и представления, лежащие в основе радикальных сообществ и их взаимодействия в интернете.

Все рассмотренные методы классификации экстремистских и террористических материалов в интернете имеют свои сильные стороны и ограничения. Однако использование комбинации этих методов может составить более точное и детальное представление об интернет-контенте, связанном с экстремизмом и терроризмом, что в свою очередь содействует разработке эффективных стратегий противодействия распространению подобных материалов и радикализации поведения пользователей.

Пример экстремистских и террористических материалов в интернете:

Халифат Вильяят – это информационное агентство, связанное с группировкой ИГИЛ, которое в 2014-2016 гг. активно использовало сеть Интернет для распространения террористической пропаганды, включая видео с казнями, аудиозаписи, заявления и информационные бюллетени на разных языках, включая русский. Одной из целей деятельности данного агентства было привлечение новых сторонников к идеям ИГИЛ, вербовка боевиков и распространение идеологии этой группировки.

Методы противодействия террористической пропаганде в интернете

Для противодействия террористической пропаганде в сети Интернет страны используют различные подходы, средства и мероприятия, включая:

а) *Законодательные меры.* Принятие и совершенствование законов, направленных на борьбу с террористическими деяниями и пропагандой, установление санкций и ответственности за их нарушение, включая административную, гражданско-правовую и уголовную ответственность.

б) *Сотрудничество с операторами интернета и администраторами сайтов*. Рабочие контакты с операторами связи и провайдерами интернет-услуг, обсуждение с ними методов блокировки, удаления и ограничения доступа к экстремистской и террористической информации.

в) *Создание специализированных подразделений*. Формирование в центральных и региональных подразделениях ФСБ России и полиции профессиональных отрядов по борьбе с распространением террористической пропаганды в интернете, обеспечение им соответствующих средств и организационно-технической базы.

г) *Международное сотрудничество*. Обмен опытом и информацией с представителями законодательных органов и спецслужб других стран, обсуждение на межгосударственном уровне мер по предотвращению террористической пропаганды в интернете, разработка совместных стратегий и программ.

д) *Профилактика и образование*. Проведение информационно-просветительской работы среди населения, включая детей и молодежь, активное использование средств массовой информации и социальных сетей, проведение социологических исследований и мониторинга массового сознания в области терроризма и экстремизма.

е) *Реабилитационные программы*. Создание условий для реабилитации лиц, замешанных в террористических деяниях или являющихся жертвами террористической пропаганды, обеспечение им возможности вернуться к нормальной социальной жизни и преодоления последствий участия в незаконных структурах и деятельности.

ж) *Развитие альтернативных средств информации*. Поддержка социальных проектов и инициатив, направленных на пропаганду мира, толерантности и неприятия терроризма и экстремизма, создание позитивного информационного поля и противовеса деструктивным идеям и агрессивной пропаганде.

з) *Использование технологий машинного обучения и искусственного интеллекта*. Применение автоматизированных систем и алгоритмов для определения, обнаружения и блокировки содержания террористической

пропаганды в интернете, в том числе в социальных сетях и на платформах видеохостинга.

и) *Привлечение населения к борьбе с террористической пропагандой.* Вовлечение активных общественных организаций, гражданских активистов и добровольцев в процессы выявления и противодействия террористической пропаганде, использование «горячих линий» и других средств непосредственной коммуникации с гражданами, готовыми содействовать в отслеживании и ликвидации источников экстремистской информации.

Для успешного противодействия пропаганде террористического характера необходимо комплексное, целенаправленное и последовательное применение всех вышеперечисленных мер и подходов, что способствует созданию благоприятных условий для предотвращения процессов радикализации общества и склонности к насильственным формам деятельности.

Российский опыт

В России экстремистские материалы определены в ст. 1 ФЗ «О противодействии экстремистской деятельности» от 25 июля 2002 г. № 114-ФЗ. Согласно законодательству, экстремистские материалы включают тексты, изображения, аудио- и видеозаписи, призывающие к насилию, терроризму, дискриминации и иным антисоциальным действиям [1].

Примеры:

– Публикации, призывающие к сепаратизму и национальной неприязни;

– Материалы, пропагандирующие националистическую, расовую или религиозную нетерпимость;

– Информация о создании и использовании взрывчатых веществ и других опасных средств для совершения террористических актов.

Африканский опыт

Несмотря на разнообразие законодательных систем африканских стран, многие из них сталкиваются с проблемой экстремизма и терроризма. В Африке

преобладают материалы, связанные с религиозным экстремизмом и террористическими группировками, такими как «Боко Харам» и «Аль-Шабаб» [2].

Примеры:

– Видеозаписи с казнями и пытками, совершаемыми террористами;

– Призывы к джихаду и распространение идеологии радикального ислама;

– Обучающие материалы для совершения террористических актов и вербовки новых членов группировок.

Международный опыт

На международном уровне, экстремистские и террористические материалы часто связаны с транснациональными террористическими организациями, такими как «Аль-Каида» и «Исламское государство» [3]. Основные примеры таких материалов включают:

✓ Информацию о террористических актах и угрозах, направленных против определенных стран или населения;

✓ Пропагандистские материалы, призывающие к насилию и экстремизму на основе идеологии террористических организаций;

✓ Методы вербовки и обучения террористических групп, а также координации их действий через интернет.

Противодействие распространению экстремистских и террористических материалов в интернете

Российские меры

В России действует множество законов и правил, направленных на противодействие распространению экстремистских и террористических материалов в интернете. Ключевыми органами, занимающимися этой проблемой, являются ФСБ, МВД и Роскомнадзор [4]. Основные меры включают:

– Блокировку доступа к интернет-ресурсам, содержащим экстремистские и террористические материалы;

– Штрафы и уголовное преследование за распространение экстремистской и террористической информации;

– Сотрудничество с международными партнерами по обмену информацией и опытом в области борьбы с экстремизмом и терроризмом.

Африканские меры

Африканские страны также предпринимают усилия для борьбы с экстремистскими и террористическими материалами в интернете. Многие страны Африки сотрудничают с международными организациями, такими как Африканский союз и ООН, для разработки и реализации стратегий противодействия [5]. Ключевые направления деятельности включают:

– Усиление контроля над интернет-контентом, связанным с экстремизмом и терроризмом;

– Развитие правовой базы для пресечения распространения экстремистских и террористических материалов;

– Обучение специалистов и учреждение специализированных подразделений для мониторинга и блокировки экстремистского контента.

Международное сотрудничество

Это сотрудничество играет важную роль в борьбе с распространением экстремистских и террористических материалов в интернете. Организации, такие как ООН, Европейский союз, БРИКС, ШОС, G7 и другие, активно участвуют в разработке новых подходов и технологий для противодействия данной проблеме [6]. Основные направления сотрудничества включают:

– Обмен информацией и опытом между странами и специализированными органами;

– Разработка международных стандартов для мониторинга и регулирования интернет распространением экстремистских и террористических материалов в интернете.

Проблемы и вызовы в борьбе с экстремистским и террористическим контентом в сети Интернет

Несмотря на значительные усилия государств и международных организаций, борьба с экстремистским и террористическим контентом в интернете сталкивается с рядом проблем и вызовов:

1. Технологические проблемы

Одним из основных вызовов является быстрое развитие технологий и интернет-платформ, что затрудняет контроль над распространением экстремистского и террористического контента. Террористические группировки активно используют шифрование, анонимные сети, децентрализованные платформы и другие средства для обхода блокировок и мониторинга со стороны правоохранительных органов [7].

2. Юридические и этические проблемы

Борьба с экстремистским и террористическим контентом в интернете порой может противоречить принципам свободы слова и защиты частной жизни. Вопрос о границах между законными ограничениями и нарушением прав на свободу информации и личную неприкосновенность является предметом оживленных дебатов и критики [8].

3. Нескоординированные действия на международном уровне

Хотя международное сотрудничество играет важную роль в борьбе с экстремистским и террористическим контентом в интернете, существует определенная степень разрозненности и нескоординированности действий различных стран и организаций. Это может приводить к дублированию усилий и ресурсов, а также к проблемам с обменом информацией и совместной координацией действий [9].

Борьба с распространением экстремистского и террористического контента в интернете является актуальной и сложной проблемой. Чтобы справиться с этим вызовом, необходимо применять комплексный подход, включающий разработку и реализацию законодательства, технологические инновации и международное сотрудничество. Важно также учесть юридические

и этические аспекты, чтобы не нарушать основные права и свободы пользователей интернета.

Заключение

В данной статье были рассмотрены основные определения, критерии и классификации экстремистских и террористических материалов в интернете, а также Российский и международный (практический) опыт по выявлению и пресечению таких материалов. Учитывая масштабы и глобальный характер данной проблемы, сотрудничество между государствами, провайдерами интернет-услуг и платформами является ключевым фактором в борьбе с распространением экстремистских и террористических материалов в интернете.

Литература

1. Африканский союз. Конвенция о предотвращении и борьбе с терроризмом [1999]. URL:https://au.int/sites/default/files/treaties/7759-file-african_union_convention_on_ the_prevention_and_combating_of_terrorism.pdf.

2. Стратегия ЕС по борьбе с терроризмом [2005]. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52005XG1217%2801%29.

3. Козлов, А. Борьба с экстремизмом и терроризмом в Центральноафриканской Республике: особенности законодательства и международное сотрудничество. Вестник Международных Организаций, 11(4), 2019 – С. 56-70.

4. Козлов, Д. Анализ международного сотрудничества в области противодействия терроризму. Вестник МГИМО-Университета, 12(4), 2019 – С. 141-155. URL: https://cyberleninka.ru/article/n/analiz-mezhdunarodnogo-sotrudnichestva-v-oblasti-protivodeystviya-terrorizmu.

5. Министерство Юстиции РФ. Федеральный список экстремистских материалов. URL: http://minjust.ru/extremist-materials.

6. Организация американских государств. Центр по борьбе с терроризмом. Стратегия ОАГ по борьбе с терроризмом [2011]. http://www.oas.org/cicte/strategy/strategy/pdfs/strategy.pdf.

7. Организация по безопасности и сотрудничеству в Европе [2012]. Декларация по противодействию терроризму. https://www.osce.org/files/f/documents/9/c/103919.pdf.

8. Резолюция Совета Безопасности ООН № 2178 [2014] о предотвращении и пресечении террористических действий, связанных с иностранными боевиками. https://www.un.org/ru/documents/ods.asp?m=S/RES/2178.

9. Соловьев, А. Борьба с терроризмом в современном мире: основные стратегии и подходы. Международная безопасность, 5(2), 2018 – С. 45-56. URL: https://www.researchgate.net/publication/325635996_Bor'ba_s_terrorizmom_v_sovremennom_mire_osnovnye_strategii_i_podkhody.

10. Соловьев, А. Проблемы определения экстремистских и террористических материалов в интернете: международной и национальный опыт. Право и Интернет, (2), 2018 – С. 2-9.

11. Уголовный кодекс Российской Федерации от 13 июня 1996 г. № 63-ФЗ. [Электронный ресурс] http://www.consultant.ru/document/cons_doc_LAW_10699.

12. Федеральный закон «О противодействии экстремистской деятельности» от 25 июля 2002 г. № 114-ФЗ. URL: http://www.consultant.ru/document/cons_doc_LAW_37852.

13. Berger, J. M. (2018). The Development and Anatomy of the Martyrdom Media Complex. The Program on Extremism at George Washington University.

14. Botha, A. (2014). Radicalisation in Kenya. Recruitment to al-Shabaab and the Mombasa Republican Council. Institute for Security Studies. https://issafrica.org/research/papers/radicalisation-in-kenya-recruitment-to-al-shabaab-and-the-mombasa-republican-council.

15. Conway, M. et al. Disrupting Daesh: Measuring Takedown of Online Terrorist Material and Its Impacts. Studies in Conflict & Terrorism, 42(1-2), 2019. – pp. 141-160.

16. Freilich, J. D., Chermak, S. M., Gruenewald, J. A. Mapping Extremist Crimes: A State-Level Analysis of CST Data from 1995 to 2014. Studies in Conflict & Terrorism, 40(4), 2015 – pp. 338-356.

17. Greene, K. J. (2015). Combating Terrorism in a New Media Operating Environment: Toward Legal and Policy Frameworks that Promote Public Safety, Privacy, and the Rule of Law. Yale Journal of International Law, 40(1), – pp. 225-261.

18. Hafez, A., Mullins, C. The Radicalization Puzzle: A Theoretical Synthesis of Empirical Approaches to Homegrown Extremism. Studies in Conflict & Terrorism, 11), 2015. – pp. 958-975.

19. Klausen, J. Tweeting the Jihad: Social media of fighters in Syria and Iraq. Studies in Conflict & Terrorism, 38(1), 2015. – pp. 1-22.

20. Schmid, A. P. (2013). Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review. The International Centre for Counter-Terrorism – The Hague.

21. Shrestha, M., & Adamic, L. A. (2019). Quantifying the Effectiveness of Detection Algorithms in Identifying Extremist Content Online. In Proceedings of the Thirteenth International Conference on Web and Social Media.

22. Valenzuela-Morales, J. (2020). Network Analysis: A Means to Study Organizational Structures of Extremist Groups and Transnational Criminal Organizations. International Behavioral Neuroscience Society.

Сведения об авторах

Жмурко Даниил Юрьевич, кандидат экономических наук**,** доцент, старший преподаватель кафедры информатики и математики Краснодарского университета МВД России; e-mail: danis1982@list.ru.

Кунгбала Моконзикуа Нарцисс Сильвер, следователь национальной полиции третьего округа (префектуры) бригадир (капитан полиции) Центральноафриканской Республики (ЦАР) (г. Банги).

Журбин Григорий Евгеньевич,
Акименко Григорий Александрович,
Купцов Павел Васильевич

НЕКОТОРЫЕ ВОПРОСЫ ПЕРЕДАЧИ ШИРОКОПОЛОСНОГО ТЕЛЕВИЗИОННОГО СИГНАЛА ПО УЗКОПОЛОСНЫМ ЛИНИЯМ СВЯЗИ

Видеоизображение находит большое применение, причём ареал распространения очень сильно увеличивается. Большое количество видеокамер можно увидеть в любом месте города. Видеоинформация используется для решения различных задач. Имеет место широкое распространение систем охранного телевидения, позволяющих контролировать доступ к наиболее важным объектам критической информационной структуры любых сотрудников и граждан. Так, например, все электроподстанции в городе Ростов-на-Дону, обеспечены системой охранного телевидения. Видеоинформация должна размещаться и храниться в соответствии с требованиями действующего законодательства [1] в течение двух месяцев. В каждом охраняемом объекте нерентабельно создавать сервер для хранения видеоинформации. Поэтому есть смысл размещать видеосервер в головном офисе. Тогда возникает вопрос о передаче видеоинформации на расстояние по имеющимся каналам связи между сервером и объектами наблюдения. Видеоинформация может содержать в себе персональные данные сотрудников. Следовательно, передача видеоинформации должна происходить по защищенным линиям связи, либо через интернет или по телефонной линии связи с использованием технологий VPN.

В качестве закрывающей аппаратуры могут использоваться программно-аппаратные решения, сертифицированные ФСТЭК. Применение криптографических решений будет сопровождаться снижением скорости передачи видеоинформации в канале. Не всегда имеется возможность передачи сигналов СОТ по широкополосным каналам связи.

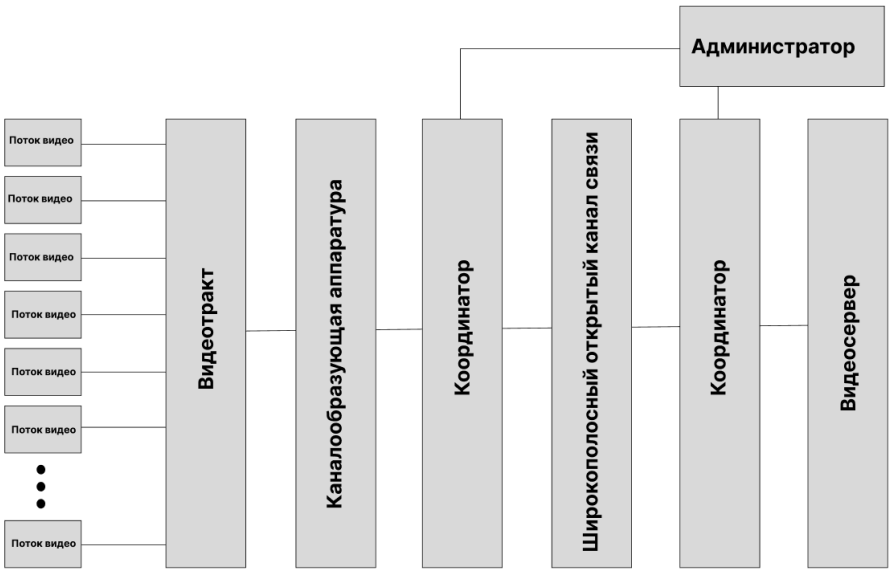


Рис. 1. Схема варианта передачи сигнала СОТ на видеосервер по широкополосному каналу

Таким образом, для решения задачи передачи видеоинформации в реальном масштабе времени неизбежно разрешение противоречия между низкой скоростью доступных узкополосных каналов связи и широкополосной природой видеосигнала, усиленной избыточностью криптографической обработки.

Для разрешения противоречия необходимо согласовать широкополосный сигнал с узкополосным каналом связи. Для этого можно использовать различные методы, среди них:

MP4 – Формат MP4/MPEG-4, выпущенный в 2001 году в соответствии со стандартом ISO/IEX 14496-1:2001, использует технологию кодирования AAC, которая предусматривает сжатие с потерями для недопущения копирования данных пользователем [2].

Вейвлет-преобразования, которые с помощью группировки значений полусуммы и полуразности яркости пикселов меняют их диапазон, позволяя использовать меньшую разрядность, тем самым сжимают видеоинформацию [3].

После применения сжатия уменьшается количество разрядов кодирования единицы информации, содержащейся в одном пикселе изображения, тем самым

снижается требование к быстродействию линии передачи. В случае невозможности передачи сжатой видеоинформации в режиме реального времени по узкополосному каналу связи предлагается распараллелить передаваемую информацию между несколькими каналами связи.

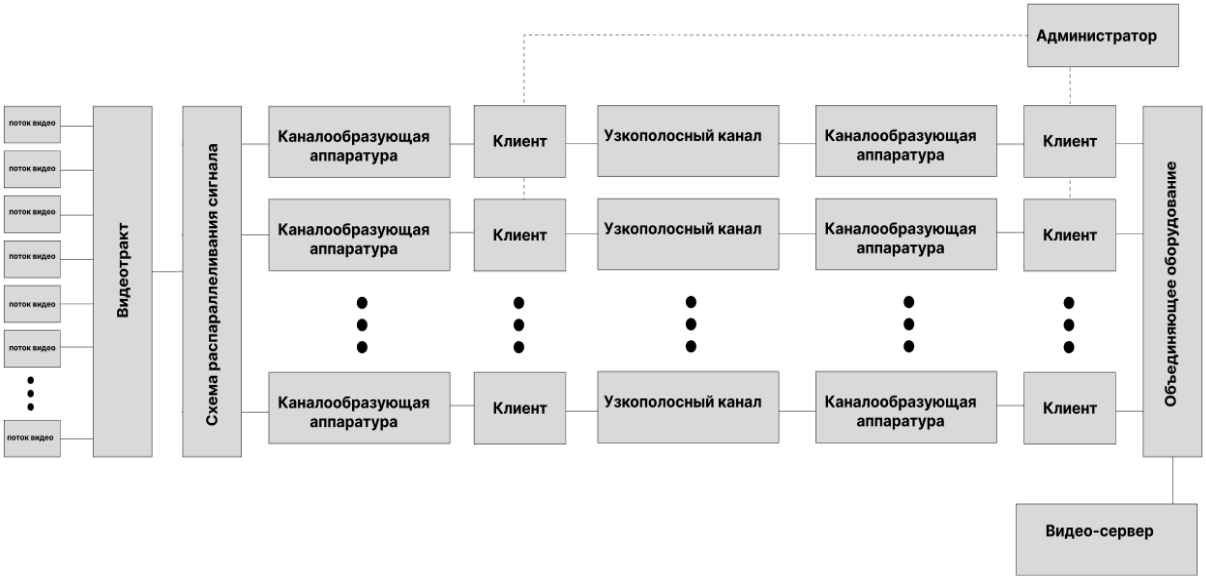


Рис. 2. Структурная схема передачи видеоизображения по узкополосным каналам от СОТ к серверу видеоизображения

Авторами предлагается несколько вариантов распараллеливания информации. Функциональные схемы предлагаемых решений представлены на рисунках 3-5.

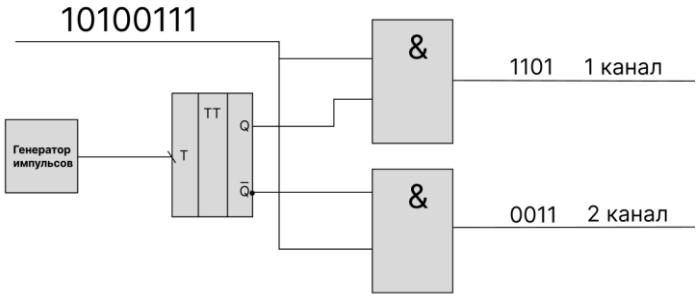


Рис. 3. Двухканальное распараллеливание потока информации

Схема состоит из генератора импульсов, Т-триггера и элементов «И».

При передаче кода 10100111 происходит его распараллеливание на два потока информации 1101 и 0011, снижая в два раза требования к пропускной способности канала.

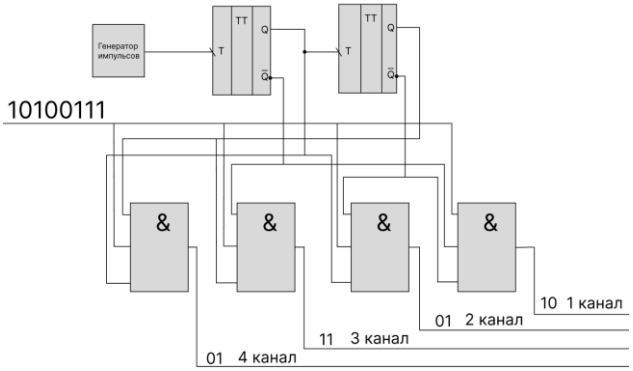


Рис. 4. Четырёхканальное распараллеливание потока информации

Схема включает в себя генератор импульсов, счётчик импульсов на двух Т-триггерах, и четыре логических элементов «И».

При передаче кода 10100111 происходит его распараллеливание на четыре потока информации 10; 01; 11; 01. Требование к пропускной способности канала снижаются в четыре раза.

Аналогичным способом работает и восьмиканальное распараллеливание потока информации.

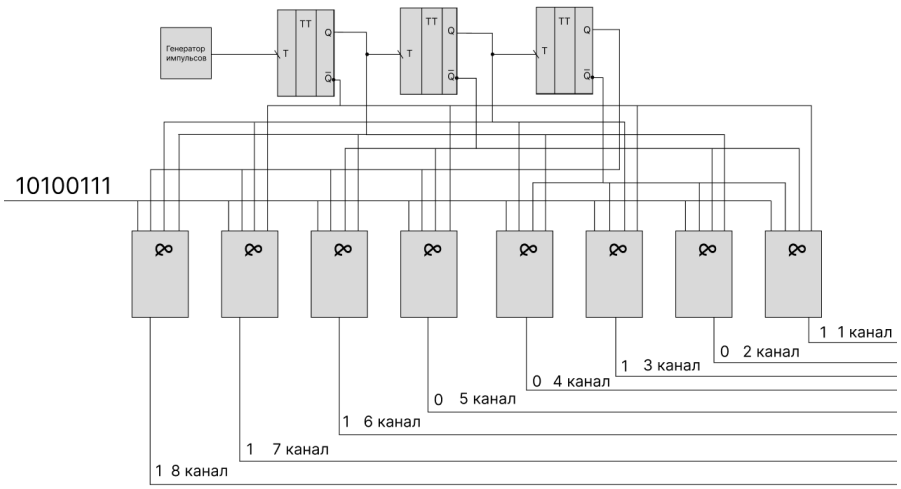


Рис. 5. Восьмиканальное распараллеливание потока информации

Таким образом, передающее устройство производит демультиплексирование передаваемого сообщения на 2^n каналов. Приёмное

устройство производит обратный процесс. Таким образом, функциональные схемы объединения потоков в приёмном устройстве примут вид, представленный на рис. 6-8:

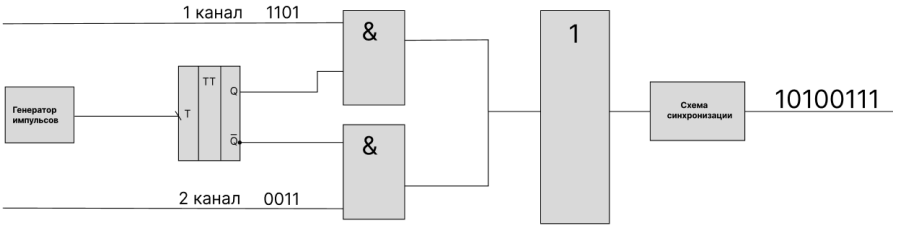


Рис. 6. Схема объединения двух каналов

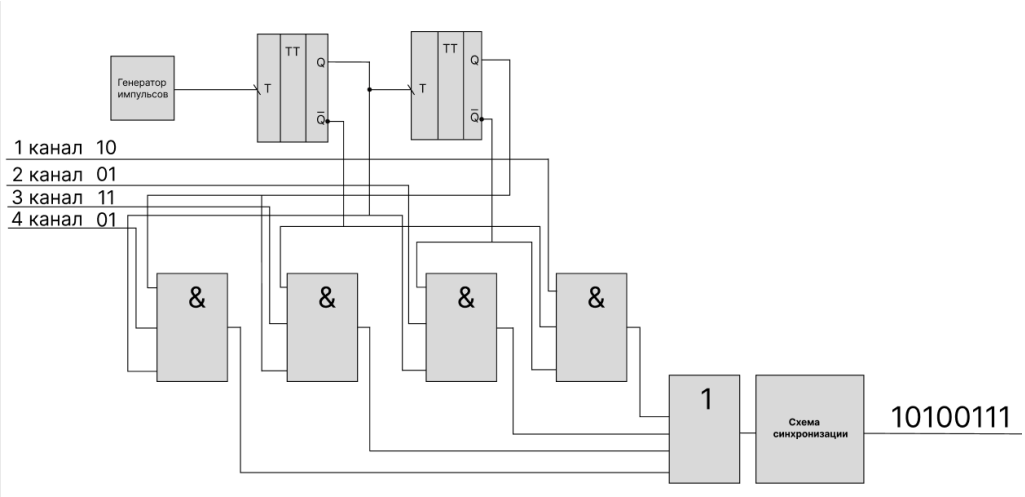


Рис. 7. Схема объединения четырех каналов

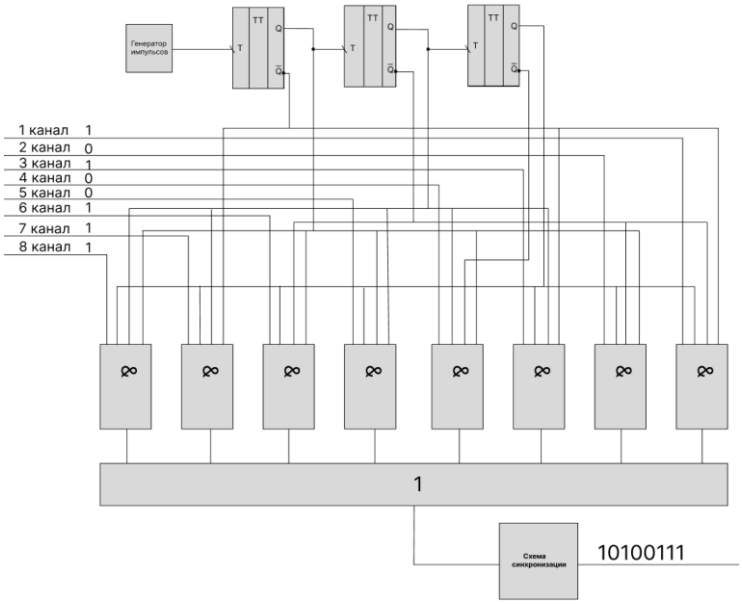


Рис. 8. Схема объединения восьми каналов

Таким образом, в зависимости от пропускной способности имеющихся в наличии узкополосных каналов, применяя предложенные методы сжатия и распараллеливания широкополосного потока видеоинформации можно добиться ее передачи по нескольким узкополосным каналам без закупок дорогостоящего широкополосного линейного оборудования.

Литература

1. Федеральный закон от 6 июля 2016 г. N 374-ФЗ "О внесении изменений в Федеральный закон "О противодействии терроризму" и отдельные законодательные акты Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности" "Российская газета" от 8 июля 2016 г. N 149.

2. Карякин В.Л. Цифровое телевидение: учебное пособие для вузов, 2-е изд., переработанное и дополненное / В.Л. Карякин. – М.: СОЛОН-ПРЕСС, 2013. – 448с.

3. Вейвлет-анализ в примерах: Учебное пособие. / Нагорнов О.В., Никитаев В.Г., Простокишин В.М., Тюфлин С.А., Проничев А.Н., Бухарова Т.И., Чистов К.С., Кашафутдинов Р.З., Хоркин В.А. – М.: НИЯУ МИФИ, 2010. – 120 с.

Сведения об авторах

Журбин Григорий Евгеньевич, кандидат технических наук, доцент кафедры автоматики и телемеханики Южно-Российского государственного политехнического университета имени М.И. Платова; e-mail: gregazov@yandex.ru.

Акименко Григорий Александрович, факультет информационных технологий и управления Южно-Российского государственного политехнического университета имени. М.И. Платова; e-mail: grigoriq2002@gmail.com.

Купцов Павел Васильевич, факультет информационных технологий и управления Южно-Российского государственного политехнического университета имени М.И. Платова; e-mail: pavel.kuptsov.2002@yandex.ru.

Иванов Вячеслав Юрьевич

ИСПОЛЬЗОВАНИЕ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОПРЕДЕЛЕНИЯ ПРИМЕРНОГО РОСТА ЧЕЛОВЕКА

Обработка эмпирических данных – наиболее востребованная функция в тех областях деятельности, где сложно выявить функциональные зависимости между параметрами. Для этих целей привычно использовать достижения математической статистики, основанные на подсчете математического ожидания, среднеквадратического отклонения, осуществления регрессионного и корреляционного анализа, проверки критериев Пирсона, Колмогорова-Смирнова и т.д. Однако в современном мире с появлением искусственного интеллекта, некоторые задачи можно решить гораздо проще и наиболее эффективно.

Не вдаваясь в оценку выбора тех или иных методов искусственного интеллекта, рассмотрим пример использования модели дерева решений для определения роста человека по длине его стопы на основании эмпирических данных, полученных в результате исследования 8459 человек 16 национальностей из которых 3804 мужчин и 4655 женщин. Их возраст варьировался от 11 до 63 лет [1-3]. (рис. 1)

	A	B	C	D	E	F	G	H
1	cpol	nlen_st	nrost	nvozrast	nves	ctelo	cmesto	
2	1	280	170,0	19	58	0	1	
3	0	250	170,0	21	54	1	1	
4	1	290	174,0	47	64	1	1	
5	0	230	158,0	45	67	1	1	
6	1	280	174,0	24	56	0	1	
7	0	250	169,0	21	55	1	1	
8	0	250	170,0	24	57	0	1	
9	0	240	164,0	44	74	1	1	
10	1	250	174,0	25	76	1	1	
11	1	250	170,0	36	72	1	1	
12	1	260	181,0	46	80	0	0	
13	0	245	161,0	38	65	1	1	
14	0	250	171,0	34	77	1	1	

Рис. 1. Входные эмпирические данные в виде Книги MS Excel

Столбцами таблицы являлись следующие значения:

- cpol – пол человека, «0» - женщина, «1» - мужчина;

- nlen_st – длина босой стопы человека в мм;
- nrost – рост человека в см;
- nvozrast – возраст человека в годах;
- nves – вес человека в кг;
- ctelo – телосложение, «0» - «худощавое», «1» - «среднее», «2» - полное;
- cmesto – место жительство до совершеннолетия, «0» - «деревня, село», «1» - город.

Первым шагом в любом проекте машинного обучения является ознакомление с данными. Для этого воспользуемся библиотекой Pandas языка программирования Python 3. Pandas — это основной инструмент, который используется для изучения и манипулирования данными. Также нам понадобится библиотека openpyxl для работы с таблицами Microsoft Excel.

Для установки данных библиотек в командной строке выполним следующие команды:

pip install pandas;

pip install openpuxl.

Наиболее важной частью библиотеки Pandas является фрейм данных, который представляет из себя таблицу, похожую на лист MS Excel или таблицу данных SQL. Для работы с таким типом данных у Pandas есть очень хорошие методы, которые позволят нам обработать первоначальный эмпирический материал и получить на основе него модель машинного обучения для определения примерного роста человека по длине его стопы.

```
# подключение библиотеки pandas с именем pd
import pandas as pd

name_file = "D:/YandexDisk/Python/foot/foot.xlsx"
# создаем фрейм данных из книги Microsoft Excel (...foot.xlsx) и сохраняем его в data_file
data_file = pd.read_excel(name_file)
# вывод фрейма данных не экран
print(data_file)
```

Рис. 2. Перевод книги Microsoft Excel во фрейм данных библиотеки Pandas

Напишем код, который переводит книгу Microsoft Excel во фрейм данных библиотеки Pandas (рис. 2).

Результат работы данного кода указан ниже (рис. 3)

```
      cpol  nlen_st  nrost  nvozrast  nves  ctelo  cmesto
0        1      280  170.0        19  58.0      0       1
1        0      250  170.0        21  54.0      1       1
2        1      290  174.0        47  64.0      1       1
3        0      230  158.0        45  67.0      1       1
4        1      280  174.0        24  56.0      0       1
...    ...      ...    ...       ...   ...    ...     ...
8454     1      253  176.0        20  64.0      1       0
8455     1      264  172.0        21  70.0      2       0
8456     1      256  174.5        22  74.0      1       0
8457     1      268  181.0        23  78.0      2       0
8458     1      272  182.5        18  69.0      1       0

[8459 rows x 7 columns]

Process finished with exit code 0
```

Рис. 3. Результат работы кода

Для реализации модели дерева решений нам необходимые входные тестовые данные для ее обучения. В качестве входных параметров возьмём следующие колонки: cpol (пол), nlen_st (длина стопы), nvozrast (возраст), nves (вес), ctelo (телосложение) и cmesto (место жительства до совершеннолетия). На выходе мы должны получить рост человека nrost (рис. 4).

```
# входные данные
x_hangle = ['cpol', 'nlen_st', 'nvozrast', 'nves', 'ctelo', 'cmesto']
x = data_file[x_hangle]
# выходные данные
y = data_file.nrost
```

Рис. 4. Данные для модели дерева решений

Библиотека Pandas позволяет нам случайным образом разбить наши данные на 2 части, первую часть для обучения (переменные train_x, train_y), а вторую часть для проверки (val_x, val_y). Это позволит проверить полученную модель на качество прогнозирования примерного роста человека. Для создания

модели дерева решений воспользуемся библиотекой sclicit-learn, в коде она записывается как sklearn (рис. 5).

```
# подключение библиотеки sclicit-learn для создания модели дерева решений
from sklearn.tree import DecisionTreeRegressor
# подключение функции train_test_split для разделения данных на 2 части
from sklearn.model_selection import train_test_split
# разделение данных на 2 части
train_x, val_x, train_y, val_y = train_test_split(x, y)
# создание модели дерева решений
data_model = DecisionTreeRegressor(random_state=1)
# обучение модели
data_model.fit(train_x, train_y)
# получение примерного роста человека по входным параметрам после обучения модели
prognostic = data_model.predict(val_x )
# вывод полученных значений примерного роста человека
print("Предсказанные значения роста: ", prognostic)
# вывод тестовых значений роста человека
print("Тестовые значения роста: ", val_y.values)
```

Рис. 5. Создание модели дерева решений

В результате работы получим следующий результат (рис. 6)

```
C:\Users\ivsl7\AppData\Local\Programs\Python\Python39\python.exe D:/YandexDisk/Python/foot/test.py
Предсказанные значения роста:  [165.  159.  177.  ... 179.5 157.  160. ]
Тестовые значения роста:  [165. 165. 175. ... 175. 153. 160.]

Process finished with exit code 0
```

Рис. 6. Результат работы

Для проверки качества полученной модели найдём среднюю абсолютную ошибку между предсказанными и тестовыми значениями. Для этого воспользуемся функцией mean_absolute_error библиотеки sclicit-learn (рис. 7)

```
# подключение функции mean_absolute_error для определения средней абсолютной ошибки
from sklearn.metrics import mean_absolute_error
# нахождение средней абсолютной ошибки
mistake = mean_absolute_error(val_y, prognostic)
print(mistake)
```

Рис. 7. Нахождение средней абсолютной ошибки

После запуска данного кода получим следующий результат (рис. 8)

```
C:\Users\ivsl7\AppData\Local\Programs\Python\Python39\python.exe D:/YandexDisk/Python/foot/test.py
4.104261623325453

Process finished with exit code 0
```

Рис. 8. Результат работы

Как видно средняя абсолютная ошибка составляет примерно 4.1 см. Однако возникает вопрос, можно ли уменьшить эту ошибку? Для решения этого вопроса сравним абсолютную среднюю ошибку для моделей дерева решений различной степени глубины. Напишем функцию, которая в качестве входного параметра будет принимать значение максимального количества листовых узлов модели дерева решений max_leaf_nodes, а возвращать среднюю абсолютную ошибку (рис. 9)

```
def get_mae(max_leaf_nodes, train_X, val_X, train_y, val_y):
    model = DecisionTreeRegressor(max_leaf_nodes=max_leaf_nodes, random_state=0)
    model.fit(train_X, train_y)
    preds_val = model.predict(val_X)
    mistake = mean_absolute_error(val_y, preds_val)
    return mistake
```

Рис. 9. Функция нахождения средней абсолютной ошибки

Используем эту функцию и рассмотрим значения средней абсолютной ошибки со следующими максимальными количествами листовых узлов: 5, 25, 50, 100, 250, 500, 1000, 2500 и 5000. (рис. 10)

```
# создадим массив с различными значениями максимальных листовых узлов
candidate_max_leaf_nodes = [5, 25, 50, 100, 250, 500, 1000, 2500, 5000]
# найдём среднюю абсолютную ошибку для каждого количества узлов
my_mae = {leaf_size: get_mae(leaf_size, train_x, val_x, train_y, val_y) for leaf_size in candidate_max_leaf_nodes}
# посмотрим массив ошибок
for i in my_mae:
    print(i,": ",my_mae[i])
# найдём наименьшую ошибку
min_mae = min(my_mae, key=my_mae.get)
print("Минимальное значение ошибки при max_leaf_nodes = ",min_mae, ": ",my_mae[min_mae])
```

Рис. 10. Поиск минимальной средней абсолютной ошибки

```
C:\Users\ivsl7\AppData\Local\Programs\Python\Python39\python.exe D:/YandexDisk/Python/foot/test.py
5 :  4.686313702032456
25 :  4.101950915773701
50 :  4.042352460868977
100 :  3.9499947606448966
250 :  3.915069835042892
500 :  3.9692297961278156
1000 :  4.031026276224999
2500 :  4.275865630701896
5000 :  4.145807722616234
Минимальное значение ошибки при max_leaf_nodes =  250 :  3.915069835042892

Process finished with exit code 0
```

Рис. 11. Результат работы программы

В соответствии с результатами работы программы видно, что минимальное значение ошибки достигается при максимальном количестве листовых узлов равном 250 и составляет примерно 3,9 см.

Следовательно, на основании построенной модели дерева решений мы можем предсказывать вероятный рост человека на основании длины его стопы и ряда других факторов со средней абсолютной ошибкой 3,9 см.

Литература

1. Максимов, Н.В. Влияние разных факторов на зависимость между ростом и длиной стопы человека // Судебная экспертиза. 2017. № 3 (51). С. 37-48.

2. Чулахов В.Н., Машин Н.К., Максимов Н.В. Об антропометрической зависимости между длиной стопы и ростом у новорожденных детей и взрослых // Судебно-медицинская экспертиза. 2018. Т.61. №3. С.27-30.

3. Чулахов В.Н., Максимов Н.В. О закономерностях распределения значений роста человека для конкретной длины стопы // Судебно-медицинская экспертиза. 2019. Т.62. №4. С.30-36.

Сведения об авторе

Иванов Вячеслав Юрьевич, кандидат технический наук, доцент кафедры информатики и компьютерных технологий Санкт-Петербургского горного университета императрицы Екатерины II; e-mail: Ivanov_VYu@pers.spmi.ru.

Иванов Игорь Петрович,
Жмурко Даниил Юрьевич

ПРОГНОЗЫ И ПЕРСПЕКТИВЫ РАЗВИТИЯ WEB3 С УЧЕТОМ ВЗАИМОДЕЙСТВИЯ ТЕХНОЛОГИЙ МУЛЬТИЧЕЙН И L2-РЕШЕНИЙ

В статье анализируется развитие технологий WEB3, появление которых способно привести к новому этапу расширения интернета. Главный акцент сделан на применение мультичейн и L2-решений для решения актуальных проблем технологии блокчейн, таких как масштабируемость, безопасность и производительность сетей. Рассматриваются основные прогнозы и перспективы их взаимодействия в области децентрализованных приложений и веб-инфраструктур.

Введение

WEB3, или децентрализованный интернет, является технологией будущего, призванной обеспечить существенное расширение возможностей современных интернет-сервисов [1]. Мультичейн и L2-решения представляют собой ключевые инновации, способные обеспечить трансформацию блокчейн и повышение производительности сетей [2]. В данной статье будут рассмотрены (исследованы) прогнозы и перспективы применения этих технологий в области WEB3.

Мультичейн технологии

Данные технологии предусматривают создание многочисленных параллельных блокчейн-сетей, обеспечивающих легкий переход активов и информации между сетями [3]. Благодаря мультичейн системам, сети способны легко интегрироваться и решать проблемы масштабируемости, обеспечивая увеличение производительности систем. Примерами платформ, предоставляющих мультичейн решения, являются Polkadot [4] Cosmos [5].

L2-решения

L2-решения (решения второго уровня) направлены на повышение масштабируемости и производительности блокчейн-сетей за счет использования off-chain транзакций и других инновационных механизмов [6]. Такие решения

позволяют разгружать основные сети, сокращая нагрузку и обеспечивая ускорение обработки транзакций на низком уровне. Примерами таких решений являются Plasma [7], а также L2-решения на базе Ethereum, такие как Optimistic Rollup [8] и ZK-rollup [9].

Интеграция мультичейн и L2-решений для решения существующих проблем ИТ индустрии

С развитием блокчейн технологий возрастает необходимость решения проблем масштабируемости, производительности и интероперабельности между различными блокчейнами и L2-решениями, такими как каналы передачи состояния, структуры хранения и вложенные блокчейны [1]. Мультичейн представляет собой связь между различными блокчейнами, позволяющую обеспечить интероперабельность и разработку децентрализованных приложений (dApps) без ограничений одной платформы [2].

Обзор проблем масштабируемости и производительности

Одной из ключевых проблем блокчейн-технологии является ограниченная масштируемость и производительность. Биткоин и Ethereum, два самых популярных блокчейна, сегодня сталкиваются с проблемами задержек и высоких комиссий из-за ограниченности обработки транзакций в блоках [3]. Для решения проблемы масштабируемости, предложено два подхода. Один из них заключается в использовании L2-решений, другой – в формировании межцепочных сетей, так называемого мультичейна [4].

Подходы к интеграции мультичейн и L2-решений

Использование каналов передачи состояния

Каналы передачи состояния приводят к высокой пропускной способности путем оффчейн обработки транзакций и обновления состояний блокчейна. Примером такой технологии является Lightning Network для блокчейна Биткоина [5]. Мультичейн-интеграция с каналами передачи состояния состоит в создании каналов между различными блокчейнами для выполнения непосредственных оффчейн транзакций и обеспечения интероперабельности.

Применение плазма

Плазма является L2-решением, которое позволяет создавать дочерние блокчейны отдельно от основной цепочки [6]. Основные блокчейны сравнивают состояние дочернего блокчейна в случае спорных транзакций. Используя мультичейн-концепцию, эти дочерние блокчейны могут быть интегрированы с другими блокчейнами для обеспечения эффективной передачи сообщений и ценности.

Работа вложенных блокчейнов

Вложенные блокчейны связаны с основным через двусторонние каналы или «язычки» (англ. peg), которые позволяют передачу токенов и других данных между различными цепочками. Поскольку эти цепочки работают параллельно, они могут обрабатывать свои собственные транзакции без необходимости одобрения или подтверждения со стороны основного блокчейна. Таким образом, вложенные блокчейны способствуют децентрализации и созданию модульных, персонализированных решений для различных потребностей [16].

Преимущества вложенных блокчейнов

Вложенные блокчейны предлагают ряд преимуществ для пользователей и разработчиков блокчейн-приложений. Они обеспечивают высокую пропускную способность и низкую задержку, так как транзакции осуществляются локально в каждой цепочке, что уменьшает нагрузку на основную сеть. Кроме того, снижаются транзакционные издержки, так как менее крупные транзакции не видны для участников основной цепи.

Вложенные блокчейны также обеспечивают улучшенную безопасность и конфиденциальность, поскольку пользователи могут передавать информацию между цепочками без раскрытия данных всем участникам сети. Наконец, эти подсистемы предоставляют разработчикам возможность создавать более гибкие и масштабируемые приложения, которые могут адаптироваться к различным нуждам пользователей [15].

Недостатки и сложности вложенных блокчейнов

Несмотря на их преимущества, существуют и некоторые сложности, связанные с использованием вложенных блокчейнов. Одним из отрицательных

моментов вложенных блокчейнов является сложность координации и поддержания согласованности данных между различными цепочками. Ошибки, возникающие при передаче данных, могут привести к рискам безопасности и некорректной работе системы. Кроме того, создание и поддержание вложенных блокчейнов требует дополнительных временных и финансовых затрат на разработку, тестирование и развертывание.

Примеры использования вложенных блокчейнов

Вложенные блокчейны используются в различных отраслях и сферах применения, таких как: финансы, образование, логистика и государственное управление. Примеры разработанных проектов включают составные и децентрализованные финансовые платформы, решения для цифровой идентификации и приватность, а также многоуровневые системы голосования и сертификации [13].

Таким образом, вложенные блочейны представляют собой перспективное решение, которое позволит устранить ограничения, связанные с производительностью и масштабируемостью традиционных блокчейн-сетей. Они обеспечат гибкость, безопасность и возможность кастомизации для создания специализированных подходов и решений.

1. *Финансы*. Децентрализованные финансовые платформы (DeFi) используют вложенные блокчейны для оптимизации операций лендинга, стейкинга и торговых операций. В частности, проекты, такие как Plasma, xDai и OMG Network предоставляют решения для масштабирования сетей Ethereum, разрабатывая параллельные цепочки для обработки транзакций быстрее и дешевле.

2 *Образование*. Вложенные блокчейны могут быть использованы для цифровой сертификации образовательных документов, таких как дипломы и сертификаты курсов. Например, проект Blockcerts предлагает решение для создания, выдачи и верификации цифровых документов на основе блокчейна с использованием вложенных цепочек.

3. *Логистика*. В промышленности и сфере логистики, вложенные блокчейны могут обеспечивать безопасное и прозрачное отслеживание товаров, от производителя до конечного потребителя. Примером может служить проект VeChain, который использует параллельные цепочки для улучшения управления поставками и обеспечения сетифицированного контроля качества продукции.

4. *Государственное управление.* Технологии блокчейна могут реализоваться в государственном управлении для обеспечения прозрачности голосования и сертификации. Вложенные блокчейны могут быть использованы для разработки многоуровневых систем, которые позволят гражданам подтверждать свою личность и голосовать онлайн с минимальными рисками мошенничества и подлога.

Приведенные примеры иллюстрируют широкий спектр возможностей вложенных блокчейнов и их качественный потенциал для улучшения различных отраслей и сфер деятельности человека. Они могут привести к более эффективным, безопасным и прозрачным решениям для множества глобальных направлений деятельности [14].

Прогнозы и перспективы развития

1. Объединение мультичейн и L2-решений для создания экосистем.

В перспективе, лидерами блокчейн технологии станут платформы, способные предлагать собственные решения по масштабируемости и производительности. Вместе с этим ожидается активное развитие совместных проектов и продуктов на основе мультичейн и L2-решений для осуществления комплексного подхода к повышению производительности сетей [10].

2. Создание децентралилизованных приложений (dApps) и веб-инфраструктур.

Мультичейн и L2-решения способствуют созданию более мощных и эффективных децентрализованных приложений (dApps) [11]. Работа dApps на мультичейн-системах позволит обеспечивать лучшую оптимизацию, быстроту и надежность работы, что будет способствовать их более широкому распространению. В рамках WEB3, совокупное применение мультичейн и L2-

решений предварительно ожидается в таких областях, как децентрализованные финансы (DeFi) [12], децентрализованный доступ к данным и цифровым системам идентификации, а также создание устойчивых и безопасных сетей обмена информации.

3. Развитие децентрализованных платформ и сервисов.

Технологии WEB3, включая мультичейн и L2-решения, позволит разработчикам создавать децентрализованные платформы и сервисы, обеспечивая при этом значительное улучшение пользовательского опыта и безопасности данных. Предполагается, что благодаря развитию децентрализованных интернет-технологий возникнет новый класс веб-приложений и служб, предоставляющих надежные и гибкие услуги.

4. Рост взаимодействия и интеграции между блокчейн-сетями.

Прогнозируется, что применение мультичейн и L2-решений может привести к развитию «интернета цепочек» (англ. interchain), где блокчейн-сети различных поколений и технологических платформ будут тесно взаимодействовать друг с другом [13], обеспечивая передачу данных и оперирование активами между различными экосистемами. Это может способствовать появлению сильных связей между разными проектами и укрепления децентрализованных экосистем.

Заключение

В данной статье проводится анализ и исследование новых парадигм и возможностей, связанных с развитием Web3.

Во-первых, авторы статьи обращают внимание на то, что Web3 является следующим значительным шагом в эволюции Всемирной паутины и имеет потенциал переопределить интернет, в отличие от того, каким мы его знаем сейчас. Web3 будет основан на децентрализации, безопасности и прозрачности благодаря таким технологиям, как блокчейн, мультичейн и L2-решения.

Во-вторых, в статье изложены ключевые прогнозы и перспективы, связанные с развитием Web3. В частности, авторы подчеркивают, что будущее развитие Web3 будет определено такими факторами, как:

1. Рост применения мультичейн технологии, которая позволяет межсетевое взаимодействие различных блокчейнов и обеспечит более высокую оперативную эффективность, масштабируемость и безопасность.

2. Использование L2-решений, таких как каналы состояния, сайдчейны и плазма, которые обрабатывают транзакции вне основных блокчейнов, что делает их быстрее и экономичнее.

3. Внедрение децентрализованных приложений (dApps), которые будут развернуты на мультичейн и L2-решениях, усиливая изначальные преимущества технологий.

4. Усиление сотрудничества между стартапами, корпорациями и академическим миром для создания надежных и масштабируемых решений в децентрализованном интернете.

5. Создание резервной инфраструктуры и управленческих механизмов для обеспечения долгосрочной устойчивости и успешного развития Web3.

В заключение, авторы подчеркивают, что вышеупомянутые прогнозы и перспективы станут ключевыми направлениями этапов развития децентрализованной мировой паутины. Однако успех Web3 также зависит от устранения ряда сложностей, таких как управление, безопасность и регуляторные меры. Более того, несмотря на значительный технический прогресс, массовое принятие Web3 все еще зависит от разработки релевантных приложений, образованности пользователей и дополнительной интеграции с существующими интернет-экосистемами. Поэтому, перспективы Web3 требуют дальнейших более глубоких исследований, сотрудничества и адаптации, так как они представляют направления создания более открытой, прозрачной и разнообразной интернет-экосистемы.

Следует отметить, что регуляторные органы и правительственные институты играют значительную роль в развитии Web3. Разумные правила и ограничения могут способствовать зрелости и устойчивости Web3, одновременно предотвращая мошенничество, злоупотребления и проблемы безопасности.

При работе над Web3, разработчики и специалисты по интернет-технологиям должны учитывать потребности и ожидания конечных пользователей. Удобство использования, доступность и интуитивно понятный пользовательский интерфейс являются ключевыми элементами для успешного проникновения Web3 на мировой рынок.

Таким образом, статья подчеркивает значение междисциплинарного и интегративного подхода для успешного развития новых веб-технологий. Важно осознавать, что Web3 не является просто технической эволюцией, а представляет собой инновационный путь для создания нового вида интернета, который будет обслуживать интересы общества в целом. Ответственный и осознанный подход к развитию Web3, в сотрудничестве с различными участниками рынка и учетом потребностей пользователей, обеспечит формирование интернета будущего, основанного на децентрализации, безопасности и прозрачности.

Литература

1. Benet J. IPFS – Content Addressed, Versioned, P2P File System, arXiv:1407.3561, 2014.

2. Afshar P., Kasireddy S., Kalodner H., and Shelat A. Blockchain Shift, Proceedings of the 1st ACM Conference on Advances in Financial Technologies, 2019.

3. Baruffaldi A. and Teixeira J.T. Heavy is The Head That Wears The Crown: The Wise Role of The Crypto-Industry in The Contest between Central Bank Digital Currencies, arXiv:2011.00459, 2020.

4. Poon, J. Buterin, V. Plasma: Scalable Autonomous Smart Contracts. Plasma White Paper, 2017.

5. Buterin V.A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum White Paper, 2013.

6. Zohar M. Bitcoin: Under the Hood, Communications of the ACM, vol. 58, no. 9, pp. 104 – 113, 2015.

7. Poon J. and Dryja T. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments, Draft Version 0.5.9.2, 2016.

8. Khalil R. and Gervais A. Revive: Rebalancing off-blockchain payment networks, Proceedings of the 2017 ACM SIGSAC Conference, 2017.

9. Akhtar S. Cosmos – Blockchain Interoperability: Building an Internet of Blockchains, Technical Paper, 2021.

10. Cachin C. Architecture of the Hyperledger blockchain fabric, Workshop on Distributed Cryptocurrencies and Consensus Ledgers, vol. 310, 2016.

11. Bernhard R., Cross-Chain Bridges: Challenges and Opportunities, 2021.

12. Sergey I. Creating and Analyzing a Multichain DeFi Ecosystem: Current Market Conditions, Challenges, and Opportunities, 2021.

13. Danser J. The Emergence of Interchain: A Retrospective on Blockchain Evolution, 2021.

14. Swan M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

15. Mougayar W. (2016). The Business Blockchain: Promise, Practice, and Application of the Next Internet Technology. John Wiley & Sons.

16. Tapscott D., Tapscott, A. Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. Penguin. 2016.

Сведения об авторах

Иванов Игорь Петрович, кандидат педагогических наук, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: iv_on_off@mail.ru.

Жмурко Даниил Юрьевич, кандидат экономических наук, доцент, старший преподаватель кафедры информатики и математики Краснодарского университета МВД России; e-mail: danis1982@list.ru.

Иванушкин Сергей Александрович,
Мальков Алексей Викторович

ПЕРСПЕКТИВЫ РАЗВИТИЯ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ ОТ УТЕЧКИ ПО АКУСТИЧЕСКОМУ РЕЧЕВОМУ КАНАЛУ

На данный момент времени важнейшим направлением в сфере технической защиты информации остается обеспечение акустической защищенности помещений. Дело в том, что переговоры, ведущиеся в помещении, являются самым информативным каналом утечки, к которому предъявляются наибольшие требования по его закрытию. Средой распространения этого канала являются воздух, конструкции и инженерные системы комнаты.

Главными плюсами акустического канала для злоумышленника являются [1]:

– возможность ведения разведки, находясь вне помещения;

– сложность нахождения аппаратуры съёма информации, в особенности той, что находится вне здания;

– большое разнообразие в размещении средств получения данных;

– широкий выбор программно-аппаратных комплексов съема сигнала;

– компактные габариты комплексов, надежность и автономность;

– низкая цена по сравнению с другими системами.

Существующие требования предъявляются в основе своей к информации, которая может содержать государственную тайну. Так или иначе, актуальность проблемы не снижается, когда речь идет о персональных данных, просто требования превращаются в рекомендации.

Защита акустической информации включает в себя пассивные и активные методы [2].

Пассивный метод подразумевает проведение специальных технологических мероприятий во время строительства помещений. Активный метод нацелен на использование акустических и вибрационных помех. Неоспоримым плюсом активных средств защиты является мобильность и узкая

направленность, что и стало следствием их широкого применения.

Если пассивными методами защиты не представляется возможным обеспечить требуемый уровень безопасности, тогда могут применяться генераторы шума.

В генераторах шума основным средством защиты являются защитные помехи типа «Белый шум» или его производные [3].

На сегодняшний день в сфере защиты информации от акустической речевой разведки существует несколько серьёзных проблем:

- постоянное развитие компактных микрофонов, применяемых в различной технике;

- постоянное совершенствование методов распознавания человеческой речи с использованием нейросетевых технологий. Для примера, анализ человеческой речи с помощью Yandex SpeechKit показывает хорошие результаты, а именно 84% правильно распознанных запросов на общую тематику и 94% правильно распознанных запросов на направленную тематику в условиях различных шумов;

- разработка и совершенствование методов шумоочистки акустического сигнала (NVIDIA RTX Voice, iZotope RX). Применение данных методов, упрощает возможность анализа речевой информации в полученном сигнале. Встроенные методы и алгоритмы анализа сигнала, совместно с использованием алгоритмов машинного обучения выводят речевую разведку на качественно новый уровень. Анализ полученной в ходе разведки записи может проводиться в специально оборудованных для этого лабораториях.

Речеподобная помеха может стать решением существующей проблемы. Использование помехи, похожей на человеческую речь, позволит во множестве случаев понизить уровень защитной помехи и снизить возможности злоумышленника по очистке шумов.

Данные помехи похожи по своей структуре на человеческую речь не только по структуре сигнала, но и на слух.

Очевидными плюсами использования этой помехи является то, что её:

- характеристики совпадают с характеристиками записи голоса;

- можно использовать совместно с «Белым шумом»;

- составляющие могут содержать характерные особенности голоса диктора;

- возможно улучшить путем добавления дополнительных голосов, тем самым снижая возможность распознавания речи на 18 – 20% [4].

Дополнительная избыточность в шумовой помехе уменьшит возможность к успешному получению исходного сигнала.

Основной проблемой этой помехи на сегодняшний день остается отсутствие единой терминологии и методики создания речеподобной помехи. Каждый создатель активного генератора шума фактически сам разрабатывает её заново. Это создает множество вариаций помехи, не имеющей фактического подтверждения эффективности каждой из них.

Для определения параметров, влияющих на эффективность данного типа помех, необходимо создать соответствующую методику оценки защищённости речи в помещениях с применением данной помехи. В рамках этого исследования необходимо проанализировать результаты разработок в сфере распознавания человеческой речи, параметров речевого сигнала, влияющих на её словесную разборчивость, которые понадобятся при генерации маскирующих и проверочных сигналов.

Вывод: Существующие методы формирования речеподобной помехи не обладают объективными оценками их эффективности. Новые методы создания помехи должны учитывать современное развитие и возможности распознавания речи. При оценке защищенности речи аналогично необходимо применять актуальные технологические решения в сфере анализа акустических сигналов.

Для создания новой методики оценки защищённости речи в помещениях с применением данной помехи нужно создать модель угроз безопасности речевой информации, включив в неё уязвимости, создаваемые инструментами

машинного обучения.

С целью закрытия акустического речевого канала необходимо использовать активные средства защиты, в основе которых будет применение именно речеподобной помехи. Эти помехи должны быть приведены к единому стандарту и войти в систему сертификации средств активной защиты от акустической речевой разведки.

Литература

1. Алфиренко В.М. Основы защиты информации: Практикум для студ. спец. «Техническое обеспечение безопасности» и «Моделирование и компьютерное проектирование радиоэлектронных средств» дневной, вечерней и заочной форм обучения: В 2 ч. Ч.1/В.М. Алефиренко, Ю.В. Шамгин. – Мн.: БГУИР, 2004. – 43 с.

2. Киреев К.К., Русин Н.А., Заборских П.С. Елгин Ю.И. Основные параметры и разновидности речеподобных сигналов, применяемых для защиты речевой информации / Сборник КВВУ им. Штеменко, 2020.

3. Дидковский В.С., Дидковская М.В., Продеус А.Н. Акустическая экспертиза каналов речевой коммуникации. – Киев, 2008. – 420 с.

4. Покровский Н.Б. Расчет и измерение разборчивости речи. – М.: Связьиздат, 1962.

Сведения об авторах

Иванушкин Сергей Александрович, начальник научно-исследовательской лаборатории Краснодарского высшего военного училища имени генерала армии С.М. Штеменко; e-mail: nr.kvvu@yandex.ru.

Мальков Алексей Викторович, научный сотрудник научно-исследовательской лаборатории Краснодарского высшего военного училища имени генерала армии С.М. Штеменко**.**

Ивкин Артем Валерьевич,
Вызулин Сергей Александрович,
Годовых Оксана Васильевна

АВТОМАТИЗАЦИЯ КОНТРОЛЯ ПОДЛИННОСТИ ЭЛЕКТРОННЫХ ДОКУМЕНТОВ И ИХ ИНФРАСТРУКТУРЫ В СИСТЕМЕ ЗАЩИЩЕННОГО ИНФОРМАЦИОННОГО ОБМЕНА

Аннотация. В статье рассматривается разработка универсальной подсистемы автоматизированного контроля подлинности инфраструктуры электронных документов и информационных процессов в системе защищенного информационного обмена. Актуальность разработки определяется необходимостью создания единой системы информационного обмена в Вооружённых Силах Российской Федерации.

Ключевые слова: система защищенного информационного обмена, блокчейн технологии, смарт-контракты, электронная подпись, электронный документ.

В Вооружённых Силах Российской Федерации (ВС РФ) используются разного рода автоматизированные системы (АС). Эти системы не взаимоувязаны и обеспечивают только информационный обмен неформализованными графическими и текстовыми файлами. Данный факт не позволяет эффективно осуществлять управление подразделениями в условиях современных конфликтов. Информационное пространство ВС РФ не является единым. Распределенная инфраструктура хранения и обработки данных не создана. Нет единых правил и порядка описания, представления, формирования и использования информационных ресурсов, как следствие, отсутствует единая система защиты не только при передаче, но и при хранении информации [1].

Необходимо создать единую (взаимоувязанную) систему информационного обмена (ЕСИО) ВС РФ, обладающую:

1) устойчивостью к деструктивным воздействиям;

2) адаптивностью на всех звеньях управления к изменениям обстановки, состава сил и средств;

3) унифицированностью и формализованностью информационных процессов в защищенном сегменте АС ВН и управление ими.

Добиться таких качеств АС можно путем внедрения перспективных организационных и технических решений и технологий для организации информационной безопасности [2].

Задача организации защиты информации в ЕСИО ВС РФ актуальна.

Цель работы – разработать универсальную подсистему автоматизированного контроля подлинности инфраструктуры электронных документов (ЭД) и информационных процессов в системе защищенного информационного обмена.

Возможный способ решения задачи защиты информации – совместное применение:

блокчейн технологии [3];

технологии электронной подписи (ЭП) [4];

технологии цифровых смарт-контрактов (договоров) (СК) [5].

Это позволит:

многократно повысить эффективность информационного обмена ВС РФ, соединений и воинских частей вплоть до отдельного военнослужащего;

построить единую систему идентификации пользователей в АС ВН и обеспечить юридическую значимость информационных процессов;

регламентировать условия доступа ко всем информационным объектам, реализовать ролевую модель разграничения доступа [6].

Требования к подсистеме многоуровневого автоматизированного контроля подлинности инфраструктуры электронных документов (ЭД) в системе защищенного информационного обмена: многоуровневый контроль инфраструктуры ЭД, унифицированность и формализованность информационных процессов в защищенном сегменте АС ВН и управление ими.

Для автоматизации контроля подлинности ЭД и их инфраструктуры в системе защищенного информационного обмена разработана подсистема

трехуровневого контроля инфраструктуры и ЭД на основе технологии распределенных реестров.

Автоматическая проверка подлинности инфраструктуры ЭД осуществляется на уровнях:

транзакций в цепной блочной записи в распределенном реестре;

сертификата электронной подписи;

смарт-контракта.

Блок-схема предлагаемой многоуровневой подсистемы контроля подлинности ЭД представлена на рисунке 1.

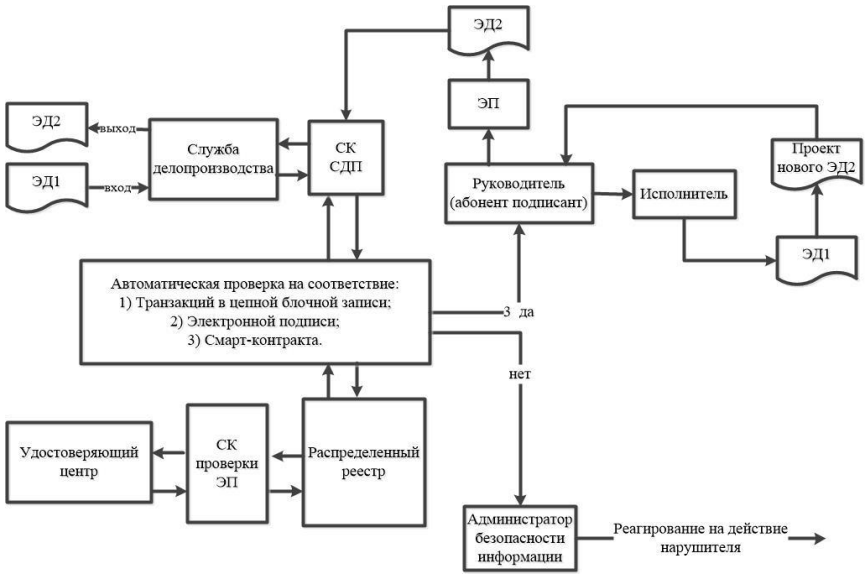


Рис. 1. Блок-схема подсистемы трехуровневого контроля подлинности ЭД

В результате строится гибкая система принятия решения руководителем о её подлинности. Автоматическое информирование администратора безопасности информации о нарушении инфраструктуры ЭД позволяет своевременно выявлять и реагировать на действия нарушителя.

Структура многоуровневой подсистемы контроля подлинности ЭД.

Распределенный реестр. Распределенный реестр формируется из СК взаимодействия узлов и транзакционных пар, сформированных в результате исполнения смарт-контрактов. Распределенный реестр имеет структуру цепной блочной записи данных. Для каждого блока реестра формируется метка времени.

Синхронизация и обработка данных в распределенном реестре осуществляется на основе правил, записанных в СК, в соответствии с политикой информационной безопасности.

Усовершенствованная электронная подпись. Подписание созданного ЭД осуществляется усовершенствованной электронной подписью (УЭП). УЭП автоматически программно генерируется в виде отдельного файла. Файл УЭП формируется на основе ключа ЭП и суммы значений хэш-кода цифрового отпечатка (ЦО) ЭД и хэш-кода ЭД. Генерация ЦО осуществляется программно. ЦО формируется на основе избыточной информации об ЭД и идентификатора абонента. УЭП является средством подтверждения подлинности экземпляров ЭД. Процесс формирования ЦО ЭД, подписания УЭП и записи в блокчейн представлен на рисунке 2.

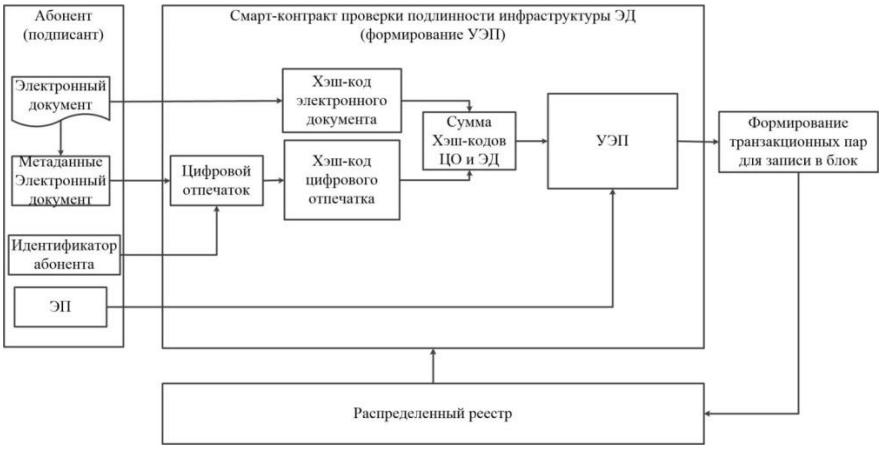


Рис. 2. Подписание созданного ЭД. Автоматическое формирование регистрирующей записи в распределенном реестре

ЦО ЭД предназначен для формирования УЭП и осуществления узлом СДП контроля доступа к экземплярам ЭД и контроля формирования электронных копий, созданных на их основе.

Смарт-контракт. Смарт-контракт взаимодействия абонента со службой делопроизводства (СК АБ с СДП) функционирует с целью автоматической регистрации действий с ЭД и контроля доступа к нему.

Все транзакции в системе автоматически (программно) подтверждаются и записываются в реестр. В случае если абонент-подписант не сформировал УЭП и не записал ее в транзакцию запроса о подтверждении регистрации проекта ЭД, СК АБ с СДП автоматически оповещает администратора узла СДП об отсутствии УЭП.

Смарт-контракт взаимодействия абонента с удостоверяющим центром (СК АБ с УЦ) функционирует с целью выдачи данных о текущем статусе сертификата ключа проверки ЭП абонента или с целью отзыва сертификата ключа проверки ЭП узлом АРМ абонента, имеющего на это право.

Алгоритм определения текущего статуса сертификата ключа проверки ЭП заключается с поиска в распределенном реестре момента записи СК АБ с УЦ до момента последнего присоединенного к цепи блока подтвержденной транзакционной пары узла АРМ абонента, в которой СК АБ с УЦ выдал код ответа, означающий, что «статус сертификата ключа проверки ЭП абонента с блокчейн-адресом отозван». Если данная транзакционная пара автоматически найдена, то данный код ответа копируется в транзакцию запроса о текущем статусе сертификата ключа проверки ЭП, в противном случае – программно формируется код ответа, означающий, что «статус сертификата ключа проверки ЭП абонента с блокчейн-адресом действительный».

Алгоритм отзыва сертификата ключа проверки ЭП реализован на основе применения метода «Доказательство с нулевым разглашением ZK STARK». В качестве хэш-кодов, необходимых для формирования корня дерева Меркла, который записывается в СК АБ с УЦ, используются поля данных сертификата ключа проверки ЭП и «кодовое слово» для его отзыва. СК АБ с УЦ, обрабатывая транзакции запросов в распределенном реестре в случае, если в теле транзакции найден код запроса об отзыве сертификата ключа проверки ЭП и запись в виде хэш-кода «кодового слова», формирует корень дерева Меркла и сравнивает его с корнем, который был записан в СК АБ с УЦ при его начальной записи в распределенный реестр. Если данные идентичны, то вырабатывается код ответа

и добавляется к исходной транзакции запроса, означающий, что «статус сертификата ключа проверки ЭП абонента с блокчейн-адресом отозван». Сформированная транзакционная пара автоматически записывается в распределенный реестр, после чего она считается подтвержденной.

Вывод**:** разработана многоуровневая подсистема автоматизированного контроля подлинности инфраструктуры электронных документов для системы защищенного информационного обмена.

Трехуровневая проверка инфраструктуры электронного документа обеспечивает гибкую систему принятия решений руководителем о подлинности инфраструктуры поступившего ЭД путем:

проверки идентификационных метаданных файлов, записанных в блокчейн-систему;

проверки подлинности ЭП на основе применяемых смарт-контрактов процессов обработки запросов узлов;

применения нового способа формирования транзакций и проверки структуры распределенного реестра.

Литература

1. Концепция развития единого информационного пространства Вооруженных Сил Российской Федерации на период до 2027 года.

2. Ивкин А.В., Вызулин С.А., Годовых О.В., «Технология распределенного реестра (блокчейн) в обеспечении защищенного электронного документооборота» Сборник трудов XXVI Международная научно-техническая конференция «Радиолокация, навигация, связь» (RLNC 2020), секция 1 Общие проблемы передачи и обработки информации. Цифровая обработка сигналов. г. Воронеж, 2020 Т.2 – с. 44-48.

3. Приказ Министерства цифрового развития, связи и массовых коммуникаций РФ от 23 апреля 2020 г. N 195 «Об утверждении методик расчета показателей федерального проекта «Цифровые технологии» национальной программы «Цифровая экономика Российской Федерации» (Дорожная карта

развития «сквозной» цифровой технологии «Системы распределенного реестра»).

4. Федеральный закон ФЗ-63 «Об электронной подписи» от 6 апреля 2011 г.

5. Постановление Правительства РФ N 1750 от 28 октября 2020 г. «Об утверждении перечня технологий, применяемых в рамках экспериментальных правовых режимов в сфере цифровых инноваций».

6. Ивкин А.В., Вызулин С.А., Годовых О.В., «Система защиты информации Единого информационного пространства на основе технологии распределенных реестров (блокчейн)» Сборник трудов XXVIII Международной научно-технической конференции «Радиолокация, навигация, связь» (RLNC 2022) г. Воронеж, 2022 Т.1 367с. – 251-258.

Сведения об авторах

Ивкин Артем Валерьевич, кандидат технических наук, заместитель начальника отдела - начальник научно-исследовательской лаборатории Краснодарского высшего военного училища имени генерала армии С.М. Штеменко; e-mail: artemdtuproff@gmail.com.

Вызулин Сергей Александрович, доктор физико-математических наук, доцент, старший научный сотрудник научно-исследовательской лаборатории Краснодарского высшего военного училища имени генерала армии С.М. Штеменко; e-mail: vyzulin@mail.ru.

Годовых Оксана Васильевна, младший научный сотрудник научно-исследовательской лаборатории Краснодарского высшего военного училища имени генерала армии С.М. Штеменко; e-mail: o.godovykh@mail.ru.

Карпика Анатолий Григорьевич,
Лемайкина Светлана Владимировна

МЕТОДЫ ПРОТИВОДЕЙСТВИЯ БЕСПИЛОТНЫМ ЛЕТАТЕЛЬНЫМ АППАРАТАМ, ИСПОЛЬЗУЕМЫМ В НЕЗАКОННЫХ ЦЕЛЯХ

Быстрое распространение БПЛА привело к увеличению их неправомерного использования в незаконных целях, включая несанкционированное наблюдение, контрабанду, террористические атаки и нарушение работы критически важной инфраструктуры.

Незаконные летательные аппараты создают ряд проблем, которые вызывают все большую обеспокоенность у органов государственной власти, правоохранительных органов и общественности. Анализ материалов, представленных в прессе, аналитических статьях, позволил выявить ряд ключевых проблем, связанных с использованием аппаратов в незаконных целях.

Вторжение в частную жизнь. БПЛА, оснащенные камерами, используются для несанкционированного наблюдения, вторжения в частную жизнь людей или сбора конфиденциальной информации. Они могут совершать полеты над территорией, на которой находятся объекты частной собственности, общественными местами, а также над зонами ограниченного доступа, записывая видеоматериалы, делая снимки без согласия собственника, или уполномоченного органа.

Угрозы безопасности. Устройства могут использоваться и активно используются в качестве инструментов для создания и эскалации инцидентов в области безопасности, включая террористические акты, перевозку (сопровождение) контрабандных, или незаконных грузов, проведение воздушных атак. Вариативное конструктивное исполнение обеспечивает возможность перемещения в различных средах, а достаточная грузоподъемность позволяет использовать их в качестве потенциального транспортного средства для доставки взрывчатых веществ, наркотиков, или оружия.

Нарушение критически важной инфраструктуры. Операторы БПЛА способны воздействовать на критически важную инфраструктуру, такую, как

аэропорты, электростанции, правительственные, общественные здания либо физически повреждая объекты, либо вмешиваясь в ее работу.

Проблемы общественной безопасности. Безответственное или незаконное использование беспилотных аппаратов может поставить под угрозу общественную безопасность. Они могут мешать операциям по реагированию на чрезвычайные ситуации, сталкиваться с пилотируемыми летательными аппаратами, вызывать аварии, врезаясь в людей или транспортные средства.

Риски кибербезопасности. Дроны, использующие беспроводные системы связи, уязвимы для взлома или кибератак. Несанкционированный доступ к системе управления дроном может позволить злоумышленникам получить контроль над дроном, изменить траекторию его полета, перехватить данные, которые он собирает.

Этические проблемы: неправомерное использование дронов поднимает этические дилеммы, особенно в отношении конфиденциальности, наблюдения и возможности неизбирательного нацеливания. Баланс между преимуществами технологии дронов и этическими соображениями имеет решающее значение для обеспечения ответственного и законного использования.

Анализ открытых источников [1], [2], [3] позволил классифицировать основные типы БПЛА по ряду признаков.

1. Конструкция крыла.

Дроны с неподвижным крылом – дроны имеют конструкцию, аналогичную традиционным самолетам. Им требуется взлетно-посадочная полоса для взлета и посадки и они обычно используются для полетов на большие расстояния, аэрофотосъемки или наблюдения. Дроны с роторным крылом, также известные как многороторные дроны. Эти устройства имеют несколько винтов, которые обеспечивают вертикальный взлет и посадку.

2. Цель применения.

Коммерческие дроны. Предназначены для различных коммерческих приложений, таких как аэрофотосъемка и видеосъемка, проверка инфраструктуры, сельское хозяйство, службы доставки и геодезия.

Военные дроны. Специально разработаны для военных операций, включая наблюдение, разведку, обнаружение целей и выполнение боевых задач.

Рекреационные дроны. Предназначены для личного использования и развлечения. Часто используются для аэрофотосъемки, видеосъемки и развлекательных полетов.

Исследовательские дроны. Используются для научных исследований, мониторинга окружающей среды, отслеживания дикой природы и сбора данных. Они оснащены различными датчиками и инструментами для сбора определенных данных.

3. Массо-габаритные показатели.

Микродроны. Размером с ладонь или меньше. Имеют небольшой вес, высокую маневренность.

Минидроны. Несколько больше, чем микродроны, но все же компактны и портативны. Популярны среди любителей, оснащены камерами для аэрофотосъемки или гонок.

Дроны малого и среднего размера. Относятся к более широкому диапазону размеров и обычно используются для профессиональных приложений, таких как аэрофотосъемка, инспекции и наблюдение.

Большие и тяжелые дроны. Значительны по размеру и могут нести более тяжелые полезные нагрузки. Они используются для таких задач, как промышленные инспекции, поисково-спасательные работы, перевозка грузов различного назначения.

4. Конструктивные особенности:

Автономные дроны. Оснащены современными навигационными системами, датчиками и алгоритмами искусственного интеллекта, которые позволяют им работать независимо, без вмешательства человека.

Гибридные дроны. Сочетают в себе черты как самолетов, так и вертолетов, обеспечивая преимущества вертикального взлета и посадки, а также эффективного полета вперед. Могут переключаться между вертикальным и горизонтальным режимами полета.

Роевые дроны. Работают группами или роями, координируя свои действия для коллективного выполнения задач. Они могут общаться друг с другом и сотрудничать для достижения таких целей, как наблюдение, поисковые операции или картографирование.

Следует отметить, что приведенная классификация дронов не может считаться исчерпывающей, т.к. по мере развития технологий и разработки новых приложений могут появляться новые классификационные категории.

Противодействие беспилотным летательным аппаратам включает в себя обнаружение, отслеживание и идентификацию, обезвреживание.

Обнаружение – первый шаг в противодействии их неправомерному использованию. Для обнаружения применяются:

Радары и радиочастотные датчики. Могут находить дроны, анализируя их радиочастотные сигнатуры, и предоставлять информацию в режиме реального времени об их местоположении, высоте и скорости.

Электрооптические и инфракрасные датчики. Обнаруживают дроны с помощью визуального и тепловизионного изображения.

Акустические датчики. Обнаруживают отчетливые звуки, издаваемые дронами. Анализируя акустическую сигнатуру, эти датчики могут различать дроны и другие воздушные объекты.

Отслеживание и идентификация. После обнаружения БПЛА, имеют решающее значение отслеживание его перемещений и идентификация оператора. Некоторые технологии, используемые для этой цели, включают:

GPS (ГЛОНАС) отслеживание. Используя технологию геопозионирования, дроны можно отслеживать в режиме реального времени, что теоретически позволяет правоохранительным органам отслеживать траектории их полета и определять их место отправления и назначения.

Системы идентификации дронов. Присваивают аппаратам уникальные идентификационные коды, что позволяет идентифицировать оператора и отслеживать действия дрона.

Компьютерное зрение и искусственный интеллект. Позволяют

анализировать изображения или видеоматериалы с дронов для определения модели устройства, оператора и исходящих потенциальных угроз.

Обезвреживание. Для обезвреживания незаконных дронов и предотвращения их деятельности по прямому назначению разработаны различные меры противодействия, в том числе:

Заглушение и спуфинг GPS. Заглушение сигналов GPS может нарушить работу навигационной системы дрона, лишив его возможности поддерживать заданную траекторию полета. Spoofing атака на GPS – атака, которая пытается обмануть GPS-приемник, широковещательно передавая немного более мощный сигнал, чем полученный от спутников GPS, такой, чтобы быть похожим на ряд нормальных сигналов GPS. Эти имитировавшие сигналы изменены таким способом, чтобы заставить получателя неверно определять свое местоположение, считая его таким, какое отправит атакующий.

Подавление сигналов связи. Заглушая сигналы связи между дроном и его оператором, можно помешать аппарату получать команды или передавать данные, фактически отключая его функции.

Оружие направленной энергии. Использует лазеры или мощные микроволновые лучи для вывода из строя или уничтожения дронов. Эти технологии могут нарушить работу электроники дрона, повредить его компоненты или привести к потере управления.

Перехватчики дронов и системы сеток. Дроны-перехватчики, оснащенные сетями или другими механизмами захвата, могут физически захватывать незаконные дроны в полете, не давая им достичь намеченных целей.

Решения в области кибербезопасности. Направлены на недопущение захвата, или взлома БПЛА злоумышленниками с целью их контроля.

Таким образом, можно сделать следующие выводы. Несмотря на достаточно широкий арсенал технологий противодействия, по мере развития технологии БПЛА развиваются и методы, используемые злоумышленниками.

В связи с этим, для создания опережающего задела в этой области, необходимо вести постоянные исследования и разработки, обеспечивая

требуемую эффективность мер противодействия преступному использованию БПЛА. Сочетая технологические инновации с совершенствованием нормативно-правовой базы, возможно обеспечить лучшее решение проблем, связанных с незаконным использованием подобных устройств, в интересах защиты общественной безопасности, конфиденциальности и критически важной инфраструктуры.

Литература

1. Классификация БПЛА по летным характеристикам // [Электронный документ] https://docs.geoscan.aero/ru/master/database/const-module/classification/classification.html // Дата ознакомления: 01.06.2023.

2. Типы беспилотных летательных аппаратов. Обзор. // [Электронный документ] https://aviatest.aero/articles/tipy-bespilotnykh-letatelnykh-apparatov-obzor/ / Дата ознакомления: 01.06.2023.

3. В.С. Фетисов, Л.М. Неугодникова и др. «Беспилотная авиация: терминология, классификация, современное состояние». // [Электронный документ] https://arsenal-info.ru/b/book/3398882726/1 / Дата ознакомления: 01.06.2023.

Сведения об авторах

Карпика Анатолий Григорьевич, кандидат технических наук, доцент кафедры информационного обеспечения органов внутренних дел Ростовского юридического института МВД России; e-mail: akarpika@yandex.ru.

Лемайкина Светлана Владимировна, начальник кафедры информационного обеспечения органов внутренних дел Ростовского юридического института МВД России; e-mail: lemajkina67@mail.ru.

Кенжалиева Светлана Заировна,
Ожиредов Михаил Юрьевич,
Беленький Валентин Дмитриевич

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ ДЛЯ РАЗРАБОТКИ ФУНКЦИОНАЛЬНОЙ СХЕМЫ ЛИНЕЙНОГО И РЕВЕРСИВНОГО РЕКУРРЕНТНОГО РЕГИСТРА

В современных условиях, когда постоянно расширяются возможности разведки противника и приобретает все большее значение фактор внезапности, из-за наличия у противоборствующих сторон средств ядерного нападения, роль скрытого управления войсками резко возрастает. В этих условиях повышенные требования предъявляются и к средствам защиты информации, которые должны обеспечить надежное сохранение втайне от противника содержания передаваемых сведений, их достоверность и высокую оперативность.

Проблема обеспечения скрытого управления войсками – задача сложная и многообразная. Важное место в ее решении принадлежит специальной связи. Материальной основой специальной связи являются математические основы криптографической защиты информации (МОКЗИ). Отмеченные обстоятельства определяют также необходимость высоких темпов дальнейшего развития теоретических и практических аспектов использования МОКЗИ.

Безопасность специальной связи обеспечивается комплексом организационно-технических мероприятий, среди которых важное место занимает обеспечение безопасности криптографических алгоритмов. Стойкость любого криптографического алгоритма сосредоточена в ключе. Криптографические ключи должны иметь достаточную длину и случайные значения битов. Следовательно, секретные ключи представляют собой основу криптографических преобразований.

Основная проблема классической криптографии заключается в трудности генерирования случайных двоичных последовательностей большой длины с применением короткого случайного ключа. Для получения ключей применяются датчики псевдослучайных чисел.

Приведём некоторую необходимую справку о рекуррентном регистре сдвига с линейной обратной связью и далее опишем созданную нами учебную программу разработки последовательности линейного рекуррентного реверсивного регистра сдвига - RRS.

Регистр – это схема, состоящая из связанных между собой однобитовых элементов памяти. Такие схемы умеют записывать, хранить, считывать n-разрядные двоичные данные. Предлагается рассмотреть вид регистра, называемый регистром сдвига. Это сдвиговый регистр битовых слов, у которого значение входного бита однозначно задается некоторой функцией, исходя из значений остальных битов регистра до сдвига. Чаще всего регистр сдвига собирается на основе последовательно соединенных D-триггеров, притом количество этих триггеров равно числу разрядов n. Регистр сдвига может представлять собой некоторую электрическую схему, составленную из дискретных компонентов: транзисторов, резисторов, также может быть интегрирован в микросхему или же реализован в программе.

Добавление обратной связи превращает регистр сдвига в генератор псевдослучайных чисел, который находит широкое применение в криптографии. ПСП — последовательность чисел, которая была вычислена по некоторому определённому арифметическому правилу, но имеет все свойства случайной последовательности чисел в рамках решаемой задачи.

Линейный рекуррентный регистр (ЛРР) сдвига - генератор двоичной псевдослучайной последовательности, основанный на рекуррентном соотношении

$$a_{n+k} = a_{k-1}a_{n+k-1} + a_{k-2}a_{n+k-2} + \cdots + a_2a_{n+2} + a_1a_{n+1} + a_0a_n,$$

$$\forall i(a_i \in GF(2)), \forall j(a_j \in GF(2)).$$

Полученная таким образом ПСП задается многочленом $P_k(x) = x^k + a_{k-1}x^{k-1} + a_{k-2}x^{k-2} + \cdots + a_2x^2 + a_1x + a_0$, над полем Галуа GF(2).

Регистры сдвига с линейной обратной связью (РСЛОС) издавна применяются в качестве генераторов псевдослучайной последовательности для

потоковых шифров (особенно в военной криптографии). Однако РСЛОС представляет собой линейную схему и в некоторых случаях может быть легко взломан. Например, криптоаналитик может перехватить часть зашифрованного текста и по нему с помощью алгоритма Берлекэмпа-Мэсси восстановить РСЛОС минимального размера, который имитирует оригинальный РСЛОС. Затем перехваченный текст может быть подан на полученный регистр и расшифрован.

На сегодняшний день из открытых разработок нелинейных поточных шифров наибольшую популярность получили три класса алгоритмов. Это комбинирующие, фильтрующие и динамические поточные шифры. Все они в качестве базовых элементов используют линейные рекуррентные регистры сдвига, причем только те, которые порождают последовательности наибольшей длины. Во всех трех методах основной целью становится получение большого периода порождаемой гаммы, высокой нелинейности, устойчивости к атакам по открытому тексту и корреляционным атакам.

Фильтрующие шифры имеют, пожалуй, наиболее простую структуру из нелинейных поточных шифров. Они строятся на базе одного ЛРР созданием от его ячеек дополнительных отводов, никак не связанных с отводами обратной связи. Значения, получаемые по этим отводам, смешиваются на основе какой-нибудь нелинейной функции – фильтра. Бит-результат данной функции подается на выход схемы как очередной бит гаммы.

Комбинирующие шифры строятся на основе нескольких ЛРР, объединяя нелинейной функцией биты, порождаемые каждым из них на очередном шаге. Одной из основных проблем комбинирующих шифров является возможность просачивания информации из одного или нескольких ЛРР в выходную гамму.

Специальное учебное программное обеспечение предназначено для построения схемы и выходной последовательности RRS с линейной обратной связью.

Предварительная установка ПО не требуется, его можно переписать в заранее определенную пользователем папку и запускать напрямую оттуда.

Ввод пользователем полинома

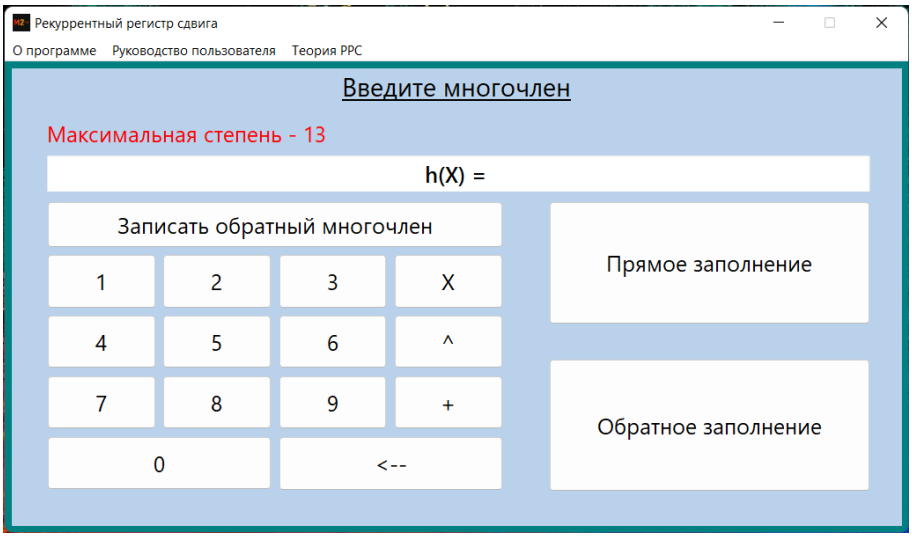


Рис.1. Интерфейс ввода полинома

После ввода полинома пользователь выбирает какое заполнение ему нужно выполнить (прямое или обратное) и нажимает на соответствующую кнопку. Далее открывается окно, в котором нужно ввести количество шагов и начальное заполнение таблицы выходной последовательности.

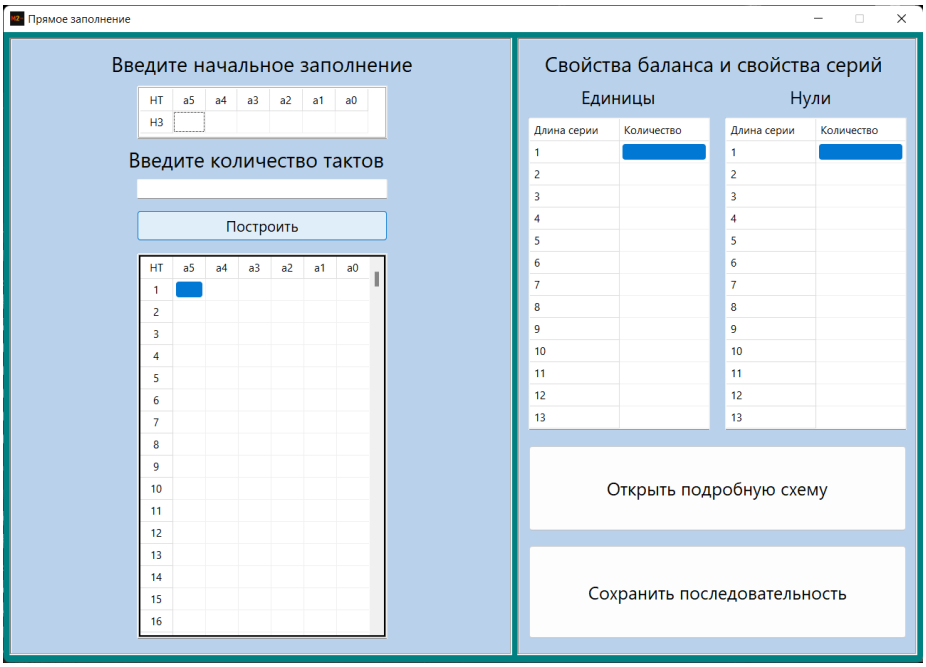


Рис. 2. Прямое (обратное) заполнение

Модуль построения таблицы выходной последовательности: при нажатии на кнопку «Построить» заполняется таблица выходной последовательности, а также производится подсчёт количества серий нулей и единиц в выходной последовательности.

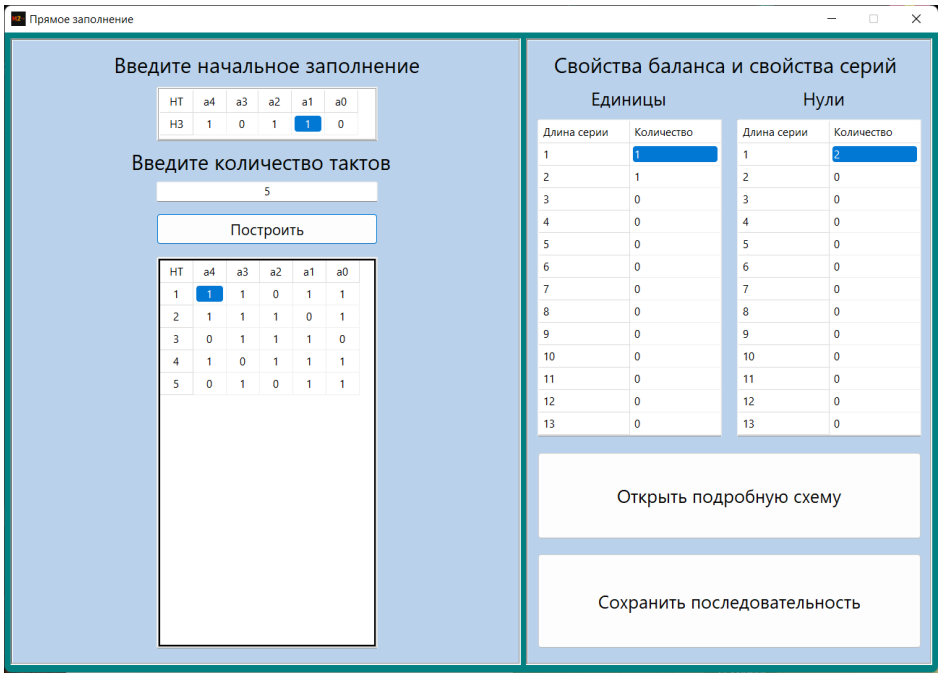


Рис. 3. Прямое (обратное) заполнение

Модуль построения схемы: при нажатии на кнопку «Открыть подробную схему» строится схема. При необходимости перерисовать схему нужно нажать на кнопку «Обновить».

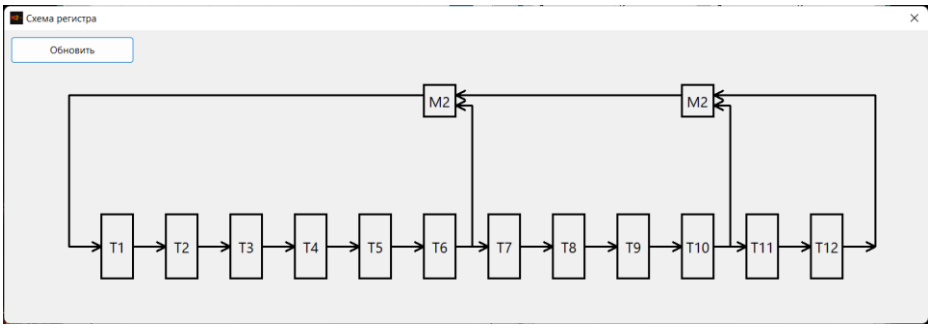


Рис. 4. Схема РРС

Модуль сохранения выходной последовательности: при необходимости сохранить выходную последовательность нужно нажать на кнопку «Сохранить последовательность» и выбрать текстовый файл, в который будет записана последовательность.

Для оказания методической помощи при работе со специальным учебным программным обеспечением RRS – реализации процедур шифрования данных

гаммированием в автоматизированных системах военного назначения для операционных систем Windows, приводятся методические рекомендации.

Методические рекомендации разработаны в соответствии с ГОСТ 19.505-79 ЕСПД «Руководство оператора. Требования к содержанию и оформлению», содержат рекомендации по корректному использованию программного продукта операторами и требования по обеспечению работоспособности программного продукта на ПЭВМ оператора.

Литература

1. Сизоненко А.Б., Меньших В.В. Функциональное моделирование и синтез аппаратных криптографических средств защиты информации на линейных рекуррентных регистрах сдвига. // Журнал радиоэлектроника -2015 - № 4 – С. 1-7.

2. Сизоненко А.Б. Параллельная схемотехническая реализация линейного рекуррентного регистра сдвига // Проектирование и технология электронных средств - 2012 - № 2 - С. 43-47.

Сведения об авторах

Кенжалиева Светлана Заировна, кандидат педагогических наук, доцент Краснодарского высшего военного училища имени генерала армии С.М. Штеменко; e-mail: szk67@mail.ru.

Ожиредов Михаил Юрьевич, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко; e-mail: Ozhiredovip@mail.ru.

Беленький Валентин Дмитриевич, Краснодарское высшее военное училище имени генерала армии С.М. Штеменко; e-mail: val174rus1@mail.ru.

Кирюшин Иван Иванович,
Осинцева Людмила Михайловна

ФОРМИРОВАНИЕ ЦИФРОВЫХ КОМПЕТЕНЦИЙ И НАВЫКОВ ОБУЧАЮЩИХСЯ ПРИ ИСПОЛЬЗОВАНИИ СОВРЕМЕННЫХ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Современная Россия ориентирована на экономическое и социальное развитие общества, следовательно, она нуждается в компетентных специалистах, повышении роли и значения их подготовки в системе профессионального образования. При этом сам процесс развития общества обусловлен значительным увеличением информационных потоков, ростом научно-технического прогресса, внедрением цифровых технологий во все сферы жизнедеятельности, в том числе, и в образование.

Цифровые технологии в образовании – это способ организации современной образовательной среды. Многие сферы деятельности переходят на цифровые системы.

Эксперты все чаще говорят о переходе, прежде всего, школьной программы (как основной) на электронный формат. Когда эта задумка воплотится в жизнь, изменится не только система образования, но и ее смысл и предназначение.

Учебные материалы, планы, занятия, журналы и дневники – все это перейдет на онлайн-версии. Обучающиеся смогут участвовать в учебном процессе, не выходя из дома. Будут созданы электронные ресурсы, на которых они найдут подробную информацию для занятий. Учебные заведения будут оснащены современными технологиями: компьютерами и планшетными панелями. В каждом учебном заведении установят интернет для доступа к информационному контенту. Преподавателям придется обучаться новой системе образования. Эта профессия полностью изменится. Цифровизация подразумевает самостоятельное изучение материала. Педагог выступит в роли

помощника, куратора, к которому придется обращаться лишь при необходимости [3].

Ни для кого не секрет, что использование цифровых технологий считается основным требованием во многих профессиональных областях. Это требование в первую очередь относится к образованию. С помощью цифровых технологий преподаватели могут эффективнее преподносить учебный материал и возможности обучения значительно расширятся.

Изменения в сфере формирования ключевых компетенций у выпускников общеобразовательных учреждений стремительно меняются, человек все больше «погружается» в цифровую среду, что, в свою очередь, ведет к увеличению компонентов в структуре такой компетенции, в большей степени, в рамках неформального образования. Это относится и к студентам гражданских образовательных организаций. В образовательных организациях МВД России, в силу специфики организации учебного процесса и быта, таких возможностей меньше.

Формирование профессиональных компетенций у обучающихся в образовательных организациях системы МВД России средствами цифровых образовательных технологий заключается в поиске педагогических решений профессиональной подготовки будущего работника системы МВД, когда у него, наряду с формированием компетенций, обусловленных требованиями стандарта, сформирована потребность обретения ключевых компетенций, появляющихся вследствие стремительного развития ИКТ.

Особенности и специфика формирования профессиональной компетенции при обучении в образовательных организациях системы МВД России.

В период карантина при пандемии в 2020 году Барнаульский юридический институт был полностью переведен на дистанционное обучение.

В современной педагогической науке проблема индивидуализации неразрывно связана с понятием дифференциации обучении. Индивидуализация современного образовательного процесса, как способ повышения его общей

эффективности, имеет достаточно богатую историю развития в отечественном высшем образовании, начинающуюся ещё в советское время. Попытки индивидуализации, предпринимаемые педагогами – новаторами того времени, в основном, заключались в индивидуальном подходе к студентам, определяемом их способностями и уровнем подготовленности, и, в конечном итоге, сводились к дифференциации обучения. Анализируя эту ситуацию, необходимо учитывать особенности отечественной внутренней политики в области идеологии, в сфере влияния которой, безусловно, находилась и высшая школа.

При высоком уровне подготовки преподавательского состава вузов, отличной инженерной подготовке специалистов – выпускников вузов, внесших существенный вклад в научный и технический потенциал Родины, нельзя не отметить методическую ограниченность учебного процесса стандартными формами проведения занятий: лекциями, практическими и лабораторными занятиями по естественно-научным и техническим дисциплинам, семинарами по гуманитарным. Тем временем, теоретические разработки и практические наработки зарубежных и отечественных педагогов в направлении индивидуализации учебного процесса уже в современной трактовке этого термина, складывались в единую систему – теорию индивидуализации.

Организация образовательного процесса, кроме своей прямой задачи – образования обучающегося, решает и ряд социально-психологических задач. В первую очередь – это формирование социально активной, интеллектуально развитой личности, стремящейся к своему постоянному профессиональному и социальному росту. Для общества такие личности являются источником формирования среднего класса – основы стабильности и благополучия общества.

В педагогическом отношении личности, получающие многоуровневое образование, на последующих его этапах, зачастую, являются активными субъектами образовательного процесса. Попадая под воздействие квалифицировано подобранных фасилитационных факторов, эти субъекты активно развиваются в образовательном, профессиональном и, главное, в

личностном плане. Организуется решение основной задачи индивидуализации – формирование личности, ориентированной на непрерывное обучение.

Усвоение учебного материала обучающимся осуществляется самостоятельно, под руководством преподавателя. Образовательный процесс идёт последовательно на систематической основе в соответствии с целью задания. Дидактическая цель формулируется для обучающегося в соответствующих методических рекомендациях и содержит в себе не только указание на объем изучаемого содержания, но и на уровень его усвоения.

Обучающийся максимум времени работает самостоятельно, учится рациональному самопланированию, эффективной самоорганизации, самоконтролю и адекватной самооценке. Это дает возможность ему осознать себя в деятельности, самому определять уровень усвоения знаний, видеть пробелы в своих знаниях и умениях.

Эта совокупность положительных качеств может вполне обоснованно рассматриваться как личностно-ориентированное направление методики, как средство развития профессиональных компетенций. Каждый обучающийся получает от преподавателя общие рекомендации относительно индивидуальной траектории освоения учебной дисциплины, определяемые его индивидуальным уровнем базовой подготовки по ранее изученным дисциплинам. Кроме того, преподавателем даются конкретные советы и ответы обучающемуся по вопросам, возникающим у него в процессе выполнения заданий на аудиторных занятиях, в ходе пробного тестирования и самостоятельной подготовки. Указанное взаимодействие обучающегося с преподавателем осуществляется в устной форме на аудиторных занятиях, групповых и индивидуальных консультациях, а также в письменной форме с использованием информационных средств и сети Интернет, а также специализированных образовательных локальных корпоративных информационных ресурсах, как вариант взаимодействия с обучающимися, осваивающими учебную программу по заочной форме.

В отношении целей обучения на каждой ступени индивидуальной учебно-образовательной программы сформулированы конкретные задачи, решение и реализация которых позволяет формировать у обучающихся не только субъектную позицию, но и важные для их дальнейшего развития конкретные способы учебно-образовательной деятельности [1].

Из практики реализации индивидуализации обучения можно отметить: возможность выбора обучающимися очной и заочной форм обучения изучаемых дисциплин из списка альтернативных, предлагаемых рабочим учебным планом; высокую степень индивидуализации образовательного процесса обучающихся заочной формы обучения, включающую в себя большинство аспектов из имеющихся в теории индивидуализации. Эта категория обучающихся занимается по наиболее индивидуализированной программе, реализованной именно на этих принципах обучения, по информационным технологиям в деятельности ОВД для различных категорий обучающихся по очной и заочной формам обучения: имеются методические рекомендации по изучению содержания учебного материала темы для обучающихся, планы практических занятий с практическими заданиями для преподавателя, рубежный контроль, итоговый контроль – по мере прохождения, имеются задания различного уровня сложности для учёта уровня индивидуальной подготовки каждого из обучающихся.

Необходимо отметить, что нужны изменения в программах обучения, теоретической части формирования профессиональных компетенций при подготовке специалистов по направлениям «Правовое обеспечение национальной безопасности» и «Правоохранительная деятельность» [2]. Добавить в рабочую программу дидактический материал, содержащий индивидуальный подход, реализованный средствами цифровых образовательных технологий, способствующих эффективному использованию цифровых технологий при получении высшего юридического образования в образовательных организациях системы МВД России.

Литература

1. Газашвили Е.С., Шапранова Л.Г. Индивидуальный подход в обучении или индивидуализация процесса образования? // Материалы V Международной студенческой научной конференции «Студенческий научный форум» URL: https://scienceforum.ru/2013/article/2013006109 (дата обращения: 19.05.2023).

2. Кирюшин И.И. Формирование профессиональных компетенций у обучающихся системы МВД России средствами цифровых технологий. Тенденции развития науки и образования. 2021. № 79-4. С. 84-88.

3. Стукалова, В.О. Достоинства и недостатки цифровизации образования / В.О. Стукалова, В.И. Хомякова // #ScienceJuice2019: Сборник статей и тезисов студенческой открытой конференции, Москва, 18 ноября – 09 2019 года. Том 1. – Москва: Издательство Парадигма, 2020. – С. 397-399. – EDN SRKIMN.

Сведения об авторах

Кирюшин Иван Иванович, старший преподаватель кафедры информатики и специальной техники Барнаульского института МВД России; e-mail: kii22@rambler.ru.

Осинцева Людмила Михайловна, преподаватель кафедры информатики и специальной техники Барнаульского института МВД России; e-mail: osinal77@mail.ru.

Комерцов Вячеслав Викторович

СИСТЕМЫ И КОМПЛЕКСЫ ОБУЧЕНИЯ В ОРГАНАХ ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ

Ведущие тенденции современного развития и функционирования правоохранительных органов Российской Федерации прямо пропорционально зависят от политической и экономической ситуации в стране, а также от всеобщего мирового, регионального и национального направления в развитии как всей мировой тенденции в целом, так и в отдельных требованиях, предназначенных для сотрудников правоохранительных органов.

Помимо этого, стоит отметить, что вся деятельность органов внутренних дел РФ носит специфический характер, который нельзя считать присущим для других образовательных учреждений, поэтому и обучение имеет свою определенную направленность, которая обуславливается определенными дополнительными нагрузками для функционирования всей системы образования.

ОВД – одна из самых действенных структурных организаций в правоохранительной системе Российской Федерации, поэтому и требования к обучению будущих сотрудников носят явно выраженный с начала курса обучения профессиональный характер.

Такой подход к подготовке аргументируется тем, что каждый сотрудник изначально должен иметь представление и понимание всей служебной деятельности, быть не только ответственным в учебной и правовой сфере, но и нести свою службу в порядке, предусмотренном Кодексом отдельной образовательной организации МВД.

Сотрудники органов внутренних дел осуществляют исключительную, сложную и многоуровневую деятельность, связанную с охраной общественного порядка, пресечением и предупреждением преступности, ведают вопросами миграционной первоначальной службы, осуществляют оперативно-розыскную деятельность, а также при введении чрезвычайных ситуаций или военного

положения активно участвуют в новой для них сфере деятельности, оказывая поддержку другим подразделениям и параллельным для них службам.

Ключевые слова: правоохранительные органы, ОВД РФ, обучение сотрудников, профессиональная подготовка.

Введение. В МВД РФ сформирована особая определенная непрекращающаяся система развития и обучения профессиональной деятельности сотрудников, прошедших вступительные испытания. Кадры для ОВД подготавливаются в зависимости от самого профессионального образования: общее образование, профессиональное образование и т.д. Также выделяют на основе профессионального образования специализацию: правоохранительная деятельность и правовое обеспечение национальной безопасности.

От выбранной специализации и образования зависит дальнейшая учёба будущего сотрудника. Так, для двух разных специализаций системой МВД предусмотрена определенная программа, специфические предметы, профессиональная теоретическая и практическая подготовка, а в дальнейшем – практическая деятельность в выбранном территориальном органе.

На постоянной основе в системе МВД РФ функционируют следующие образовательные организации: 3 университета, 4 академии, 13 институтов, 16 филиалов, 6 суворовских военных училищ, кадетский корпус.

Данные образовательные учреждения направлены на формирование у будущих сотрудников ряда профессиональных и общих знаний, которые в будущем станут основой для их деятельности.

Образовательные учреждения составляют учебный план, основываясь на действии нормативно-правовых актов, регулирующих деятельность институтов образовательной системы МВД, а также на собственных Кодексах, составленных руководством института и направленных на конкретизацию определенных норм и статей, предусмотренных в соответствующем ФЗ.

Однако система и комплексы обучения сотрудников ОВД РФ остаются едиными для всех образовательных организаций, в которых обучают будущих сотрудников правоохранительных органов.

Подготовка кадров для системы МВД РФ производится согласно действующим Положениям МВД России с помощью внедрения в образовательную программу профессиональных и других, дополнительных, раскрывающих сущность основного программного обеспечения, направленного на выработку профессиональных знаний у сотрудников.

Система подготовки сотрудников органов внутренних дел формируется благодаря созданной и утвержденной программе образований, обеспечением разработанных программ для научно-педагогических кадров, являющихся постоянным составом образовательной организации и в установлении для них квалификационных требований.

Закон о службе в ОВД четко закрепляет уровень и систему подготовки кадров органов внутренних дел.

Однако основное профессиональное развитие каждого сотрудника МВД необходимо рассматривать через призму самосовершенствования и самообразования кадров правоохранительных органов, в связи с интеграционными явлениями в знании, повсеместном развитии в профессиональной среде, личном росте, изучении нового.

Для сотрудников также предусмотрено заочное обучение, которое проходит в течение нескольких месяцев и направлено на повышение квалификации обучающихся сотрудников, которые уже несли служебную деятельность в органах внутренних дел РФ.

Основной профессиональной тенденцией, вошедшей в российское правоохранительное образование, стало непрерывное обучение. Смысл такого новшества заключается в том, что для каждого сотрудника предусмотрена программа по включению его в современные, профессиональные правоотношения, урегулированные нормами права.

Такая необходимость обуславливается постоянно развивающимися общественными отношениями, появлениями преступных деяний, не урегулированных нормами права (преимущественно в сфере киберпреступности) или способов совершения преступлений. Самообразование, саморазвитие и дополнительное прохождение определенных курсов или иных мероприятий, предусмотренных в соответствующем нормативно-правовом акте, способствуют своевременной адаптации сотрудника к постоянно изменяющимся условиям жизнедеятельности общества.

Комплексы обучения сотрудников органов внутренних дел напрямую зависят от выбранного ими уровня образования. Так, согласно с Федеральными законами и Постановлением, принято выделять следующие уровни образовательных организаций, которые осуществляют подготовку сотрудников правоохранительных органов:

1. Профессиональные образовательные учреждения, находящиеся в системе МВД России;

Отвечают за подготовку сотрудников по трем направлениям – начальное, среднее и высшее профессиональное образование.

2. Начальное профессиональное образование;

Осуществляется подготовка вновь принятых сотрудников на службу в определенных субъектах России. Отличительной характеристикой такого образования является то, что главной его целью выступает обучение сотрудников по всем основным направлениям служебной деятельности

3. Среднее профессиональное образование;

Возможно получить данный уровень образования как вновь принятым на службу сотрудникам, так и имеющим практический опыт деятельности.

4. Высшее профессиональное образование.

Образовательные учреждения МВД России принимают для обучения лиц, которые уже имели определенный опыт работы в системе МВД, а также тех, кто впервые пробует себя в данной деятельности. Основной целью выступает

подготовка сотрудников до определенного уровня на базе уже имеющегося как профессионального, так и среднего общего образования. Также еще основной целью выступает углубление и расширение уже имеющихся знаний и профессиональных навыков и получение новых, которые будут отвечать современным требованиям и тенденциям развития.

Структура высшего профессионального и послевузовского образования МВД имеет свою систему, которая утверждается согласно с решением высших уполномоченных на то лиц:

1. Федеральные государственные образовательные стандарты высшего профессионального образования, предъявляемые к послевузовскому образованию;

2. Учебные заведения, которые имеют лицензию на осуществление подготовки или переподготовки сотрудников для их дальнейшей служебной деятельности;

3. Органы, осуществляющие управленческую деятельность в системе МВД для подготовки сотрудников;

4. Другие общественные и государственно-общественные образовательные организации.

Таким образом, необходимо отметить, что вся система МВД России носит практически ориентированный образовательный характер, направленный на достижение наук и техник в деятельности правоохранительных органов. А комплексы, применяемые для обучения, выстраиваются и применяются в соответствии с ФЗ и отвечают основным тенденциям развития как правоотношений, так и всех остальных общественных отношений в целом.

Литература

1. Федеральный закон от 30.11.2011 N 342-ФЗ (ред. от 14.04.2023) "О службе в органах внутренних дел Российской Федерации и внесении изменений в отдельные законодательные акты Российской Федерации".

2. Бондарев А.А., Мальцева В.Р. Дисциплина «Основы профессиональной деятельности» как основа профессионального обучения (профессиональной подготовки) курсантов вузов МВД России // сборник научных трудов II Международной конференции.

3. О высшем и послевузовском образовании в Российской Федерации: Федеральный закон РФ от 22 августа 1996 г. № 125-ФЗ (в ред. от 10 февраля 2009 г.).

4. Об утверждении Наставления по организации профессиональной подготовки сотрудников органов внутренних дел Российской Федерации: приказ МВД РФ от 29 июня 2009 г. № 490.

5. О введении в действие Руководства по работе с кадрами рядового и начальствующего состава органов внутренних дел: приказ МВД СССР от 15 июня 1975 г. № 150.

6. Об информатизации образовательных учреждений МВД России: приказ МВД РФ от 5 июля 1996 г. № 362 // СПС Гарант.

Сведения об авторе

Комерцов Вячеслав Викторович, преподаватель кафедры информационного обеспечения ОВД Ростовского юридического института МВД России; e-mail: komercov@yandex.ru.

Копыткова Людмила Борисовна,
Копытков Олег Борисович,
Фурсов Алексей Алексеевич

ТЕОРЕТИКО-ЧИСЛОВЫЕ МЕТОДЫ В РЕШЕНИИ ЗАДАЧ ШКОЛЬНОЙ МАТЕМАТИКИ

Одна из основных содержательно-методических линий отечественного математического образования - теоретико-числовая линия. Для определения содержательной части этой линии была проанализирована Примерная основная образовательная программа, Примерные рабочие программы для базового и углубленного уровня, школьные учебники. Был выявлен тематический план, объем и глубина освоения вопросов исследуемой линии. Теоретико-числовая линия прослеживается в курсе математики и алгебры в 5-9 классах и в старших классах новых теоретических сведений учащиеся в рамках этой линии не получают. В то же самое время анализ вариантов ЕГЭ по математике как базового, так и профильного уровней показывает важность изучать основы теории чисел в рамках школьного курса математики, показывать методы решения подобных задач. Между базовым и профильным уровнем в подобных заданиях разница состоит лишь в формулировке. Если в базовом уровне предлагается привести пример одного из чисел, обладающего указанными свойствами, то в профильном уровне уже надо найти все такие числа. Раннее изучение темы «делимость» оставляет без вывода ряд положений, а методы их доказательства как раз бы могли помочь в решении ряда подобных задач. Задания профильного уровня часто относят ещё и к классу олимпиадных задач, поэтому без специальной подготовки, без повторения известных фактов теории делимости на более высоком уровне, без изучения некоторых формул и положений теории чисел решение этих заданий для школьников будет весьма проблематичным.

Результаты государственной итоговой аттестации выпускников 11-х классов свидетельствуют о низком уровне навыков решения теоретико-числовых задач. С задачей № 19 базового уровня ЕГЭ по математике

справляются около 50% выпускников [2], задачей № 18 профильного – около 8% [4, 5]. Одна из причин этого состоит в том, что современная методика обучения учащихся решению теоретико-числовых задач, в том числе и нестандартных, разработана недостаточно. Практически отсутствуют современные учебно-методические пособия для старших школьников, ориентированные на формирование навыков решения теоретико-числовых задач [2]. Подготовить даже сильных учащихся к решению этих заданий, которые часто позиционируют как олимпиадные, в условиях базовой школы не представляется возможным. Для этого необходима серьёзная кружковая работа и/или проведение факультативных занятий по данной проблематике. При этом глубина изложения зависит от возраста учеников.

Для решения поставленной проблемы выделим основные дидактические единицы теоретико-числовой линии.

- Делимость без остатка в области целых чисел. Признаки делимости. Деление с остатком. Теорема о делении с остатком.
- Простые и составные числа. Решето Эратосфена. Основная теорема арифметики. НОД и НОК чисел. Алгоритм Евклида.
- Числовые функции (целая часть и дробная часть числа, число и сумма делителей натурального числа, функция Эйлера) и их приложения.
- Числовые сравнения. Теоремы Эйлера и Ферма.
- Линейные сравнения. Цепные дроби, их применение для решения линейных сравнений.
- Неопределённые уравнения и методы их решения.

При решении задач на делимость могут применяться различные методы – метод математической индукции; метод разбиения множества целых чисел на классы, в зависимости от остатка от деления; представление числа в виде произведения нескольких последовательных чисел и применении свойств делимости (произведение двух последовательных чисел делится на 2, трех последовательных чисел – делится на 6, четырех – на 24 и т.д.). Приведём пример решения одной из задач на делимость.

Задача 1. Может ли разность двух различных трехзначных чисел, из которых второе записано теми же цифрами, что и первое, но в обратном порядке, быть квадратом натурального числа? [3]

При решении этой задачи воспользуемся систематической записью числа и свойствами делимости. Пусть $\overline{abc} = 100a + 10b + c$ – трехзначное число, где a, b, c – цифры, причем $a \neq 0,\ c \neq 0,\ a \neq c$. Тогда,

$$\overline{abc} - \overline{cba} = 100a + 10b + c - (100c + 10b + a) = 99a - 99c = 99(a - c) = 3^2 \cdot 11(a - c)$$

Для того чтобы рассматриваемая разность была квадратом натурального числа, необходимо, чтобы a-c было кратно 11, но $a - c < 10$, поэтому разность $\overline{abc} - \overline{cba}$ не может быть равна квадрату какого-либо натурального числа.

Следующая задача демонстрирует один из способов нахождения остатка от деления, который связан со свойством периодичности остатков.

Задача 2. Определите последние две цифры числа 50607076^{2014}. Ответ обоснуйте [2].

Последние две цифры числа есть остаток от деления этого числа на 100. Поэтому заметим, что, прежде всего, последние две цифры числа 50607076^{2014} будут совпадать с последними двумя цифрами числа 76^{2014}. Далее рассматривая возведение числа 76 в квадрат, замечаем, что квадрат, а, следовательно, и любая степень будет оканчиваться на 76.

Заметим, что можно было доказывать и более общее свойство, что произведение любых двух целых чисел, оканчивающихся на 76, тоже будет оканчиваться на 76. Последние две цифры числа 76.

Решение следующей задачи демонстрирует необходимые приемы, связанные с нахождением НОДа и НОКа.

Задача 3**.** Вычислить НОК трех чисел $[153,119,204]$.

При решении задач этого типа следует иметь в виду, что $[a_1, a_2, ..., a_{n-1}, a_n] = [[a_1, a_2, ..., a_{n-1}], a_n]$. А так же следует пользоваться формулой,

выражающей связь НОДа и НОКа двух чисел $[a_1, a_2] = \frac{a_1 \cdot a_2}{(a_1, a_2)}$, где (a_1, a_2) находят одним из известных способов, например, по алгоритму Евклида.

Следующие задачи демонстрируют приложения числовых функций

Задача 4**.** Сколькими нулями оканчивается число 1316!?

Решение сводится к нахождению показателя, с которым число 10 входит в произведение 1316!

Мы знаем, что для определения показателя, с которым простое число входит в каноническое представление числа *n*! необходимо воспользоваться формулой

$$\alpha = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \ldots$$

Показатель, с которым число 10 входит в произведение 1316!, равен показателю, с которым входит наибольший из простых делителей числа 10, т.е. число 5. Учитывая все сказанное выше, находим:

$$\alpha = \left[\frac{1316}{5}\right] + \left[\frac{1316}{5^2}\right] + \left[\frac{1316}{5^3}\right] + \left[\frac{1316}{5^4}\right] = 263 + 52 + 10 + 2 = 327.$$

Следовательно, число 1316! Оканчивается 327 нулями.

Задача 5**.** Найти число и сумму делителей числа 50400.

Если каноническая запись числа *n* имеет вид $n = p_1^{k1} \cdot p_2^{k2} \cdot \ldots \cdot p_m^{km}$, то число натуральных делителей *n* равно $\tau(n) = (k_1 + 1)(k_2 + 1)\ldots(k_m + 1)$, а сумма всех натуральных делителей выражается формулой $\sigma(n) = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_m^{k_m+1} - 1}{p_m - 1}$.

Каноническая запись числа 50400 имеет вид $50400 = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7$.

Следовательно, $\tau(50400) = (5+1)(2+1)(2+1)(1+1) = 6 \cdot 3 \cdot 3 \cdot 2 = 108$

$$\sigma(50400) = \frac{2^6 - 1}{2 - 1} \cdot \frac{3^3 - 1}{3 - 1} \cdot \frac{5^3 - 1}{5 - 1} \cdot \frac{7^2 - 1}{7 - 1} = \frac{64 - 1}{1} \cdot \frac{27 - 1}{2} \cdot \frac{125 - 1}{4} \cdot \frac{49 - 1}{6} = 203112.$$

Одна из важнейших функций в теории чисел – это функция Эйлера. Её приложения часто опираются на теоремы Эйлера и Ферма (малая теорема). Для удобства, решение проведём на языке сравнений. Заметим, что вопросы, связанные с теорией сравнения выходят за рамки школьного курса. Однако, в рамках задач ЕГЭ теория сравнений применяется для решения тех же классов, что и теория делимости, но решение приобретает более компактную форму. Для учителя полезно научиться использовать символику теории сравнений и, возможно, показать её своим ученикам, или переводить решения на язык теории делимости.

Задача 6. Чему равен остаток от деления числа 11^{243} на 20?

Учитывая $(11,20)=1,$ то по теореме Эйлера $11^{\varphi(20)} \equiv 1 (\mathrm{mod}\ 20).$

Найдём функцию Эйлера: $\varphi(20)=2^2 \cdot 5\left(1-\frac{1}{2}\right)\cdot\left(1-\frac{1}{5}\right)=8.$ Тогда $11^8 \equiv 1(\mathrm{mod}\ 20).$

По теореме о делении с остатком $243=8\cdot 30+3.$

Тогда $11^{243}=\left(11^8\right)^{30}\cdot 11^3 \equiv 11^3(\mathrm{mod}\ 20)=121\cdot 11\equiv 1\cdot 11(\mathrm{mod}\ 20)\equiv 11(\mathrm{mod}\ 20).$

Таким образом, остаток от деления 11^{243} на 20 равен 11.

Изучение с учащимися методов решения неопределённых уравнений предполагает знакомство с цепными дробями, с установлением взаимосвязи между сравнениями и неопределёнными уравнениями, с линейным представлением НОДа.

Проведённый анализ теоретико-числовой линии школьного курса математики и основных типов задач теоретико-числового содержания, встречающихся на ЕГЭ, показал, что необходимо разработать факультативный курс «Теоретико-числовые методы в решении задач школьной математики» для успешной подготовки учащихся к итоговым испытаниям. Учителю необходимо постоянно поддерживать интерес школьников, развивать их мышление, интуицию, предлагая головоломки, задачи повышенной сложности и нестандартные (олимпиадные) задачи, показывать различные способы

рассуждений, приемов математических доказательств [1].

Литература

1. Давыдов В.В. Теория развивающего обучения. - М.: ИНТОР, 1996.
2. Жмурова И.Ю. О теоретико-числовой подготовке будущего учителя математики. Международный научно-исследовательский журнал. 2017. № 9-1 (63). С. 133-135.
3. Садовничий Ю.В. ЕГЭ 2017. Задание 19. Решение задач и уравнений в целых числах- М.: Экзамен, 2017.
4. Хамов Г.Г., Тимофеева Л.Н. О совершенствовании профессиональной подготовки будущего учителя математики //Международный научно-исследовательский журнал. 2016, № 1 (43), ч.4. С. 57-60.
5. Харламова К.П. Элементы теории чисел на занятиях курса внеурочной деятельности в основной школе / К. П. Харламова. — Текст: непосредственный // Молодой ученый. — 2023. — № 20 (467). — С. 224-226. — URL: https://moluch.ru/archive/467/102962/ (дата обращения: 05.06.2023).

Сведения об авторах

Копыткова Людмила Борисовна, кандидат физико-математических наук, доцент кафедры Математического анализа, алгебры и геометрии факультета Математики и компьютерных наук имени профессора Н.И. Червякова Северо-Кавказского федерального университета; e-mail: d212.256.08@mail.ru.

Копытков Олег Борисович, магистр, направление подготовки 44.04.01 – Педагогическое образование факультета Математики и компьютерных наук имени профессора Н.И. Червякова Северо-Кавказского федерального университета; e-mail: gleb.kopytkov@mail.ru.

Фурсов Алексей Алексеевич, магистр, направление подготовки 02.04.01 – Математика и компьютерные науки факультета Математики и компьютерных наук имени профессора Н.И. Червякова Северо-Кавказского федерального университета; e-mail: goch_valeria@mail.ru.

Коробов Николай Васильевич,
Сибаров Константин Дмитриевич,
Яковлева Наталья Александровна

ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОСТИ ВЫПОЛНЕНИЯ ЗАДАНИЙ ПРИ УДАЛЁННОМ ОБУЧЕНИИ С ИСПОЛЬЗОВАНИЕМ РЕДАКТОРА WORD

Цель разработки и применения рассматриваемых приёмов – обеспечение самостоятельности выполнения работ обучающимися при использовании редактора Word для сохранения качества образования в условиях удалённого обучения.

Введение.

С весны 2020 года из-за пандемии короновируса во многих вузах стали появляться отрезки времени перевода обучающихся на удалённые формы, что коренным образом изменило всю обстановку обучения, породив прежде неизвестные сложности и выдвинув новые задачи перед преподавателями.

Современные средства обмена цифровыми данными позволяют обучающимся не только попарно обмениваться работами, но также сообща создавать облачное хранилище работ своего учебного подразделения, куда выкладываются все выполненные задания. Неучёт этих обстоятельств чреват тем, что преподаватель будет получать на проверку достаточно малое количество самостоятельно выполненных работ. И это можно считать крушением обучения. Причём со стороны всё будет выглядеть весьма пристойно: задания рассылаются, выполненные работы обучающимися обратно отправляются, оценки за них выставляются (удобно и незатратно как для недобросовестных обучающихся, так и для нерадивых преподавателей).

Задача обеспечения самостоятельности удалённого выполнения заданий решалась применительно как к изучению редактора Word на информатике, так и к проверке отчётов, сделанных в редакторе Word, по другим дисциплинам.

Разработка заданий.

Дополнительные требования к разрабатываемым заданиям следующие:

- задания должны закладывать в отчётные материалы набор признаков, снижающих вероятность их совпадения в работах разных обучающихся;

- трудоёмкость переделки чужого задания нерадивым обучающимся должна быть сопоставима с трудоёмкостью самостоятельного выполнения.

Приведём перечень используемых нами приёмов.

1. В начале работы над заданием обучающийся должен создать новый документ, присвоив ему имя на кириллице. Создание нового документа прописывает в свойствах файла имя пользователя, создавшего документ, и дату создания содержимого. Выполнение в облачных приложениях не допускается.

2. Текст в нужном объёме, подлежащий обработке при изучении редактора Word, должен быть взят из внешних источников (Всемирной паутины). Хорошо, если предусмотрена вставка изображений на заданную тему также из внешних источников.

3. В подзаданиях, по возможности, делаются варианты – от двух до пяти, с чередованием выбора в зависимости от номера в списке группы. Составление перечислений, если таковые встречаются, можно обязывать делать с привязкой к буквам фамилии обучающегося или, опять же, к номеру в списке.

4. Должна быть предусмотрена вставка в отчёт захватов экрана (обязательно целиком!) с промежуточными итогами выполнения, например, список созданных файлов в Проводнике с видом «Таблица». Обстановка на экране, время и дата на линейке задач придают отчёту неповторимость.

5. Итог выполнения отправляется преподавателю по почте только после закрытия файла отчёта для заполнения свойства «Время изменения».

6. Возможна «прошивка» всего созданного отчёта инициалами с помощью команды «Найти и заменить» – об этом дальше отдельно.

Проверка свойств файла отчёта.

Поскольку редактор Word не предоставляет развёрнутых средств учёта последовательности действий с файлом, то должны быть использованы те его возможности, которые созданы для обычного документооборота.

Если количество обучающихся не слишком велико, и сдача работ не слишком растянута во времени, преподаватель в состоянии держать в памяти мельчайшие подробности недавно проверенных работ. Для быстрого поиска сходства с одной из уже проверенных работ подходят служебные программы, способные выполнять поиск по образцу текста внутри файлов. В качестве образца следует выбирать редко встречающееся слово или словосочетание.

Проверка отчётов на Word во всех случаях выполняется с отображением непечатаемых знаков. Например, если в пустой документ целиком скопирована и вставлена чужая работа из другого окна Word, то поддельная работа, вероятнее всего, будет иметь на 1-2 пустых строки в конце больше.

Важные сведения о том, как создавался файл, дают свойства файла, на которые нерадивые обучающиеся обычно внимания не обращают.

«Авторы». Свойство существенно, если файл, согласно заданию, нужно было создавать из пустого документа. Но поле доступно для правки.

«Кем сохранён». Обычно при изучении редактора Word выполняется несколько заданий в течение нескольких недель, поэтому преподавателю полезно вести учёт имён пользователей из списка свойств файла для возможности их сопоставления.

«Дата создания содержимого». Свойство перезаписывается текущим временем операционной системы, если с чужим файлом в редакторе Word выполняется действие «Сохранить как».

«Дата последнего сохранения». Свойство перезаписывается, если с файлом в редакторе Word выполняется действие «Сохранить как».

«Дата создания» и «Дата изменения» перезаписываются при скачивании файла с сервера электронной почты, поэтому они не дают сведений о времени.

«Время редактирования». Счёт времени редактирования ведётся в Word, пока окно программы активно. Свойство существенно, если файл, согласно заданию, нужно было создавать из пустого документа. Значение свойства обнуляется, если с файлом в редакторе Word выполняется действие «Сохранить как». Время проверки преподавателем файла также добавляется ко времени

редактирования. Если время выполнения большого задания около 1 минуты, то весьма вероятно, что был открыт чужой файл и тут же было выполнено действие «Сохранить как» с присвоением файлу другого имени. При этом сохраняется значение в поле «Авторы», но оно доступно для правки.

«Редакция». Свойство показывает, сколько раз файл сохранялся. Каждое действие «Сохранить» увеличивает значение свойства на единицу даже без закрытия файла.

Совокупное рассмотрение всех этих свойств служит основой для вывода.

Другие пути.

Самым надёжным старым способом является создание обособленных заданий равной сложности для каждого обучающегося. Однако это не только весьма трудоёмко, но иногда и неприемлемо. Например, изучаемые приёмы работы в редакторе Word должны быть выполнены всеми и проверены у всех.

Другим путём обеспечения самостоятельности при едином задании для всех является подготовка файлов задания, помеченных для каждого обучающегося цифровым способом, и выдача их каждому лично с предписанием всё делать прямо в выданном файле. Свойства файла Word содержат такие обычно пустые поля: «Название», «Тема», «Теги», «Категории», «Комментарии» и др. Для этих полей может быть разработано заполнение, различное для каждого обучающегося.

Вторым способом цифровой пометки файлов является изменение внутренних редко используемых настроек файлов. Каждому выдаётся свой по-особому помеченный пустой файл (как именно – наша служебная тайна). Очевидна ощутимая трудоёмкость подготовки таких помеченных пустых файлов. Но будучи сделанными единожды, они могут использоваться на разных заданиях и не один год подряд. Возможна также автоматизация подготовки таких файлов путём создания макроса на языке VBA Word, вписывающего в цикле нужные значения в поля свойств файла и каждый раз выполняющего его сохранение с именем, содержащим увеличивающийся номер. Возможна автоматизация и проверки файла с цифровой пометкой – также с применением

макроса. Этот приём нами успешно применяется уже три года при изучении электронных таблиц Excel.

Учитывая, что редактор Word является основным средством для подготовки отчётов по многим другим дисциплинам, и, перепробовав описанные выше способы, мы остановились на следующем умеренно трудоёмком. Обучающимся вместе с файлом задания высылается заготовка файла отчёта с предписанием делать только на его основе, иначе беспристрастно выставляется оценка «неудовлетворительно». В конце подготовки отчёта должно быть сделано его «подписание» своими инициалами: замена шрифта всех совпадающих с инициалами букв на редко используемый шрифт, например, Arial Black с помощью диалогового окна «Найти и заменить» во всём документе (!). Для невозможности отката этого действия при желании использовать чужую «подписанную» работу в эту заготовку отчёта помещается проверочная строка – все прописные и строчные буквы – также редко используемым шрифтом, например, Courier New. А весь отчёт должен выполняться шрифтом Times New Roman. Эта проверочная строка прячется (как именно – служебная тайна). При замене на Arial Black, а затем обратно на Times New Roman в этой строке, выполненной шрифтом Courier New, с помощью диалогового окна «Найти и заменить» исходные инициалы приобретут начертание Times New Roman. Инициалы желающего использовать чужую работу с высокой вероятностью не будут иметь полного совпадения с исходными. Возврат видимости проверочной строки ответит на вопрос о самостоятельности. Для скрытия этой строки нами использована цепочка из четырёх действий, основанных на редко используемых возможностях редактора Word. Можно добавить и ещё два, но они нами не применяются, т.к. и того, что есть до настоящего времени оказывалось достаточным.

Как можно видеть, успешность описываемых способов обусловлена тем, что преподаватель на порядок лучше знает редактор Word, чем обучающийся, а тем более такой, который не желает вникать в тонкости редактора.

Заключение.

Без цифровой пометки заданий самостоятельность работы может быть установлена лишь на основе умозрительного соотнесения множества формальных и содержательных признаков присланного файла в сравнении его с полученными ранее. Проверка работ на самостоятельность в условиях удалённого обучения – это, в полном смысле этого слова, экспертиза, преподавательская экспертиза. Для повышения её надёжности задания должны содержать действия, придающие отчёту узнаваемость и неповторимость, а проверка должна опираться, в том числе, на цифровые свойства файлов. Как показывает наш трёхлетний опыт, для целой группы совокупные затраты времени на такую экспертизу, переписку по электронной почте с пояснениями недочётов и повторной проверкой присланных исправлений могут быть в разы больше, чем два часа занятия в компьютерном классе с беглым просмотром сделанного по экранам обучающихся в последние 10-15 минут. Справедливо приравнять проверку одного такого учебного задания проверке письменной контрольной работы – 0,4 часа. Для подтверждения предоставляется переписка.

Сведения об авторах

Коробов Николай Васильевич, кандидат технических наук, доцент кафедры математики и информатики Санкт-Петербургского университета МВД России; e-mail: nv-korobov@yandex.ru.

Сибаров Константин Дмитриевич, кандидат технических наук, доцент кафедры математики и информатики Санкт-Петербургского университета МВД России; e-mail: konstantin_siba@mail.ru.

Яковлева Наталья Александровна, кандидат психологических наук, доцент, начальник кафедры математики и информатики Санкт-Петербургского университета МВД России; e-mail: kumirova@mail.ru.

Кубасов Игорь Анатольевич

МАТЕМАТИЧЕСКИЕ МЕТОДЫ ИССЛЕДОВАНИЯ СОЦИАЛЬНЫХ СИСТЕМ КАК ОСНОВНОЙ ИНСТРУМЕНТАРИЙ ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЕЯТЕЛЬНОСТИ ОРГАНОВ ВНУТРЕННИХ ДЕЛ

Развитие любой социальной системы, в том числе и органов внутренних дел Российской Федерации (далее – ОВД), происходит в тесной взаимосвязи с окружающей ее средой. Для эффективного управления ОВД, как сложной социальной системой, необходимо иметь не только полное понимание о происходящих внутренних процессах функционирования системы и их закономерностях, но и о влиянии самой системы на внешнюю среду [1].

Деятельность органов внутренних дел на современном этапе характеризуется достаточно обширным набором различных внутренних и внешних показателей, которые отражают криминальную ситуацию, складывающуюся в регионах, динамические характеристики этой ситуации, результаты деятельности по регистрации, расследованию и раскрытию преступлений, охране общественного порядка и др. Многие из этих показателей взаимообусловлены, отдельные находятся в причинно-следственной связи, а значения их, в основном, зависят от уровня информационно-аналитического обеспечения деятельности ОВД [2, 3].

В последние годы использование математических методов исследования социальных систем приобрело особую важность и актуальность в информационно-аналитическом обеспечении деятельности ОВД из-за стремительного роста больших данных, бурного развития информационных технологий и необходимости применения более сложных аналитических инструментов для эффективного решения оперативно-служебных задач [4,5,6,7].

Основой этих методов исследования социальных систем являются фундаментальные законы теории вероятностей и математической статистики, положения теории игр, марковских процессов, теории автоматов и т.д.

Одним из наиболее важных приложений этих математических методов, как инструментария информационно-аналитического обеспечения деятельности в ОВД, является предиктивный анализ преступности.

Предиктивный анализ преступности – это процесс использования данных для выявления моделей и тенденций преступной деятельности, а также для разработки стратегий предотвращения и раскрытия преступлений. Математические модели выступают важным инструментом для криминальных аналитиков, позволяющим выявлять корреляции и тенденции в больших наборах данных, которые было бы трудно или невозможно выявить с помощью ручного анализа. Анализируя данные о предыдущих преступлениях, сотрудники могут использовать предиктивную аналитику для выявления областей и лиц, которые подвержены высокому риску преступной деятельности в будущем. Затем эту информацию можно использовать для управления патрулированием и другими действиями, помогая предотвратить преступление до его совершения.

Анализируя статистические данные о преступлениях, прогностические модели могут выявлять закономерности и тенденции, которые обеспечивают более эффективно использование ресурсов ОВД [8, 9].

Некоторые из общих математических методов, используемых в предиктивном анализе преступности, включают:

1. Корреляционно-регрессионный анализ: это статистический метод, используемый для определения взаимосвязи между переменными. В прогнозирующей деятельности полиции корреляционно-регрессионный анализ может использоваться для определения взаимосвязи между уровнем преступности и различными факторами, такими как время суток, погодные условия и демографические данные.

2. Анализ временных рядов. Этот метод используется для анализа данных во времени для выявления закономерностей и тенденций, например, для выявления сезонных моделей преступности, таких как увеличение числа краж со взломом в праздничный сезон.

3. Географические информационные системы (ГИС): технология ГИС позволяет ОВД отображать данные о преступлениях и выявлять горячие точки. Анализируя пространственные модели преступности, ГИС может помочь определить области, на которых следует сосредоточить ресурсы.

Одной из наиболее распространенных математических зависимостей, используемых в предиктивном анализе преступности, является распределение Пуассона. Распределение Пуассона – это математический инструмент, используемый для моделирования вероятности редких событий, происходящих в течение определенного периода времени. В контексте ОВД распределение Пуассона можно использовать для моделирования вероятности различных видов преступлений, совершенных в определенной географической области в течение определенного периода времени. Затем эту информацию можно использовать для разработки стратегий предотвращения и раскрытия преступлений в этой области.

Еще один важный математический метод основан на применении теоремы Байеса. Теорема Байеса – это математическая формула, используемая для расчета вероятности наступления события на основе априорных знаний о связанных событиях. Теорему Байеса можно использовать для расчета вероятности того, что подозреваемый виновен на основании имеющихся доказательств. Эта информация может использоваться для направления расследований, принятия решений об арестах и судебных преследованиях, а также для обеспечения отправления правосудия. Байесовскую вероятность можно использовать для определения вероятности виновности подозреваемого на основании результатов применения методов геномного анализа ДНК [10]. На сегодняшний день теорема Байеса активно применяется в технологиях искусственного интеллекта.

2. Распознавание образов. Распознавание образов – это метод, используемый для выявления закономерностей в данных. В криминалистическом анализе распознавание образов может использоваться для

выявления сходства между вещественными доказательствами, найденными на разных местах преступления.

3. Обработка сигналов. Обработка сигналов – это метод, используемый для анализа таких сигналов, как аудио- или видеозаписи. В криминалистическом анализе обработка сигналов может использоваться для улучшения записей с целью выявления важной информации.

Сотрудники ОВД используют широкий спектр математических моделей и алгоритмов, которые помогают им анализировать данные и разрабатывать эффективные стратегии предотвращения и раскрытия преступлений. Эти модели и алгоритмы можно применять для анализа данных из различных источников, включая социальные сети, камеры наблюдения и другие источники информации [11].

Поскольку технология продолжает развиваться и становятся доступными новые источники данных, вполне вероятно, что использование математических методов в ОВД будет продолжать расти и развиваться в ближайшие годы.

В заключение следует отметить, что при проведении научных исследований и получении качественно новых результатов, востребованных для повышения эффективности информационно-аналитического обеспечения деятельности ОВД, необходимо не только иметь объективное представление об основных процессах и направлениях развития данной социальной системы, но и уметь учитывать сложное взаимосвязанное многообразие факторов, оказывающих существенное влияние на это развитие. Такие результаты исследований можно получить только используя современный инструментарий – методы исследования социальных систем, позволяющие исследователю разобраться в огромном количестве стохастической информации в ходе оперативно-служебной деятельности ОВД и среди множества различных вероятностных моделей выбрать единственную, наилучшим образом отражающую изучаемый процесс или явление.

Литература

1. Горошко И.В., Торопов Б.А., Макаров В.Ф., Гонов Ш.Х. Математические методы исследования социальных систем: курс лекций – М.: Академия управления МВД России, 2018. – 83 с.

2. Информационные технологии в управлении и организация защиты: учебник / В.В. Баранов и др. под ред. И.В. Горошко – М.: Академия управления МВД России, 2018. – 376 с.

3. Баторов Б. О., Кубасов И. А., Торопов Б. А. Управление в социальных и экономических системах: курс лекций. – Москва: Академия управления МВД России, 2022. – 116 с.

4. Кубасов И.А., Цаганов А.В. Использование систем и технологий искусственного интеллекта в деятельности органов внутренних дел Российской Федерации. Специализированный ведомственный журнал «Научно-технический портал МВД России». 2021. № 4 (40). С. 3-10.

5. Кубасов И.А., Ливанский А.Г., Пучков Г.Ю. К вопросу о внедрении средств интеллектуального видеонаблюдения в деятельность органов внутренних дел Российской Федерации. Вестник МВД России. 2022. №5. С. 55 – 61.

6. Кластеризация объектов со слабо формализуемыми признаками на основе нейронной сети в виде слоя Кохонена / И.А. Кубасов, А.В. Мельников, С.А. Мальцев, И.Р. Нарушев // Вестник Воронежского государственного университета инженерных технологий. – 2018. – Т. 80, № 3(77). – С. 86-91. – DOI 10.20914/2310-1202-2018-3-86-91. – EDN YPWTEL.

7. Стеганоанализ цифровых изображений: монография/ Р.А. Солодуха, И.В. Атласов, И.А. Кубасов. – Воронеж: Воронежский институт МВД России. – 2022. –172с.

8. Кубасов, И.А. Математическая модель оценки эффективности информационно-аналитического обеспечения подразделения в специальной операции / И.А. Кубасов // Состояние и перспективы развития современной

науки по направлению «АСУ, информационно-телекоммуникационные системы»: сборник статей II Всероссийской научно-технической конференции, Анапа, 18 июня 2020 года / Военный инновационный технополис "ЭРА". Том 3. – Анапа: Федеральное государственное автономное учреждение "Военный инновационный технополис "ЭРА", 2020. – С. 109-116. – EDN BLJJLM.

9. Кубасов, И. А. Определение количества элементов запаса по условиям безопасности функционирования системы / И.А. Кубасов, О.А. Бобр, Е.В. Швед // Двойные технологии. – 2006. – № 1(34). – С. 68-72. – EDN KUDMSL.

10. Кубасов, И.А. Разработка методов ДНК-фенотипирования для расследования и раскрытия преступлений / И.А. Кубасов // Вестник Воронежского института МВД России. – 2022. – № 2. – С. 166-172. – EDN GTSQNB.

11. Кубасов И.А., Лекарь Л.А. Поиск и анализ больших данных в социальных сетях и Интернете для информационно-аналитического обеспечения оперативно-розыскной деятельности // Оперативно-розыскной портал: право и технологии. 2022. № 2 (2). С. 16-19.

Сведения об авторе

Кубасов Игорь Анатольевич, доктор технических наук, доцент, профессор кафедры информационных технологий Академии управления МВД России; e-mail: igorak@list.ru.

Курамагомедова Алина Курамагомедовна

СИСТЕМА УЧЕТА ВРЕМЕНИ ПОЛЬЗОВАТЕЛЯ

В современном мире существует актуальная проблема неэффективного использования персонального времени и необходимости его контроля и правильного распределения в зависимости от конкретных потребностей [1]. Для учета личного времени существует несколько методов, однако они могут быть рутинными и трудоемкими при использовании бумажных носителей. В связи с этим возникает необходимость в разработке современных инструментов для контроля персонального времени, которые были бы удобными для использования и не создавали дополнительных трудностей для пользователя [2].

Одним из таких инструментов может быть мобильное приложение или веб-сайт, так как мобильные устройства стали неотъемлемой частью жизни человека. В современных технологиях мобильные приложения и веб-сайты состоят из клиентской и серверной частей, обменивающихся сообщениями по протоколу. В статье описывается разработка веб-сервиса, который охватывает серверную часть общей аналитической системы контроля персонального времени.

В результате проделанной работы была разработана информационная система, которая предназначена для консолидации, хранения, обработки и управления доступом к данным о персональном времени. Информационная система позволяет оптимизировать использование персонального времени, а также анализировать и управлять наиболее затратными и важными задачами и занятиями. Благодаря разработке такой информационной системы можно достичь эффективного контроля над своим персональным временем и повысить свою эффективность в работе и повседневной жизни.

Система работает по протоколу HTTPS и принимает запросы в формате JSON от клиентской части. Каждый запрос верифицируется внешней системой аутентификации и авторизации Keycloak, которая предотвращает доступ к системе для пользователя, не прошедшего аутентификацию. В качестве протокола аутентификации используется протокол OpenId Connect.

В качестве основных сущностей системы используются следующие: контексты, категории, записи, комментарии. Контекст является группой логически связанных видов деятельности, каждый из которых представляет отдельный вид деятельности в рамках контекста. Запись описывает конкретное событие для конкретного пользователя в определенный момент времени, а комментарий предоставляет пользователю дополнительную информацию для идентификации записи в будущем.

Система REST API предоставляет ряд функций, включая операции CRUD для контекстов, категорий, записей и комментариев. Кроме того, система обладает инструментами для регистрации и аутентификации пользователей, работает в режиме анонимного пользователя и имеет интегрированный сервис по сохранению изображений в файловой системе.

Дополнительно система поддерживает локализацию на русском, немецком и английском языках, а также позволяет пользователям с определенными привилегиями, такими как администраторы, выполнять дополнительные административные функции.

Система также обладает возможностью добавления пользовательских категорий, хранит вероятностную модель для вычисления удобных для пользователя контекстов в данный момент и предоставляет инструменты по вычислению аналитических показателей расхода времени за выбранный период. Важным аспектом системы также является возможность работы с документацией REST API. Внешний сервер аутентификации и авторизации Keycloak интегрирован в систему для проверки доступа пользователя к сервису перед обработкой каждого запроса. Выбран фреймворк Swagger для документирования API, который предоставляет спецификации веб-сервисов. Основной язык программирования проекта - Java 8, а многослойная архитектура MVC обеспечивает возможность легкого расширения функционала и замены реализации.

На api-уровне серверной части имеются хорошо задокументированные Java-аннотации и автогенерированные документы в двух форматах: JSON и GUI.

Swagger API инструмент используется для визуализации документации, позволяя трансформировать JSON в удобный для пользователя HTML-формат. Проект, представленный в виде war-файла, написан на Java 8 с использованием внешних библиотек и фреймворков и развернут внутри контейнера сервлетов и HT-сервера Jetty. GitHub используется в качестве веб-сервиса для хранения исходного кода серверной части при закрытом репозитории и лицензии MIT.

В результате работы был создан веб-сервис как серверная часть широкой аналитической системы для контроля персонального времени. Кроме того, была спроектирована база данных с четкими связями между всеми необходимыми для работы системы сущностями. Веб-сервис обеспечивает API для множества операций с описанными выше сущностями. Созданный веб-сервис и база данных, при желании, могут быть легко интегрированы с другими технологическими решениями для максимальной эффективности решаемых задач.

Литература

1. Кувшинов, И.С. Исследование проблем автоматизации учета затрат личного времени / И.С. Кувшинов // EurasiaScience: Сборник статей IX международной научно-практической конференции, Москва, 31 мая 2017 года. Том Часть 1. – Москва: Общество с ограниченной ответственностью "Актуальность.РФ", 2017. – С. 147-148. – EDN YTLHRL.

2. Бобырь, М. В. Исследование адаптивной системы учета рабочего времени / М.В. Бобырь, А.В. Скринникова // Известия Юго-Западного государственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. – 2016. – № 1(18). – С. 42-52. – EDN VVSALD.

Сведения об авторе

Курамагомедова Алина Курамагомедовна, ассистент кафедры информационных технологий Кубанского государственного университета; e-mail: a30121999@bk.ru.

Лаптев Владимир Николаевич,
Лаптев Сергей Владимирович

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ КОМПЛЕКСНОГО ПРИМЕНЕНИЯ ЕСТЕСТВЕННОГО И ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В МВД РФ

Работа посвящена актуальной проблеме автоматизации механизма адаптивного управления открытыми системами (МАУ ОС), решение которой позволяет обеспечить успешную реализацию национальной стратегии развития искусственного интеллекта (ИИ) на период до 2030 года, в которой определены цели и основные задачи его использования в РФ, а также меры, направленные на использование его развития в целях обеспечения национальных интересов и реализации стратегических национальных приоритетов, в том числе и области научно-технического развития [1, 3-5, 11].

Суть проблемы, исследуемой нами, состоит в отсутствии должного состояния оперативной обстановки (ОО) в ряде АТЕ страны, зависящей от умелого управления МВД РФ, как открытой системы (ОС), процессами, происходящими во внешней среде (ВС). Решение сформулированной выше проблемы состоит в исключении, где это возможно, человека из процесса управления деятельностью полиции. Иначе, предлагаемое нами решение проблемы состоит в возложении на МВД РФ автоматического выполнения его функций не только в типичных (когда $ОС_m$=$ВС_k$), но и в ряде проблемных ситуаций (когда $ОС_m$≠$ВС_k$), поддерживая тем самым приемлемую оперативную обстановку (ОО) не только в текущих типовых, но и в улучшенных и проблемных стоп-кадровых ситуациях с одинаковым для всех временном интервале Δt_n. Механизмы, объединяющие в себе эти две функции, называются автоматами. Человек, при этом, выполняет работу уже другого уровня и квалификации, а именно творческую работу по четкой идентификации типовых, рациональных и проблемных ситуаций и обучению ЦЭВМ, успешному их разрешению с пользой для себя, ОВД, страны и определяет суть успешного решения текущих задач и проблем, стоящих перед человечеством. Такой способ повышения производительности труда сотрудников МВД РФ получил название

автоматизации [9], которой обязательно предшествует творческая формализация деятельности разумного человека (организации). Мы утверждаем, что описанный нами способ разрешения человеком и человечеством этих ситуаций с пользой для себя имеет место и в деятельности любого сотрудника и МВД России в целом. Следовательно, массовое использование такого подхода всеми сотрудниками и коллективами ОВД позволит нашей полиции обеспечить разумную и своевременную автоматизацию ее деятельности на базе правильного использования представленных в данной работе теоретических положений и технологий их корректного применения. В этом состоит научная новизна и актуальность (практическая значимость) данной работы. Ее объект – МАУ ОВД, а предмет – ускоренная правильная автоматизация процесса решения типовых, оптимальных и проблемных вопросов на базе совместного использования новейших достижений естественного и искусственного интеллектов (ЕИ и ИИ) [11]. Цель работы – дать краткое описание научных основ такой автоматизации МАУ МВД России.

Для достижения поставленной нами цели в данной работе мы описываем апробированные на практике теоретические основы комплексного применения естественного и искусственного интеллекта в МВД РФ и приводим перечень действий, которые реально обеспечили решение стоящих перед нами проблем и задач: 1) выявление, на базе комплексного использования новейших достижении ЕИ и ИИ, технологии решения задач и проблем, способной реально обеспечить кардинальное улучшение управления индивидуальной и коллективной работой личного состава МВД РФ; 2) определение критерия, позволяющего реально отслеживать совершенствование работы МАУ ОС, на базе разработанных авторами математических моделей и алгоритмов их работ в типовых, улучшенных и проблемных ситуациях; 3) представление обобщенного алгоритма работы программного комплекса «Эйдос-АСА», адекватно реализующего представленные нами математические модели МАУ ОВД; 4) краткое описание позитивных конечных результатов (+Кр), полученных авторами при практическом использовании описанной в данной работе

технологии комплексного применения ИИ и ЕИ в силовых структурах СССР и РФ**,** подтверждающих высокую эффективность описанного в данной работе математического аппарата при правильном его использовании.

1. Выявление проблемы, решение которой обеспечит существенное улучшение управления наукой, образованием и практической деятельностью МВД РФ особого труда не составило, ибо она четко сформулирована в целевой установке данного исследования.

2. Выбор правильного критерия, позволяющего ОС выживать в постоянно изменяющей ВС, наши предшественники просто проигнорировали, хотя он был четко сформулирован еще в 30-е годы XX столетия академиком П.К. Анохиным в его теории функциональных систем (ТФС) [2,4-5]. Им оказался позитивный конечный результат (+Кр), обеспечивающий выживание человека в течение одного и того же типового временного интервала Δt_n, при выполнения следующего условия

$$|Y_m(x_n)–Y_k(x_n)| \le \varepsilon,$$

где $Y_k(x_n)$ – текущая стоп-кадровая математическая модель (ММ) воздействия внешней среды – $ВС_k$, а $Y_m(x_n)$ – ММ, это стоп-кадровая модель, правильная реализация которой с допустимой на практике погрешностью ε, обеспечивает выживание ОС в текущем *n*-ом стоп-кадре взаимодействия $ОС_m \leftrightarrow ВС_k$, когда $ОС_m = ВС_k$.

Мозг творческого человека фиксирует совпадение математических моделей $Y_m(x_n)$ и $Y_k(x_n)$, а затем, используя законы диалектики природы и резонанса [2, 4], организует в течение временного интервала Δt_n синхронную (коллективную) работу q функциональных элементов ($ФЭ_q$) с «эффектом системы» $y=e^q$, уравновешивает, в течение Δt_n), текущее воздействие внешней среды ($ВС_k$). Коллективная работа q $ФЭ_q$, позволяет использовать при этом, в реальном масштабе времени (РМВ), оптимальные $Y_m^{opt}(x_n)$ и новые $Y_m^{new}(x_n)$ математические модели, совпадающие с $Y_k(x_n)$, но дающие уже иные «эффекты системы» (при $ОС_m = ВС_k$), адекватные новой для ОС текущей ситуации, способствуя тем самым выживанию ОС и в ней. В конкретной текущей ситуации

ММ $Y_m^{opt}(x_n)$ и $Y_m^{new}(x_n)$ дают иные спектры резонансных частот $\omega_1, \omega_2, ..., \omega_p$, а, следовательно, и иные «эффекты системы» ОС. Именно поэтому в компьютерную программу «Эйдос-АСА» включена программа БПФ (Быстрого Преобразование Фурье), которая вычисляет уже другие спектры резонансных частот $\omega_1, \omega_2, ..., \omega_p$, присущие уникальным ММ $Y_m^{opt}(x_n)$ и $Y_m^{new}(x_n)$. Освоение и творческое применение природой взаимосодействия КОНтинуальной (непрерывной) и дисКРЕТНОЙ (дискретной) т.е. КОНКРЕТНОЙ математики /КМ/), позволяет человеку с помощью современной математики реально обеспечивать эффективное использование новейших достижений ЕИ и ИИ [3-4, 6].

При этом необходимо отметить, что все представленные выше математические модели используют вероятностные характеристики, которые представлены в унифицированном безразмерном виде (в долях единицы). Именно они представляют собой текущие поведенческие акты (ПА) – стоп-кадры реального взаимодействия ОС с ВС, протекающие в течение одинаковых по длительности временных интервалов Δt_n, в которых ОС обеспечила свое выживание. Символ n указывает (через приращения $\Delta x_n = n(x_{n+1}-x_n)/N$) на последовательное "пробегание" аргументом Δx_n каждого из N временных интервалов длиной $1/N$, на которые разбит отрезок [0,1], а символ k указывает общее число совпадений модели $Y_k(x_n)$ с ММ $Y_m(x_n)$ и $Y_k(x_n)$ с допустимой при этом погрешностью ε.

Для распознавания типичной, оптимальной и новой ситуации необходимо совпадение их моделей, т.е. выполнение условия $Y_k(x_n)=Y_m(x_n)$ /при их равенстве/. Ситуация $Y_k(x_n)\neq Y_m(x_n)$ указывает на то, что текущий стоп-кадр представляет не типичную для ОС ситуацию ее взаимодействия с внешней средой. Для превращения ее в типичную ситуацию МАУ ОС должен улучшить одну из типичных моделей $Y_m^{opt}(x_n)$ или сконструировать новую $Y_m^{new}(x_n)$ и реализовать их, обеспечивая желаемый +Кр, т.е. сбалансированность стоп-кадр $ВС_k$ с одним стоп-кадров $ОС_m$. Таким образом, формализованным дискретным критерием выживания ОС в подобных ситуациях, являются неравенства:

$$|Y_k(x_n) - Y_m(x_n)| \leq \varepsilon,\ |\Delta x_n| = n|x_{n+1} - x_n|/N \leq \delta,$$

где ε и δ – допустимые на практике погрешности в указанных измерениях значений $Y_k(x_n)$, $Y_m(x_n)$ и Δx_n, которые должны сличаться до и после проведения ПА, подтверждая получение желаемого +Кр.

В совокупности конечное множество всех моделей (мощности M) представляет собой непрерывную функцию от N дискретных переменных x_1, x_2, ..., x_N, числовые значения которых (параметры), отражают процесс стоп-кадровое взаимодействия $ОС_m \leftrightarrow ОС_k$ и заранее определяют ход и исход реализации частных моделей $Y_m(x_n)$ в конкретных ПА:

$$Y_m(x)=\sum Y_m(x_n) +\varepsilon=\sum Y_m(x_n(N)) +\varepsilon. \quad Y_k(x)=\sum Y_k(x_n) +\varepsilon=\sum Y_k(x_n(N)) +\varepsilon,$$

где $Y(x)$ – непрерывная функция непрерывного аргумента x, однотипно представляющая текущую дискретную математическую модель, хранящуюся в памяти человека, т.е. $Y_m(x_n)$ и стоп-кадровой модели текущего воздействия ВС на ОС, представленной дискретной моделью $Y_k(x_n)$; M – общее число дискретных функции Y_m (x_n) при разложении $Y(x)$ в дискретный ряд, а K – общее число дискретных значений $Y_k(x_n)$ переменных x_n, с помощью которых описываются все текущие дискретные функции $Y_k(x_n)$. М всегда равно К; ε – остаточный член ряда или допустимая из практических соображений погрешность совпадения $Y(x)$ с $\sum_m Y^M(x_n)$.

Дискретные функции $Y_m(x_n)$ представляют стоп-кадры, т.е. срезы процесса непрерывного развития ОС в изменяющейся ВС, а $Y_k(x)$ есть второй интегральный критерий развития ВС при ее взаимодействии с изменяющейся внешней средой. Этот факт в математике подтверждается теоремой Колмогорова А.Н. [8]

Теорема Колмогорова: Любая непрерывная функция Y от N переменных $Y(x_1, x_2,..., x_N)$, определенная на N –мерном единичном кубе, может быть представлена в виде суммы $2N+1$ суперпозиций непрерывных и монотонных отображений единичных отрезков, т.е. в виде:

$$Y(x_1, x_2,..., x_N) = \sum_{n=1}^{2N+1}\left(g_n \sum_{m=1}^{N}\left(h_{mn}(x_m)\right)\right),$$

где g_n и y_{mn} – непрерывные функции, причем y_{mn} не зависят от функции Y.

Слева в формуле стоит непрерывная произвольная функция, $Y(X)=Y(x_1, x_2,..., x_N)$, определенная на многомерном кубе (размерности N), справа функции определенные на отрезках [0, 1]. Монотонные непрерывные отображения y_{mn} могут иметь достаточно сложную структуру, но не зависят от конкретной функции Y. Эта теорема означает, что для реализации функций многих переменных достаточно операций суммирования и композиции функций одной переменной. Удивительно, что в этом представлении лишь функции g_n зависят от представляемой функции Y, а функции y_{mn} универсальны. До сих пор считалось, что определение функций y_{mn} и g_n для функции Y представляет собой математическую проблему, для которой пока не найдено общего строгого решения.

Нам с помощью Колмогорова А.Н. [8] удалось определить эти функции и установить конкретный вид функции $Y(x)$.

$$Y(x)=Y(x_1, x_2, \dots, x_N)=Y_m(x_n)=\sum\sum log_2(x_n)=\sum\sum log_2(N_{nm}N/N_nN_m),$$

где $Y(x)=Y(x_1, x_2,..., x_N)$ – непрерывная обобщенная математическая модель управления ОВД, представляемая в виде упорядоченного конечного множества дискретных типичных стоп-кадров, $Y_m(x_1,..., x_N)$, которые как дискретные *ММ* управления имеют вид

$$Y_m(x_1, x_2,..., x_N)=\sum log_2(x_n)$$

и отражают устойчивые (сбалансированные) срезы взаимодействия $ОС_m \leftrightarrow ОС_k$ в которых ОС (человек или коллектив выжила); m – текущий номер стоп-кадра взаимодействия $ОС_m \leftrightarrow ВС_k$, изменяющийся, от 1 до М; M – это общее количество типичных стоп-кадров $Y_m(x_n)$ или мощность множества ($M \le N$); N – число параметров, описывающих все типичные стоп-кадры; N_n – суммарное число встреч n-го параметра у всех $Y_m(x_n)$; N_m - суммарное число встреч различных параметров у m-й $Y_m(x_n)$; N_{nm} - суммарное число встреч n-го параметра у m-й $Y_m(x_n)$.Заметим, что функция $Y(x)$ зависит от целых чисел N, N_n, N_m и N_{nm}, которые представляют любое $x_n=N_{nm}\ N/N_n\ N_m$ в безразмерном виде (в долях единицы). Использование логарифмической функции с интервалом изменения [0, N] и метода дихотомии позволяет разложение функции $Y(x)$ в ряд следующего вида

$Y(x) = log_2(x) = \sum (-1)^{n-1} (x^n/n) = \sum (-1)^{n-1} (x_n^n)/n + \varepsilon = \sum (-1)^{n-1} 1/n\ (x_n)^n + \varepsilon,$

где $\varepsilon = (-1)^N 1/N\ [(1/N)^{N+1}]$ – остаточный член, стремящийся в пределе к 0.

В случае корректного использовании метода дихотомии (последовательного деления интервалов на отрезке [0, 1] пополам, то тогда функции $Y_m(x_n)$ и $Y_k(x_n)$) целесообразно для корректного сравнения представлять суммой $2N$ упорядоченных набором столбиков площадью $y_n \Delta x_n/2$., и высотой y_n, равной $y_n = 1/N^2\ (\Delta x_n/N)^{n-1}$, и основанием $\Delta x_n/2$. Тогда предыдущая формула корректно заменяется формулой []

$$Y_m(x_n) = \sum (-1)^{n-1} (\Delta x_n y_n) = \sum (-1)^{n-1} \Delta x_n\ [(\Delta x_n\ n)/N]^{n-1}/N^2.$$

Сформулированные дискретный и интегральный критерии успешного функционирования и развития ОС в изменяющейся ВС открывают возможность совместного использования методов исследования дискретных и непрерывных систем, т.е. методов конкретной математики. Ниже мы представим обобщенный алгоритм работы программного комплекса «Эйдос-АСА» [1], который адекватно реализует математические модели МАУ ОС.

А теперь мы проанализируем положения теории функциональных систем (ТФС) академика П.К. Анохина, раскрывшего диалектическую связь между естественным интеллектом (ЕИ) творческого человека и искусственным интеллектом (ИИ) на базе которого работают все ЦЭВМ (компьютеры) и цифровые средства связи. Заметим, что любая математическая модель, используемая человеком, обладает, как и сам объект, уникальными качественными характеристиками, присущими конкретному объекту, которые хранятся в его мозгу. Именно это обстоятельство сделало математику самым универсальным и эффективным инструментом познания. Это обусловлено тем, что все цифры, математические символы, буквы всех алфавитов и иероглифы, а также конечные множества из них обладают уникальными качествами. И только с их помощью человек однозначно отличает разные объекты и процессы, происходящие в природе и обществе. Именно это обстоятельство и делает математические модели главным и надежным инструментом познания реальных объективных (не зависящих от людей) законов и процессов [1,3-6,9-10]. Здесь

информатика (т.е. информация и автоматика вместе) являются самым надежным и эффективным инструментом познания реальных процессов, происходящих в природе и обществе, а использование +Кр, как критерия системно-образующего фактора, позволяет его организму лучше всех живых существ адаптироваться к изменениям окружающей его ВС– природы. Исследование взаимодействия континуального (непрерывного) и дискретного описания математических моделей убедительно показало их диалектическую связь. Они гармонично уравновешивают друг друга только в случае разложения непрерывной функции в числовые ряды в конкретной области ее определения – в множестве дискретных значений (в 2х-мерном квадрате 1×1). С этих позиций и следует рассматривать основные положения ТФС, используемые в системе «Эйдос-АСА» [1].

Ниже представлена обобщенная модель деятельности человека (самой эффективной в мире ОС), который обеспечивает свое выживание в изменяющейся ВС на основе использования положений ТФС и закона резонанса в процессе успешной реализации следующего алгоритма [1-2,9-10]:

1. построение стоп-кадровой модели $Y_k(x_n)$ воздействия ВС на ОС;

2. сличение $Y_k(x_n)$ с моделями $Y_m(x_n)$ [$(Y_m^{opt}(x_n), Y_m^{new}(x_n)]$, хранящимися в памяти ОС и выбор одной из них, совпавшей с допустимой погрешностью ε с $Y_k(x_n)$, для ее реализации в текущем стоп-кадре Δt_n (принятие решения);

3. вероятностное предвидение реального +Кр, связанного с использованием в выбранной модели q ФЭ$_q$, синхронная работа которых, при использовании закона резонанса и функции $y=e^q$, создает «эффект системы», обеспечивающий в течении текущего временного интервала Δt_n выживание ОС (акцептор результата действия);

4. реализация ОС совместной синхронной работы q задействованных в ней ФЭ$_q$, обеспечивающей в течение временного интервала Δt_n достижение должного эффекта системы» или +Кр, описываемого формулой $y=e^q$ при условии, что $Y_m(x_n)=Y_k(x_n)$;

5. дается реальная оценка коллективного действия q ее $ФЭ_q$, т.е. исполнительных или функциональных) элементов, обеспечивающих выживание ОС во временном интервале Δt_n, (результат действия);

6. делается оценка поведения организма, обеспечивающего его выживание в новых условиях взаимодействия $ОС_m \leftrightarrow ОС_k$ (результат действия);

7. устанавливаются параметры - количество исполнительных (функциональных) элементов уточненной (оптимальной) $Y_m^{opt}(x_n)$ или новой модели $Y_m^{new}(x_n)$, обеспечивающих выживание ОС новых условиях взаимодействия $ОС_m \leftrightarrow ОС_k$.

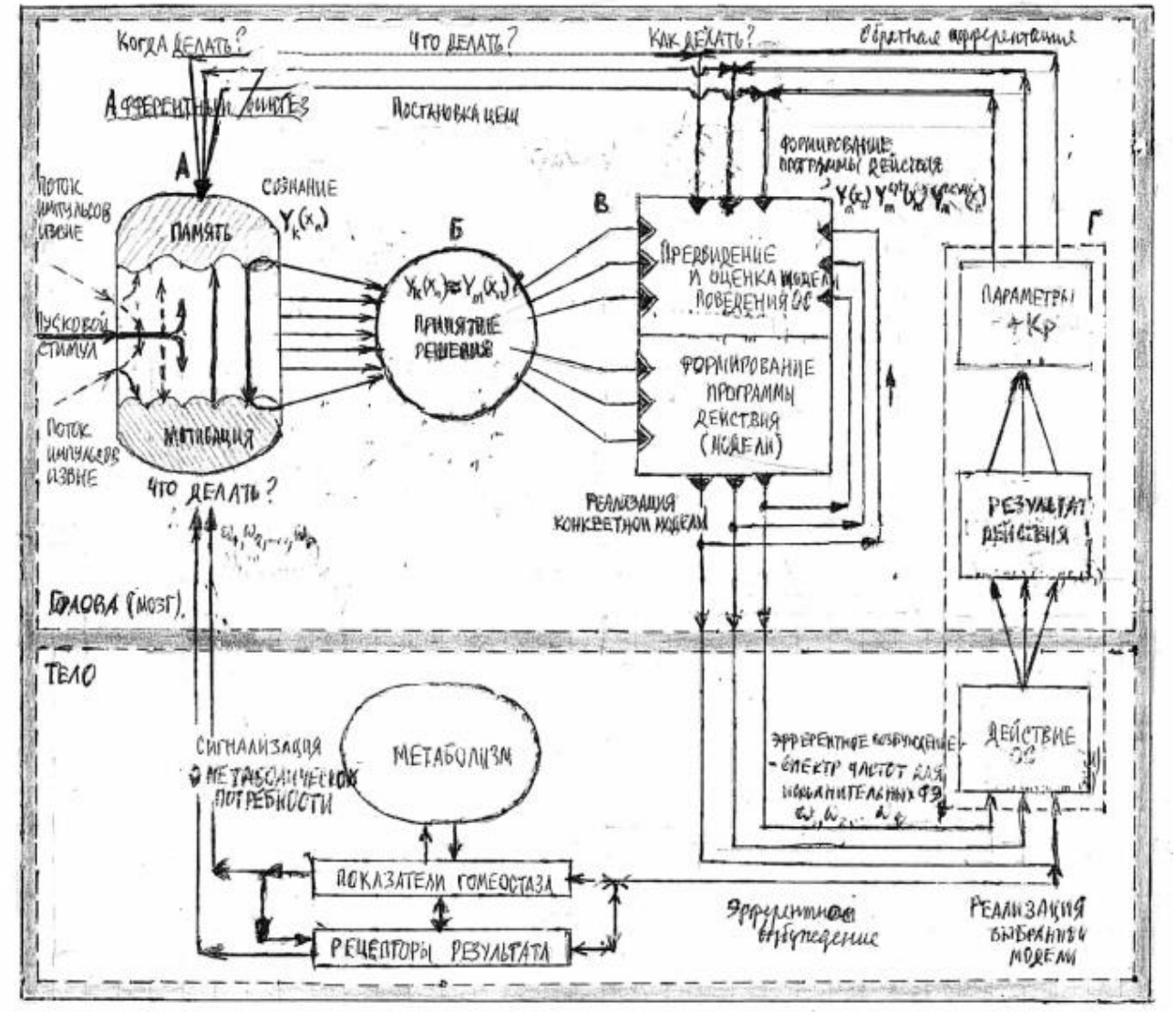


Рис. 1. Базовая схема функционирования и развития человеческого организма как самой совершенной ОС в мире

На рисунке 1 представлена структура функционирования и развития ОС, где А – блок построения текущей модели взаимодействия ОС с внешней средой $Y_k(x_n)$; Б – блок сравнения $Y_k(x_n)$ с типовыми моделями $Y_m(x_n)$, хранящимися в памяти ОС; В – блок разработки программы синхронной работы q функциональных элементов (ФЭ) для достижения $+Кр_m$; Г – блок фиксации наличие/отсутствия баланса $ОС_m=ОС_k$.

Для получения ожидаемого конечного результата, когда функция $Y_k(x_n)$, с допустимой погрешностью ε совпадает с одной из функций $Y_m(x_n)$, $Y_m^{opt}(x_n)$ или $Y_m^{new}(x_n)$ (хранящихся в памяти ЦЭВМ), одна из этих математических моделей и запускается в работу.

После этого выполняется переход к очередному *(k+1)-му* стоп-кадру взаимодействия $ОС_m \leftrightarrow ОС_{k+1}$ и т.д., потому, что человеку до сих пор удавалось создавать указанные выше модели, т.е. успешно решать эту проблему.

Архитектоника целенаправленного поведенческого акта человека в типовых и нетиповых для него ситуациях представлена, в блоке В, состоящем из 2-х под-блоков В.1– предвидения и оценки поведения ОС и В.2 – реализации одной из трех конкретной модели, адекватной текущей ситуации. В блоке Г указаны 3 этапа реализации выбранной человеком модели $Y_m(x_n)$. Из него в блок за счет обратной связи подаются спектры резонансных частот $\omega_1, \omega_2, ..., \omega_q$, обеспечивающие создание требуемого для выживания ОС «эффект системы», уравновешивающий в течение Δt_n все текущие внешние воздействие $ВС_k$ (т.к. $ОС_m=ВС_k$) с помощью моделей $Y_m(x_n)$, $Y_m^{opt}(x_n)$ и $Y_m^{new}(x_n)$. Туда же от рецепторов результата поведения и внутренних потребностей организма передаются параметры типовых воздействий внешней среды и внутренних потребностей организма $Y_m(x_n)$ [2-4, 7-10]. Суть его правильных поведенческих актов, обеспечивается корректным использованием требования $|Y_k(x_n)–Y_m(x)|\leq\varepsilon$ в новых математических моделях. В блоке принятия решения эти модели сравниваются текущей моделью $Y_k(x_n)$. При их совпадении с допустимой на практике погрешностью ε, т.е. при выполнения требования $|Y_k(x_n)–Y_m(x)|\leq\varepsilon$ в блоке В.1 принятия решения эфферентные (выходные) возбуждения вычисляются

резонансные частоты $\omega_1, \omega_2, ..., \omega_q$ *ФЭ* для импульса $Y_m(x_n)$, создающие «эффект системы» $ОС_m$, уравновешивающий воздействие внешней среды $ВС_k$ на организм человека в текущем стоп-кадре. Затем происходит переход к следующему *(k+1)* стоп-кадру взаимодействия ОС с ВС.

При несовпадении $Y_k(x_n)$ *с* $Y_m(x_n)$ мозг либо 1) оптимизирует матрицу типовых знаний (МТЗ), либо 2) заново ее пересчитывает, формируя одну/несколько моделей $Y_m(x_n)$, $Y^{opt}{}_m(x_n)$, или создают новую МТЗ, где $Y^{new}{}_m(x_n)$ формируются заново. Процессы автоматической реализации $Y_m(x_n)$, $Y^{opt}{}_m(x_n)$ и $Y^{new}{}_m(x_n)$ включают в себя построение указанных моделей и их сличение с $Y_k(x_n)$.

Функциональные системы (ФС) организма – это динамические, саморегулирующиеся центрально-периферические структуры организации, обеспечивающие своей деятельностью полезные для метаболизма организма и его приспособления к окружающей среде результаты. Метаболизм – это совокупность процессов превращения и обмена веществ, энергии в живом организме человека (ОС) или между ним и окружающей его постоянно изменяющейся ВС. Для достижения полезных для организма результатов в его ФС избирательно объединяются функциональные элементы (ФЭ) разных уровней (ткани органов, механизмы нервной и гуморальной регуляции). Регуляторные взаимодействия свойственные ФС, обеспечивают: 1) необходимую адаптивную устойчивость результатов их деятельности и 2) взаимосодействие ФЭ для достижения ПКР для всего организма (как ОС) в целом. Общий принцип работы ФС - принцип саморегуляции. Отклонение результата деятельности ФС от уровня, обеспечивающего оптимальную жизнедеятельность организма, стимулирует активность процессов, направленных на возвращение этого результата к норме. Любая ФС имеет однотипную организацию и типовые механизмы. Механизм адаптивного управления ОС (человеком) – это система, определяющая порядок конкретного вида деятельности организма человека (ОС): а) получение полезного приспособительного результата от поведения человека; б) работу рецепторов; в) передачу сигналов от рецепторов в ЦНС, спинной и головной мозг; г) работу по

избирательному объединению нейронов различных уровней, моделирующих процесс взаимодействия организма с ВС; д) совместную деятельность исполнительных компонентов организма как ОС, обеспечивающую (через сигналы управления, поступающие из головного мозга) реализацию конкретной модели поведения человека в ходе его взаимодействии с изменяющейся внешней средой [1-6]. Анохин П.К подчеркивал, что каждый организм представляет собой динамическое сочетание устойчивости и изменчивости, в котором изменчивость служит его приспособительным реакциям и, следовательно, защите его наследственно закрепленных констант, а физиологический смысл адаптации организма к внешним и внутренним воздействиям заключается именно в поддержании гомеостаза и, соответственно, жизнеспособности организма практически в любых условиях, на которые он в состоянии адекватно реагировать [2].

Согласно его концепции у компонентов, участвующих в построении одной системы, обязательно ограничиваются степени свободы для их участия в другой. При этом ФС "стремится" получить запрограммированный результат и ради этого может пойти на самые большие возмущения во взаимодействиях своих компонентов. Поэтому системой по Анохину П.К. можно назвать лишь такой комплекс избирательно вовлеченных компонентов, у которых взаимодействие и взаимоотношения приобретают характер взаимосодействия компонентов на получение фокусированного полезного результата. Системообразующим фактором ОС является +Кр. Он неотъемлемый компонент ОС, инструмент, создающий упорядоченное взаимодействие между всеми его компонентами.

Отметим, что МАУ ОВД России – эта универсальная система, определяющая порядок управления конкретными видами деятельности МВД РФ – это ОС: а) по получению приспособительного +Кр ее поведения; б) по обеспечению нормальной работы ее рецепторов; в) по передаче сигналов от рецепторов в орган моделирования; г) работой по избирательному конструированию нужных для выживания МВД России математических моделей $Y_k(x_n), Y_m(x_n), Y_m^{opt}(x_n)$ и $Y_m^{new}(x_n)$, моделирующих процесс

взаимодействия ОС с ВС; совместную деятельность исполнительных ее органов организма, обеспечивающую (через сигналы управления, поступающие центра управления) реализацию конкретной модели поведения ОС в ходе ее взаимодействия с изменяющейся внешней средой.

Взаимодействие ОС с постоянно изменяющейся внешней средой (ОС) в типичных (устойчивых) и нетипичных (неустойчивых) ситуациях представлено на рисунке 2 в виде алгоритмической модели работы МАУ ОВД. Она обеспечивает создание нужного для ее выживания в конкретном *m*-м стоп-кадре «эффекта системы» [2-3,7,9-10]. В правом верхнем углу указана матрица типовых знаний (МТЗ), а в нижнем левом – иерархические оргструктуры из *q* функциональных элементов ($ФЭ_q$), синхронная, работа которых создает нужные для выживания ОС «эффекты системы» $+Кр_m=ОС_m=ОС_k$. При совпадении $Y_m(x_n)$ с $Y_k(x_n)$ ОС выживает в текущем *k*-м стоп-кадре ее взаимодействия с изменяющейся ВС. МТЗ состоит из *m* строк типовых функций $Y_1(x_n)$, ..., $Y_m(x_n)$,..., $Y_M(x_n)$ от *n* переменных x_n, которые сравниваются с текущей функцией $Y_k(x_n)$. При выполнении условия $|Y_k(x_n)–Y_m(x)|\leq \varepsilon$, в блоке ДПФ (дискретное преобразование Фурье) вычисляются собственные круговые частоты $\omega_1, \omega_2, ..., \omega_q$ для $Y_m(x_n)=Y_k(x_n)$, создающие «эффект системы» $ОС_m$, уравновешивающий воздействие внешней среды $ВС_k$ на ОС в текущем *k*-м стоп-кадре [1-5].

На рисунке 2 используются следующие обозначения: Фк – фиксация/не фиксация параметров внешнего текущего воздействия на ОС; Оц – оценка параметров внешнего (из среды) и внутренних (от ОС) воздействий или возврат в блок Фк; Кд – кодирование параметров воздействия или возврат в блок Оц; $Y_k(x_n)$ – построение повой модели текущего стоп-кадра или возврат в блок Кд; Ид – идентификация модели типового текущего стоп-кадра $Y_k(x_n)$ путем его сравнения с типовыми $Y_m(x_n)$ из МТЗ (при совпадении $Y_m(x_n)=Y_k(x_n)$ переход в блок Авт – автоматики, иначе возврат в блок Кд); Авт – блок автоматики, где ОС принимается решение о формальном, т.е. автоматическом создании нужного «эффекта системы» за счет перехода в блок ДПФ, иначе переход в блок ФЛ – формальной логики; ДПФ – блок автоматического вычисления спектра круговых

частот $\omega_1, \omega_2, \ldots, \omega_q$, обеспечивающих, за счет синхронной работы q $ФЭ_q$, должный для выживания ОС «эффект системы», иначе возврат в блок Авт; Об – общая передача спектра команд управления $\omega_1, \omega_2, \ldots, \omega_q$ исполнительным элементам и обеспечение ими, за счет коллективной работы требуемого «эффект системы», иначе возврат в блок Авт; блок +Кр – оценка полученного +Кр, если он получен управленческий кадр окончен, иначе переход к блоку Об [2-3].

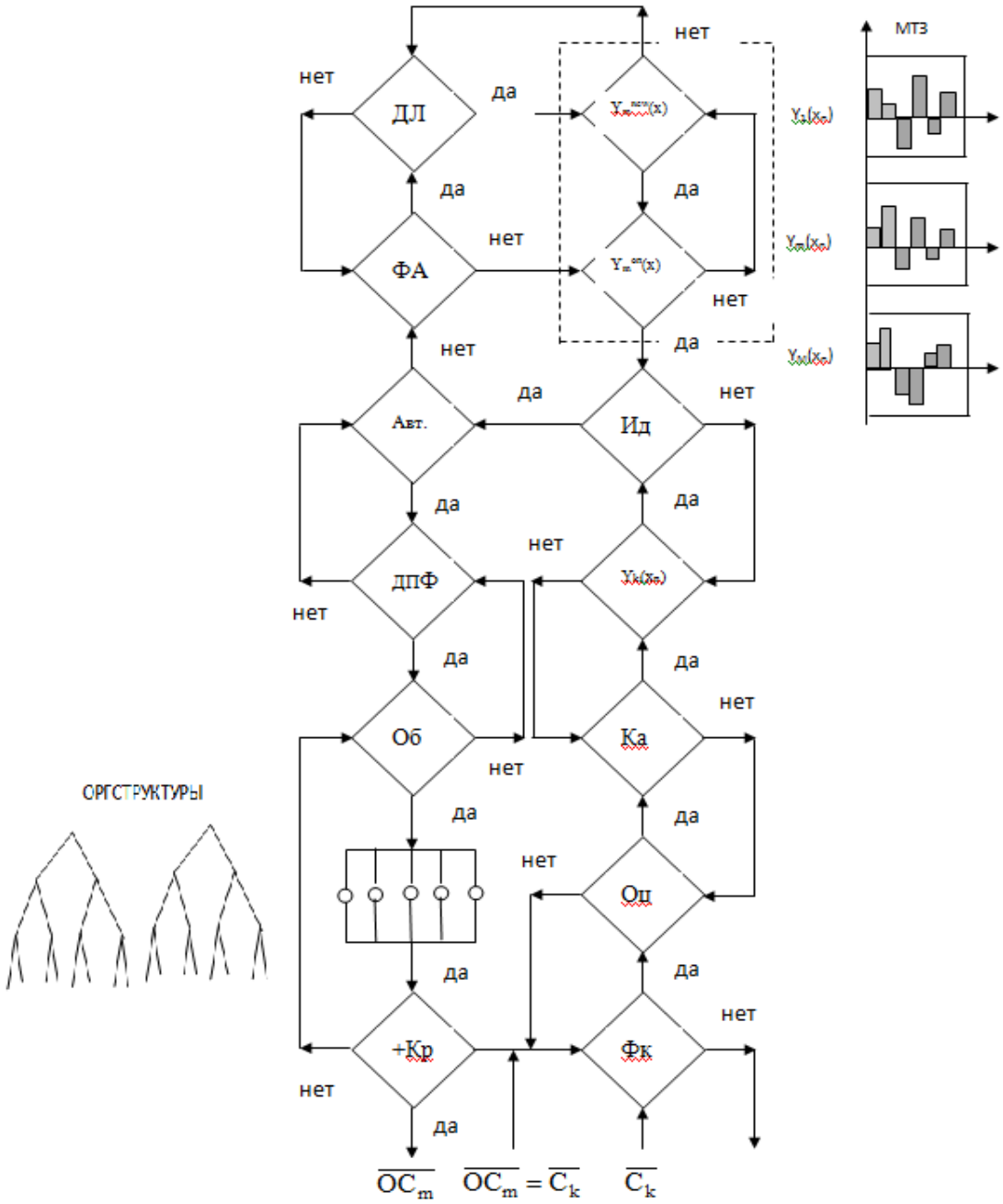


Рис. 2. Концептуальная алгоритмическая модель работы МАУ ОС

Все указанные в верхнем абзаце блоки используются для автоматической реализации типовых моделей поведении ОС. Однако в организме человека природа отработала еще 2 запасных варианта, обеспечивающих его выживание. Первый вариант основывается на частичном улучшении некоторых типовых моделей $Y_m(x_n)$ за счет их оптимизации – создания моделей $Y_m^{opt}(x_n)$. Второй вариант реализует полный пересчет МТЗ, $Y_m(x_n)$, т. е. создание новой МТЗ, где все модели $Y_m^{new}(x_n)$ обладают принципиально новыми уникальными качествами [1-3].

Поясним суть оптимизации и построения новой МТЗ. Оптимизация МТЗ представляет собой промежуточный вариант ее кардинального обновления. ФЛ – блок формальной логики, где выясняется, можно ли формально улучшить одну или несколько функций $Y_m(x_n)$. Если можно, то переход в блоке $Y_m^{opt}(x_n)$, иначе возврат в блок Авт; ДЛ – блок диалектической логики, где устанавливается возможность кардинального улучшения МТЗ и осуществляется переход к блоку $Y_m^{new}(x_n)$, иначе возврат в блок $Y_m^{opt}(x_n)$; $Y_m^{new}(x_n)$ – блок пересчета всей МТЗ на базе новейших достижений науки и техники, иначе возврат в $Y_m^{opt}(x_n)$ [2-3,10-11].

Краткое описание позитивных конечных результатов (+Кр), полученных авторами при практическом использовании описанной в данной работе технологии комплексного применения естественного и искусственного интеллекта в силовых структурах СССР и РФ**,** подтверждающих высокое качество идей и математического аппарата используемого в системе «Эйдос» и ее усовершенствованных вариантах.

1. Подготовка в течение 1 месяца необученного личного состава (из Узбекистана) к эффективной боевой работе личного состава зенитно-артиллерийской (ракетной) батареи – комплекса С-60 (имеющей на вооружении ПЗРК, 8 57 мм зенитных орудий, ПУАЗО, СОН-9А и всего 2 офицерами вместо 6 (причем 1 из их двухгодичник, прибывший в КДВО после окончания с отличием мехмата) к реальным боевым стрельбам (КДВО, 1972). Батарея выполнила стрельбы на «отлично».

2. Совершенствование системы оповещения и сбора личного состава МВД Казахской ССР, а также отработка рациональных действий личного состава в

экстремальных ситуациях (при природных и иных катаклизмах, массовых беспорядках, захвате заложников, беспорядках в СИЗО, ИТК. (1981-1986гг.)).

Таблица 1. Рост эффективности системы оповещения и сбора л/с МВД Казахской ССР

Время оповещения и сбора личного состав МВД Казахской ССР	XI. 1981	II. 1981	III. 1981	VI. 1981	XII. 1981	II. 1982	Далее стабильно
Время доведения сигнала до всего л/с (мин)	55-60	52	45	12	8	5	3-4
Доля л/с, своевременно прибывшего ОВД (10-20 мин)	-	87.5%	90.6%	84.7%	96.7%	98.7%	99-100%
Рост производительности труда системы оповещения	1	1.14	1.34	5	7.5	12	20

Отработка до автоматизма рациональных действий личного состава в экстремальных ситуациях обеспечили отличные действия ОВД при авиакатастрофе пассажирского самолета и беспорядках в г. Алма-Ате, также при пресечении беспорядков в СИЗО и ИТК, дислоцирующихся в Алма-Атинской области.

3. Обоснование использования не 1, а 33 пунктов управления для распределенных систем оперативного управления силами и средствами ПВО г. Москвы и ГУВД г. Москвы, обеспечивающих по сути дела, многократное повышение производительности труда в обоих ведомствах за счет весьма эффективного использования моделей коллектива вычислителей в обоих ведомствах: МО СССР и МВД СССР (1983-1985 гг.).

4. Моделирование, обучение и реализация личным составом ОВО УВД Алма-Аты (1985-1987) самого лучшего в МВД СССР МАУ оперативного реагирования на сообщения о преступлениях. С его помощью достигнуто 100% раскрытие квартирных краж, грабежей и разбоев в г. Алма-Ате с миллионным населением. "Подлетное время" групп задержания, т.е. их прибытие на место происшествия составляло $t_{реаг} \leq$ 1-1,5 мин, среднее время обслуживания $t_{обсл} \leq$ 2-2,5 мин (всего 3-4 мин.).

5. Использование на практике и в процессе обучения разработанной в городском ОВО г. Алма-Аты компьютерной программы ASAFO, обеспечивающей быстрое установление и грамотное рациональное использование модели коллектива личным составом, аттестованными и гражданскими лицами 8 отделов ОВО (сотрудниками пультов централизованно охраны (ПЦО), групп задержания (ГЗ) и патрульно-постовой службы (ППС) г. Алма-Аты), направленными на место происшествия для быстрого и качественного обслуживания тревог, поступающих с охраняемых объектов и мест происшествий (на ПЦО отделов вневедомственной (ОВО) и в дежурную часть (ДЧ) РОВД). Компьютерная программа ASAFO позволяла весьма эффективно имитировать процесс эффективного уравновешивания внешних воздействий (потока тревог, сообщений о преступлениях и массовых беспорядках, поступающий в полицию и ОВО), что позволило во время беспорядков в г. Алма-Ате (в 1986 г.) быстро и эффективно ликвидировать их, а также обеспечить 100% раскрытие квартирных краж.

6. В 1995 году с помощью компьютерной программы "Эйдос" в КЮИ МВД РФ, по указанию руководства ГУВД Краснодарского края, было проведено тестирование 87 офицеров-сотрудников ОВД, имеющих высшее образование не по правоохранительному профилю. Оно установило, что 3 из этих сотрудников служба в ОВД России противопоказана. Это неожиданный результат всех развеселил, ибо все посчитали, что это просто розыгрыш. Однако из ОВД они были уволены в течение 1 года после тестирования, причем по отрицательным мотивам, т.е. прогноз компьютера оказался достоверным. Самое интересное, что методические материалы, по системе «Эйдос», используемой в КЮИ МВД РФ при тестировании, и описание основных идей компьютерной программы «Эйдос» были обнаружены через 1,5 года в библиотеке Конгресса США.

Литература

1. Адаптивная автоматизированная система управления «Эйдос-АСА» (Система «Эйдос-АСА). Е.В. Луценко, В.Н. Лаптев // Свидетельство о регистрации программы для ЭВМ RU 2008610098. Заявка №2007613723.

2. Анохин П.К. Избранные труды. Философские аспекты теории функциональных систем. – М.: Наука, 1978. – 399 с.

3. Аршинов Г.А. Повышение экономической и эксплуатационной надежности трубопроводных сооружений совершенствованием методов обнаружения микродефектов / Г.А. Аршинов. Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2021. – №06(170).

4. Денисов А.А. Информационные основы управления. – Л.: Энергоатомиздат, 1983. – 72 с.

5. Информационная безопасность: учеб. пособие /В.И. Лойко, В.Н. Лаптев, Г.А. Аршинов, С.В. Лаптев. – Краснодар: КубГАУ, 2020. – 332 с.

6. Грэхмен Р. Конкретная математика: Основания информатики. / Р. Грэхмен, Д. Кнут, О. Паташник. – М.: Мир, 2006. – 703 с.

7. Евреинов Э.В. Однородные вычислительные системы, структуры и среды. – Радио и связь, 1981. – 208 с.

8. Колмогоров А.Н. О представлении непрерывных функций нескольких переменных в виде суперпозиций непрерывных функций одного переменного и сложения. /Доклады АН СССР, 1957, т.114, - С. 953-956.

9. Моисеев Алгоритмы развития. – М.: Наука, 1987. – 703 с.

10. Стабин И.П. Автоматизированный системный анализ / И.П. Стабин, В.С. Моисеева – М.: Машиностроение, 1984. – 304 с.

11. Указ Президента РФ от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации».

Сведения об авторах

Лаптев Владимир Николаевич, кандидат технических наук, доцент кафедры компьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина; e-mail: lvn4828@yandex.ru.

Лаптев Сергей Владимирович, кандидат физико-математических наук, доцент кафедры компьютерных технологий и систем Кубанского государственного аграрного университета имени И.Т. Трубилина; e-mail: laptevsergey76@mail.ru.

Левачева Юлия Валерьевна

ПРИМЕНЕНИЕ МУЛЬТИМЕДИЙНЫХ ТЕХНОЛОГИЙ В ОБРАЗОВАТЕЛЬНОМ ПРОЦЕССЕ

Стремительное развитие мультимедийных технологий обеспечивает техническую поддержку высшему образованию и заставляет его двигаться в направлении автоматизации и информатизации. Мультимедийные технологии приходят на смену традиционному режиму образования, постепенно вытесняя и заменяя его.

Мультимедиа технологии в век цифровизации оказали огромное влияние и внесли свои коррективы в качество передаваемого материала в целый ряд областей науки, одной из таких областей является образование.

Мультимедийные технологии – создание продукта, с помощью которого возможно информировать аудиторию с помощью использования новых технологий. Кроме визуальных и аудиоэффектов данная совокупность методов и инструментов включает в себя способы управления интерактивным интерфейсом. [5]

В 1945 году американскими учеными Ваннивером и Бушем была осуществлена концепция организации памяти “MEMEX”, которая по своей сути является идеальным положением происхождения технологии мультимедиа. Благодаря рассмотренному тезису поиск информации осуществлялся не по формальным признакам (по алфавитному порядку, цифровому или индексовому), а в соответствии с ее семантическим содержанием. [8]

Ступени развития мультимедиа:

1. Структура гипертекста (работа с комбинацией текстовых материалов).

2. Гиперсреда (система, работающая с комбинацией графики, звука, видео и мультфильма).

3. Мультимедиа, которая объединила структуру гипертекста и гиперсреду в единое целое.

Более 30 лет назад мультимедиа технологии начали постепенно внедряться в образование. В 1986 году в американские школы поступила первая мультимедийная энциклопедия Groiler.

В перспективе развития области образования мультимедиа вносят коррективы в информатизацию учебного процесса, а именно, его методического и программного совершенствования, повышение квалификации преподавательского состава.

Компьютер и видеопроектор, как основные средства донесения и представления информации, позволяющие в наиболее доступном виде, визуально-вербальным способом донести до восприятия обучающимся необходимую информацию.

В настоящее время изменение системы образования предполагает построение новой модели преподавания. Довольно сложно представить современный образовательный процесс без самой известной мультимедийной технологии – презентации. Они являются наиболее применяемым педагогами мультимедийным продуктом, так как презентации просты в использовании и являются общедоступным продуктом.

Зачастую, презентации используются для сопровождения учебного процесса, с демонстрацией наглядного материала и его текстовым описанием. Для того, чтобы презентация имела новизну в дидактическом плане, а не являлась лишь средством пассивного отображения изучаемого материала, необходимо в полной мере использовать все возможности данного продукта, а именно: гиперссылки, триггеры, анимацию, все то, что превращает обычную презентацию в интерактивный объект. [2]

Мультимедиа технологии обладают рядом преимуществ:

- широкая доступность,
- многократность использования мультимедиа (возможность постоянного наполнения, корректировки и совершенствования),
- снижение учебной нагрузки на преподавателя,

- индивидуальная вовлеченность студентов и глобальность,

- длительный срок хранения.

Некоторые учащиеся могут усваивать мультимедийные материалы лучше, чем в любом другом формате. Возможности этой среды для студентов с предпочтениями в слуховом или визуальном стиле обучения - беспрецедентны.

Так называемая «Пирамида обучения», наглядно демонстрирует средний процент усвояемости и запоминания информации. [7]

Рис.1. Пирамида обучения

Как видим из приведенного выше примера (Рис.1), если занятия проходят с применением мультимедиа технологий, то процент усвоения полученной информации значительно увеличивается.

Использование при проведении занятий мультимедийных технологий позволяет преподавателю более гибко выстраивать модель передачи информации от преподавателя к обучающемуся, а также с легкостью менять формы учебного взаимодействия.

К примерам использования мультимедиа со стороны учебно-методической деятельности можно отнести:

- оперативный контроль (на этапе изучения нового материала направлен на активизацию внимания);

- при закреплении полученных знаний и навыков в процессе обучения, интерактивное взаимодействие с компьютером, на этапе повторения и закрепления материала;

- текущий и итоговый контроль на всем этапе обучения от промежуточных итогов к завершающему контрольному тестированию с подведением итога усвоенной информации.

В современных реалиях мультимедиа в образовании облегчило его получение и помогло сделать образование более эффективным и доступным, в котором задействованы все органы, служащие для восприятия информации. Стал возможным индивидуальный подбор обучения для каждого человека, появилась возможность домашнего обучения дистанционно. [3]

Преимущества применения мультимедийных технологий в образовании:

1. Обеспечение гибкости и интерактивности учебного процесса.
2. Использование в сочетании аудио, видео, комментариев, анимации с параллельным сочетанием на экране.
3. На любом этапе обучения возможен самоконтроль, что является немаловажным для дистанционного, а также самостоятельного обучения.
4. Знания, полученные в ходе обучения с применением мультимедиа технологий, являются наиболее глубокими, и остаются в памяти на долгий срок. Происходит быстрое восстановление полученных таким образом знаний после повторения, для применения их на практике.
5. Уменьшаются затраты на повышение квалификации, ведь ее можно пройти дистанционно. Происходит экономия времени и экономия затрат.
6. Увеличивается заинтересованность обучаемых в получении информации, представленной с применением мультимедиа технологий, также возрастает количество обучаемых на одного преподавателя.

К недостаткам применения мультимедийных технологий в образовательном процессе можно отнести следующее:

1. Самым главным недостатком является уменьшение живого общения между преподавателем и обучающимся.

2. Все еще сохраняется проблема обеспечения рабочего места компьютерно-ориентировочным сопровождением учебного процесса.

3. Отсутствие соответствующего учебно-методического обеспечения. [4]

Подводя итог, можно отметить, что положительные стороны применения мультимедийных технологий в учебном процессе все же преобладают над отрицательными. Смена традиционных методов обучения неизбежна, и, полагаю, с развитием информационных технологий количество положительных аспектов будет постепенно увеличиваться, а отрицательных соответственно уменьшаться.

В результате применения мультимедийных технологий в образовательном процессе, интерес у обучающихся к изучаемой дисциплине возрастает, обучающийся становится активным субъектом учебной деятельности, который заинтересован в процессе усвоения материала и достижению целей в профессиональном образовании.

Литература

1. Андреев, А. А. Введение в Интернет-образование: учеб. пособие / А.А. Андреев. – М.: Логос, 2003. – 73 с.

2. Андресен, Бент. Б. Мультимедиа в образовании: специализированный учеб. курс: [пер. с англ] / Бент. Б. Андерсен, Катя Ван Ден Бринк. – 2-е изд.; испр. и доп. – М.: Дрофа, 2007. – 221 с.

3. Захарова, И. Г. Информационные технологии в образовании: [учебное пособие для высших педагогических учебных заведений] / И.Г. Захарова. – М.: Академия, 2003. – 188 с.

4. Новиков, С.П. Применение новых информационных технологий в образовательном процессе / С.П. Новиков // Педагогика. – 2003. – N9. – С. 32-38.

5. Смолянинова, О. Мультимедиа для ученика и учителя / О. Смолянинова // Информатика и образование. – 2002. – N2. – С. 48-54.

6. Виртуальный компьютерный музей. История развития программного обеспечения: Ванневар Буш и система Memex: [Электронный ресурс] //, [сайт]. [2023]. URL: https://computer-museum.ru/histsoft/bush.htm (дата обращения: 13.03.2023).

7. «Пирамида Дейла» правда ли, что обучение на практике лучше любой теории? [Электронный ресурс] //, [сайт]. [2021]. URL: https://skillbox.ru/media/education/piramida-deyla-pravda-li-chto-obuchenie-na-praktike-luchshe-lyuboy-teorii/ (дата обращения: 20.04.2023).

8. Ярушин А.В. Мультимедийные технологии [Электронный ресурс] //, Лекционный курс: [сайт]. [2019]. URL: http://www.tula.net/tgpu/resouces/yakushin/html_doc/doc08/doc08index.htm(дата обращения: 20.04.2023).

Сведения об авторе

Левачева Юлия Валерьевна, преподаватель кафедры информатики и математики Волгоградской академии МВД России; e-mail: sulikojul@mail.ru.

Левина Любовь Владимировна,
Пеньков Виктор Борисович,
Левин Максим Юрьевич,
Марахова Ирина Игоревна

ЭНЕРГЕТИЧЕСКИЙ МЕТОД ГРАНИЧНЫХ СОСТОЯНИЙ ДЛЯ РЕШЕНИЯ ЗАДАЧ МАТЕМАТИЧЕСКОЙ ФИЗИКИ

Постановка задачи.

Все нижеизложенное имеет безразмерную форму. Однополостный однородный изотропный полушар находится в состоянии термостатического равновесия. Поверхность полушара (например, поверхность земли) поддерживает постоянную температуру, отсчитываемую от нулевого уровня: $T\big|_{S_1} = 0$. Уровень температуры боковой поверхности полушара равномерно убывает по глубине: $T\big|_{S_2} = 10\sin\theta$. Сферическая полость расположена на глубине $h \in \{3; 2.5;\ 2; 1.5\}$ от плоской границы полушара, на ее границе удержана постоянная отрицательная температура («холодильник») $T\big|_{S_3} = -3$. Требуется проанализировать изменение поля температуры от глубины залегания сферической полости и дать рекомендации о корректном использовании свойств среды для обеспечения работоспособности сферического «холодильника».

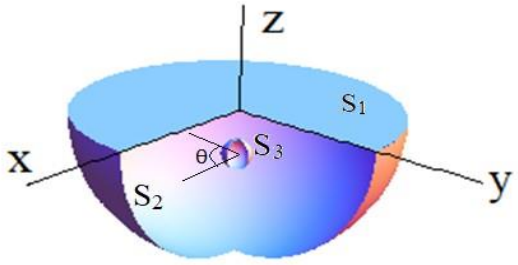


Рис. 1. Полушар с полостью

Метод решения.

Задача решается энергетическим методом математической физики, а именно методом граничных состояний (МГС) [1].

Основополагающим понятием в МГС является понятие состояния среды – любого частного решения определяющих уравнений среды. В термостатической

среде определяющим является уравнение теплопроводности (тензорно-индексная форма записи)

$$T_{,ii} = -\frac{1}{\kappa} Q,\ x \in V \in R^3, \qquad (1)$$

где V – область, занятая телом, $x = \{x_i\}_3$, T – поле температуры, Q – объемный теплоисточник, κ – коэффициент температуропроводности. Способ решения рассмотрен в [2]. Подробнее рассмотрим алгоритм решения поставленной задачи. Реализация решения произведена в системе Mathematica 7.0 в авторском разработанном пакете ILION.

Алгоритм решения термостатической задачи для полушара с полостью предполагает ряд действий:

1. Определение геометрических и физических свойств тела. Параметризация области представлена в таблице.1.

Таблица 1. Описание формы области

Подобласть 1	Параметризация	{x → r Cos[fi] Cos[teta], y → r Cos[teta] Sin[fi], z → r Sin[teta]}
	Якобиан	$r^2 \mathrm{Cos}[\mathrm{teta}]$
	Ограничения	$\left\{\{\mathrm{fi}, -\pi, \pi\}, \left\{\mathrm{teta}, -\frac{\pi}{2}, 0\right\}, \{\mathrm{r}, 0, 10\}\right\}$
	индикатор +	1
	Обр. параметризация	$\left\{\mathrm{r} \to \sqrt{x^2+y^2+z^2},\ \mathrm{fi} \to \mathrm{ArcTan}\left[\frac{y}{x}\right] + \frac{1}{2}\pi\,(1 - \mathrm{Sign}[x])\,\mathrm{Sign}[y],\ \mathrm{teta} \to \mathrm{ArcTan}\left[\frac{z}{\sqrt{x^2+y^2}}\right]\right\}$
	Окрестности особ.точек	{{{0, 0, -3}, 0.01}}
Подобласть 2	Параметризация	{x → r Cos[fi] Cos[teta], y → r Cos[teta] Sin[fi], z → -3 + r Sin[teta]}
	Якобиан	$r^2 \mathrm{Cos}[\mathrm{teta}]$
	Ограничения	$\left\{\{\mathrm{fi}, -\pi, \pi\}, \left\{\mathrm{teta}, -\frac{\pi}{2}, \frac{\pi}{2}\right\}, \{\mathrm{r}, 0, 1\}\right\}$
	индикатор +	-1
	Обр. параметризация	$\left\{\mathrm{r} \to \sqrt{x^2+y^2+(3+z)^2},\ \mathrm{fi} \to \mathrm{ArcTan}\left[\frac{y}{x}\right] + \frac{1}{2}\pi\,(1 - \mathrm{Sign}[x])\,\mathrm{Sign}[y],\ \mathrm{teta} \to \mathrm{ArcTan}\left[\frac{3+z}{\sqrt{x^2+y^2}}\right]\right\}$

Задание граничных условий (ГУ) выполнено в соответствии с постановкой задачи. Параметризация границы области представлена таблицей 2.

2. Генерирование исходного базиса пространства внутренних состояний однополосного ограниченного тела.

При отсутствии теплоисточников исходный базис формируется по двум шаблонам:

1) для ограниченной области его элементами являются гармонические

многочлены: $T \in \{x, y, z, yz, xz, xy, ..\}$;

2) для внешности неограниченной полости – инверсные образы этих полиномов $T \in \{\frac{1}{r}, \frac{x}{r^3}, \frac{y}{r^3}, \frac{z}{r^3}, \frac{yz}{r^5}, \frac{xz}{r^5}, ..\}$,

Таблица 2. Описание границы области

Граница 1	Параметризация	{x → r Cos[fi], y → r Sin[fi], z → 0}
	Якобиан	r
	Обр. параметризация	$\left\{r \to \sqrt{x^2+y^2},\ fi \to \text{ArcTan}\left[\frac{y}{x}\right] + \frac{1}{2}\pi\,(1 - \text{Sign}[x])\,\text{Sign}[y]\right\}$
	Ограничения	{{r, 0, 10}, {fi, -π, π}}
	Нормаль	{0, 0, 1}
	Касательная 1	{Cos[fi], Sin[fi], 0}
	Касательная 2	{-Sin[fi], Cos[fi], 0}
Граница 2	Параметризация	{x → 10 Cos[fi] Cos[teta], y → 10 Cos[teta] Sin[fi], z → 10 Sin[teta]}
	Якобиан	100 Cos[teta]
	Обр. параметризация	$\left\{fi \to \text{ArcTan}\left[\frac{y}{x}\right] + \frac{1}{2}\pi\,(1 - \text{Sign}[x])\,\text{Sign}[y],\ teta \to \text{ArcTan}\left[\frac{z}{\sqrt{x^2+y^2}}\right]\right\}$
	Ограничения	$\left\{\{fi, -\pi, \pi\}, \left\{teta, -\frac{\pi}{2}, 0\right\}\right\}$
	Нормаль	{Cos[fi] Cos[teta], Cos[teta] Sin[fi], Sin[teta]}
	Касательная 1	{-Sin[fi], Cos[fi], 0}
	Касательная 2	{-Cos[fi] Sin[teta], -Sin[fi] Sin[teta], Cos[teta]}
Граница 3	Параметризация	{x → Cos[fi] Cos[teta], y → Cos[teta] Sin[fi], z → -3 + Sin[teta]}
	Якобиан	Cos[teta]
	Обр. параметризация	$\left\{fi \to \text{ArcTan}\left[\frac{y}{x}\right] + \frac{1}{2}\pi\,(1 - \text{Sign}[x])\,\text{Sign}[y],\ teta \to \text{ArcTan}\left[\frac{3+z}{\sqrt{x^2+y^2}}\right]\right\}$
	Ограничения	$\left\{\{fi, -\pi, \pi\}, \left\{teta, -\frac{\pi}{2}, \frac{\pi}{2}\right\}\right\}$
	Нормаль	{-Cos[fi] Cos[teta], -Cos[teta] Sin[fi], -Sin[teta]}
	Касательная 1	{-Sin[fi], Cos[fi], 0}
	Касательная 2	{Cos[fi] Sin[teta], Sin[fi] Sin[teta], -Cos[teta]}

где r – расстояние от центра полости до точки $\mathbf{r} = \{x, y, z\}$.

Для каждого гармонического многочлена вычисляется градиент температуры. Набор $\xi^T = \{T, T_{,i}\} \in \Xi^T$ называем внутренним состояние термостатической среды. Совокупность линейно независимых элементов этого набора составляют исходный базис пространства внутренних состояний. Ему ставится в соответствие базис пространства граничных состояний: $\gamma^T = \left\{T, \frac{dT}{d\mathbf{n}}\right\} \in \Gamma^T$.

3. Ортогонализация исходного базиса в соответствии со скалярным произведением $(\xi^{Ti}, \xi^{Tj})_\Xi = \int_V T^i_{,k}\, T^j_{,k}\, dV$, $(\gamma^{Ti}, \gamma^{Tj})_\Gamma = \int_{\partial V} T^i \frac{dT^j}{d\mathbf{n}}\, dV$.

4. Решение бесконечной системы линейных уравнений (БСУ): $A\mathbf{c} = \mathbf{b}$.

В поставленной задаче (Дирихле) $A = E$, следовательно, $\mathbf{c} = \mathbf{b}$: $b_i = \int\limits_{\partial V} f_D \dfrac{dT^{(i)}}{d\mathbf{n}} dS$, где f_D – заданные ГУ

5. Построение результирующих термостатических полей. Внутреннее результирующее термостатическое состояние вычисляется через ряды Фурье:

$T = \sum\limits_k c_k T^{(k)}$, $T_{,i} = \sum\limits_k c_k T_{,i}^{(k)}$, где коэффициенты Фурье c_k найдены в п. 5, а $T, T_{,i}$ – составляющие элементов ортонормированного базиса, вычисленные в п. 4. Граничное результирующее состояние: $T\big|_{\partial V} = \sum\limits_k c_k T^{(k)}\big|_{\partial V}, \dfrac{dT}{d\mathbf{n}} = \sum\limits_k c_k \dfrac{dT}{d\mathbf{n}}^{(k)}$.

Точность найденного решения вычисляем через среднеквадратичную интегральную невязку заданных ГУ и полученного граничного состояния.

Результаты решения.

Результаты решения имеют аналитическую форму. Из-за громоздкости ответа, представим результаты решения в графической форме.

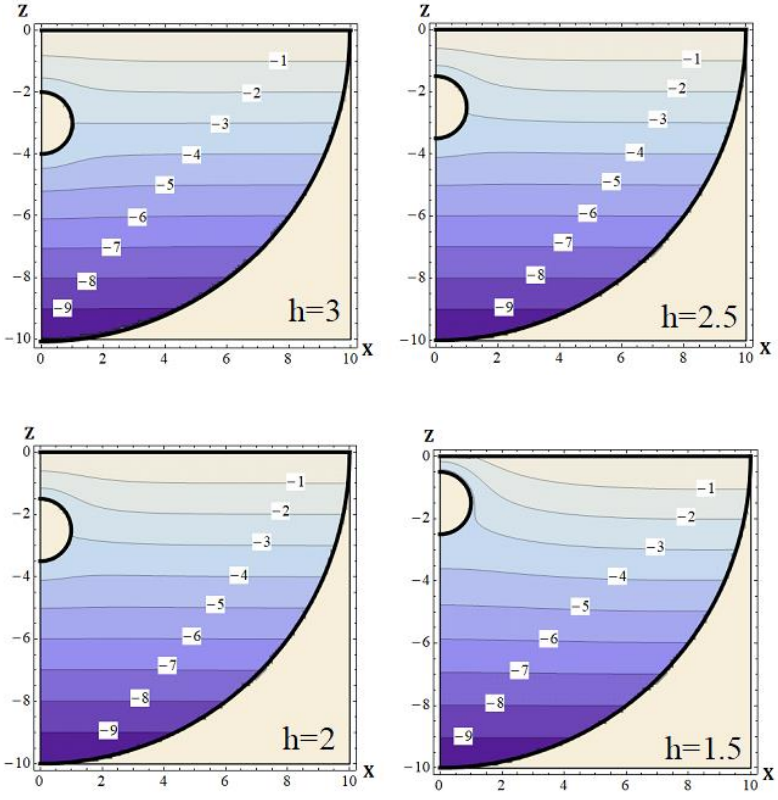


Рис. 2. Изолинии температур в сечении y=0

На рисунках 2 и 3 изображены линии уровня температуры (их значения отмечены).

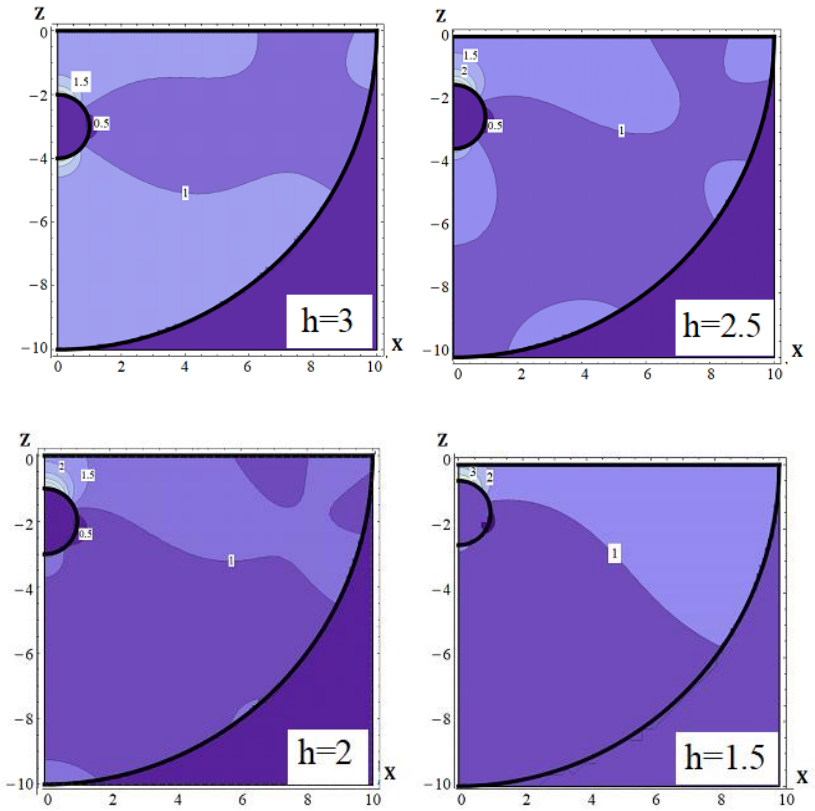


Рис. 3. Изолинии осевой компоненты градиента температуры в сечении y=0

На рис. 4 представлен график зависимости распределения температуры от глубины залегания полости.

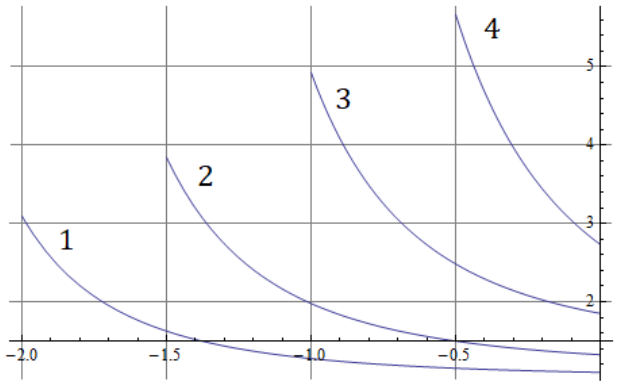


Рис. 4. Зависимость распределения температуры от глубины залегания полости 1 – h=3; 2 – h=2.5;3 – h =2;4 – h=1.5.

Сопоставление графиков распределения градиентов температуры по толщине слоя между полостью и внешней поверхностью свидетельствует о существенном возрастании теплового потока при уменьшении его толщины. Следовательно, для поддерживания требуемого уровня температуру внутри полости потребуются большие затраты энергии. Таким образом, для организации хладохранилища в грунте предпочтительнее обеспечивать как можно более глубокое «залегание».

Литература

1. Саталкина Л.В. Метод граничных состояний в задачах теории упругости неоднородных тел и термоупругости // Диссертация на соискание ученой степени кандидата физико-математических наук / Тульский государственный университет. Липецк, 2010.

2. Levina, L., Penkov, V. The Thermostatic State of a Homogeneous Body under the Influence of Surface and Volume Factors // Proceedings – 2022 4th International Conference on Control Systems, Mathematical Modeling, Automation and Energy Efficiency, SUMMA 2022, 2022. pp. 133–137.

Сведения об авторах

Пеньков Виктор Борисович, доктор физико-математических наук, профессор кафедры общей математики Липецкого государственного технического университета; e-mail: vbpenkov@mail.ru.

Левина Любовь Владимировна, кандидат физико-математических наук, доцент кафедры прикладной математики Липецкого государственного технического университета; e-mail: satalkina_lyubov@mail.ru.

Левин Максим Юрьевич, доктор технических наук, профессор Липецкого государственного технического университета.

Марахова Ирина Игоревна, кафедра прикладной математики Липецкого государственного технического университета.

Логачева Екатерина Юрьевна

ОПЫТ ИСПОЛЬЗОВАНИЯ ЭЛЕКТРОННЫХ ОБРАЗОВАТЕЛЬНЫХ РЕСУРСОВ В ПРОЦЕССЕ ПРЕПОДАВАНИЯ ЕСТЕСТВЕННО-НАУЧНЫХ ДИСЦИПЛИН В РАМКАХ РЕАЛИЗАЦИИ УЧЕБНОГО ПРОЦЕССА ПО СПЕЦИАЛЬНОСТИ СУДЕБНАЯ ЭКСПЕРТИЗА

Электронные образовательные ресурсы являются неотъемлемой частью современного учебного процесса, выступая как эффективные технические средства обучения для повышения качества образования и достижения нового образовательного результата.

Одно из неоспоримых преимуществ внедрения электронных учебных средств в образовательный процесс в рамках профессиональной подготовки экспертов-криминалистов заключается в возможности виртуализации производства судебных экспертиз. Виртуальный формат обучения приобретает особую актуальность в тех случаях, когда отсутствует необходимое оборудование или объекты для осуществления реальной учебной экспертизы.

В данной статье рассмотрим один из методических подходов по использованию виртуального контента в целях формирования профессиональных компетенций на примере организации учебной работы по изучению темы «Криминалистическое исследование наркотических средств (НС), психотропных (ПВ), сильнодействующих (СВ), ядовитых веществ их прекурсоров», рассматриваемой в рамках дисциплины «Криминалистическое исследование веществ, материалов и изделий», предусмотренной учебным планом по специальности «Судебная экспертиза».

Важное значение указанной темы при подготовке будущих экспертов-криминалистов обусловлено высоким уровнем преступлений, связанных с незаконным оборотом НС. Данный факт, свидетельствует о том, что любой эксперт-криминалист системы МВД России в своей профессиональной деятельности столкнется с необходимостью обнаружения, изъятия, фиксации и упаковки наркотиков.

Ввиду вышесказанного очевидно, что формирование представлений об особенностях исследования наркотических средств является одной из приоритетных задач учебной дисциплины «Криминалистическое исследование веществ, материалов и изделий». Необходимые знания, умения и навыки при этом приобретаются в контексте такой профессиональной компетенции, как способность использовать естественно-научные методы при исследовании вещественных доказательств.

Трудностью организации учебного процесса в рамках указанной темы является тот факт, что, во-первых, хранение объектов экспертного исследования запрещено действующим законодательством, во-вторых, для реализации лабораторного исследования требуется дорогостоящее высокотехнологичное аналитическое приборное оборудование. Данные обстоятельства препятствует проведению практических занятий в формате экспериментальной работы непосредственно с наркотиками.

Поэтому поиск альтернативных форм организации обучения, позволяющих получить знания о практической деятельности эксперта-криминалиста при работе с объектами, относящимися к наркотическим средствам, является инновационной педагогической задачей, для решения которой необходима разработка соответствующего методического обеспечения. В качестве такой альтернативы можно рассматривать подходы, основанные на виртуализации судебной экспертизы и криминалистического исследования НС. Материальной базой для реализации данной модели организации учебного процесса станут электронные образовательные ресурсы (ЭОР), которые будут выступать как носители учебной информации.

В целях реализации идеи виртуализации учебной экспертизы НС и демонстрации предлагаемого подхода разработан электронный образовательный ресурс «Криминалистическое исследование наркотических средств, психотропных веществ и их прекурсоров» (URL:

https://sites.google.com/view/uchebnajaexp), вид стартовой страницы которого представлен на рисунке 1

Рис. 1. Стартовая страница ЭОР «Криминалистическое исследование веществ, материалов и изделий из них»

Предложенный нами электронный образовательный ресурс построен по принципу веб-сайта, страницы которого соответствуют определенным тематическим модулям. Составляющими элементами ЭОР являются следующие разделы: «Лекции»; «Учебные экспертизы», «Нормативно-правовые акты (НПА)», «Типовая методика», «Форма отчета», «Вопрос преподавателю», «Библиотека научных статей». Взаимодействие с учебным материалом осуществляется посредством интерактивных гиперссылок, обеспечивающих как доступ к разделам ресурса, так и взаимосвязь обучающихся с педагогом.

В разделе «Лекции» рассмотрены теоретические основы методов экспертного исследования наркотических средств: хромато-масс-спектрометрии, газовой хроматографии, качественного химического анализа. Блок НПА содержит нормативно-правовые и законодательные акты, регулирующие контроль за незаконным оборотом наркотических средств, психотропных веществ и их прекурсоров на территории России. На странице «Типовая методика» приведены методические рекомендации по исследованию

наркотических средств, получаемых из растений конопли и мака, которые входят в перечень типовых экспертных методик вещественных доказательств, рекомендованных МВД РФ. Раздел «Библиотека научных статей» включает опубликованные в периодических изданиях материалы научных исследований по проблемам судебной экспертизы наркотических средств.

Основной частью ЭОР является блок «Учебные экспертизы». Эмпирическую базу для формирования контента ЭОР составили материалы экспертных заключений по результатам производства судебных экспертиз, выполненных сотрудниками ЭКЦ ГУ МВД России по Краснодарскому краю.

Рис. 2. Структура виртуальной учебной экспертизы

Каждая учебная экспертиза (рис.2) состоит из взаимосвязанных модулей, соответствующих структуре экспертного заключения и последовательности действий эксперта при производстве физико-химической экспертизы наркотических веществ:

1. Обстоятельства дела;
2. Объект исследования;
3. Исследование;
4. Сведения о выявленном компоненте.

Освоение учебного материала в названной последовательности обеспечит формирование представлений об особенностях производства экспертизы НС.

На странице «Обстоятельства» дела курсанты знакомятся с краткой фабулой происшествия, описанием поступившего на экспертизу объекта, и поставленными перед экспертом вопросами в редакции инициатора экспертизы. На странице «Объект» исследования дано подробное описание изъятого вещества и его упаковки, отражены результаты визуального осмотра.

Модуль «Исследование» состоит из подстраниц, материалы которых отражают этапы лабораторного экспертного исследования, которое выполняется экспертом для установления принадлежности поступившего на экспертизу объекта к наркотическим веществам:

1. Определение массы;
2. Пробоподготовка;
3. Предварительное исследование методом качественных аналитических реакций;
4. Физико-химический анализ.

Каждая из вышеуказанных подстраниц содержит цель производимого экспертом действия, сведения о применяемом оборудовании, методику и результат эксперимента.

Перейдя на страницу «Определение массы», пользователь может ознакомиться с целью, с которой проводятся измерения массы, знакомиться с описанием применяемых весов, методикой работы, полученным численным значением массы НС. В разделе «Пробоподготовка» описана методика перевода твердого образца, поступившего на экспертизу, в форму, пригодную для проведения последующего физико-химического исследования – гомогенный экстракт, конечный вид которого пользователь наблюдает, нажав на кнопку «Результат». На странице «Предварительное исследование методом качественных реакций» отражены особенности исследования объекта с применением хромогоенных химических реакций, цель которого состоит в предварительном определении природы анализируемого вещества. Изучив методику проведения качественной реакции, курсанты знакомятся с ее

результатом, который выражается в появлении характерной окраски реакционной смеси. По характеру окраски делают вывод о природе анализируемого вещества. Учебный материал страницы «Физико-химический анализ» содержит результаты, получаемые экспертом с применением инструментальных методов аналитической химии – газовой хроматографии и масс-спектрометрии. «Паспортом» экспертизы являются хроматограмма и масс-спектр. О природе вещества (а, следовательно, его принадлежности к НС) судят на основе значения времени удерживания пика компонента на хроматограмме и совпадения масс-спектра исследуемого вещества с масс-спектром конкретного наркотического вещества, содержащегося в базе данных (библиотеке масс-спектров).

Для контроля степени усвоения учебного материала, а также формирования умений применять полученные в результате экспертизы сведения предназначена «Форма отчета», в которой необходимо заполнить данные о выявленном веществе:

– описать внешний вид объекта по результатам визуального осмотра;

– перечислить методы исследования по установлению химической природы вещества;

– указать название выявленного вещества;

– привести его структурную формулу;

– заполнить данные о принадлежности к контролируемым веществам, отметив, входит ли выявленное вещество в один из Списков Перечня наркотических средств, психотропных веществ и их прекурсоров, подлежащих контролю в Российской Федерации;

– указать массу изъятого вещества;

– по численному значению массы классифицировать размер изъятого вещества для целей статей УК, назначающих наказание за незаконный оборот НС и ПВ.

Таким образом вопросы, приведенные в форме отчета, предполагают формирование умений интерпретировать результаты экспертизы, характеризовать криминалистически значимые признаки объекта, работать с нормативно-правовой базой.

Для осуществления консультации курсанта с преподавателем предусмотрена форма «Вопрос преподавателю» (в качестве обратной связи), в которой курсанты формулируют вопросы, возникающие в процессе выполнения задания. Макет формы позволяет задать вопрос как в текстовом варианте, так и сопроводить его иллюстрациями в случае необходимости.

Представленный в докладе ЭОР был апробирован в процессе преподавания дисциплины Криминалистическое исследование веществ, материалов и изделий в рамках темы «Криминалистическое исследование наркотических средств, психотропных, сильнодействующих, ядовитых веществ и их прекурсоров» и в процессе преподавания дисциплины «Естественно-научные методы судебно-экспертных исследований» в рамках темы «Гибридные методы анализа». Электронный образовательный ресурс при этом использовался в качестве дидактического материала при организации практических занятий и самостоятельной подготовки курсантов.

Говоря о результатах применения разработанного электронного образовательного ресурса в практике преподавания, хотелось бы отметить следующее. Представленный подход по виртуализации экспертного исследования и разработанный для его реализации ЭОР можно рассматривать в качестве эффективного ТСО, открывающего ряд возможностей по оптимизации образовательной деятельности по направлению подготовки «Судебная экспертиза» в рамках изучения темы «Криминалистическое исследование наркотических средств, психотропных веществ и их прекурсоров»:

– организация учебного процесса в тех случаях, когда существуют ограничения для проведения занятий в реальном режиме;

– успешное формирование профессиональных компетенций (знания об особенностях производства экспертизы наркотических веществ необходимы будущему эксперту – криминалисту для грамотного осуществления обнаружения и изъятия данных объектов при участии в процессуальных действиях и оказании содействия следователю);

– организация дистанционного обучения;

– формирование научного мировоззрения и межпредметных связей по дисциплинам «Криминалистика», «Участие специалиста в процессуальных действиях», «Естественно-научные методы судебно-экспертных исследований».

Литература

1. О наркотических средствах и психотропных веществах: Федеральный закон от 08.01.1998 № 3-ФЗ // СПС КонсультантПлюс.

2. Церюльник А.Ю. Использование дистанционного формата обучения студентов в образовательном процессе / А.Ю. Церюльник // Международный научно-исследовательский журнал. – 2020. – № 6-3 (96). – С. 92-95.

3. Колошеин А.П. Применение электронных образовательных ресурсов в высшем учебном заведении / А.П. Колошеин // Вестник РУДН, серия Информатизация образования. – 2014. - № 1. – С. 82-86.

Сведения об авторе

Логачева Екатерина Юрьевна, кандидат химических наук, старший преподаватель кафедры судебно-экспертной деятельности Краснодарского университете МВД России, e-mail: k.logacheva@mail.ru

Малофей Олег Павлович,
Малофей Александр Олегович,
Павленко Татьяна Александровна

ИСПОЛЬЗОВАНИЕ КОМБИНИРОВАННЫХ РЕШЕНИЙ ДЛЯ КОРРЕКЦИИ ОШИБОК В СИСТЕМАХ УПРАВЛЕНИЯ СТРАТЕГИЧЕСКИМИ ОБЪЕКТАМИ

Достаточно актуальной является задача обеспечения достоверности передачи данных в современной системе передачи информации. Если при передаче текстовых сообщений искажается информация или в ходе общения по телефону начинается специфическое «бульканье», то это говорит о наличии ошибок в канале связи. Абонент, идентифицирующий смысл сообщения, в таком случае легко может обнаружить ошибки самостоятельно. Искажение всего лишь одного единичного символа на тысячу переданных может сильно повлиять на полученное сообщение и качество информации в целом [5].

Требуемая достоверность информационных сообщений в системах управления стратегическими объектами должна быть не ниже 10^{-9} с точки зрения вероятностной оценки. Реальные каналы связи зачастую подвержены воздействию помех, что снижает этот показатель до $10^{-3} - 10^{-4}$ [2]. Такое снижение вероятности недопустимо, так как получатель информации в системе управления стратегическими объектами вначале получает недостоверные данные, которые в дальнейшем становятся не актуальными.

Существует множество методов, обеспечивающих достоверную и надежную передачу информации. Средства достижения цели обеспечения достоверности могут быть различны, время передачи-получения и обработки информации зависят от объёма передаваемых данных и также могут существенно отличаться.

Методы повышения достоверности информации реализуются в аппаратной и программной части системы передачи информации как на передающей, так и на приёмной стороне. При этом не всегда программная и аппаратная часть реализуются в равных соотношениях.

В числе многочисленных методов защиты от ошибок выделяются три группы методов: групповые методы, помехоустойчивое кодирование и методы защиты от ошибок в системах передачи с обратной связью.

Исправление стираний в кодах с повторением позволяет значительно повысить помехоустойчивость достаточно простыми средствами. [2, 7]. Представляет интерес использование в стирающем канале кодов малой плотности с проверкой на чётность (LDPC код). Их сложность компенсируется возможностью достаточно простой реализации в современной элементной базе. На сегодняшний день такие коды являются частью стандарта 802.11n, 802.11ac, группы DVB-x2 (спутниковой связи после внедрения стандартов DVB-S2/S2X) и радиочасти сетей мобильной связи 5G (NR – New Radio).

При этом вероятность трансформации элемента p определяется формулой

$$p = \int_{-\infty}^{-v} f_1(y)\,dy = \int_{v}^{\infty} f_0(y)dy, \tag{1}$$

а вероятность стирания - формулой

$$s = \int_{-v}^{v} f_0(y)dy = \int_{-v}^{v} f_1(y)dy. \tag{2}$$

Из выражений (2) и (3) очевидно, что

$$\begin{aligned} s &= p_s + q_s; \\ p_0 &= p + p_s; \\ q_0 &= q + q_s; \end{aligned} \tag{3}$$

где p_s – вероятность правильного стирания элемента, q_s – вероятность ложного стирания, p_0 – вероятность искажения элемента, q_0 – вероятность правильного приема элемента.

Стирания Θ, отмечающие надежные элементы принимаемой кодовой комбинации, могут быть использованы для повышения помехоустойчивости приема так же, как используются апостериорные вероятности ошибки P_j в оптимальных и квазиоптимальных методах. Известны три метода обработки избыточных кодов с использованием стираний [4].

При этом вероятность необнаруженных ошибок может быть вычислена по формуле

$$P_{\text{НО}}(s,n) \approx \frac{1}{2^r}\sum_{i=d}^{n} C_n^i p_0^i (1-p_0)^{n-i} + \frac{1}{2^r}\sum_{i=1}^{d-1}\sum_{j=d-i}^{n} C_n^i p_0^i q_s^i \,(1-p_0)^{n-i}\, C_{n-i}^i p^j (1 - p)^{n-(i+j)}. \quad (4)$$

Приближенное выражение получим, если выделим составляющие члены, имеющие наибольший вес:

$$P_{\text{НО}}(s,n) \approx \frac{1}{2^r} C_n^d p_0^d + \frac{1}{2^r} C_{n-1}^{d-1} n p_0 q_s p^{d-1}. \quad (5)$$

Вероятность обнаруженных ошибок, характеризующая потери информации при приеме второго повторения, может быть вычислена по формуле

$$P_{\text{ОО}}(s,n) = \sum_{i=1}^{d-1}\sum_{j=0}^{d-1-i} C_n^i C_{n-i}^j p_0^i q_s^i p^j (1-p_0)^{n-i}(1-p)^{n-(i+j)}, \quad (6)$$

или приближенно по формуле

$$P_{\text{ОО}}(s,n) \approx n p_0 q_s. \quad (7)$$

Техническая реализация данного метода рассмотрена в работе [8].

Обширные экспериментальные исследования эффективности корректирующих кодов в реальных радиоканалах показали, что в режиме исправления ошибок при $n \leq 511$ коды повышают достоверность не более, чем на один порядок, а потери вследствие избыточности кода при этом достигают $50 - 80\%$. Расчеты свидетельствуют, что с увеличением длины комбинации до $64 - 128$ единичных символов потери в скорости уменьшается до $6 - 10\%$, а коэффициент повышения верности увеличивается на два порядка [2].

В системах передачи данных в целях достижения максимального выигрыша в верности приема могут использоваться одновременно несколько кодовых и несколько косвенных способов обнаружения ошибок.

Комбинированным является такой принцип обнаружения ошибок, при котором особое значение приобретает согласование способов обнаружения ошибок [3].

Рассмотрим вероятностное пространство ошибок при приеме. Ошибки имеют различный характер: $0 \to 1$ или $1 \to 0$, разную кратность и случайный характер распределения в пределах принимаемой кодовой комбинации. Пусть $P -$ вероятность ошибочного приема единичных символов. Применение того или иного способа обнаружения ошибок обеспечивает выявление какой-то их части. Обозначим пространство элементарных событий-ошибок через Ω, а его элементы через $\omega_1, \omega_2, \dots$. Следовательно, $\Omega = \{\omega_i, i = 1,2,3, \dots N\}$, где $N -$ число элементов в Ω. Пусть ошибки, обнаруживаемые первым способом, составляют число A_1, которое является подмножеством Ω, т.е. $A_1 \in \Omega$. Тогда

$$P(A_1) = \sum_{\omega_i \in A_1} P(\omega_i), \tag{8}$$

а вероятность необнаруживаемых ошибок

$$P_{\text{но}} = P - P(A_1). \tag{9}$$

Если использовать комбинированно два способа обнаружения ошибок (косвенный и кодовый), вероятность совместного обнаружения ошибок определится суммой событий A_1 и A_2, т.е. объединением подмножеств $A_1 \cup A_2$ и пересечением $A_1 \cap A_2 = \emptyset$, где

$$P(A_1 \cup A_2) = \sum_{\omega_i \in A_1 \cap A_2} P(\omega_i) = P(A_1) + P(A_2) - P(A_1 \cap A_2). \tag{10}$$

При одновременном использовании нескольких способов (косвенных и кодовых) вероятность обнаружения ошибок

$$P\left(\bigcup_{i=1}^{\alpha} A\right) = \sum_{i=1}^{\alpha} P(A_i) - \sum_{i<1}^{\alpha} P(A_i A_j) + \sum_{i<j<\gamma} P(A_i A_j A_\gamma) - \cdots + (-1)^{\alpha-1} P\left(\bigcap_{i=1}^{\alpha} A_i\right). \tag{11}$$

Тогда вероятность необнаруживаемых ошибок

$$P_{\text{но}} = P - P\left(\bigcap_{i=1}^{\alpha} A_i\right). \tag{12}$$

При таком комбинированном контроле ошибок способы обнаружения должны меньше дублировать и больше дополнять друг друга, т.е. вероятности пересечений множества A_i должны стремиться к нулю [7, 9].

Вводя в систему передачи информации детектор качества, наряду с кодовыми методами защиты информации можно удешевить аппаратуру передачи данных. Кроме того, учет параметров пакетирования искажений позволяет, например, с помощью детектора качества сигналов с оптимальными зонами стираний, уменьшить вероятность необнаруженной ошибки на два-три порядка, уменьшить величину потерь скорости передачи в системах с переспросом, снизить избыточность кода [4].

Использование сигнала, учитывающего качество канала связи Θ для коррекции однократных ошибок в одноименных символах второго и всех последующих до $2^p - 1$ включительно повторений сообщения, позволяет увеличить помехоустойчивость. Это можно показать на примере определения вероятности потерь информации, сравнивая рассмотренный метод и метод адаптивного мажоритарного декодирования [2, 8, 9].

Потери информации для каждого из сравниваемых методов можно найти при помощи выражений

$$P_n = nC_{2m-1}^{m} P_0^m \tag{13}$$
$$P_n' = nC_{2(m-1)}^{m-1} P_0 P^{m-1}$$

Отношение этих величин позволит определить степень снижения потерь информации

$$\eta = \frac{P_n}{P_n'} = \frac{C_{2m-1}^{m}}{C_{2(m-1)}^{m-1}} P_0^{m-1} P^{1-m} \tag{14}$$

Если взять конкретные значения $P_0 = 10^{-2}, P = 10^{-3}, m = 2,$ что соответствует наличию семи повторений $N = 7, \rho = 3$, то

$$\eta = 1{,}75 \cdot 10^3.$$

В настоящее время весьма активно исследуется корректирующая способность LDPC кодов в стирающем канале. Имеется длинный список работ в этой области. Например, в работе [1] исследуется исправление стираний композицией LDPC кодов с кодом Хэмминга, при этом выводятся и используются (в каскадной схеме декодирования) точные оценки доли исправляемых стираний большого веса для двоичного кода Хэмминга. Хотелось бы также отметить работу [3], где рассматривается доля стираний, исправляемых недвоичными кодами. Для оценки доли исправляемых комбинаций стираний полезны результаты, связанные с исследованием минимальных слов в линейных кодах. Характер изменения вероятности потерь от числа повторов для алгоритмов [1 – 3, 8, 9] показывает, что новый алгоритм имеет улучшенные вероятностно-временные характеристики и может быть использован в системах радиосвязи с каналами связи плохого качества.

Литература

1. F. Qiao, P. Zhu, L. Pan, H. Liu, Z. Zhang, and J. Xu, "New FN/BBHH Combined Erase Scheme for Scalable SONOS Device", 2014 International Symposium on Next Generation Electronics (ISNE), 2014, pp. 1-2, doi: 10.1109 / ISNE.2014.6839330.

2. H. Lue et al., "Investigation of the charge loss mechanism of SONOS type devices using hot hole erasure and charge retention improvement techniques", 2006 IEEE International Reliability Physics Symposium, 2006, pp. 523-529, doi: 10.1109 / RELPHY .2006.251273.J.

3. Chen, G. Xie, K. Luo, W. Cheng, P. Lu и Y. Wang, "Исследование характеристик полосы стирания и записи в магнитной записи с заменой сопряженных композитных носителей", 2018 IEEE International Magnetics Conference (INTERMAG), 2018, стр. 1-1, doi: 10.1109 / INTMAG.2018.8508564.

4. Акимов П. С. Сигналы и их обработка в информационной системе // Акимов П. С., Сенин А. И., Соленов В. И. – М. Радио и связь. 1994. – 256 С.

5. Вернер М. Основы кодирования. Учебник для ВУЗов. // Пер. с нем. – М.: Техносфера, 2005. - 288 С.

6. Давыдов А.А., Томбак Л.М. О количестве слов минимального веса в блоковых кодах. Проблемы передачи информации, 1988, т. 24, № 1, С. 11-24.

7. Зяблов В.В., Рыбин П.С. Исправление стираний кодами с малой плотностью проверок. Проблемы передачи информации, 2009, т. 45, № 3, стр. 15-32.

8. Малофей О.П., Малофей А.О., Кучуков В.А., Малофей М.С., Харечкина Ю.О., Харечкин А.Н. Модифицированное устройство коррекции ошибок с учетом сигнала стирания. Патент на изобретение RU 2711035 C1, 14.01.2020. Заявка № 2019114114 от 08.05.2019.

9. Малофей А.О. Повышение помехоустойчивости приема при помощи модифицированного алгоритма мажоритарного декодирования, реализующего коррекцию с учетом сигнала стирания. Актуальные проблемы формирования профессиональной компетентности у курсантов и слушателей вузов МВД России. // Электронный сборник материалов межвузовского круглого стола 09.02.2016. Ставрополь, 2016. С. 205-209.

Сведения об авторах

Малофей Олег Павлович, кандидат технических наук, профессор кафедры математического анализа алгебры и геометрии факультета математики и компьютерных наук Северо-Кавказского федерального университета имени профессора Н.И. Червякова; e-mail: opmalofey@yandex.ru.

Малофей Александр Олегович, кандидат технических наук, доцент кафедры тактико-специальной подготовки Ставропольского филиала Краснодарского университета МВД России; e-mail: tc_op@mail.ru.

Павленко Татьяна Александровна, аспирант факультета математики и компьютерных наук Северо-Кавказского федерального университета имени профессора Н.И. Червякова.

Михайленко Евгений Владимирович

О РАЗРАБОТКЕ ПРОГРАММНЫХ КОМПЛЕКСОВ ДЛЯ ОБЕСПЕЧЕНИЯ ДИСЦИПЛИНЫ «ВЫСШАЯ МАТЕМАТИКА»

Настоящая статья посвящена технологиям подготовки программных модулей для автоматизированной подготовки индивидуальных комплектов практических заданий, выполняемых в рамках практикума по дисциплине «Высшая математика» курсантами Краснодарского университета МВД России, обучающимися по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере, а также методам верификации выполненных работ.

Дисциплина «Высшая математика» включает такие разделы математики, как линейная алгебра и аналитическая геометрия, общая алгебра, математический анализ, теория вероятностей и математическая статистика, дискретная математика, методы оптимизации. По каждой из двадцати шести темам дисциплины предусмотрены расчетные задания, которые выполняются курсантами на практических занятиях и в часы самостоятельной подготовки. Описываемые программные продукты предназначены для избавления преподавателей от трудоемкой работы по подбору типовых задач и проверки их решений на бумажных носителях, кроме того, каждый обучающийся получает свой уникальный вариант заданий, сгенерированных по разработанным алгоритмам, что исключает списывание готовых уже рассчитанных решений курсантов друг у друга [1].

Представляемые комплексы программных продуктов реализованы в среде Microsoft Office, но также при необходимости могут использоваться в офисных приложениях OpenOffice и LibreOffice [4]. Так, при переходе компьютерного центра университета на операционную систему Astra Linux преподаватели продолжали работать на Windows в MS Office, а одновременно с этим обучаемые использовали LibreOffice.

Суть описываемого метода заключается в создании шаблонов типовых расчетных заданий, размещенных на листах книг MS Excel, в которые после выполнения макросов будут добавлены сгенерированные числовые, строковые

или графические компоненты заданий [2]. Преподаватель может сгенерировать условия заданий как для одного курсанта, так и одновременно для всей учебной группы. Подготовленные файлы со сгенерированными заданиями помещаются в доступное для обучаемых облачное пространство или папку на сервере, имена файлов содержат номера тем и практических занятий, а также фамилии курсантов [9].

Обучающиеся, выполняя задания, вписывают свои решения в поля для ввода числовых или текстовых ответов и предоставляют решенные задания с ответами для проверки. Теперь, получив файлы с решениями, преподавателю достаточно будет обработать их соответствующими макросами, которые автоматически откроют выполненные работы, проверят промежуточные и окончательные решения, а также, согласно установленным критериям, выставят оценки [6].

Приведем примеры реализации таких программ.

Рассмотрим задание 3 «Определить смешанные стратегии игроков S_A и S_B, а также цену игры v» из практической работы «Решение матричных игр» раздела «Теория игр и принятия решений» (рис. 1).

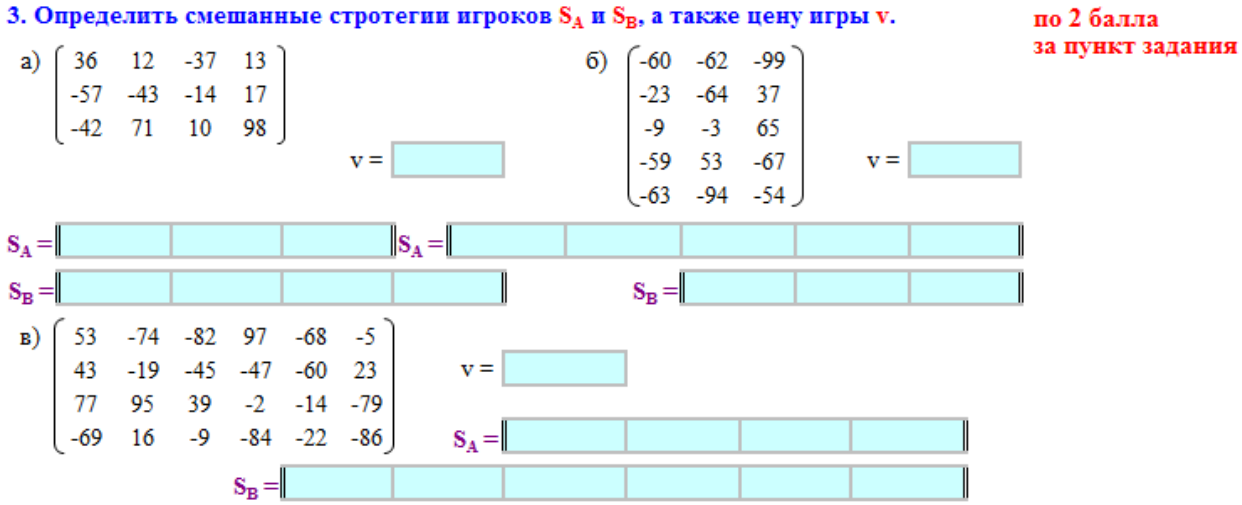


Рис. 1. Задание Определить смешанные стратегии игроков S_A и S_B, а также цену игры v»

Задание состоит из трех задач нарастающей сложности. Решая эти задачи, обучаемые должны упростить платежную матрицу до двух строк и двух столбцов, найти нижнюю α и верхнюю β цены игры, применить вероятностные

подходы для расчета смешанных стратегий игроков *A* и *B*, а затем, учитывая найденные вероятности применения каждой стратегии, рассчитать цену матричной игры [3].

```
Do
  Do        'Находим коэффициенты платежной матрицы mA(i,
    For i = 1 To 4
      For j = 1 To 6
        Do
          mA(i, j) = Round(Rnd(V) * 200 - 100)
          k = 0
          For i0 = 1 To 4
            For j0 = 1 To 6
              If mA(i, j) = mA(i0, j0) Then k = k + 1
          Next j0, i0
        Loop Until k = 1
    Next j, i
                    'Находим нижнюю границу Alfa
    For i = 1 To 4
      mAlfa(i) = mA(i, 1)
      For j = 1 To 6
        If mA(i, j) < mAlfa(i) Then mAlfa(i) = mA(i, j)
      Next j
    Next i
    alfa = mAlfa(1)
    For i = 1 To 4
      If mAlfa(i) > alfa Then alfa = mAlfa(i)
    Next i
                    'Находим верхнюю границу Betta
    For j = 1 To 6
      mBetta(j) = mA(1, j)
      For i = 1 To 4
        If mA(i, j) > mBetta(j) Then mBetta(j) = mA(i, j)
      Next i
    Next j
    betta = mBetta(1)
    For j = 1 To 6
      If mBetta(j) = betta Then betta = mBetta(j)
    Next j
  Loop Until alfa < betta
```

Рис. 2. Расчет коэффициентов платежной матрицы.

Опишем методы подбора параметров задачи 3.в. Программный код генерации параметров задания можно условно разбить на две части. В первой из них происходит предварительный расчет платежной матрицы (рис. 2). Как видим из листинга программы, при определении коэффициентов матрицы в каждой итерации производится верификация на уникальность генерируемого элемента.

Для сформированной матрицы находятся нижняя *alfa* и верхняя *betta* цены игры, и в случае появления седловых точек, когда игра решается в чистых стратегиях, происходит возврат к генерации коэффициентов. В случае неравенства *alfa* и *betta* матрица заносится в массив *mA0*.

Вторая часть генерации задания упрощает сформированную платежную матрицу, уменьшая их размерность путем исключения дублирующих и заведомо невыгодных стратегий. На рисунке 3 представлен фрагмент программного кода, в котором происходит поиск и удаление дублирующих и доминируемых стратегий игрока *A*.

```
m = 4: n = 6
For p = 1 To 10
                    'Проход слева направо
  qi = 0
                    'Находим доминируемую строку
  For i1 = 1 To m - 1
    For i2 = i1 + 1 To m
      k1 = 0: k2 = 0
      For j = 1 To n
        If mA(i1, j) <= mA(i2, j) Then k1 = k1 + 1
        If mA(i2, j) <= mA(i1, j) Then k2 = k2 + 1
      Next j
      If k1 = n Then qi = i1
      If k2 = n Then qi = i2
  Next i2, i1
                    'Удаляем доминируемую строку
  If qi > 0 Then
    For i = qi To m - 1
      For j = 1 To n
        mA(i, j) = mA(i + 1, j)
    Next j, i
    m = m - 1
  End If
```

Рис. 3. Поиск и удаление дублирующих и доминируемых строк.

Аналогичным образом (рис. 4) в программе попарно анализируются столбцы платежной матрицы, а также удаляются дублирующие и доминируемые стратегии игрока *B*.

Если после десяти проходов упрощения платежной матрицы у каждого из игроков останутся по две стратегии, то рассчитанная в первой части программы матрица размерностью 4x6 выводится на лист заданий. В противном случае

происходит повторное генерирование платежной матрицы. Опыт использования программного продукта показал, что при генерации курсантами заданий совершаются десятки итераций, однако скорость нахождения платежной матрицы, сводящейся после преобразований к двум строкам и двум столбцам, достаточно велика.

```
                    'Проход сверху вниз
    qj = 0
                    'Находим доминируемый столбец
    For j1 = 1 To n - 1
      For j2 = j1 + 1 To n
        k1 = 0: k2 = 0
        For i = 1 To m
          If mA(i, j1) >= mA(i, j2) Then k1 = k1 + 1
          If mA(i, j2) >= mA(i, j1) Then k2 = k2 + 1
        Next i
        If k1 = m Then qj = j1
        If k2 = m Then qj = j2
    Next j2, j1
                    'Удаляем доминируемый столбец
    If qj > 0 Then
      For j = qj To n - 1
        For i = 1 To m
          mA(i, j) = mA(i, j + 1)
      Next i, j
      n = n - 1
    End If
  Next p
Loop Until m = 2 And n = 2
                    'Выводим платежную матрицу
For i = 1 To 4
  For j = 1 To 6
    Cells(i + 48, j + 1) = mA0(i, j)
Next j, i
```

Рис. 4. Поиск и удаление дублирующих и доминируемых столбцов.

Процесс проверки задания рассматривать не будем. Достаточно сказать, что алгоритм нахождения платежной матрицы здесь такой же, как и описанный ранее, а для нахождения оптимального решения в смешанных стратегиях используется вероятностный подход.

Рассмотрим задание 2 «Решить транспортную задачу» практического задания «Транспортная задача. Метод потенциалов» раздела «Задачи математического программирования» (рис. 5). Условие представленной задачи содержит текстовую и табличную части одновременно.

2. Решить транспортную задачу.

У поставщиков A_1, A_2, A_3, A_4 имеются однородные грузы в количествах 7, 22, 14 и 17 тонн, которые требуется доставить потребителям, B_1, B_2, B_3, B_4, B_5. Потребности грузополучателей составляют 10, 11, 24, 9 и 6 тонн соответственно.

Таблица издержек (тыс. руб.)

	B_1	B_2	B_3	B_4	B_5
A_1	3	4	1	2	7
A_2	4	11	4	6	2
A_3	6	5	10	6	7
A_4	3	12	4	3	5

Известны стоимости доставки грузов от каждого поставщика каждому потреьителю. Необходимо минимизировать затраты на перевозку.

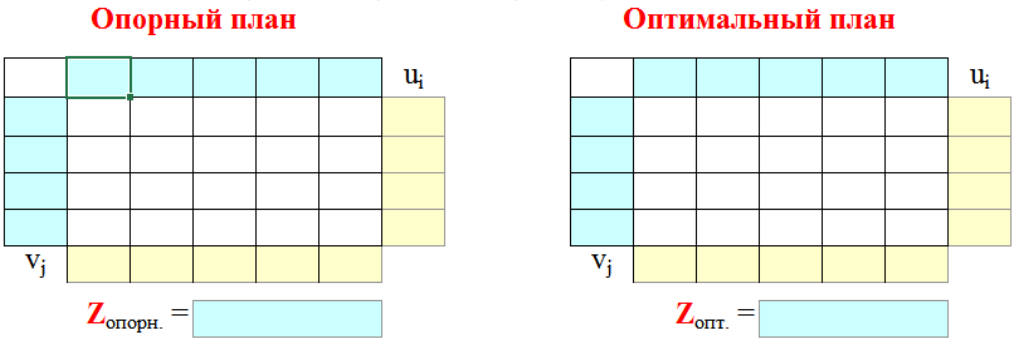


Рис. 5. Задание «Решить транспортную задачу»

Для формирования задания сперва определим наличие груза у отправителей и потребности адресатов (рис. 6). При расчете коэффициентов в циклах Do .. Loop Until будем выполнять проверку на повторения значений.

```
'2. Решить транспортную задачу. (Закрытая задача)
Do          'Определяем наличие и потребность грузов
  Do
    Sr = 0: Sc = 0
    Do      'Наличие груза у отправителей с проверкой на повторения
      k1 = 0
      For i = 1 To 4
        mX(i, 0) = Rnd(v) * 1000 Mod 20 + 5
        For j = 1 To i - 1
          If mX(i, 0) = mX(j, 0) Then k1 = k1 + 1
        Next j
        Sr = Sr + mX(i, 0)
      Next i
    Loop Until k1 = 0
    Do      'Потребности адресатов  с проверкой на повторения
      k2 = 0
      For j = 1 To 4
        mX(0, j) = Rnd(v) * 1000 Mod 20 + 5
        Sc = Sc + mX(0, j)
      Next j
      mX(0, 5) = Sr - Sc
      For j = 2 To 5
        For i = 1 To j - 1
          If mX(0, j) = mX(0, i) Then k2 = k2 + 1
      Next i, j
    Loop Until k2 = 0
```

Рис. 6. Расчет наличия и потребности грузов

Осуществим верификацию сгенерированного массива на повторения значений у поставщиков и потребителей и некоторые ограничения задачи (рис. 7) и в случае невыполнения требований вернемся к генерации основных параметров задачи. Затем рассчитаем значения платежной матрицы.

```
    k = 0
    For i = 1 To 4
      For j = 1 To 5
        If mX(i, 0) = mX(0, j) Then
          k = k + 1
        End If
      Next j, i
    Loop Until mX(0, 5) >= 5 And mX(0, 5) <= 25 And k = 0
                              'Расчет таблицы издержек
    For i = 1 To 4
      For j = 1 To 5
        mIz(i, j) = Rnd(v) * 11 Mod 20 + 1
    Next j, i
```

Рис. 7. Верификация массива данных и расчет таблицы издержек

Методом минимального элемента сформируем начальный опорный план решения задачи линейного программирования (рис. 8).

```
For i = 0 To 4              'Нахождение опорного плана
  For j = 0 To 5            'методом минимального элемента
    mT(i, j) = mX(i, j)
Next j, i
                            'Определение опорного плана
Do
  Min_Iz = 1000
  For i = 1 To 4
  For j = 1 To 5
    If mIz(i, j) < Min_Iz And mT(i, 0) > 0 And mT(0, j) > 0 Then
      vRow = i:  vCol = j: Min_Iz = mIz(vRow, vCol)
    End If
  Next j, i
  If Min_Iz < 1000 Then
    If mT(vRow, 0) > mT(0, vCol) Then
        mT(vRow, vCol) = mT(0, vCol)
        mT(vRow, 0) = mT(vRow, 0) - mT(0, vCol)
        mT(0, vCol) = 0
      Else
        mT(vRow, vCol) = mT(vRow, 0)
        mT(0, vCol) = mT(0, vCol) - mT(vRow, 0)
        mT(vRow, 0) = 0
    End If
  End If
Loop Until Min_Iz = 1000
```

Рис. 8. Определение опорного плана транспортной задачи

Исследуем полученный опорный план на вырожденность. Для невырожденности плана количество базисных ячеек должно быть равно: $N_{баз} = m + n - 1$, где m и n – количество строк столбцов опорного плана [8].

Рассчитаем количество базисных решений нашего опорного плана (рис. 9) и в случае, если решений будет меньше восьми, снова возвращаемся в начало алгоритма расчета параметров задачи.

```
    kbaz = 0                    'Подсчет базисных решений
    For i = 1 To 4
      For j = 1 To 5
        If mT(i, j) > 0 Then kbaz = kbaz + 1
    Next j, i
  Loop Until kbaz = 8
```

Рис. 9. Расчет количества базисных решений опорного плана

В случае невырожденности опорного плана транспортной задачи осуществляется вывод условия задачи на лист задания (рис. 10). Сначала заполняем таблицу издержек, а затем формируем текстовую часть задания.

```
For i = 1 To 4              'вывод таблицы издержек
  For j = 1 To 5
    Cells(i * 2 + 59, 13 + j) = mIz(i, j)
Next j, i
t = "    У поставщиков A1, A2, A3, A4 имеются однородные грузы в количествах "
t = t + st(mX(1, 0)) + ", " + st(mX(2, 0)) + ", " + st(mX(3, 0)) + " и " _
    + st(mX(4, 0)) + " тонн, которые требуется доставить потребителям, "
k1 = Len(t)
t = t + "B1, B2, B3, B4, B5.  Потребности грузополучателей составляют "
t = t + st(mX(0, 1)) + ", " + st(mX(0, 2)) + ", " + st(mX(0, 3)) + ", " + _
    st(mX(0, 4)) + " и " + st(mX(0, 5)) + " тонн соответственно."
Cells(57, 1) = t
Cells(57, 1).Characters(20, 1).Font.Subscript = True
Cells(57, 1).Characters(24, 1).Font.Subscript = True
Cells(57, 1).Characters(28, 1).Font.Subscript = True
Cells(57, 1).Characters(32, 1).Font.Subscript = True
Cells(57, 1).Characters(k1 + 2, 1).Font.Subscript = True
Cells(57, 1).Characters(k1 + 6, 1).Font.Subscript = True
Cells(57, 1).Characters(k1 + 10, 1).Font.Subscript = True
Cells(57, 1).Characters(k1 + 14, 1).Font.Subscript = True
Cells(57, 1).Characters(k1 + 18, 1).Font.Subscript = True
Cells(70, 1) = "Известны стоимости доставки грузов от каждого поставщика " _
                                                + "каждому потребителю."
Cells(72, 1) = "Необходимо минимизировать затраты на перевозку."
```

Рис. 10. Вывод условия транспортной задачи

Как видно из приведенного фрагмента программы, после вывода сформированной строки t в записях «A_1, A_2, A_3, A_4» и «B_1, B_2, B_3, B_4, B_5»

устанавливаем подстрочный шрифт для цифровых индексов [5].

Рассмотрим верификацию выполненного задания. Не будем описывать процесс расчета всех параметров задания. Он будет такой же точно, что и при генерации курсантом. На проверку выносятся два плана: опорный и оптимальный. Начнем с исследования опорного плана транспортной задачи.

Считываем опорный план (рис. 11). В построенном плане необходимо игнорировать знаки «+» или «–», которые обучающие используют для пометки вершин контура перераспределения поставок.

```
For i = 0 To 4                'Считываем построенный опорный план
  For j = 0 To 5
    mS(i, j) = NoSpace(Cells(i * 2 + 77, j + 2))
    If mS(i, j) = "+" Or mS(i, j) = "-" Then mS(i, j) = ""
    mT(i, j) = Val(mS(i, j))
Next j, i
m1 = 0                        'Проверяем построенный опорный план по строкам
For i = 1 To 4
  If mT(i, 0) = mX(i, 0) Then m1 = m1 + 1 Else Call krest(i * 2 + 77, 2)
  S = 0
  For j = 1 To 5
    S = S + mT(i, j)
  Next j
  If mX(i, 0) = S Then
      m1 = m1 + 1
    Else
      For j = 1 To 5
        Call krest(i * 2 + 77, j + 2)
      Next j
  End If
Next i
For j = 1 To 5                'Проверяем построенный опорный план по столбцам
  If mT(0, j) = mX(0, j) Then m1 = m1 + 1 Else Call krest(77, j + 2)
  S = 0
  For i = 1 To 4
    S = S + mT(i, j)
  Next i
  If mX(0, j) = S Then
      m1 = m1 + 1
    Else
      For i = 1 To 4
        Call krest(i * 2 + 77, j + 2)
      Next i
  End If
Next j
If m1 = 18 Then mark = mark + 2 Else Call krest(74, 19)
```

Рис. 11. Считывание и проверка опорного плана по строкам и столбцам

В условии задания не указан способ нахождения опорного плана и курсанты по выбору могут использовать методы северо-западного угла, минимального элемента или Фогеля. Следовательно, проверяем строки и столбцы опорной транспортной таблицы на соответствие условию задачи: суммы элементов строк должны соответствовать наличию грузов у поставщиков, а суммы элементов столбцов – потребности получателей.

Следующий элемент верификации задания – это проверка рассчитанных курсантами потенциалов транспортной таблицы (рис. 12). В программе считываются потенциалы опорного плана, определяются пустые или заполненные пробелами ячейки, а затем с использованием базисных ячеек и таблицы издержек проверяются значения на соответствие двум формулам:

$$v_j = u_i + c_{ij} \quad \text{и} \quad u_i = v_j - c_{ij},$$

где u_i и v_j – потенциалы соответствующих строк и столбцов, а c_{ij} – значения платежной матрицы [7].

```
m2 = 0                          'Считываем потенциалы для опорного лпана
For i = 1 To 4
  mu(i, 2) = Val(Cells(i * 2 + 77, 8))
  If NoSpace(Cells(i * 2 + 77, 8)) = "" Or m1 < 18 Then
    m2 = m2 + 1
    Call krest(i * 2 + 77, 8)
  End If
Next i
For j = 1 To 5
  mv(j, 2) = Val(Cells(87, j + 2))
  If NoSpace(Cells(87, j + 2)) = "" Or m1 < 18 Then
    m2 = m2 + 1
    Call krest(87, j + 2)
  End If
Next j
For i = 1 To 4                  'Проверка потенциалов
  For j = 1 To 5
    x = Val(mS(i, j))
    If x > 0 Or Left(mS(i, j), 1) = "0" Then
       If (mv(j, 2) <> mIz(i, j) + mu(i, 2)) Or m1 <> 18 Then
         m2 = m2 + 1
         Call krest(i * 2 + 77, 8)
         Call krest(87, j + 2)
       End If
    End If
Next j, i
If m2 = 0 Then mark = mark + 1 Else Call krest(76, 19)
```

Рис. 12. Проверка потенциалов

Последний проверяемый элемент опорного плана транспортной задачи – это стоимость перевозок (рис. 13). В случае неверного расчета стоимости зачеркивается не только поле, содержащая ответ, но и для наглядности надпись, справа от задания, указывающая на количество начисляемых баллов за верное выполнение задания.

```
Z = 0                          'Проверка расчета стоимости опорного плана
For i = 1 To 4
  For j = 1 To 5
    Z = Z + mT(i, j) * mIz(i, j)
Next j, i
If m1 = 18 And Z = Cells(90, 5) Then
    mark = mark + 1
  Else
    Call krest(90, 5)
    Call krest(78, 19)
End If
```

Рис. 13. Проверка расчета стоимости опорного пана.

При верификации оптимального плана транспортной задачи таким же образом, как и для опорного осуществляется считывание плана, проверка строк и столбцов транспортной таблицы на соответствие условию задачи, определяются и сравниваются потенциалы. Однако в данном случае мы проверяем заполненную таблицу на оптимальность (рис. 14). Все небазисные ячейки оптимального плана транспортной задачи должны отвечать критерию оптимальности: $c_{ij} - v_j + u_i \geq 0$.

```
m3 = 0                         'Рассчет коэффициентов критерия оптимальности
k = 0
DeltaMin = 0
For i = 1 To 4
  For j = 1 To 5
    If mT(i, j) = 0 Then
      k = k + 1
      Delta(k) = mIz(i, j) - mv(j, 2) + mu(i, 2)
      If Delta(k) < 0 Then
         Cells(i * 2 + 77, j + 11).Interior.ColorIndex = 12
         m3 = m3 + 1
      End If
    End If
Next j, i
If m1 = 18 And m2 = 0 And m3 = 0 Then
     mark = mark + 3
  Else
     Call krest(82, 19)
End If
```

Рис. 14. Проверка транспортной таблицы на оптимальность.

Все представленные в статье программные продукты успешно используются в учебном процессе Краснодарского университета МВД России при изучении дисциплины высшая математика курсантами, обучающимися по специальности 10.05.05 Безопасность информационных технологий в правоохранительной сфере.

Литература

1. Лаптев, В.Н. О технологиях разработки программных приложений для генерирования и проверки практических заданий по математическим дисциплинам / В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2020. – №01(155). С. 164 – 177. – IDA [article ID]: 1552001013. – Режим доступа: http://ej.kubagro.ru/2020/01/pdf/13.pdf, 0,875 у.п.л.

2. Лаптев, В.Н. Основные принципы использования офисных приложений для подготовки и верификации электронных практических заданий / В.Н. Лаптев, Е.В. Михайленко // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2021. – №09(173). С. 76 – 92. – IDA [article ID]: 1732109007. – Режим доступа: http://ej.kubagro.ru/2021/09/pdf/07.pdf, 1,062 у.п.л.

3. Михайленко, Е.В. Математика: учебник / Е. В. Михайленко. – Краснодар: Краснодарский университет МВД России, 2023. – 478 с.

4. Михайленко, Е.В. Методы создания компьютерных программ для автоматизации подготовки и проверки практических заданий на базе офисных приложений. / Е.В. Михайленко // Математические методы и информационно-технические средства [Электронный ресурс]: материалы XVIII Междунар. науч.-практ. конф. (17 июня 2022 г.) – Электрон. дан. – Краснодар: Краснодарский университет МВД России, 2022. – 1 электрон. опт. диск. С. 109 – 116

5. Михайленко, Е.В. Объектно-ориентированное программирование: учебно-практическое пособие / Е.В. Михайленко, В.А. Епифанцева. – Краснодар: Краснодарский университет МВД России, 2021. –109 С.

6. Михайленко, Е.В. Особенности разработки компьютерных приложений для генерации и верификации практических заданий, включающих обработку матриц / Е.В. Михайленко // Проблемы информационного обеспечения деятельности правоохранительных органов: сборник статей 7-й Всероссийской научно-практической конференции. – Белгород: Белгородский юридический институт МВД России имени И.Д. Путилина, 2020. – С. 3 – 20.

7. Михайленко, Е.В. Технологии программирования: учеб. пособие / Е.В. Михайленко, А.К. Назаров – Краснодар: Краснодарский университет МВД России, 2019. 510 с.

8. Старостенко И.Н. Прикладная математика: учебник / И.Н. Старостенко, Е.В. Михайленко, А.А. Хромых. – Краснодар: Краснодарский университет МВД России, 2023. – 346 с.

9. Старостенко, И.Н. К вопросу об использовании информационных технологий при организации самостоятельной работы обучающихся / И.Н. Старостенко, Е.В. Михайленко // Проблемы современного педагогического образования. – Ялта: РИО ГПА, 2019. № 65-1. С. 257 - 262.

Сведения об авторе

Михайленко Евгений Владимирович, кандидат физико-математических наук, доцент, заместитель начальник кафедры информатики и математики Краснодарского университета МВД России; e-mail: evmikhaylenko@mail.ru.

Меняйло Дмитрий Васильевич,
Хайминова Ксения Евгеньевна

ИННОВАЦИОННЫЕ МЕТОДЫ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

На данный момент происходит стремительное развитие информационных технологий, которые быстро и неуклонно проникают во многие сферы нашей жизни. К сожалению, несмотря на множество положительных сторон современных технологий, существуют и отрицательные стороны. Одним из ярко выраженных примеров является рост киберугроз. Вопросы безопасности и защиты информации приобретают все большую актуальность в современном мире.

Криптография - наука о методах защиты информации - играет важную роль в этом процессе. С каждым годом технологии криптографической защиты становятся все более сложными и инновационными, чтобы обеспечивать надежную защиту данных от различных видов угроз.

История развития криптографии насчитывает несколько тысячелетий. Еще в Древнем мире были первые упоминания о шифровании информации. В древнем обществе не каждый мог читать и писать, поэтому письменность была некоторой криптографической системой. В дальнейшем люди начали придумывать способы преобразования текста, чтобы скрыть информацию от нежелательных получателей. Они использовали различные числа, иероглифы, картинки и другие символы вместо букв. Первые профессиональные криптографы появились при Иване Грозном. Задача криптографов заключалась в разработке более сложного шифра, так как с развитием государства и общества, секретная информация стала доступной не только им. Они отвечали за внешнюю политику государства, а типичным шифром того времени были замены одной буквы на другую.

В связи с этим, история криптографии уходит далеко в прошлое, и она является основой защиты информации. Криптография является одним из

наиболее эффективных способов защиты данных. Она не защищает доступ к получению информации, а шифрует ее, что обеспечивает повышенную степень секретности. Однако, с появлением компьютерной техники и возможности обработки больших объемов данных, классические методы стали уязвимы для атак.

Среди инновационных методов криптографии можно выделить шифрование с использованием квантовых ключей, который позволяет создавать шифры, которые невозможно взломать даже самыми мощными компьютерами.

Также значительный интерес представляют алгоритмы шифрования на основе искусственного интеллекта и машинного обучения. Эти методы позволяют создавать более сложные коды и анализировать поведение злоумышленников для предотвращения атак.

Сегодня инновационные методы криптографической защиты информации предлагают новые подходы к решению проблем безопасности. Одним из таких методов является асимметричное шифрование. Это позволяет передавать сообщения без необходимости использования одного и того же ключа для шифрования и дешифрования сообщений.

Другим инновационным методом является квантовая криптография. Этот метод использует свойства квантовой механики для гарантированной защиты передаваемых данных от любых прослушивателей.

Также существуют новые алгоритмы шифрования, которые устойчивы даже при использовании высокопроизводительных компьютеров. Один из таких алгоритмов - AES (Advanced Encryption Standard) - используется для защиты данных в банковской сфере, правительственных учреждениях и других критических инфраструктурах.

Современные технологии и инновационные методы криптографической защиты информации помогают предотвратить кибератаки и защитить конфиденциальную информацию. Одним из таких методов является использование алгоритмов шифрования с открытым ключом, которые

обеспечивают высокий уровень безопасности данных. Эти алгоритмы используют два разных ключа для шифрования и дешифрования информации.

Также в последнее время все большую популярность получает метод шифрования на основе блокчейна. Данный метод позволяет создать цепочку блоков, каждый из которых содержит уникальную информацию о предыдущем блоке, что делает его невозможным для изменения или подделки.

Еще одним инновационным методом является применение машинного обучения для определения возможных угроз безопасности и автоматического реагирования на них. Такие системы могут быстро обнаруживать необычное поведение пользователей или программ и предотвращать потенциальные кибератаки.

Важно отметить, что при выборе инновационных методов криптографической защиты информации необходимо учитывать как их эффективность, так и стоимость внедрения и поддержки. Также следует помнить о том, что никакой метод не гарантирует абсолютную безопасность данных, поэтому требуется использование комплексных мер для защиты информации.

Также активно разрабатывается квантовая криптография, которая использует принципы квантовой физики для создания абсолютно безопасных связей между устройствами. Это позволяет устранить возможность перехвата или изменения передаваемых данных.

Квантовая криптография - это инновационный метод защиты информации, основанный на использовании квантовых физических свойств. Она позволяет создать абсолютно безопасную систему передачи данных, которую невозможно взломать даже с помощью самых мощных вычислительных машин.

Основной принцип квантовой криптографии заключается в использовании квантовых состояний частиц для передачи информации. Каждый бит информации представляется одним из двух возможных состояний: вертикальной или горизонтальной поляризации фотона. Передаваемые данные кодируются в виде последовательности поляризаций фотонов.

Получатель использует специальное устройство для измерения поляризации каждого фотона и получения исходного сообщения. Если злоумышленник попытается перехватить переданные данные, он изменит состояние каждого фотона и нарушит целостность сообщения.

Квантовая криптография уже используется в коммерческих системах передачи данных, где защита конфиденциальности является первостепенной задачей. Например, банки используют квантовую криптографию для защиты финансовых транзакций, а правительственные организации - для передачи секретной информации.

В настоящее время криптографическая защита информации является одной из ключевых технологий в области информационной безопасности. Однако с развитием технологий и появлением новых угроз появляются вызовы для будущего криптографии.

Одним из главных вызовов становится возможность квантового компьютера, который может ломать существующие алгоритмы шифрования. Для решения этой проблемы разрабатываются новые методы, основанные на квантовых технологиях, такие как квантовая криптография.

Еще одним вызовом является расширение интернета вещей (IoT), которое приводит к необходимости защищать огромное количество устройств и данных. В данном случае инновационные методы должны быть эффективными и экономически выгодными.

Также стоит отметить растущую значимость защиты персональных данных, которая требует разработки новых методов шифрования и контроля доступа.

Кроме того, перспективами развития криптографии являются применение искусственного интеллекта и машинного обучения для улучшения качества шифрования, а также развитие криптовалют и блокчейн-технологий.

Таким образом, уровень преступлений в информационной сфере возрастает с каждым днем, вместе с развитием общества. Криптография является

одним из наиболее эффективных способов защиты персональных данных и имеет глубокие корни, проходящие несколько этапов развития. В современном мире тема криптографической защиты информации актуальна и предоставляет возможность научной деятельности для будущих исследований.

Литература

1. Бабаш А.В., Баранова Е. К. Криптографические методы защиты информации. – 2022. – 189 с.

2. Борлакова М.А., Болатов М.Х. Современные методы и средства защиты информации // Вестник Академии знаний. – 2023. – №. 54 (1). – С. 68-72.

3. Ахметов Р.Д., Тимергалин А.Р., Князев О.А. Изучение проблем кибербезопасности и методов её обеспечения // «Мировая наука». №7(52). – 2021. С. 108-113.

4. Закревская П.А., Воробьева Т.И., Малолетко Н.Е. Внедрение криптографических методов защиты информации в систему безопасности МВД России // Тенденции развития науки и образования. – 2022. – № 84-2. – С. 14-18.

Сведения об авторах

Меняйло Дмитрий Васильевич, кандидат юридических наук, доцент, начальник кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: menyilo.dmitriy@yandex.ru.

Хайминова Ксения Евгеньевна, курсант факультета правоохранительной деятельности Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: haiminovak@mail.ru.

Назаренко Игорь Святославович

АКТУАЛЬНЫЕ ВОПРОСЫ ПРИМЕНЕНИЯ ИНФОРМАЦИОННО-ТЕХНИЧЕСКИХ СРЕДСТВ ПОДРАЗДЕЛЕНИЯМИ ОВД ПРИ РАСКРЫТИИ ПРЕСТУПЛЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

В статье рассматриваются особенности применения информационно-технических средств, предназначенных для поиска, извлечения и анализа цифровых следов при раскрытии преступлений, совершаемых с использованием информационно-коммуникационных технологий, сотрудниками правоохранительных органов.

Значительный рост преступлений, совершаемых с использованием информационно-коммуникационных технологий, за последнее десятилетие обусловил активную разработку и внедрение в правоохранительную деятельность информационно-технических средств, предназначенных для поиска, извлечения и анализа цифровых следов противоправных деяний. На территории Российской Федерации создана правовая база для применения соответствующих информационно-технических средств в процессе осуществления правоохранительной деятельности. В частности, статья 11 Федерального закона от 07.02.2011 № 3-ФЗ «О полиции» предоставляет право использовать сотрудникам органов внутренних дел достижения науки и техники, информационные системы, сети связи, а также современную информационно-телекоммуникационную инфраструктуру. Например, сотрудниками полиции активно используются информационно-технические средства при документировании обстоятельств совершения преступлений, административных правонарушений, обстоятельств происшествий, в том числе в автоматическом режиме, а также для фиксации действий сотрудников органов внутренних дел и иных участвующих лиц при проведении следственных действий, оперативно-

розыскных мероприятий, экспертиз, исследований и иных служебных обязанностей [1].

Отличительной особенностью преступлений, совершаемых с использованием информационно-коммуникационных технологий, от преступлений общеуголовной направленности является наличие цифровых следов противоправного деяния, которые имеют закономерность своей локализации. Для выявления цифровых следов существует большое количество специализированного программного обеспечения, реализующего узкие задачи: по изъятию информации из дампов памяти, образов дисков, либо структурированию информации из журналов событий программ-браузеров. Специализированные программно-аппаратные комплексы имеют в своих наборах как информационно-техническое оснащение, так и наиболее востребованные кабели подключения, различные портативные решения для «клонирования» накопителей информации с целью недопущения ее модификации при поиске цифровых следов злоумышленника. Как показал анализ практики, наиболее востребованными у специалистов экспертных подразделений Белгородской области являются такие программно-аппаратные комплексы как «UFED» и «Мобильный Криминалист». Поскольку наиболее популярным в последние техническим устройством, используемым злоумышленниками при совершении преступлений с использованием информационно-коммуникационных технологий, является смартфон, то большинство средств, применяемых для поиска и фиксации цифровых следов, ориентированы на работу именно с ними. Информационно-технические средства также содержат серьезный инструментарий, применяемый к персональным компьютерам, ноутбукам, планшетам, телефонам, а также другим техническим устройствам. Дополнительно они позволяют находить техническую информацию, хранящуюся в «облачных хранилищах», но имеющую точку входа с терминала связи либо домашнего компьютера – резервные копии приложений и мессенджеров.

Например, комплекс для поиска и исследования цифровых следов «Мобильный криминалист» в максимально расширенном наборе имеет программно-аппаратное исполнение. Функционал комплекса разнообразен как по спектру устройств, с которыми он умеет работать: стационарные и портативные компьютеры, «классические» мобильные телефоны и смартфоны, дроны, устройства, реализованные на распределенных системах хранения («облачные хранилища»), так и по возможности поиска и извлечения информации из различных популярных приложений и операционных систем разных семейств. Стоит обратить внимание, что помимо поиска и извлечения цифровых следов преступлений и иной оперативно-значимой информации, возможно извлечение, в том числе, и удаленных данных, обход защитных механизмов, препятствующих получению хранимых сведений или переходов, а также анализ полученных данных и отображение в виде «граф-связей», группировок данных и построения хронологии событий. Получение данных из терминала связи («классического» мобильного телефона либо смартфона) посредством комплекса «Мобильный Криминалист» потребует подключения к устройству с установленным соответствующим программным обеспечением. «Мобильный криминалист» позволяет обойти технологию встроенного аппаратного шифрования для устройств, использующих чипсеты «MTK», «Qualcomm», «Spreadtrum», а также брендов «LG» и «Samsung». Для этого указанное информационно-техническое средство модифицирует загрузочный раздел встроенного в гаджет флеш-накопителя информации или отправляет на устройство модифицированный файл образа загрузчика, открывая таким образом доступ к правам суперпользователя [2]. В комплектах расширенных версий программно-аппаратного комплекса предусмотрены наборы соответствующих шлейфов и кабелей, позволяющих использовать широкий спектр интерфейсов, в том числе возможно подключение посредством интерфейса «JTAG». Программная адаптация происходит за счет широкого набора входящих в комплектацию драйверов.

К сожалению, в связи с введением санкционной политики со стороны зарубежных государств, в настоящее время имеются проблемы с обновлением программного обеспечения и использованием программно-аппаратного комплекса иностранного производства «UFED» (Universal Forensic Extraction Device). Процессуальная сторона процесса извлечения данных с использованием UFED представляет собой оформление протокола осмотра предметов с приложением аналитического отчета и справки специалиста или заключения эксперта. При этом процесс извлечения и анализа максимально автоматизирован, задача практического сотрудника – установление носителя значимой информации. Наиболее популярная в использовании комплектация комплекса уже в себе содержит модули по извлечению данных, составлению на их основе отчетов, комплексному анализу извлеченных данных с составлением графов связей абонентских устройств. Комплекс также позволяет рассматривать даже удаленную информацию и неочевидную – нестандартные файлы или данные компонентов сопрягаемых устройств, «геоданные» – как привязка события в метаданных файла [3]. Указанная оперативно-значимая техническая информация может сыграть значимую роль в качестве доказательства, поскольку содержит технические сведения о привязке к местности, например, при поиске тайника с наркотическими средствами, при восстановлении удаленных файлов, содержащих порнографическое изображение несовершеннолетних, при восстановлении маршрута следования заподозренного лица.

Несмотря на существование широкого спектра информационно-технических средств, в том числе программно-аппаратных комплексов, острой остается проблема подготовки специалистов, обладающих навыками и допуском работы с ними, поскольку длительное время остается высокая нагрузка на проведение компьютерно-технических исследований и экспертиз. В качестве пути решения указанной проблемы, возможно рассмотреть вопрос о введении в органах внутренних дел должности следователя-криминалиста (на примере СК

России), его обучении методике поиска, изъятия и анализа цифровых следов с использованием вышеуказанных программно-аппаратных комплексов при расследовании дел, совершенных с использованием информационно-коммуникационных технологий, что позволит существенно снизить нагрузку на экспертные подразделения и сократить сроки предварительного следствия.

Литература

1. Федеральный закон от 07.02.2011 № 3-ФЗ (ред. от 06.02.2023) «О полиции», // СПС «Консультант Плюс».

2. «МКО системы» [Электронный ресурс] URL: https://mko-systems.ru/mobile-kriminalist (дата обращения: 19.06.2023).

3. Рогова И.А., Бурцева Е.В. Практика применения UFED – универсального устройства для криминалистического исследования мобильных устройств // Евразийский Союз Ученых. 2015. №7-5 (16). [Электронный ресурс] URL: https://cyberleninka.ru/article/n/praktika-primeneniya-ufed-universalnogo-ustroystva-dlya-kriminalisticheskogo-issledovaniya-mobilnyh-ustroystv (дата обращения: 19.06.2023).

Сведения об авторе

Назаренко Игорь Святославович, старший преподаватель кафедры информационно-компьютерных технологий в деятельности органов внутренних дел Белгородского юридического института МВД России имени И.Д. Путилина; e-mail: belregion_k@mail.ru.

Параскевов Александр Владимирович,
Невенчанная Виктория Николаевна

ИССЛЕДОВАНИЕ МЕТОДОВ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЕЙ МОБИЛЬНЫХ ПРИЛОЖЕНИЙ

Проблема надежности и простоты идентификации пользователя, а также удобная аутентификация на мобильных устройствах являются актуальными задачами на сегодняшний день. Это можно объяснить тем, что по своей природе человек постоянно испытывает интерес к окружающей его информации. Поэтому еще с древних времен люди придумывались речевые пароли, специальные печати и подписи, а появление таких механических устройств аутентификации, как замок и ключ, значительно упростило задачу.

В связи с глобальным развитием технологий стали появляться более совершенные устройства защиты данных. В век информационных технологий все личные данные были оцифрованы и им стали требоваться новые методы борьбы с кражей информации.

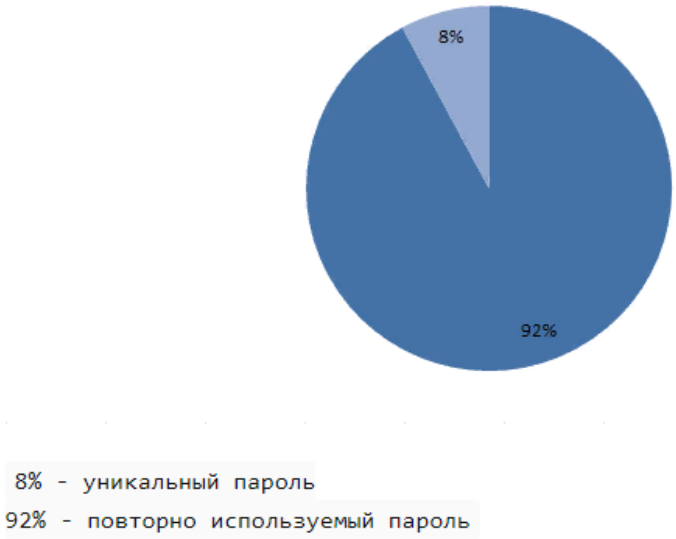


Рис. 1. Статистика использования ключевых слов

Современные мобильные приложения предоставляют пользователям широкий спектр возможностей, начиная от общения и развлечений, заканчивая банковскими операциями и покупками. Однако, с увеличением

функциональности приложений, возрастает и риск несанкционированного доступа к личным данным пользователей. Для защиты от таких угроз используются различные методы аутентификации пользователей [1].

Рис. 2. Использование клавиш

Методы аутентификации.

1. Пароль. Метод аутентификации с помощью пароля является одним из самых распространенных и простых способов проверки подлинности пользователя. Все простейшие системы аутентификации используют именно парольный принцип. Чтобы получить доступ к желаемому ресурсу, от пользователя требуется лишь знать заранее установленный набор символов и правильно его ввести. Поэтому данный тип аутентификации является более распространенным.

2. PIN-код. PIN-код (Personal Identification Number) – это метод аутентификации, который используется для проверки личности пользователя. Он состоит из цифр и может быть использован для доступа к различным системам и устройствам, таким как банкоматы, мобильные устройства, компьютеры и т.д.

3. Биометрическая аутентификация. Биометрическая аутентификация – это метод аутентификации, который использует биологические характеристики

человека, такие как отпечатки пальцев, голос, лицо, сетчатка глаза и другие, для проверки личности пользователя.

4. Двухфакторная аутентификация. Двухфакторная аутентификация (2FA) – это метод, требующий от пользователя предоставления двух различных форм идентификации для подтверждения своей личности. Это может быть пароль и одноразовый код, полученный через приложение или SMS-сообщение, отпечаток пальца или другие комбинации.

5. Аутентификация на основе токенов. Метод аутентификации на основе токенов (Token-based authentication) является одним из наиболее распространенных методов аутентификации в современных веб-приложениях. Токен – это уникальный код, который выдается пользователю для подтверждения его личности при входе в систему. Он может быть сгенерирован программно или физически представлен в виде устройства, например, USB-ключа или смарт-карты. При использовании двухфакторной аутентификации, токен может быть одним из факторов, который пользователь должен предоставить для подтверждения своей личности, помимо пароля или другого фактора, такого как отпечаток пальца или голосовое распознавание. Также он обычно имеет ограничения по сроку действия количеству применений, что повышает безопасность аутентификации.

6. Генерация временных паролей. Он заключается в том, что при входе в приложение пользователю генерируется уникальный временный пароль, который действителен только на короткое время. Этот пароль можно получить только на заранее зарегистрированный телефон или электронную почту. Такой метод аутентификации обеспечивает высокий уровень защиты, так как злоумышленник не сможет получить доступ к уникальному паролю.

7. Методы аутентификации на основе биометрических данных, которые используют данные о голосе, лице, отпечатке пальца и др. Однако, для того чтобы использовать эти методы, мобильные устройства должны иметь соответствующее оборудование.

Самым скачиваемым приложением в 2022 году стал «TikTok» (672 млн. скачиваний). Ведутся постоянные работы по защите пользовательских аккаунтов и обучению цифровой гигиене, чтобы данные были максимально защищены. Оповещение системы безопасности (указывает на подозрительные события, недавние изменения пароля, вход с нового устройства), пароль (не менее 12 символов, состоящий из букв, цифр и специальных символов), двухэтапная верификация (дополнительный уровень защиты сторонних устройств) [2].

Остальные приложения с высоким рейтингом скачивания:

— Instagram: 548 млн., настроены – пароль, двухфакторная аутентификация;

— WhatsApp: 424 млн., используются – сквозное шифрование, (декодирование передаваемой информации только вами и получателем), двухфакторная аутентификация, также предусмотрено скрытие сведений о себе;

— Snapchat: 337 млн., внедрены – пароль, двухфакторная аутентификация;

— Telegram: 310 млн., настроена – двухфакторная аутентификация (облачный пароль, предшествуют – указание номера, ввод одноразового пароля – необходимо для входа как на новом устройстве, так и после переустановки приложения);

— Госуслуги: 70 млн., используются: пароль и методы на основе биометрических данных (по биометрии).

Вне зависимости от разнообразия используемых методов аутентификации в данных приложениях, распространенная проблема – кража аккаунтов пользователей злоумышленниками и утечка большого количества личных данных. Отсюда вывод: насколько бы надежен не был ваш пароль, данные методы не самые надежные для использования.

Выбор наиболее эффективного метода аутентификации зависит от конкретной задачи и от уровня защиты, которую необходимо обеспечить. Однако, важно учитывать, что не существует абсолютно надежного метода

аутентификации, и поэтому необходимо использовать несколько методов одновременно. При этом стоит добавить, что как бы пользователь не комбинировал методы аутентификации, необходимо понимать, что, каким сложными и совершенными не были средства аутентификации самым уязвимым местом в безопасности является человек. Следует серьезно подходить к вопросу хранения собственных данных, прежде чем установить тот или иной метод защиты к ним.

Литература

1. Параскевов А.В. Перспективы и особенности разработки чат-ботов / А.В. Параскевов, А.А. Каденцева, С.И. Мороз // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2017. – №06(130). С. 395 – 404. – IDA [article ID]: 1301706030. – Режим доступа: http://ej.kubagro.ru/2017/06/pdf/30.pdf, 0,625 у.п.л.

2. Бабенков И.М. Средства и методы защиты информации в экономической сфере / И.М. Бабенков, А.В. Параскевов // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета (Научный журнал КубГАУ) [Электронный ресурс]. – Краснодар: КубГАУ, 2016. – №05(119). С. 653 – 665. – IDA [article ID]: 1191605047. – Режим доступа: http://ej.kubagro.ru/2016/05/pdf/47.pdf, 0,812 у.п.л.

Сведения об авторах

Параскевов Александр Владимирович, старший преподаватель кафедры компьютерных технологий и систем Кубанского государственного аграрного университета им. И. Т. Трубилина; e-mail: paraskevov.alexander@yandex.ru.

Невенчанная Виктория Николаевна, факультет прикладной информатики Кубанского государственного аграрного университета им. И. Т. Трубилина; e-mail: nevvikusyaaa@gmail.com.

Печатнова Елена Владимировна,
Лапина Дарья Дмитриевна

ПРЕДУПРЕЖДЕНИЕ ПРЕСТУПЛЕНИЙ, СВЯЗАННЫХ С НЕЗАКОННЫМ ОБОРОТОМ НАРКОТИКОВ, СОВЕРШАЕМЫХ НЕСОВЕРШЕННОЛЕТНИМИ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СЕТЕЙ

Выбранная тема приобрела особую актуальность в период бурного развития информационных технологий и внедрения цифровизации во все сферы жизни общества, в том числе и в криминальную сферу [1]. Проблема подростковой наркомании является наиболее актуальной на сегодняшний день, ведь каждый год в нашей стране происходит «омоложение» наркозависимых. В связи с развитием интернет-пространства, распространение наркотиков стало доступным в информационно-коммуникационных сетях. Важнейшее значение данный тезис приобрел в период пандемии коронавируса в 2020 году, а также в период постпандемии восстановления экономики и общества России в 2021 году. Длительное самоизоляционное состояние затронуло почти весь российский рынок, включая наркопотребителей. Общая нервозность, дезорганизованность подростков и молодежи дистанционным обучением, безработица, попытки получения дохода за счет производства и распространения наркотиков – все эти факторы привели к росту наркотрафика.

Наркомания является тяжелым заболеванием, проявляющимся в частом приеме и склонности к большим дозировкам наркотиков, прекращение их употребления влечет за собой ухудшение физического и психического состояния и стойкую зависимость от наркотиков.

Цель работы – анализ понятия и структуры бесконтактной торговли наркотиками с использованием интернет-сети и влияния их на общее структурирование и динамику распространения наркотических веществ.

Примерно десятилетием ранее, продажа наркотических средств производилась «из рук в руки», что в значительной мере затрудняло процесс

реализации наркотиков. В последние годы продажи наркотиков почти полностью переместились в глобальный Интернет и стали бесконтактными, а реализация их в обществе происходит благодаря нашему подрастающему поколению, вовлекаемому в сферу наркотиков. Криминальные функции выполняются через защищенные интернет-мессенджеры и различные электронные способы оплаты. Появились приложенеия с возможностью анонимной переписки, такие как Viber, Telegram и др. Таким образом, на сегодняшний день существует современный и усовершенствованный механизм бесконтактной продажи наркотиков, доступ к которому может получить каждый. Благодаря этому потребитель свободно может использовать свое мобильное устройство для связи с торговцем наркотиками, обеспечивая им обоим полную анонимность.

Эта тенденция отразилась и на «омоложении» участников наркоторговли: если раньше работа велась в основном с людьми старше 18 лет, то сейчас среди наркозависимых много школьников 14-15 лет. Но кроме вышеперечисленных причин также присутствуют и другие. Во-первых, вещества на основе опиума потеряли своих покупателей и на освободившееся место пришли «синтетические вещества» вроде снюса, спайсов и экстази, которые стали весьма популярны среди молодежи. Они кажутся безвредными снаружи, и организм вырабатывает толерантность при многократном использовании. Во-вторых, молодежь, как активные пользователи Интернета, и будучи неосведомленными в некоторых вопросах, касающихся наркотиков, активно были заинтересованы в данном процессе. Вещества с привлекательными названиями, такими как «Мяу», «Матильда», продвигаются как в телеграмм-каналах, так и в социальных сетях VK, Insagram, а также в развлекательных приложениях по типу Tik-Tok, который очень популярен среди подростков. При этом процесс продажи завуалирован как квест, в котором ребята должны выполнить ряд действий, чтобы найти «клад», закладку. Такое занятие не пугает, а привлекает молодых людей, не занятых работой или учебой.

Официальные данные также свидетельствуют об актуальности проблемы: заместитель генерального директора Управления по борьбе с наркотиками МВД России Кирилл Смуров заявил: «В этом году мы в полтора раза больше выявили и пресекли наркотических преступлений, совершенных с помощью IT-технологий, с использованием возможностей интернета, иных мессенджеров. Это очень много - порядка 59 тыс. преступлений зарегистрировано данной категории» [2]. Данные о возрастном распределении наркозависимых по данным ФСКН представлены на рисунке 1.

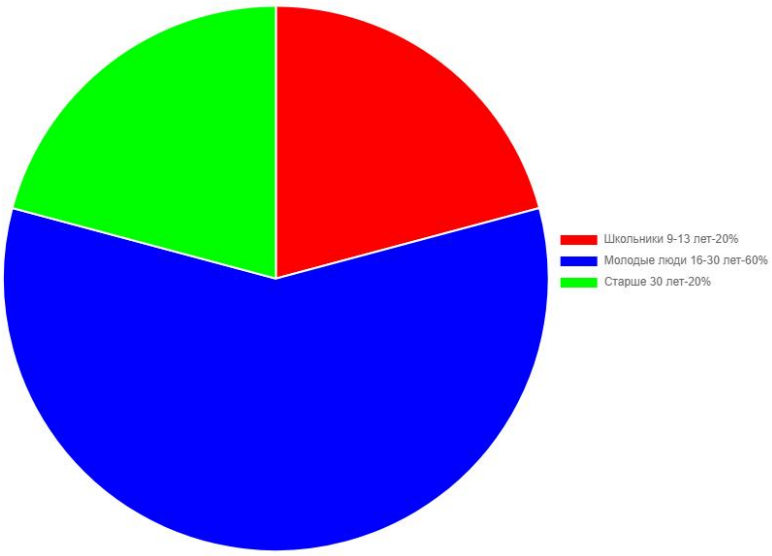


Рис. 1. Сведения о возрастных группах наркозависимых, 2021

Согласно официальным статистическим данным ГИАЦ МВД России, в 2019 году задокументировано 190 197 наркопреступлений, большинство из которых выявлено органами внутренних дел, а также установлено 85 425 лиц, совершивших указанные преступления. Вместе с тем возросло количество выявленных фактов сбыта наркотических средств, совершаемых бесконтактным способом, а также преступлений, связанных с контрабандой наркотиков [3]. Таким образом, показатели наркопреступлений с каждым годом неуклонно растут, а также повышается и рост числа лиц, употребляющих наркотические средства.

Рассмотрим механизмы планирования и реализации бесконтактных продаж лекарств в онлайн-пространстве. В период постпандемической

криминогенной обстановки в обществе как само киберпространство, так и включенные его криминальные элементы фактически вышли на новый уровень своей активности, создав массовый инструмент сегодняшнего дня - наркобизнес с четкой структурой и иерархическими связями. Эти преступления имеют длительный период из-за того, каким образом они осуществляются. В связи с изменившимся характером современных преступных ситуаций требуется новый подход и средство, которое позволит выявить виновных в незаконном обороте наркотиков, документировать их преступление и впоследствии пресечь его.

В жизни шаблонная схема криминальных связей интернет-магазина по бесконтактной продаже наркотиков путем формирования закладок выглядит следующим образом:

1. Организатор: создает интернет магазин и осуществляет общий менеджмент.

2. Оператор: консультирует клиента по правилам заказа, цены, вида наркотиков, места нахождения в тайнике-закладке, ведёт архив выполненного заказа, координирует работу интернет-чата.

3. Оптовый курьер-закладчик: по заданию диспетчера составляет крупнооптовые тайники - пакеты с наркотиком для розничных курьеров-закладчиков.

4. Розничные курьеры-закладчики: приобретают оптовые закладки, содержащие наркотики, для дальнейшей реализации в розничные сети через мелкие закладки.

Крупные розничные магазины наркотиков являются бизнес-корпорациями, в составе которых расположены подразделения, которые отвечают за рекламу и маркетинг интернета, информационное обеспечение и выбор сотрудников. Многие люди вовлечены в этот бизнес. Онлайн-форма продажи наркотиков означает наличие нескольких субъектов, осуществляющих объективные аспекты поведения в данном интернет-магазине, с четким распределением функций между ними по строгой иерархии.

С учетом вышеизложенного, наркопреступность имеет тенденцию и дальше перемещаться в киберпространство, продолжая и усиливая тенденцию роста. В будущем это может негативно сказаться на общей структуре рынка. В частности, речь идет о чрезмерном увеличении теневого элемента.

Таким образом, можно предложить следующие меры по предупреждению преступлений, связанных с незаконным оборотом наркотиков, совершаемых несовершеннолетними с использованием информационно-телекоммуникационных сетей:

1. Недостатки правового регулирования отдельных вопросов противодействия распространению в информационном пространстве сети Интернет запрещенной информации указывают на необходимость принятия нормативно-правового акта, который будет устанавливать требования к интернет-компаниям по осуществлению ими мониторинга контента сети и удалению вредной информации из интернета, а также обяжет операторов мобильной связи разграничить пользователей по возрастному критерию (до 18 лет и старше) с одновременным ограничением для первой возрастной категории доступа к сайтам криминогенного характера [4].

2. Рекомендуется создавать группы на базе ВУЗов МВД России из числа наиболее подготовленных курсантов для осуществления профилактических работ по недопущению вовлечения несовершеннолетних по распространению наркотиков с помощью информационно-телекоммуникационных сетей.

3. Рекомендуется демонстрация специализированных профилактических фильмов для школьников и подростков, сюжетная линия которых будет содержать информацию о рисках и угрозах, связанных с использованием сети Интернет в сфере оборота наркотиков.

Результаты проведенной работы подтвердили гипотезу о том, что бесконтактная продажа наркотиков через Интернет становится все более популярной и опасной. На это указывают проанализированные данные за 2021 год. Для предотвращения дальнейшего роста показателей, связанных с оборотом

наркотиков с использованием информационно-коммуникационных технологий, необходим сбалансированный подход, основанный на опыте и передовых научных исследованиях, а также концентрация внимания на проведении профилактических мероприятий среди несовершеннолетних.

Литература

1. Детков, А. А. Бесконтактный сбыт наркотических средств посредством сети Интернет: криминогенная обстановка в Алтайском крае / А. А. Детков, М. А. Стародубцева // Уголовно - исполнительное право. 2021. – Т. 16(1-4), №4. – С. 512-521. DOI: 10.33463/2687- 2122X.2021.16(1-4).4.512-521.

2. ТАСС: информационное агентство России: [сайт]. – Москва, 1999 – URL: https://tass.ru/obschestvo/13291329 (дата обращения: 18.12.2022). – Текст: электронный.

3. Министерство внутренних дел Российской Федерации: официальный сайт – Москва, 2022. – Обновляется в течение суток. – URL: http://www.mvd.ru/ presscenter/ statistics/reports/ (дата обращения: 19.12.2022). – Текст: электронный.

4. Урбан, В. В. Преступления, совершаемые с использованием информационно телекоммуникационных сетей: общая характеристика и уголовно процессуальные меры по их противодействию / В. В. Урбан // Вестник Восточно-Сибирского института МВД России. –№1 (88). – 2019. – URL: https://cyberleninka.ru/article/n/prestupleniya-sovershaemye-s-ispolzovaniem-informatsionno-telekommunikatsionnyh-setey-obschaya-harakteristika-i-ugolovno (дата обращения: 22.12.2022). DOI: 10.24411/2312-3184-2019-10005.

Сведения об авторах

Печатнова Елена Владимировна, кандидат технических наук, доцент кафедры и информатики и специальной техники Барнаульского юридического института МВД России.

Лапина Дарья Дмитриевна, Барнаульский юридический институт МВД России; e-mail: phukcia@yandex.ru.

Прокопенко Алексей Николаевич,
Жукова Полина Николаевна,
Страхов Андрей Александрович

ОСНОВНЫЕ ТРЕНДЫ В СФЕРЕ КИБЕРБЕЗОПАСНОСТИ В РОССИИ НА СОВРЕМЕННОМ ЭТАПЕ

Проблемы обеспечения безопасности информации постоянно возрастали в последние годы. Это обусловлено, как последствиями пандемии, в ходе которой значительное количество сотрудников начало работать удаленно, так и последствиями необъявленной войны НАТО против нашей страны. Помимо значительного увеличения людей, которые работают не из защищённого контура в офисе, а из дома или дачи, существенно возросло использование мобильных устройств. Также увеличилось количество устройств Интернета-вещей, которые также несут значительные угрозы безопасности информации.

Таким образом *первой и основной проблемой является существенное возрастание количества кибератак*. В 2022 году в России было зафиксировано около 510 тыс. преступлений с использованием информационных технологий против 10 тыс. в 2014-м. Таким образом, речь идет о более чем 50-кратном росте числа ИТ-преступлений. Такие цифры привел 22 мая 2023 года представитель криминалистического центра Следственного комитета Темирлан Салихов [4].

Ежедневно на информационные российские ресурсы фиксируется более 170 комплексных компьютерных атак, сообщил заместитель директора Национального координационного центра по компьютерным инцидентам (НКЦКИ) Николай Мурашов 25 мая 2023 года [3].

При этом после начала Специальной военной операции количество атак значительно выросло и приобрело системный характер. Россию уже больше года атакуют не злоумышленники, не преступники, а вражеские кибервойска и организованные группы под управлением вражеских разведок. Весной 2022 года в этом процессе участвовали только украинские группы, которые временно переключились с фишинговых атак на DDoS-атаки российских сайтов. Однако

уже к концу весны 2022 года к Украине присоединились сначала США и Великобритания, а затем практически весь Запад. В результате уголовно-наказуемые деяния в киберпространстве, если они совершаются против русских, в западных государствах в настоящий момент не только не наказываются, но и поощряются. Созданы специальные справочные ресурсы, например, Телеграмм-каналы, в которых пользователям разъясняется кого атаковать, как это делать и предоставляется весь программный инструментарий для совершения преступлений. Другие ресурсы для проведения атак ищут новых участников, которые получили названия хактивистов. Фактически данная деятельность приобрела промышленные масштабы, поскольку количество хактивистов исчисляется миллионами, а учитывая консультативную поддержку им не надо быть хакерами или даже грамотными пользователями. Нужен только компьютер и желание атаковать Россию.

Второй проблемой является возрастание количества фальшивых новостей на несколько порядков. До начала СВО файковые новости попадали в российское общество, но имели единичный характер. Однако с 2022 года существенно активизировалась деятельность Центра информационно-психологических операций (далее – ЦИПсО). ЦИПсО – это созданный в 2004 году представителями Сил специальных операций Украины центр, направленный на разжигание ненависти ко всему русскому [5]. Анализируя происходящее за последние полтора года можно констатировать, что информационные кибервойска Украины практически полностью захватили антироссийскую повестку в мировом сообществе. Они сотрудничают более чем с 2600 средствами массовой информации, в том числе со всеми ведущими западными телеканалами – CNN, BBC, CBS, NBC, ARD, Reuters и другими. Внутри нашей страны ЦИПсО, поддерживаемое спецслужбами НАТО, активно распространяет фейковые новости в соцсетях, телеграмм-каналах, других мессенджерах. Основными целями является разжигание паники и подрыв доверия к руководству государства и российской армии.

Третьей проблемой является существенная нехватка специалистов в области кибербезопасности в частности и информационной безопасности в целом. В нашей стране недостаточно не только инженеров и программистов, которые непосредственно занимаются обеспечением компьютерной безопасности, но и специалистов и руководителей, которые задействованы в организационно-правовом обеспечении безопасности информации в организациях. Например, после принятия Указа Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» [1] у большого количества организаций возникла необходимость не только в создании выделенных подразделений информационной безопасности, но и в возложении на заместителя руководителя организации полномочий по обеспечению информационной безопасности. При этом сотрудники указанных подразделений, а также указанные руководители, должны иметь или базовое образование в области информационной безопасности, или пройти профессиональную переподготовку. По разным оценкам количество требуемых специалистов составляет от 30 до 60 тысяч человек.

Наконец, *четвертой проблемой является уход западных IT-компаний с российского рынка*. Ранее приобретенное программное обеспечение или перестало работать, или лишилось лицензии. Были аннулированы подписки на облачные сервисы, включая подписки на функционал, относящийся к средствам безопасности. Удостоверяющие мировые центры перестали предоставлять услуги российским компаниям, а сертификаты, выданные не западными центрами, перестали принимать большинство представителей IT-индустрии в мире. Например, перестали принимать сертификаты от китайских удостоверяющих центров и не позволили открыться российскому центру. В результате возник кризис доверия в сфере кибербезопасности, что ведет к развалу единой всемирной отрасли в данной сфере. В настоящий момент в мире искусственно создана ситуация, позволяющая пользоваться только западными

продуктами в сфере информационной безопасности. При этом на территории России ими пользоваться нельзя. В ближайшем будущем данный кризис доверия неизбежно приведет к сегментированию отрасли обеспечения кибербезопасности.

Кроме угроз в сфере кибербезопасности необходимо обратить внимание на основные тенденции, сформировавшиеся в последние годы. В обзоре компании Gartner, подготовленном весной 2022 года выделено семь основных тенденций в сфере кибербезопасности [2].

Первой тенденцией является *расширение поверхности атаки*. До 2020 года для взлома корпоративных сетей и получения конфиденциальной информации преступникам было необходимо взломать именно компьютерную сеть корпорации. Однако в настоящий момент значительно чаще взламываются домашние компьютеры сотрудников, работающих удаленно, мобильные устройства руководителей организации и устройства Интернета-вещей. Соответственно, количество устройств, которые необходимо защищать, многократно возросло.

Устройства Интернета-вещей зачастую не обеспечены возможностью установки средств безопасности, а программное обеспечение в них не обновляется или обновляется нерегулярно. Также к ним невозможно применить накладные средства защиты. В настоящий момент для противодействия атакам на устройства Интернета-вещей используется создание отдельных подсетей с контролем трафика, а также поведенческий анализ данного трафика нейросетью.

По-прежнему самыми используемыми инструментами в кибератаках являются вирусы-шифровальщики. Например, в 2021 г. наблюдается двукратный рост атак, предпринимаемых вирусами-шифровальщиками. Так успешная атака в мае 2021 г. на американскую компанию Colonial Pipeline, обеспечивающую перекачку нефтепродуктов по всей территории США, привела к тому, что работа компании была парализована и компания была вынуждена заплатить злоумышленникам выкуп.

Помимо фишинговых атак и использования устройств Интернета-вещей, преступники для распространения шифровальщиков активно используют критические уязвимости. Учитывая, что многие западные программные продукты, используемые в России не получают обновления в последний год, найденные эксплойты несут постоянную угрозу российским пользователям. Также участились случаи сочетания шифрования и кражи конфиденциальной информации. Перед шифрованием предпринимается попытка скопировать из сети организации конфиденциальную информацию с целью двойного шантажа.

Вторая тенденция – это *возрастание риска атак на цепочки поставок*. Данная тенденция является продолжением первой и может быть названа возрастанием риска атак на недостаточно хорошо защищенные филиалы и аффилированные организации. Крупную компанию или государственную организацию взломать сложно, подобные атаки требуют существенных материальных затрат и не всегда являются успешными. Однако, у каждой организации есть филиалы и партнеры, которые имеют упрощенный доступ в защищенный контур крупной организации, но не имеют собственной адекватной защиты. В результате их локальные сети используются как плацдарм для последующей направленной атаки на крупную корпорацию. Аналогичная ситуация возникает с организациями, объединяющими различных лиц по профилю работы, например бухгалтерскими или юридическими. Подобные ассоциации так же, как правило, недостаточно защищены.

Третья тенденция – это *возрастание угроз идентификации пользователей*. Наиболее часто атака осуществляется с целью получения логина и пароля сотрудника компании. Особенная «охота» ведется за привилегированными учетными записями руководителей или IT-специалистов организаций. Преимущественным путем получения доступа к учетным записям является фишинг. Противодействие данной тенденции возможно только в случае массового внедрения многофакторной идентификации, в том числе с использованием биометрии.

Четвертая тенденция – это *увеличение ответственности различных руководителей за обеспечение кибербезопасности*. В компании Gartner данная тенденция названа распределенным принятием решений. В небольших организациях и государственных органах назначается ответственный за информационную безопасность. А в крупных компаниях ответственность за данное направление деятельности возлагается на всех представителей руководства. Подразделения по обеспечению кибербезопасности переподчиняются непосредственно руководству организации. При использовании облачной инфраструктуры ответственность распределяется между облачным сервисов, провайдером и клиентом, каждый из которых отвечает за свое направление обеспечения кибербезопасности.

Пятой тенденцией является *необходимость усилить обучение сотрудников организации*, поскольку человек по-прежнему является самым слабым звеном в кибербезопасности. При этом простое обучение уже не приносит необходимого результата и требуется регулярное проведение специализированных тренингов для вырабатывания у сотрудников организации устойчивых навыков кибергигиены.

Шестой тенденцией является *объединение или консолидация поставщиков (вендеров) программного обеспечения в сфере кибербезопасности*. Программные продукты повышают свою совместимость, что позволяет их использовать совместно. Это происходит и на уровне стандартов, и на уровне протоколов, и на уровне приложений, которые больше не конфликтуют друг с другом. Данная тенденция позволяет организациям уменьшить количество используемых программ, воспользовавшись услугами интегратора, и получать услуги обеспечения безопасности, фактически как услугу одного окна.

Седьмой тенденцией является *организация сети служб кибербезопасности* как на корпоративном, так и на национальном и всемирном уровне. Средства безопасности интегрируются с конечными устройствами, с серверами в датацентрах или облачных инфраструктурах. Концепция

предполагает, что компоненты архитектуры безопасности должны работать вместе, независимо от того, где они находятся (ПК, ЦОД или облако), обмениваться данными и в целом «усиливать» друг друга. Gartner предсказывает, что к 2024 г. организации, внедрившие подобную архитектуру, смогут снизить потери от индивидуальных инцидентов кибербезопасности на 90%.

Резюмируя вышесказанное можно констатировать, что за неполные полвека кибератаки прошли гигантский путь от угадывания паролей до deepfake – почти не отличимой цифровой копии личности со звуком и видео. Кибератаки используются массово и в них вовлечены миллионы людей, причем в отдельных политически мотивированных случаях кибератаки не признаются преступлением и не преследуются.

Развитие программного обеспечения направлено на создание комплексных решений обеспечения кибербезопасности на каждом этапе обработки, передачи и хранения информации. Однако политические решения в данной сфере ведут к практически неизбежному сегментированию мирового информационного пространства. Разные части земного шара не будут доверять друг другу и возможность свободной работы в сегменте противника исчезнет.

Нашей стране предстоит пройти путь по созданию национальной полностью автономной системы обеспечения безопасности в информационной сфере. Для этого потребуется не только создание программного обеспечения, обучение десятков тысяч специалистов, но и изменение менталитета миллионов людей.

Литература

1. Указ Президента РФ от 01.05.2022 № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации» // опубликован на Официальном интернет-портале правовой информации http://pravo.gov.ru – 01.05.2022.

2. 7 трендов информационной безопасности. Обзор: Информационная безопасности 2022. Сайт CNews. [Электронный ресурс]. URL:

https://www.cnews.ru/reviews/security2022/articles/sem_trendov_informatsionnoj_bezopasnosti.

3. ИБ-центр ФСБ фиксирует более 170 кибератак на Россию каждый день. Сайт Tadviser. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Число_кибератак_в_России_и_в_мире.

4. Число ИТ-преступлений в России с 2014 года выросло в 50 раз до 510 тыс. Сайт Tadviser. [Электронный ресурс]. URL: https://www.tadviser.ru/index.php/Статья:Число_киберпреступлений_в_России.

5. Что такое ЦИПсО? Сайт Простыми словами. [Электронный ресурс]. URL: https://proslo.ru/chto-takoe-cipso/.

Сведения об авторах

Прокопенко Алексей Николаевич, кандидат технических наук, доцент, профессор кафедры информационных технологий (в составе учебно-научного комплекса автоматизированных систем и информационных технологий) Академии Государственной противопожарной службы МЧС России; e-mail: Alex_prokop@rambler.ru.

Жукова Полина Николаевна, доктор физико-математических наук, доцент, полковник внутренней службы, заместитель начальника кафедры высшей математики и системного моделирования сложных процессов Санкт-Петербургского университета Государственной противопожарной службы МЧС России им. Героя Российской Федерации генерала армии Е.Н. Зиничева; e-mail: pnzhukova@mail.ru.

Страхов Андрей Александрович, доцент кафедры информатики и математики Московского университета МВД России имени В.Я. Кикотя; e-mail: cokr@mail.ru.

Разбегаев Павел Витальевич

ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В ОБРАЗОВАНИИ: ВЫЗОВЫ И ВОЗМОЖНОСТИ

Согласно Национальной стратегии развития ИИ на период до 2030 г., утвержденной Указом Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации», искусственный интеллект – это комплекс технологических решений, позволяющий имитировать когнитивные функции человека [2] (включая самообучение и поиск решений без заранее заданного алгоритма) и получать при выполнении конкретных задач результаты, сопоставимые, как минимум, с результатами интеллектуальной деятельности человека [6].

Президент Российской Федерации В.В. Путин в одном из своих выступлений, посвященных вопросам применения технологий искусственного интеллекта, подчеркнул высокую степень их актуальности и обратил внимание на следующие основные моменты: обозначена прямо пропорциональная зависимость результатов в области искусственного интеллекта с состоянием обеспечения суверенитета, безопасности и состоятельности РФ.

Одной из главных задач развития государства в текущем десятилетии является обеспечение массового внедрения искусственного интеллекта во все отрасли экономики, социальной сферы и в систему государственного управления; необходимо принимать качественные решения, основанные на анализе большого количества данных; важно создать базовые условия внедрения искусственного интеллекта; обеспечить высокую степень готовности и зрелости, четкую постановку задач и сроков их выполнения; деятельность по внедрению искусственного интеллекта, которая должна быть нацелена на конкретный достижимый результат, обеспечена всеми необходимыми ресурсами, современными глобально конкурентоспособными законодательными основами отраслевого регулирования по вопросам применения искусственного

интеллекта, конкретными нормативными требованиями, технологическими стандартами, регламентами, другими отраслевыми нормами [1].

В настоящее время технологии искусственного интеллекта в образовании выполняют следующие функции:

− интеллектуализация обучающих систем;

− погружение в учебный материал с помощью технологий виртуальной реальности;

− составление индивидуальной образовательной траектории обучающихся и их сопровождение;

− организация групповой работы;

− прогнозирование достижений обучающихся;

− адаптация в процессе обучения;

− проведение экзаменов;

− проверка выполненных заданий;

− организация обратной связи [4].

Элементы инновационной активности внедрены в информационно-методическое и информационно-технологическое оснащение образовательного процесса вузов системы МВД.

Рассмотрим применение искусственного интеллекта на примере вузов системы МВД России [3].

Сотрудники Московского университета МВД России имени В. Я. Кикотя [5] активно применяют при проведении занятий технологии виртуальной реальности. Виртуальная реальность - созданный техническими и программными средствами виртуальный мир, который может ощущаться органами человеческого восприятия, с использованием таких чувств, как осязание, зрение и слух.

Использование технологий виртуальной и дополненной реальности в учебном процессе представляют интерес для моделирования реальных мест происшествия в целях обучения сотрудников полиции; изучение обстановки

места происшествия с любой стороны и высоты, мгновенное перемещение на большие расстояния. При этом необходимо учитывать характеристики устройств виртуальной реальности, а именно:

- качество изображения;
- продолжительность времени комфортного использования;
- возможность взаимодействия с объектами в виртуальном мире.

В университете также используется технология дополненной реальности. При этом изображение находится на экране мобильного устройства, в котором объекты реального мира совмещены с виртуальными элементами.

Рассмотренная технология используется в процессе преподавания дисциплины «Естественно – научные методы судебно-экспертных исследований».

Данный формат был опробован при проведении занятий среди курсантов Института судебной экспертизы и слушателей факультета подготовки иностранных специалистов и показал свою эффективность при обучении в дистанционной форме. Это значимо в условиях, когда ряд слушателей находились за пределами России и имели возможность участвовать в процессе обучения только в дистанционном режиме. Подобный формат подачи лекционного материала также важен для самостоятельного изучения, если курсант или слушатель отсутствовал на занятии по какой-либо причине.

Сотрудники Уральского института МВД России используют в своей деятельности интеграцию игрового пространства и виртуальной реальности в образовательном процессе. Их целью является реализации компетентностного подхода.

Возможности оборудования виртуальной реальности позволяют подключать к одному ситуационному центру несколько комплектов оборудования. Это помогает отработать действия в составе боевых двоек, а также сымитировать встречный огневой контакт, что способствует не использовать компьютерный алгоритм, заставляя обучающегося применить все

ранее изученные навыки для выполнения поставленных задач. Такой формат наиболее близок к ситуациям, с которыми может столкнуться сотрудник полиции в своей профессиональной деятельности.

Программное обеспечение оборудования виртуальной реальности позволяет преподавателю самостоятельно выбирать ситуационный центр в зависимости от уровня владения оборудованием обучающегося, а также в зависимости от пройденного материала по учебной дисциплине. Основными ситуационными центрами являются: стрелковый тир, учебно-тренировочная база, вооруженный захват.

Проработка ситуационного центра с использованием оборудования виртуальной реальности является более трудоемким для преподавателя процессом и занимает большее количество времени по сравнению с традиционным подходом к изучению дисциплины «Личная безопасность сотрудников ОВД». В тоже время использование инновационных технологий позволяет сделать процесс обучения безопасным за счет работы с виртуальным оружием в составе двоек.

Следует отметить, что уровень компетентности профессорско-преподавательского состава повышается в связи с необходимостью приобретения новых знаний, в частности, в сфере информационных технологий, что говорит о прогрессивности использования такого подхода.

В 2021-2022 учебном году с использованием оборудования виртуальной реальности были проведены занятия практического типа по дисциплине «Личная безопасность сотрудника ОВД». В качестве достоинств применения инновационных технологий следует отметить практическую направленность представленного материала. Отмечается высокая степень удовлетворенности сопровождением учебных занятий наглядными средствами. К положительным сторонам применения оборудования виртуальной реальности следует отнести повышение интереса обучающегося к предмету, получение обучающимися дополнительных знаний по дисциплине, повышение качества обученности.

Использование современных средств обучения, таких как оборудование виртуальной реальности, позволяет максимально эффективно применять практико-ориентированную модель обучения в рамках занятий по дисциплине «Личная безопасность сотрудника ОВД». Использование ситуационных центров, заложенных в программу, позволяет максимально приблизить процесс обучения к реальным ситуациям применения огнестрельного оружия сотрудниками полиции, что при проведении обычных занятий со стрельбой сделать просто невозможно.

Оборудование виртуальной реальности обладает высоким ресурсным педагогическим потенциалом, является перспективной технологией применения компетентностного подхода в ведомственном профессиональном образовании, позволяет реализовывать практико-ориентированную модель обучения.

Таким образом, использование возможностей искусственного интеллекта в образовании, в частности погружение обучающихся в учебный материал с помощью технологий виртуальной (дополненной) реальности, позволит персонализировать и адаптировать обучение, что подразумевает подбор учебного содержания, темпа обучения и учебный подход под потребности отдельного обучающегося с учетом когнитивных и личностных особенностей, с возможностью отслеживания прогресса в обучении и изменения его траектории в зависимости от достигнутых результатов.

Литература

1. Выступление 24 ноября 2022 года Президента РФ В.В. Путина на основной дискуссии международной конференции по искусственному интеллекту и машинному обучению Artificial Intelligence Journey 2022 на тему «Технологии искусственного интеллекта для обеспечения экономического роста» [Электронный ресурс]: URL: http://www.kremlin.ru/events/president/transcripts/speeches/69927 (дата обращения 17.05.2023).

2. Мацефук Е.А., Разбегаев П.В. Аксиосфера как элемент информационной среды // «Мир науки, культуры, образования», 2017, № 6 (67). С. 57-58.

3. Разбегаев П.В. Инновационные технологии в образовательной системе МВД РФ // «Мир науки, культуры, образования», 2022, № 4 (95). С. 76-78.

4. Родионов О.В., Тамп Н.В. Технологии искусственного интеллекта в образовании // «Воздушно-космические силы. Теория и практика», 2022, № 22. С. 64-73.

5. Трущенков И. В. Использование программно-аппаратных комплексов виртуальной реальности для моделирования места происшествия в целях обучения дисциплинам криминалистического профиля. Технико-криминалистическое обеспечение раскрытия и расследования преступлений. Москва: Интерполитех, 2020. С. 199-201.

6. Указ Президента Российской Федерации от 10 октября 2019 г. № 490 «О развитии искусственного интеллекта в Российской Федерации» (вместе с «Национальной стратегией развития искусственного интеллекта на период до 2030 года») // Собрание законодательства Российской Федерации. 2019. № 41. ст. 5700.

Сведения об авторе

Разбегаев Павел Витальевич, кандидат педагогических наук, доцент, начальник кафедры информатики и математики Волгоградской академии МВД России; e-mail: pavel173@mail.ru.

Смирнова Майя Ивановна

ОБ ИСПОЛЬЗОВАНИИ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ПРИ ИЗУЧЕНИИ ИНОСТРАННОГО ЯЗЫКА КУРСАНТАМИ ВЫСШИХ ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЙ МВД РОССИИ

В современном постиндустриальном обществе информация становится ключевым объектом, средством, условием, содержанием, результатом любой деятельности. От информации, как от главного ресурса развития общества, во многом зависит функционирование и развитие многих различных научных, технических, социальных сфер жизни человека.

Информационное общество предъявляет новые требования к его членам с учетом особых ценностей. Основными ценностями информационного общества становятся не просто знания, а способность приобретать знания на основе самостоятельного мышления и умения обрабатывать и применять информацию для принятия аргументированных решений по конкретным проблемам, опираясь на соответствующий опыт.

Поскольку продуцирование, передача, интерпретация, накопление информационных ресурсов невозможно без применения соответствующих электронных средств отбора, хранения, обмена информацией, то использование информационно-коммуникационных технологий является обязательным условием, инструментом, фактором развития информационного общества. Информационно-коммуникационные технологии способны оптимизировать, сделать более результативными многие производственные и управленческие процессы, а также внести существенный вклад в развитие социально-культурной сферы. Использование возможностей информационно-коммуникационных технологий создает особые условия для развития информационного образовательного пространства, для формирования профессиональной компетентности специалистов разных областей.

Информатизация образования, заключающаяся в массовом внедрении в педагогическую практику методов и средств сбора, обработки, передачи и

хранения информации на базе микропроцессорной техники и средств передачи информации, а также педагогических технологий, основанных на этих средствах, с целью создания условий для перестройки познавательной деятельности и усиления интеллектуальных возможностей обучаемых [1].

Информатизация образования заставляет пересмотреть не только педагогические методы, приемы и формы, но и сместить акценты в контексте субъекта и объекта образовательного процесса, конечной цели учебного процесса. Достаточный уровень информационной культуры является одной из основных целей образовательного процесса в современном высшем учебном заведении. Формирование информационной культуры, включающее как развитие стиля мышления, способствующего умению ориентироваться в потоке разнообразной информации, так и создание условий для овладения навыками использования новых информационных и телекоммуникационных технологий, является важным компонентом профессиональной компетентности конкурентно способного специалиста в любой области.

Данный информационный подход делает акцент на рассмотрении педагогических технологий, основанных на внедрении и активном использовании современных информационных технологий в учебном процессе по иностранному языку при подготовке специалистов для правоохранительных органов в ведомственных высших учебных заведениях, в качестве ведущего средства развития информационной культуры.

Широкий арсенал средств информационно-коммуникационных технологий дает возможность совершенствовать аудиторную и внеаудиторную работу при изучении иностранного языка, способен оптимизировать данный процесс, сделать познавательную деятельность более мотивированной и результативной. Перечень все чаще используемых таких средств включает следующие: 1) электронные учебники и пособия, демонстрируемые с помощью компьютера и мультимедийного проектора; 2) электронные энциклопедии и справочники; 3) тренажеры и программы тестирования; 4) образовательные ресурсы Интернета; 5) DVD- и CD-диски с картинами и иллюстрациями; 6)

видео- и аудиотехника [2]; 7) мультимедийные презентации; 8) компьютерные обучающие и тестовые программы; 9) электронные библиотеки; 10) словари, текстовые и видео глоссы, используемые в обучении студентов профессионально ориентированной лексике и профессионально ориентированному чтению; 11) телекоммуникационные технологии, предоставляющие возможность посредством аудио- и видеоконференций участвовать в диалоге культур [3].

Использование каждого средства расширяет возможности интенсификации процесса формирования иноязычной коммуникативной компетенции, что определено как основная цель обучения иностранному языку в вузе данного профиля и детерминируется особенностями применения, исходя из принципов обучения иностранному языку, специфики конкретных этапов обучения, в соответствии с поставленными образовательными, методическими и развивающими целями учебного процесса.

Рассмотрим функции средств информационно-компьютерных технологий для обучения иностранному языку в соответствии с выделяемыми модулями: информационно-обучающим, тренировочным, справочным, контролирующим [4].

Информационно-обучающий модуль включает информационные программные средства с целью представления иноязычной информации и обучающие программные средства для обеспечения тренировки и контроля процесса обучения. Здесь особое место занимают средства визуализации информации и знаний, среди которых мультимедийным презентациям отводится особое место. Структурированная, кратко изложенная информация воспринимается системно, четко, как некий ментальный конструктор. В ходе интроекции происходит присвоение личностью данного конструктора [5, с. 82]. Анимационные эффекты позволяют дополнительно активизировать ощущения, воображение, мнемические процессы. Создание презентаций обучающимися способствует развитию навыков и умений интерпретации информации на иностранном языке, ее систематизации, синтеза и анализа. Составление обучающимися ментальных карт на заданную профессионально

ориентированную тематику, для выполнения определенной коммуникативной задачи и использование возможностей инфографики позволит совершенствовать навыки монологической и диалогической речи, удерживать в памяти и передавать большой объем информации, развивать память и мышление.

Тренировочный модуль охватывает звуковые и текстовые задания и дидактические материалы, тренировочные и обучающие программы, в которых программированию подлежит процесс тренировки употребления изученных языковых явлений. Программные средства позволяют создать условия для автономного, самостоятельного выполнения заданий обучающимся в индивидуальном темпе, оценить и скорректировать собственные достижения в овладении языковым материалом. Обучающиеся используют компьютер для решения алгоритмических задач с целью отработки и автоматизации употребления грамматического материала, актуализации лексических единиц, развития речевых навыков.

Фонетические и грамматические справочники, глоссарии, толковые словари, общие и специальные англо-русские и русско-английские словари серии ABBYY Lingvo представляют справочный модуль. Онлайн переводчики, в частности, Reverso, могут быть включены в данный модуль.

Контролирующий модуль содержит тесты для контроля уровня сформированности соответствующих лексической и грамматической компетенции, коммуникативных навыков во всех видах речевой деятельности, комплексных профессионально ориентированных тестов для определения уровня формируемых компетенций.

В процессе изучения иностранного языка будущими сотрудниками правоохранительных органов могут быть использованы программные продукты, не созданные специально для обучения иностранному языку, но применение которых будет способствовать как формированию иноязычной компетенции, так и развитию узко специализированных профессиональных навыков и умений обучающихся. Существует положительный опыт внедрения программы «ПАПИЛОН-KLIM-3D-PRO», предназначенной для работы с базой данных

субъективных портретов и содержит инструменты, позволяющие инициировать создание новых и редактирование созданных ранее субъективных портретов. Составляя портреты, обучающиеся решают коммуникативные задачи, формируя соответствующие лингвистические и профессионально ориентированные компетенции, связанные с выполнением оперативно-розыскных операций, овладения криминалистической техникой и программным продуктом.

Таким образом, использование информационно-коммуникационных технологий позволяет сделать процесс изучения иностранного языка в вузах системы МВД России более гибким, эффективным, удовлетворяющим основным целям формирования профессионально компетентного специалиста.

Литература

1. Коджаспирова Г.М., Коджаспиров А.Ю. Педагогический словарь. М.: Академия, 2003. 176 с.

2. Сайков Б.П. Организация информационного пространства образовательного учреждения: практическое руководство / Б.П. Сайков. – Москва: БИНОМ. Лаборатория знаний, 2005. 406 с.

3. Даирова К.Н. Соколова И.Н. Использование гипертекстовых технологий в обучении иностранного языка // Материалы VI Международной студенческой научной конференции «Студенческий научный форум» URL: https://scienceforum.ru/2014/article/2014001698 (дата обращения: 20.06.2023).

4. Алексеева Т.Е. Педагогические аспекты использования средств информационных и коммуникационных технологий в военно-техническом вузе (на примере английского языка): автореф дисс. к. пед. н. Рязань, 2006. 22с.

5. Сверчкова Ю.А. Визуализация учебной информации как средство преобразования блоковых моделей. Педагогика и психология, теория и методика обучения. Межвузовский сборник статей. ННГАСУ 2012. 650с.

Сведения об авторе

Смирнова Майя Ивановна, кандидат педагогических наук, доцент кафедры гуманитарных и социально-экономических наук Крымского филиала Краснодарского университета МВД России; e-mail: maya_smirnova@mail.ru.

Старостенко Игорь Николаевич

К ВОПРОСУ УПРАВЛЕНИЯ БЕЗОПАСНОСТЬЮ КОМПЬЮТЕРНОЙ СЕТИ

В современной сложной сетевой архитектуре и в условиях постоянно меняющейся среды угроз ИТ-специалистам трудно поддерживать безопасность на эффективном уровне. Административные задачи по обеспечению безопасности включают в себя поддержку постоянно расширяющейся таблицы пользователей, устройств, местоположений и способов применения; соблюдение требований; предоставление новых сервисов, средств контроля доступа и механизмов безопасности; оптимизацию производительности; устранение неполадок по запросу. Любые ошибки в конфигурации могут сделать сеть уязвимой к сложным угрозам и привести к нарушению нормативных требований.

Для решения этих проблем сетевым администраторам необходимо развертывать политики безопасности в сети. Однако сетевая инфраструктура может содержать тысячи политик для межсетевого экрана, которые накопились с годами. Такие правила часто организованы хаотично, дублируют друг друга, утратили актуальность или противоречат новым правилам, что непроизвольно влияет на производительность и безопасность сети.

Для снижения риска сетевых атак требуется комплексный всеобъемлющий подход, включающий создание и обслуживание политик безопасности на базе потребностей в обеспечении безопасности.

Первый шаг для определения потребностей в обеспечении безопасности включает определение вероятных угроз и проведение анализа рисков. Анализ рисков представляет собой широкомасштабное исследование рисков и неопределенных факторов. В рамках исследования оценивается вероятность и степень опасности угроз сетевой инфраструктуре, формируется список приоритетов организации. Аналитики безопасности идентифицируют риски, определяют способ и время их возникновения, оценивают последствия от потенциально возможного их воздействия. Результаты анализа рисков используются для определения необходимого для обеспечения безопасности

аппаратного и программного обеспечения, разработки политик нейтрализации рисков и дизайна сети.

Тестирование безопасности сети – неотъемлемая часть обеспечения безопасности системы. Тестирование безопасности выполняется операционной группой, чтобы обеспечить надежное функционирование всех механизмов безопасности. Операционная безопасность начинается с процесса планирования и развертывания сети. На этих этапах анализируются проекты, выявляются риски и уязвимости.

Вне зависимости от типа тестирования, сотрудники, проводящие тестирование безопасности, должны обладать устойчивыми знаниями, навыками и умениями в следующих областях знаний:

- защита оконечных устройств;
- межсетевые экраны;
- IPS/IDS;
- операционные системы;
- основы программирования;
- сетевые протоколы TCP/IP;
- уязвимости сети и снижение рисков.

Тестирование безопасности сети дает возможность проверить эффективность решения операционной безопасности и выполняется, чтобы проверить надлежащую работу всех механизмов безопасности, позволяет получать критически важную информацию, включая анализ рисков и аварийное планирование.

На начальном этапе тестирование безопасности проводится для отдельных сегментов сети, после ввода в эксплуатацию тестируется и оценивается безопасность комплексных защитных мер всей сети в целом. Выявляются проблемы с дизайном, внедрением и эксплуатацией, которые могут привести к нарушению политики безопасности, определяется степень пригодности механизмов обеспечения безопасности, надежности и свойств устройств для принудительного применения политики безопасности.

Тестирование необходимо повторять через определенные промежутки времени и каждый раз при внесении изменений в систему.

К тестам безопасности, выявляющих уязвимости, угрозы и риски относятся:

- тесты на проникновение в сеть: моделируют атаки вредоносных источников. Цель этих тестов – определить вероятность атаки и возможные последствия ее проведения;
- сканирование сети: включает программное обеспечение (ПО), которое может направлять эхо-запросы на компьютеры, сканировать порты TCP на прослушивание и отображать доступные ресурсы сети. Определенное ПО для сканирования также может обнаруживать имена пользователей, группы и общие ресурсы;
- сканирование уязвимостей: включает ПО, способное выявлять потенциальные недостатки тестируемых систем. В число этих недостатков могут входить ошибки конфигурации, использование пустых паролей или паролей по умолчанию, а также потенциальные цели DoS-атак. Некоторое программное обеспечение позволяет администраторам выводить систему из строя посредством выявляемых уязвимостей.
- взлом пароля: включает ПО, используемое для тестирования и обнаружения ненадежных паролей, которые следует изменить. Политики паролей должны включать рекомендации по предотвращению использования ненадежных паролей.
- проверка журналов безопасности: для выявления потенциальных угроз безопасности. Аномальную активность следует расследовать с помощью ПО для фильтрации для сканирования длинных файлов журнала;
- средства проверки целостности: обнаруживают изменения в системе и отправляет отчеты по ним. В основном мониторинг проводится для файловой системы. Однако, некоторые системы проверки могут отправлять отчеты по входу в систему и выходу из нее;

- ПО для обнаружения вирусов: использовать, чтобы идентифицировать и удалить вредоносный контент.

Результаты тестирования сетевой безопасности рекомендуется использовать для определения алгоритма действий по снижению опасности выявленных уязвимостей; в качестве эталона для отслеживания достижений организации в соблюдении требований безопасности; для оценки статуса выполнения требований к системной безопасности; для решения иных задач, связанных с оценкой рисков, сертификации и авторизации и программах оптимизации производительности.

Для тестирования сети можно использовать различные программные средства и инструменты:

- Nmap/Zenmap – обнаруживает компьютеры и службы в компьютерной сети, создавая схематическую карту сети;
- SuperScan – программное средство для сканирования портов, разработанное для обнаружения открытых портов TCP и UDP, позволяет определять, какие службы работают на этих портах, а также запускать запросы;
- SIEM – технология, используемая для предоставления отчетов в реальном времени и долгосрочного анализа событий безопасности;
- GFI LANguard – сканер сети и безопасности, способный обнаруживать уязвимости.
- Tripwire – оценивает и проверяет ИТ-конфигурации с помощью внутренних политик, стандартов соответствия и наилучших методов обеспечения безопасности;
- Nessus – ПО сканирования уязвимостей, позволяющее выявлять проблемы удаленного доступа, неправильные конфигурации и возможный ущерб от DoS-атак на стек TCP/IP;
- Metasploit – важное программное средство для обнаружения скрытых уязвимостей с помощью различных инструментов и утилит. Позволяет поставить себя на место хакера и использовать те же методы для разведки и проникновения в сети и серверы.

Важной составляющей в управлении безопасностью компьютерной сети является политика безопасности. Представляет собой совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которые регулируют процессы обработки, хранения, передачи и защиты критически важной информации. Политика безопасности зависит от конкретной технологии обработки информации, используемых технических и программных средств, расположения организации.

Комплексная политика безопасности устанавливает правила поведения сотрудников, обеспечивает единообразие процессов использования и технического обслуживания программного и аппаратного обеспечения, определяет правовые последствия нарушений.

Политика безопасности должна включать следующие компоненты:

- правила идентификации и аутентификации – используются для указания лиц, имеющих право доступа к ресурсам сети, а также для описания процедур верификации;
- политики паролей – обеспечивают регулярное изменение паролей и их соответствие минимальным требованиям;
- правила допустимого использования – определяют сетевые ресурсы и их использование приемлемым для организации образом;
- политики удаленного доступа – определяют, как удаленные пользователи могут подключаться к сети и какие возможности доступны через удаленный доступ;
- политики технического обслуживания сети – Определяют процедуры обновления операционных систем сетевых устройств и приложений конечных пользователей;
- политики обработки инцидентов – описывают обработку инцидентов безопасности.

Таким образом, для снижения риска сетевых атак требуется комплексный всеобъемлющий подход, включающий создание и обслуживание политик безопасности на базе потребностей организации в обеспечении безопасности.

Первый шаг для определения потребностей организации в обеспечении безопасности включает определение вероятных угроз и проведение анализа рисков. Критически важным для обеспечения сетевой безопасности является тестирование безопасности сети. В число тестов должно входить сканирование сети, сканирование уязвимостей, взлом паролей, просмотр журнала, проверка целостности, обнаружение вирусов, тестирование на проникновение и др. Политика безопасности является неотъемлемой частью системы безопасности организации. Она определяет процедуры реагирования на нарушения безопасности.

Управление безопасностью компьютерной сети предоставляет полную визуализацию сети и формирует данные для ресурсов (группирование и классификация ресурсов), межсетевых экранов, приложений, портов, протоколов, сетей VPN, механизмов преобразования сетевых адресов (NAT), политик безопасности и устройств поставщиков.

Литература

1. Старостенко, И.Н. Информационная безопасность: курс лекций / И.Н. Старостенко, Ю.Н. Сопильняк. – Краснодар: Краснодарский университет МВД России, 2012.

2. Старостенко, И.Н. Целенаправленные атаки (APT) и методы защиты от них // Проблемы информационного обеспечения деятельности правоохранительных органов. Материалы 3-й Международной научно-практической конференции, 2017. С.127-131.

3. Старостенко, И.Н. К вопросу обеспечения безопасности локальной сети на канальном уровне // Математические методы и информационно-технические средства. Материалы XV Всероссийской научно-практической конференции, 2019. С.171-174.

Сведения об авторе

Старостенко Игорь Николаевич, кандидат физико-математических наук, доцент, начальник кафедры информатики и математики Краснодарского университета МВД Росси; e-mail: staros80@mail.ru.

Тимофеев Виктор Владимирович,
Глеков Евгений Александрович

СПОСОБЫ ЗАЩИТЫ ОТ МОШЕННИЧЕСТВА НА P2P-ПЛАТФОРМАХ

Современный период развития Мировой экономики вносит в неё массу финансовых инноваций. Это связано как с усиливающейся ролью финансового рынка для экономики в целом, так и с усложнением его инструментов. Так, новеллой являются криптовалюта и иные фиатные денежные средства, обращение которых проходит в рамках P2P-кредитования. Такие относительно новые и менее регулируемые процессы содержат массу уязвимостей. Одновременно своё развитие получают новые виды мошенничества. В России объем мошенничества с криптовалютой в целом достаточно велик. Так, за первое полугодие 2021 года он составил 2,2 миллиарда рублей [1]. 2022 год отличает увеличение данного показателя. По данным зарубежных экспертов, каждая десятая афера с криптовалютами в мире происходит в России, на втором месте по этому показателю находится Перу (6,8%), на третьем – США (5,3%). В целом, как отмечается в одном из документов Банка международных расчетов, криптовалюты изобилуют мошенничеством и воровством [2].

P2P- кредитование (от англ. peer-to-peer, person-to-person – от человека к человеку, от равного к равному) – это механизм заимствования денежных средств между участниками финансовых взаимоотношений (частный инвестор и заёмщик) с помощью специальных, работающих в онлайн-режиме в сети «Интернет», площадок, иначе называемых P2P-платформами. Сама P2P-платформа – это посредник, устанавливающий правила таких взаимоотношений, осуществляющий документооборот и следящий за своевременностью протекания процессов.

Сущность процессов заключается в следующем: обращение денежных средств происходит без участия таких финансовых институтов, как банки или микрофинансовые организации. Объём денежных средств, находящихся в

обороте на P2P-платформах, по данным разных источников составляет порядка 80 миллиардов рублей в год.

Такой массив денежных средств стал привлекателен для криминальных элементов. Следствием чего необходимостью становится выработка способов защиты от мошенничества при работе на P2P-платформах.

Недобросовестная или фишинговая платформа. Это заведомо созданные для мошеннических действий платформы, посредством которых конфиденциальные данные (пароли, логины, номера кредитных карт и т.п.) теряют таковой статус. Способ защиты: проверка эскроу-счетов (условное депонирование обязательно для каждой p2p-платформы), проверка протокола безопасности Secure Sockets Layer, удостоверяющего подлинность веб-сайта и позволяющего использовать зашифрованные соединения.

Внебиржевая сделка. Платформа перенаправляет для завершения сделки в социальную сеть или мессенджер для обхода комиссий. Частный инвестор убеждает заёмщика в том, что он первый переведет денежные средства, отправляя ссылку на онлайн лже-обменник. Заёмщик теряет свои денежные средства при невозможности обратиться в службу поддержки, так как транзакции были произведены вне P2P-платформы. Способ защиты: не переходить по подозрительным ссылкам, осуществляя транзакции только через P2P-платформу.

Фишинговая служба поддержки. Пользователю платформы приходит уведомление от «службы поддержки», «Support», «Admin», с сообщением о том, что аккаунт заподозрен в мошеннических действиях, о необходимости пройти верификацию по указанной ссылке. Переходя по ссылке, пользователь лишается аккаунта или денежных средств на нём. Здесь нужно понимать, что служба поддержки не пишет первая, а работает по обращениям пользователей. Следует обращать внимание на указанный адрес ссылки.

Кроме того, основополагающим способом защиты является использование платформ, которые требуют от пользователя прохождение KYC (от англ. Know

Your Customer или Know Your Client – знай своего клиента) – идентификации личности пользователя перед тем, как предоставить ему возможность осуществлять какие-либо операции, и использующих AML (от англ. Anti-Money Laundering – противодействие отмыванию денег), ввиду того, что не редкостью становится произведение расчетов за счёт денежных средств, добытых преступным путём.

Схема «Треугольник». Мошенник опубликовывает объявление на P2P-платформе о возможности осуществления транзакции денежных средств. Путём обмана убеждает откликнувшегося на объявление заёмщика о необходимости внесения предоплаты. Затем частный лже-инвестор связывается с заёмщиком посредством P2P-платформы и получает его реквизиты для проведения расчёта. Эти реквизиты перенаправляются первоначальному покупателю (указанному в объявлении), он переводит денежные средства заёмщику в обмен на его денежные средства по выгодному курсу. Так мошенник обналичил денежные средства, добытые им преступным путём, которые поступили на банковскую карту обманутого пользователя. [3] Способ защиты: не совершать обмен денежных средств вне P2P-платформы, если же такое происходит, то стоит потребовать контрагента сфотографировать свою банковскую карту на фоне открытой на экране компьютера или телефона страницы финансовой операции, со своим лицом.

Конкурентный Coin Lock. Пользователь соглашается на поступившую ему заявку на P2P-плаформе о проведении финансовых операций с его денежными средствами, одновременно с этим «замораживается» сумма денежных средств, подлежащая обмену или продаже. Мошенник бездействует. Пользователь лишается возможности каких-либо действий в отношении той суммы своих денежных средств, которые были указаны в запросе, до момента отмены сделки. Так, потенциальный конкурент перестаёт быть таковым. Способом защиты является просмотр информации о пользователе (в частности, рейтинг), заранее

включить механизм RBF (от англ. replace-by-fee – плата за замену), позволяющий преодолевать подобные ситуации.

Каналы со связками в мессенджерах. В мессенджерах (зачастую мошенниками используется Telegram, ввиду ряда особенностей его работы) создаются чаты или чат-боты, где публикуются объявления о производимых по выгодному курсу финансовых операциях, с указанием адресов Интернет-сайтов для перехода и цен. Пользователь, переходя по ссылке, совершает обозначенную финансовую операцию, однако по цене, значительно отличающейся от первоначальной и являющейся выгодной лишь для мошенника, которому поступили денежные средства. Обезопасить себя возможно лишь совершением подобных финансовых операций посредством P2P-платформ, обладающих ранее обозначенными KYC, AML, положительными отзывами.

Кроме того, активно используется такой способ мошенничества как социальная инженерия, которая в контексте информационной безопасности означает психологическое манипулирование людьми с целью совершения ими определенных заданных действий.

Используются и классические схемы мошенничества при предоставлении финансовых услуг, такие как поддельные чеки, выписки по операциям и фишинговые СМС подтверждения операций, отправление запросов на списание денег с банковской карты.

К разряду классических стоит отнести и неточные суммы переводов. Мошенник переводит сумму равную «1931,1» вместо обещанных «19311,1» или в иной валюте или иных фиатных денежных средствах. Обманутый пользователь, несущий значительные убытки, не использовал главное средство защиты – внимательность пользователя.

Безусловно, на общегосударственном уровне ведётся борьба с подобными проявлениями мошенничества, правоохранительные органы активно работают в данном направлении. Однако всё это будет бесполезным, если пользователи P2P-платформ не будут предпринимать обозначенные способы защиты при работе на

P2P-платформах. Практическая значимость нашего исследования не вызывает сомнений ввиду обозначенной статистики, разнообразности видов мошенничества и низкой финансовой грамотности населения.

Кроме того, работа P2P-платформ с глобальными криптовалютами может подорвать национальный финансовый суверенитет – необходимо на законодательном уровне разработать правила их функционирования, что, в свою очередь, позволит обезопасить пользователей от указанных криминальных элементов и станет ведущим способом защиты [4].

Литература

1. «Известия»: объем мошенничества с токенами в РФ составил 2,2 млрд. рублей за I полугодие URL: https://tass.ru/ekonomika/12258913 (Дата обращения: 02.05.2023).

2. ESET: Russia has Become the Leader in the Number of Crypto Threats. URL: https://www. oreanda.ru/en/svyaz/eset-russia-has-become-the-leader-in-the-number-of-crypto-threats/ article1391258/ (Дата обращения: 02.05.2023).

3. Схемы мошенничества и скама в p2p-арбитраже и торговле – какие существуют и как обезопасить себя URL: https://profinvestment.com/p2p-arbitrage-scam/ (Дата обращения: 02.05.2023).

4. Нурмухаметов Р.К. Криптовалютное мошенничество и меры борьбы с ним / Р.К. Нурмухаметов, Л.Н. Воскресенская, Е.Б. Мясникова // Финансовые рынки и банки. – 2021. – № 12. – ст. 68-71.

Сведения об авторах

Тимофеев Виктор Владимирович, кандидат технических наук, доцент кафедры информатики и специальной техники Барнаульского юридического института МВД России; e-mail: v.v.timofeev@bk.ru.

Глеков Евгений Александрович, курсант 4 курса 1957 учебной группы Барнаульского юридического института МВД России; e-mail: GlekovEA@yandex.ru.

Трошков Александр Михайлович,
Малофей Олег Павлович,
Малофей Александр Олегович

АРХИТЕКТУРА АСИММЕТРИИ – УНИКАЛЬНОСТЬ СИНТЕЗА БИОМЕТРИЧЕСКИХ ХАРАКТЕРИСТИК

Интенсивное развитие и широкое внедрение геоинформационных систем выдвигает на первый план проблему обеспечения информационной безопасности в Вооруженных силах Российской Федерации. При этом представляют интерес технологии, потенциально обеспечивающие защиту циркулирующей информации в сетях организаций. Основная цель защиты информации состоит в том, чтобы предотвратить незаконное овладение ею. Существующие наработки в области защиты информации показывают, что эффективной может быть только комплексная система защиты информации, сочетающая в себе такие направления защиты как: правовая, организационная и инженерно-техническая. Систему защиты информации в общем виде можно обрисовать как совокупность всех средств, методов и мероприятий, выделяемых на военных объектах защиты информационных ресурсов.

Сегодняшнее положение о переходе на цифровизацию и повышение стойкости информационной безопасности позволяет продвинуться к изучению системной биометрии для идентификации пользователя и управления доступом к информационным ресурсам. В научной работе [1] показано, что в науку просачивается много наукообразных сведений при недостаточной степени знания анатомии, что делает методы защиты информации несовершенными. Исходя из этого, предлагается за основу отличия личности взять функциональную антропометрическую асимметрию.

Функциональная антропометрическая асимметричная архитектура, как показано на рисунке 1, классифицируется с точки зрения философии [2]. При этом фундаментальные закономерности асимметрии следует искать в специфике тех знаков и знаковых систем, которые имеют индивидуальность [3].

Рис.

Рис. 1. Классификация функциональной асимметрии

Если рассматривать личность как систему, то различные состояния этой системы осуществляются с той или иной вероятностью [4]. Вероятность *i*-го состояния W_i определяется:

$$W_i = \lim_{T\to\infty} \frac{t_i}{T}, \quad (1)$$

где t_i – время, в течении которого система находится в данном состоянии;

T – время наблюдения за системой.

Из (1) следует, что если величина W принимает состояние W_i, то это означает, что система находится в *i*-том состоянии. Если провести измерение N величины, а N_i есть число измерений, в результате которых найдено W_i, то:

$$W_i = \lim_{N\to\infty} \frac{N_i}{N}. \quad (2)$$

Суммирование W_i позволяет определить состояние системы W:

$$W = \sum_{n=1}^{i} W_i \quad (3)$$

Таким образом, использование (1), (2), (3) дает возможность понимать состояние асимметричности системы, а если эту систему применять в указанной классификации, то биологическая функциональность асимметрии с точки зрения физики вполне подходит для синтезирования биометрических характеристик человека.

Если рассматривать функциональную асимметрию в математической модели, то исследования по асимметрии человека можно наглядно изобразить в виде точек на прямой линии [5], как показано на рисунке 2.

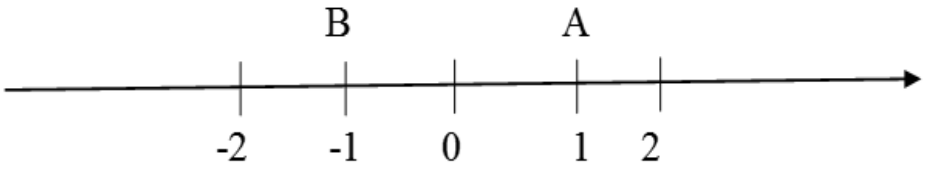


Рис. 2. Числовая ось

На рисунке 2 начальная точка 0 разбивает прямую на две части. На одной из них изображаются положительные числа «+», на другой отрицательные «-». Для того, чтобы разбить части числовой оси, на которых изображаются положительные и отрицательные числа, на оси указываются направления движения от отрицательных чисел к положительным →. С геометрической точки зрения числовая ось есть ось координат, а число на оси есть координата этой точки. Исходя из представленного, можно обосновать значения синтезируемых биометрических характеристик. Для примера, вычисление координатных точек осуществляется с помощью параболы, как показано на рисунке 3.

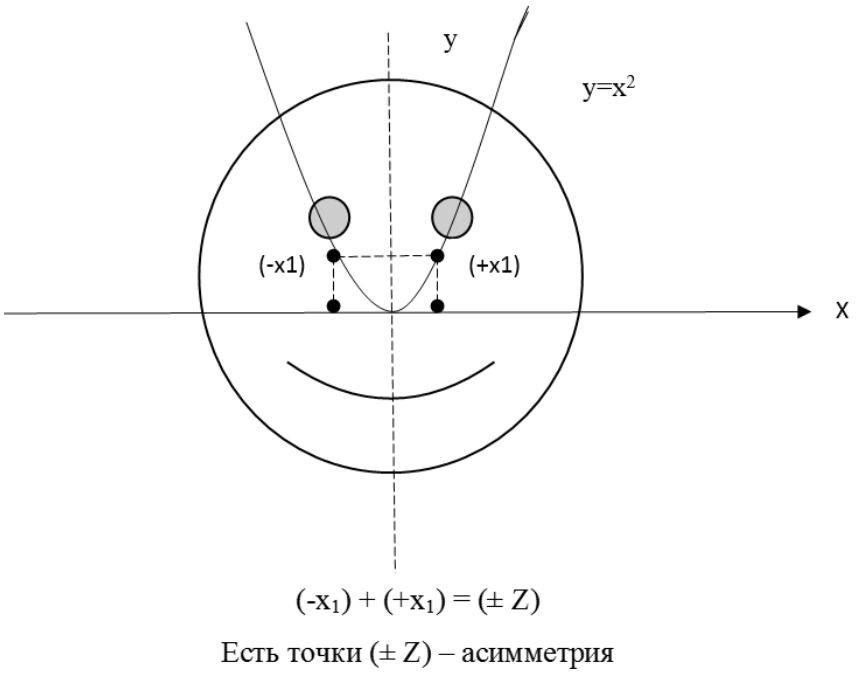


Рис. 3. Параболическое определение точки асимметрии

Без асимметрии биометрическая система ориентирована на замкнутость, что показывает регрессию по закону Больцмана [6]. Механизм проектирования диссипативных структур имеет существенные отличия от проектирования равнозначных (равновесных) биометрических структур, который основан на больцманском принципе упорядоченности. Таким образом, функциональная асимметрия может формировать биометрические характеристики другого направления. Фундаментальные биометрические характеристики человека (БХЧ) и входящие в них биометрические параметры человека (БПЧ), основанные на асимметрии антропологических параметров человека, следует искать в специфике тех биометрических параметров, которые несут самостоятельную интерпретацию. На этом основании предложена структура концепции асимметрических биометрических характеристик, как показано на рисунке 4.

Рис. 4. Структура концепции асимметрических биометрических характеристик

Из рисунка 4 видно, что структура концепции асимметрических биометрических характеристик имеет форму иерархической топографии, где в вершине выделены задача выбора мандата пользователя, которая решается по алгоритму (рисунок 5).

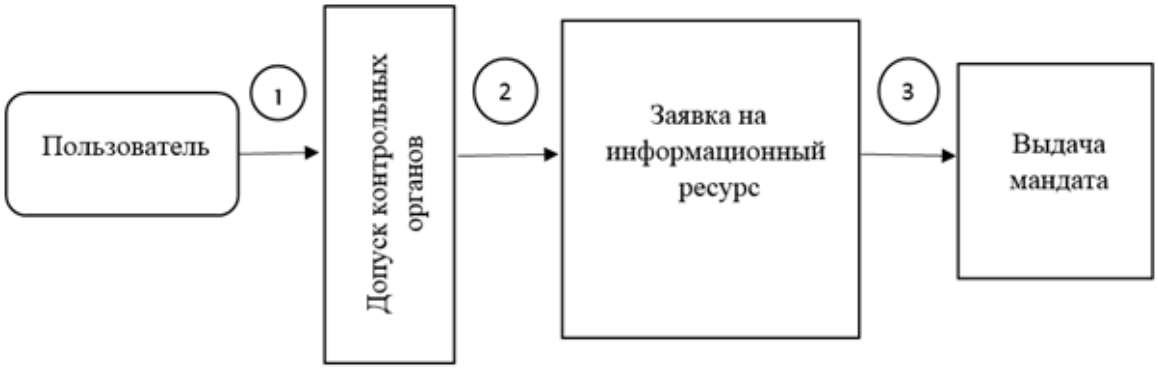


Рис. 5. Алгоритм выбора мандата

На основании выдачи (получения) мандата пользователю, производится декомпозиция сегментов доступа, как показано на рисунке 6, причем каждый сегмент имеет определенную (заданную) грифованность.

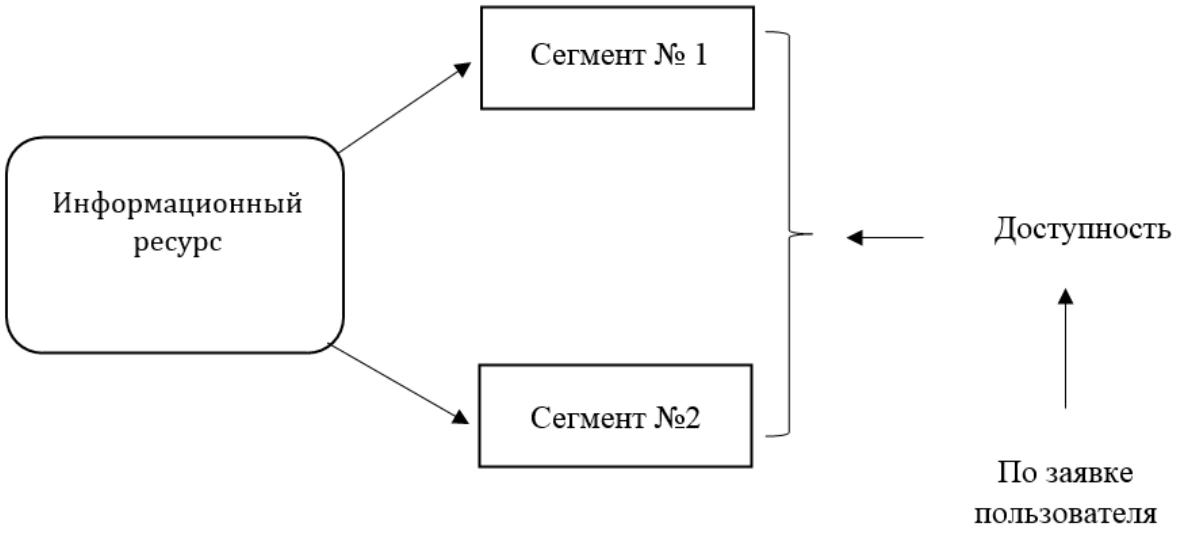


Рис. 6. Декомпозиция сегментов

Представленные сегментации и доступность по заявке пользователя предоставляет возможность синтезировать архитектуру асимметричной биометрической системы (рисунок 7), с учетом асимметрических

биометрических характеристик (АБХ) и асимметрических биометрических параметров (АБП), исходя из выбора функциональной асимметрии пользователя.

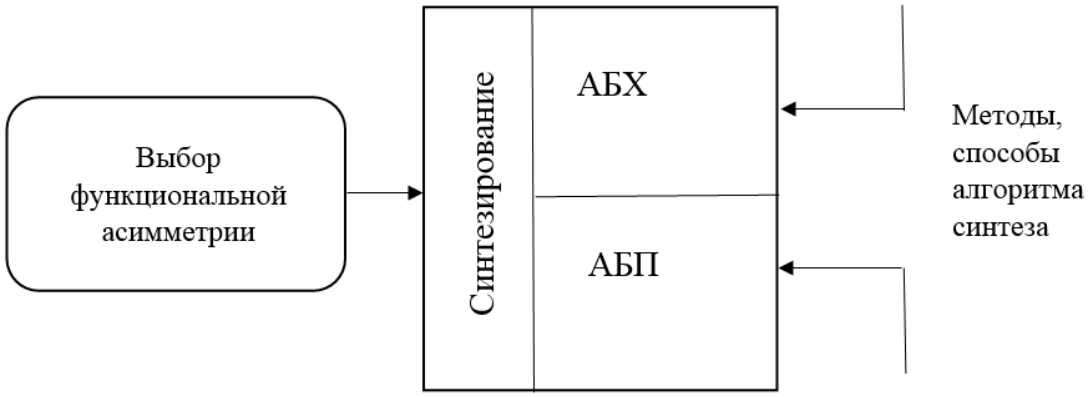


Рис. 7. Синтезирование асимметрической биометрической системы

Архитектура синтезируемых асимметричных биометрических характеристик показала новую идентификацию личности не имеющих повторений и сложность их изменения, что существенно даёт возможность утверждать о повышении качества безошибочной оценки с целью качественного принятия решения о доступе лиц пользователей к информационным ресурсам.

Литература

1. Порщнев Б.Ф. О начале человеческой истории (проблема палеопсихологии). М.: Милев, 1974. 487 с.

2. Оконская Н.К. Энтропия и асимметрия глазами философии // Успехи современной науки. 2016. Т.3. №2. С. 62-65.

3. Панов Е.Н. Знаки, символы, языки. 2-е изд., доп. М.: Знание, 1983. 248 с.

4. Яворский Б.М., Детлаф А.А.: Справочник по физике (для инженеров и студентов ВУЗов). М.: Наука, 1974. 321 с.

5. Фадеев Д.К., Соминский И.С. Алгебра (для самообразования): Учебник Изд. 3-е. М.: Наука, 1966. 297 с.

6. Марков Б.В. Люди и знаки: антропологические межличностные коммуникации. СПб.: Наука, 2011. 667 с.

7. Кфайчев Т.В. Применение весовых функций к методу адаптивных сеток при совместном использовании с методом распределения по IP-адресам. // Материалы МНПК «Информационная безопасность». Ч 2. Изд. СевКавГТУ, 2010 г. С. 73-79.

Сведения об авторах

Трошков Александр Михайлович, кандидат технических наук, доцент кафедры информационных систем Ставропольского государственного аграрного университета; e-mail: troshkov1954@mail.ru.

Малофей Олег Павлович, кандидат технических наук, профессор кафедры математического анализа алгебры и геометрии факультета математики и компьютерных наук Северо-Кавказского федерального университета имени профессора Н.И. Червякова; e-mail: opmalofey@yandex.ru.

Малофей Александр Олегович, кандидат технических наук, доцент кафедры тактико-специальной подготовки Ставропольского филиала Краснодарского университета МВД России; e-mail: tc_op@mail.ru.

Тутова Ольга Васильевна

ТИПИЧНЫЕ ОШИБКИ ПРИ РАЗРАБОТКЕ ЛЕКЦИИ-ВИЗУАЛИЗАЦИИ

В настоящее время в условиях повсеместного распространения информационно-коммуникационных технологий и увеличения объема изучаемого материала все чаще преподаватели высшей школы используют такие формы обучения, которые позволят максимально эффективно изложить большое количество нового материала. Использование наглядности в данном случае позволяет осуществить не только более успешное восприятие и запоминание изучаемого материала, но и способствует активизации умственной деятельности, формированию эвристических умений обучающихся, глубокому проникновению в сущность изучаемых явлений, подтверждает главенствующую роль образного мышления в процессе усвоения трудного материала (Р. Арнхейм, Е.Ю. Артьемьева, В.И. Якиманская и др.).

Мы считаем, что на этапе введения обучающихся в новую дисциплину, а также при изучении нового раздела целесообразно использовать такой вид лекций как лекция-визуализация. Этот вид лекции позволяет изложить новый учебный материал ярко, наглядно и запоминающе, создать проблемную ситуацию, которая даст обучающимся психологическую установку на изучение материала всей дисциплины, позволит развивать в дальнейшем навыки восприятия наглядного материала и в других видах обучения.

Как правило, для сопровождения лекций преподавателями используется средство подготовки презентаций MS Power Point, входящее в программный пакет Microsoft Office. Презентация может содержать на слайдах видео- и аудиофайлы, графические изображения, таблицы, диаграммы.

Как отмечает И.С. Галанова, при подготовке лекции-визуализации преподавателю необходимо так изменить и переконструировать учебную информацию, касающуюся темы лекционного занятия, чтобы теоретический материал был максимально лаконичным, а разработанные или найденные в сети Интернет графики, чертежи, схемы, таблицы способствовали построению наглядного образа [1].

Основной трудностью преподавателя при подготовке лекции-визуализации является выбор и подготовка таких средств наглядности, которые будут дидактически обоснованными для достижения поставленных целей лекции, а также позволят эффективно ее провести, учитывая при ее проведении психофизиологические особенности обучающихся и уровень их подготовленности [4].

Мы поддерживаем мнение И.С. Галановой о том, что эффективное проведение лекции преподавателем сводится не только к связному, подробному комментированию подготовленных наглядных материалов, которое позволит ему полностью раскрыть тему данной лекции [1]. Таким образом, представленная информация обеспечит систематизацию уже имеющихся знаний обучаемых, позволит создать проблемные ситуации и обеспечит возможность их разрешения. Кроме того, использование различных способов наглядности сделает возможным активизировать познавательную деятельность обучаемых.

Целью статьи является рассмотрение основных ошибок, которые возникают у преподавателя при разработке лекции-визуализации. Как известно, лекция – визуализация обучает курсантов и слушателей преобразовывать информацию, предоставляемую преподавателем в устном или письменном виде, в визуальную форму. Это позволяет формировать профессиональное мышление посредством систематизации изучаемого материала и выделения наиболее важных и существенных элементов содержания. Поэтому одной из важнейших задач преподавателя при разработке лекции-визуализации является правильный подбор графических элементов и видеоматериала, располагаемых на слайдах учебно-наглядного пособия.

Вся презентация должна быть оформлена в едином стиле: в спокойных тонах, контрастно и без лишних анимационных эффектов. Необходимо придерживаться единообразного оформления слайдов. Две наиболее грубые ошибки при оформлении учебно-наглядного пособия с помощью MS Power Point заключаются в следующем: используется слишком мелкий текст на слайдах и на

слайды презентации помещаются емкие таблицы или вспомогательная информация (исторических справок, малозначительной информации, примеров).

Количество графических изображений на слайде учебно-наглядного пособия должно зависеть от продолжительности его рассмотрения. Чем больше графических элементов на слайде, тем больше времени необходимо обучаемым для осознания предложенного материала. Так, считаем необходимым располагать на одном слайде не более четырех смысловых единиц. При разработке учебно-наглядного пособия для лекции-визуализации каждая смысловая единица на слайде рассматривается отдельно, поясняется и последовательно конспектируется обучаемыми. При этом лектор обращает внимание обучаемых на нее с помощью указки (лазерной или классической). Одним из эффективных способов рассмотрения информации на слайде является использование анимации или триггеров для своевременного появления смысловых единиц на слайде (рис. 1).

Рис. 1. Один из вариантов расположения смысловых единиц на слайде

Еще одной ошибкой преподавателя при проведении лекции-визуализации является абсолютное дублирование материала, расположенного на слайде, и произносимого преподавателем текста, а потому не стоит перегружать слайды текстом. Целесообразнее при разработке и определении смысловых единиц слайда учебно-наглядного пособия располагать графическое изображение, которое характеризует взаимосвязи между понятиями, сложные термины или статистическую информацию [3].

Отдельно следует отметить качество графического материала на слайде. Так, слишком пестрый или яркий цвет фона со множеством объектов или чрезмерной анимацией очень сложен для восприятия обучаемыми. Такой фон снижает концентрацию внимания на материале и напрягает зрение обучаемых.

Рисунки, которые располагаются на слайде учебно-наглядного пособия к лекции, должны быть тщательно подобраны и максимально визуализировать необходимые термины. Поэтому беспорядочное расположение или неподходящий подбор иллюстраций к понятиям темы является еще одной ошибкой преподавателя при подготовке к лекции-визуализации. В связи с тем, что процесс визуализации позволяет осуществить сворачивание мыслительных содержаний в некоторый наглядный образ, в случае восприятия этого образа, он может быть развернут и станет опорой для последующих мыслительных операций и практических действий. Кроме того, группировка преподавателем учебного материала в схемы, таблицы, графики и демонстрация их на слайдах учебно-наглядного пособия включает фотографическую память обучаемых.

Рекомендуется использовать на слайдах различные виды визуализации: натуральные, изобразительные, символические. Как по отдельности, так и в комбинации, эти виды визуализации могут быть использованы на лекции и выбираются в зависимости от содержания учебного материала.

Типичной ошибкой при разработке лекции-визуализации является попытка преподавателя изложить на занятии большое количество учебной информации. Однако следует учесть, что при переходе от текстовой информации к зрительным образам или от одного вида наглядности к другому происходит потеря некоторого количества информации. Этот факт может считаться преимуществом, поскольку позволяет сосредоточить внимание обучающихся на наиболее важных аспектах содержания лекции, способствовать его пониманию и более тщательному усвоению. Кроме того, постановка проблемы на лекции-визуализации подтолкнет обучаемых самостоятельно изучить дополнительный материал по теме и углубить изученное с помощью заданий для самоподготовки.

Кроме того, необходимо рассмотреть требования к видеоматериалам, которые демонстрируются на лекции-визуализации. Здесь пойдет речь не о создании видео-лекции, а о тех учебных видеороликах, которые демонстрируются на лекции. Видеоматериалы должны быть краткими, лаконичными. Длительность видеоролика – от 5 до 12 минут, каждый видеоролик должен быть посвящен своей проблеме или идее. Для того, чтобы сделать видеоролик необходимого размера можно использовать программу «Видеоредактор», которая позволяет не только создать, отредактировать, но и преобразовать видео. Выбор данной программы обусловлен удобством разделения видео на отдельные фрагменты вплоть до секунды, что позволяет создать небольшие видеоролики для лекционного занятия.

Так, при проведении лекции-визуализации по теме «Понятие кибербезопасности и основные виды компьютерных уязвимостей» курса «Основы кибербезопасности», мы используем фрагменты фильма «Киберпреступления: зло в сети». Данный фильм длится 44 минуты, демонстрировать его полностью нерационально, а потому мы демонстрируем фрагменты длительностью 5 – 10 минут, подготовленные с помощью программы «Видеоредактор». Нами предлагаются обучающимся на лекции-визуализации четыре видеоролика: «Вымогательство», «Даркнет», «Троян» и «Фишинг», фрагментарно вырезанные из фильма «Киберпреступления: зло в сети» [2].

Важна не только дозировка использования видеоматериала, но и мастерство и стиль общения преподавателя с обучаемыми после его просмотра. Общеизвестно, что просмотр видео на лекции будет неэффективным, если не организовать его обсуждение для того, чтобы обучаемые сделали правильные выводы. Поэтому каждый видеоролик обсуждается с обучающимися по примерному плану: 1) средство совершения киберпреступления; 2) схема совершения киберпреступления; 3) методы предотвращения киберпреступления.

Таким образом, лекция-визуализация способствует созданию проблемной ситуации, разрешение которой происходит с включением активной мыслительной деятельности обучающихся, то есть на основе анализа, синтеза,

обобщения, свертывания или развертывания информации. Основной задачей преподавателя при подготовке лекции-визуализации является использование таких средств наглядности, которые позволят не только дополнить изучаемую информацию, но и сами будут являться носителями нового материала. Такие средства наглядности должны создавать устойчивые ассоциации с изучаемым материалом, осуществлять стойкое запоминание информации и создавать проблемные ситуации, которые в процессе их обсуждения с преподавателем позволят повысить уровень мыслительной активности обучаемых, что, в свою очередь, позволит увеличить процент успешного усвоения материала обучаемыми.

Литература

1. Галанова И.С. Методические аспекты к реализации принципа наглядности в процессе организации лекции-визуализации в СПО / И.С. Галанова // Проблемы и перспективы технологического образования в России и за рубежом: сборник материалов Международной научно-практической конференции (г. Ишим, 27-28 ноября 2018 года). – Издательство: Изд-во ИПИ им. П.П. Ершова (филиал) ТюмГУ. – 2019. – С. 120 - 122.

2. Киберпреступления: зло в сети. URL: https://youtu.be/IKXPLrgvRyI (Дата обращения: 18.06.2023).

3. Разработка видеолекции: методические рекомендации / Сост.: Е.Н. Авдеева, Н.А. Лацко, О.В. Пихота, Е.Д. Сайто. – Южно-Сахалинск: Изд-во ИРОСО, 2019 – 32 с.

4. Смирнова М.И. Негативные стороны использования информационных технологий в учебном процессе в вузах системы МВД /М.И. Смирнова // Евразийский юридический журнал. – 2020. – № 11 (150). – С. 452 - 453.

Сведения об авторе

Тутова Ольга Васильевна, кандидат педагогических наук, доцент, старший преподаватель кафедры гуманитарных и социально-экономических дисциплин Крымского филиала Краснодарского университета МВД России; e-mail: tutova-ov@yandex.ru.

Уразгильдеев Булат Гамирович

ОПЫТ ВНЕДРЕНИЯ ASTRA LINUX В ДЕЯТЕЛЬНОСТЬ МВД РОССИИ

Замещение операционных систем, специального и иного программного обеспечения иностранного производства российскими аналогами является важным шагом на пути к обеспечению информационной безопасности и суверенитета страны.

Издание Постановления Правительства РФ от 16 ноября 2015 г. № 1236 стало начальным этапом по формированию и наполнению единого реестра программ для ЭВМ, установив для госсектора запрет на допуск программного обеспечения, происходящего из иностранных государств. Данное событие явилось отправной точкой на завоевание отечественными разработчиками российского госсектора, расширение разработки и развития аналогов зарубежного программного обеспечения.

В развитие описываемых идей были изданы различные приказы Минцифры России, утверждающие рекомендуемую форму плана-графика перехода на отечественное офисное программное обеспечение, Постановление Правительства Российской Федерации от 22.08.2022 № 1478, Указ Президента РФ от 30.03.2022 № 166 – для критической информационной инфраструктуры, однако МВД России не вошло в описание субъектов КИИ.

Перед началом внедрения Astra Linux в деятельность МВД России был проведен тщательный анализ требований и потребностей ведомства, определены основные цели и задачи, которые должна была решить новая ОС.

Необходимыми критериями явились универсальность применения, оперативное взаимодействие с производителем-разработчиком, пройденные испытания в системе сертификации ФСТЭК России, что позволило использовать ОС для обработки и защиты информации любой категории доступа, вплоть до использования в автоматизированных системах, в которых должны применяться

средства, соответствующие 2 уровню доверия (на 2020 год) без наложенного средства защиты информации.

После тестирования различных ОС удовлетворяющим решением стала ОС специального назначения Astra Linux Special Edition, версия 1.6, вследствие чего ОС получила особый приоритет.

Активная фаза внедрения Astra Linux Special Edition в деятельность Министерства внутренних дел Российской Федерации пришлась на 2020 год.

Astra Linux Special Edition, разработанная на базе открытых исходных кодов, является, по сути, форком дистрибутивов Debian со встроенным офисным программным обеспечением Libre Office и средствами для работы с мультимедийными данными. Наличие встроенной системы безопасности PARSEC и вклада российских разработчиков обеспечивает уровень безопасности, необходимый для работы в соответствующих информационных (автоматизированных) системах, и снижает зависимость от зарубежных поставщиков программного обеспечения.

Одной из сложностей во внедрении Astra Linux Special Edition является отсутствие должного описания настройки ОС в соответствии с необходимыми классами защищенности, вопреки заявлению производителя о соответствии Astra Linux видениям регулятора в области технической защиты информации – требованиям руководящих документов, касающихся автоматизированных систем и средств вычислительной техники, Гостекомиссии России, предшественнику ФСТЭК России. Так, наблюдать о соответствии классам защиты можно на официальном сайте astralinux.ru, однако в эксплуатационной документации – ни в руководствах администратора, ни в руководствах по комплексу средств защиты, разъяснения не содержатся. Кроме того, способ реализации меры защиты с использованием штатных средств и применяемые компоненты Astra Linux до недавних пор не содержались и в техническом портале wiki.astralinux.ru, что подтверждается историей редактирования.

Можно выделить 5 общих вариантов использования Astra Linux в МВД России, связанных назначением ее применения:

информационные (автоматизированные) системы, в которых обрабатывается информация, содержащая сведения, составляющие государственную тайну, аттестуемые в порядке, определяемом приказом ФСТЭК России от 28 сентября 2020 г. № 110;

автоматизированные рабочие места единой системы информационно-аналитического обеспечения деятельности МВД России;

иные информационные (автоматизированные) системы, аттестованные в порядке, определяемом приказом ФСТЭК России от 29 апреля 2021 г. № 77;

средства вычислительной техники, подключаемые к сети «Интернет» – в соответствии с приказом МВД России 24 декабря 2015 года № 1228;

иные персональные компьютеры, не входящие в состав информационных (автоматизированных) систем и не подключенные к сети «Интернет».

Для каждого из вариантов определяются свои организационные меры защиты, комплекс документации и технологический процесс обработки информации. Также с каждым вариантом связаны свои особенности настройки ОС.

Доработка различных автоматизированных (информационных) систем.

Так, сложности в переходе на отечественную ОС в львиной доле играют временную и экономическую составляющую. Разработанные до недавнего времени автоматизированные (информационные) (поисковые) системы, эксплуатируемые в деятельности МВД России и предназначенные для исполнения в рабочей среде семейства ОС Windows, предполагает несовместимость применения в отличных средах на базе ядра Linux. В порядке исключения в ОС доступно применение встроенных средств виртуализации qemu/kvm и эмуляции wine в случае прохождения сертификационных испытаний в составе ОС.

Однако если рассматривать вопрос в контексте перехода страны на отечественное программное обеспечение, возникает потребность заблаговременного создания программного обеспечения, по сути выполняющего аналогичные функции, что не может быть сделано в короткие сроки.

Эксплуатирующие подразделения обязаны проходить весьма долгий процесс в идее замены функционирующих систем на аналогичные, работающие на базе отечественных ОС: от заявки на новые опытно-конструкторские работы в ФКУ НПО «СТиС» МВД России до издания приказа МВД России о введении системы в эксплуатацию. Данный процесс может затянуться на долгое время буквально из-за нехватки «рабочих рук» в составлении ТЗ, необходимости сертификации в системе ФСТЭК России при реализации функций защиты информации, неуспешного выполнения поставщиком работ в рамках государственного контракта, и т.д.

Переходный период на использование исключительно отечественной ОС в данном случае связан с многочисленными бюджетными затратами, с чем можно ознакомиться на сайте единой информационной системы в сфере закупок. Однако в долгосрочной перспективе такой подход играет на руку экономике России ввиду независимости от зарубежных поставщиков и развития отечественной IT-индустрии.

Огромный пласт рабочих мест составляют АРМ ИСОД МВД России, которые, в том числе, должны соответствовать Требованиям на типовое АРМ ИСОД МВД России, утвержденных заместителем Министра внутренних дел Российской Федерации В.Д. Шуликой от 9 августа 2019 года. В этой связи важную роль играет апробация нового программного обеспечения до его распространения, чем преимущественно занимается ДИТСиЗИ МВД России, с привлечением ФКУ «ГЦСиЗИ МВД России» и пилотных регионов.

Так, постоянно тестируются новые версии скрипта автоматизированной настройки АРМ ИСОД, на данный момент происходит в том числе плавный переход на новую версию средства управления доступом к информационным

системам и ресурсам (СУДИС), постоянно разрабатываются и тестируются новые версии программного обеспечения. В рамках правил эксплуатации ИСОД МВД России и контракта с АТ Consulting оказывается услуга по техническому сопровождению эксплуатации репозитория Astra Linux – обеспечивается функционирование и администрирование репозитория, консультирование сотрудников подразделений информационных технологий, связи и защиты информации по ОС Astra Linux.

Среди прочих сложностей при переходе на отечественную ОС были непривычность пользовательского интерфейса, несовместимость отдельного программного обеспечения для разных версий и релизов Astra Linux и другие. Непривычность пользовательского интерфейса офисного редактора, функционал его форматирования документа явились неожиданностью для многих сотрудников, т.к. повседневная деятельность так или иначе связана с подготовкой самых разнообразных документов. В этом контексте встроенный в систему Libre Ofiice не оправдал ожидания пользователей. Стоит отметить, что ДДО МВД России было разрешено использовать шрифт PT Astra при разработке документов, до внесения соответствующих изменений в Инструкции по делопроизводству в органах внутренних дел Российской Федерации.

Одним из ключевых аспектов внедрения Astra Linux было обучение сотрудников работе с новой ОС. Были проведены тренинги и курсы, на которых сотрудникам объяснялись основные принципы работы с системой, ее функциональные возможности и специфика использования. Это позволило сотрудникам быстрее адаптироваться к новой системе и более эффективно использовать ее в своей работе.

Стоит отметить, что Astra Linux Special Edition была успешно интегрирована с некоторыми уже существующими системами и программными продуктами. Это позволило сохранить работоспособность и совместимость с уже используемыми решениями.

Описанное выше является лишь вершиной айсберга. Импортозамещение должно продолжаться на всех его путях, а переход ведомства на отечественное программное обеспечение является лишь его толикой. Внедрение Astra Linux в МВД России является примером успешной реализации инновационных технологий в государственной сфере и способствует обеспечению безопасности и суверенитета России.

Литература

1. Воейков Д. МВД секретным приказом переводится на Astra Linux [Электронный ресурс] // Интернет-издание о высоких технологиях – Cnews. Дата обновления: 30.07.2021. URL: https://www.cnews.ru/news/top/2021-07-30_mvd_tajno_pereshlo_na_astra_linux (дата обращения: 20.06.2023).

2. Колокольцев сообщил о большом оттоке кадров из МВД [Электронный ресурс] // Новости в России и мире – ТАСС. Дата обновления: 16.11.2022. URL: https://tass.ru/obschestvo/16343249 (дата обращения: 20.06.2023).

Сведения об авторе

Уразгильдеев Булат Гамирович, старший специалист ЦЗИ, ГЦСиЗИ МВД России; e-mail: burazgildeev@mvd.ru.

Харченко Анна Владимировна

ИССЛЕДОВАНИЕ ПРИМЕНЕНИЯ ВРЕМЕННЫХ РЯДОВ В БАНКОВСКОМ СЕКТОРЕ

Применение временных рядов в анализе денежных транзакций банковского сектора представляет собой важную тему, позволяющую осуществлять прогнозирование экономических процессов на основе предшествующих данных.

Временной ряд представляет собой последовательность наблюдений за определенным временным периодом, где каждое наблюдение соответствует конкретному моменту времени. Для анализа банковских транзакций, временные ряды могут содержать информацию о количестве транзакций за определенный период времени, размерах операций, а также о поведении клиентов в рамках своих финансовых потребностей.

Анализ временных рядов позволяет выявлять тренды, сезонные колебания, цикличность и случайный характер изменений в банковских операциях. Это позволяет банковским институтам разработать эффективные стратегии управления рисками, прогнозировать потоки денежных средств, определять пики и спады в активности клиентов, а также выявлять влияние внешних факторов на деятельность банка.

В рамках исследования была осуществлена обработка набора данных об обезличенных тратах клиентов конкретного банка путем анализа временных рядов. Данная выборка характеризует расходы клиентов в зависимости от времени года и времени суток. Рассмотрение данных с учетом указанных параметров позволяет выявить закономерности в поведении потребителей и подготовить гипотезы для дальнейшего исследования. Полученные результаты могут быть использованы в целях оптимизации банковской деятельности и повышения качества предоставляемых услуг.

Ряд данных представляет информацию о суммах транзакций в течение определенного периода времени. В процессе анализа было установлено, что за

рассматриваемый период суммы транзакций варьировались в диапазоне от 30000 до 110000 рублей, причем наиболее часто встречаемыми оказались суммы от 45000 до 80000 рублей. С использованием расширенного теста Дики-Фуллера было выявлено, что данное множество данных является стационарным с уровнем значимости 0,05 и p-значением, примерно равным 0,001. Это означает, что гипотеза о нестационарности временного ряда может быть опровергнута, и многие модели могут быть применены для прогнозирования данного ряда.

По результатам анализа трат клиентов в разрезе пола было выявлено, что обе группы потребителей (мужчины и женщины) проявляют похожий паттерн потребления. Таким образом, наличие данных о поле потребителя не является значимым фактором для прогнозирования трат по данному ряду. Для более глубокого анализа следует рассмотреть другие социально-демографические характеристики, такие как возраст, доход и образование, которые могут помочь в выявлении дополнительных факторов, влияющих на суммы транзакций клиентов.

Проанализировав различия в трате средств между мужчинами и женщинами в зависимости от времен года, можно установить, что мужчины имеют более высокий уровень средних трат, нежели женщины. Максимальные средние траты у мужчин составляют около 80000-160000 рублей, в то время как у женщин они ограничиваются 60000-70000 рублей. Анализируя данные в разрезе временных периодов, можно заметить, что осенью и весной мужчины имеют более высокие показатели средних трат, достигая уровней до 200000 и 225000 рублей соответственно. Летом у мужчин также значительные траты, которые достигают максимальной величины в размере 170000 рублей. В зимнее время года величина средних трат колеблется и изменяется изо дня в день, при этом составляет от 80000 до 160000 рублей. Таким образом, пол и время года являются значимыми факторами, влияющими на уровень средних трат. В дальнейшем исследование можно посвятить анализу более детальных факторов, влияющих на траты мужчин и женщин в различные временные периоды.

Рассмотрим траты населения в разрезе времени суток. Анализируя их, можно отметить, что расходы женщин в период с июля по сентябрь, утром, превышают расходы мужчин и находятся на одном уровне с ними. В остальном расходы обоих полов колеблются от 60000 до 170000 рублей и не имеют существенных различий. Расширяя данное исследование, следует отметить необходимость еще более детального анализа в разрешении часов, а также учета социо-экономических факторов, таких как уровень дохода или сезонность.

При анализе временных рядов можно сделать вывод о нисходящем тренде в утренних тратах, а вечерние и ночные траты имеют восходящий тренд. В то же время дневные траты не имеют определенной тенденции в поведении. Эти результаты свидетельствуют о том, что многие факторы могут влиять на поведение потребителей, что подчеркивает необходимость дальнейшего исследования данной темы.

Применение временных рядов в исследовании банковских транзакций включает в себя важный аспект, который может обеспечить полезные результаты для принятия действенных управленческих решений и управления финансовыми рисками в банковской среде. Одно из таких преимуществ состоит в возможности получения ценной информации о динамике транзакций во времени, что способствует выявлению и анализу тенденций и изменений в финансовых операциях. Кроме того, использование временных рядов позволяет определить различные факторы, которые могут повлиять на финансовые операции и, следовательно, на риски, связанные с этими операциями. Результаты исследований, проведенных с применением временных рядов, могут служить основой для принятия действенных мер по управлению рисками и повышению эффективности банковских операций.

Литература

1. Проскуряков, А.Ю. Прогнозирование изменения параметров временных рядов в задачах цифровой экономики / А.Ю. Проскуряков // Актуальные проблемы и перспективы развития радиотехнических и

инфокоммуникационных систем: сборник научных трудов III Международной научно-практической конференции, г. Москва, Россия, 13–17 ноября 2017 года / Московский технологический университет (МИРЭА). Том Часть 1. – г. Москва, Россия: Московский технологический университет (МИРЭА), 2017. – С. 80-93. – EDN YNRJQQ.

2. Урусова, А.Б. Практические мероприятия обеспечения функционирования банковской системы в условиях развития цифровых технологий / А.Б. Урусова // Вестник Московского гуманитарно-экономического института. – 2021. – № 3. – С. 274-282. – DOI 10.37691/2311-5351-2021-0-3-274-282. – EDN XZWGMN.

Сведения об авторе

Харченко Анна Владимировна, кандидат педагогических наук, доцент Кубанского государственного университета; e-mail: fz@mail.ru.

Хромых Анна Алексеевна

ПОСТРОЕНИЕ АДДИТИВНОЙ МОДЕЛИ ВРЕМЕННОГО РЯДА, ХАРАКТЕРИЗУЮЩЕГО КОЛИЧЕСТВО ПРЕСТУПЛЕНИЙ, СОВЕРШЕННЫХ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ ИЛИ В СФЕРЕ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ В КРАСНОДАРСКОМ КРАЕ

На сегодняшний день активно продолжается цифровизация практически всех сфер жизни с использованием передовых разработок искусственного интеллекта, биометрической идентификации, обработки больших данных, облачных технологий, удаленного банковского обслуживания и т.д. Изучение основных тенденций в развитии киберпреступности остается важной задачей моделирования [2]. Полученные результаты позволяют обосновывать принятие управленческих решений на всех уровнях власти, делая эту работу по-настоящему значимой и актуальной.

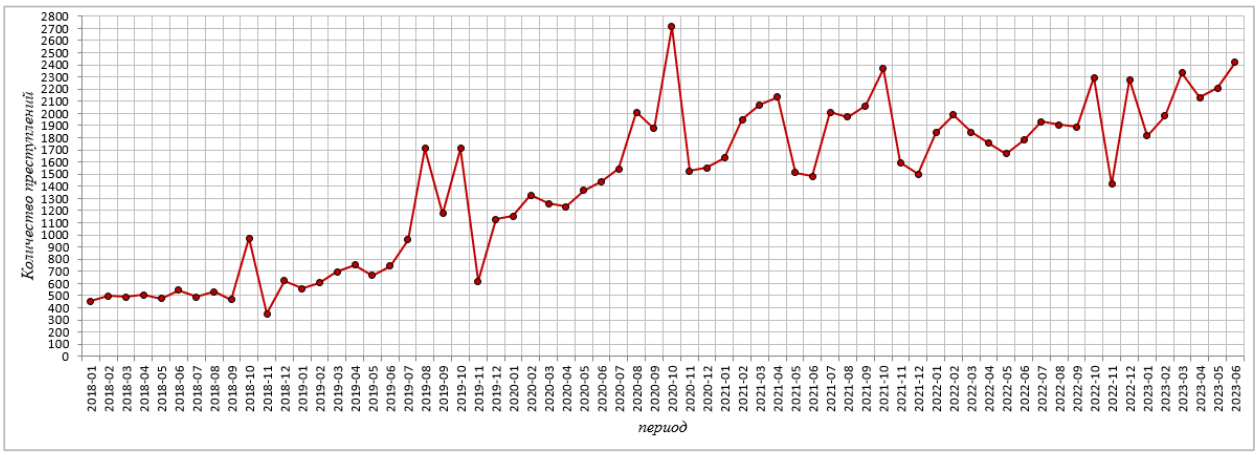


Рис. 1. График временного ряда, отражающий количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации в Краснодарском крае с января 2018 года по июнь 2023 год

В данной статье на основе статистических данных, представленных на официальных сайтах Росстата и Министерства внутренних дел Российской Федерации [1, 3, 4, 6], построена аддитивная модель временного ряда количества преступлений, совершенных в Краснодарском крае с использованием

информационно-телекоммуникационных технологий или в сфере компьютерной информации с января 2018 года по июнь 2023 года (рис. 1) и вычислим прогноз на июль 2023 года.

На графике (рис. 1), отражающем зависимость количества IT-преступлений от месяца, отчетливо выделяются повторяющиеся во времени колебания, при этом ежегодно наибольшее значение временной ряд принимает в октябре.

Аддитивная модель временного ряда определяется следующим уравнением:

$$\hat{y}_t = y_t + s_t + c_t + e_t, \quad (1)$$

где y_t – трендовая компонента; s_t – сезонная компонента; c_t – циклическая компонента; e_t – случайная компонента.

Прежде чем построить аддитивную модель временного ряда, исходные данные необходимо исследовать на стационарность. Для этого определим наличие или отсутствие в изучаемых данных трендовой компоненты, т.е. проверим гипотезу H_0 о случайности тенденции (тренда) ряда.

Разобьем исходные статистические данные на две равные половины и сравним их средние значения, рассчитав по выражению (2) статистику критерия *t*-Стьюдента:

$$t_{расч.} = \frac{\bar{y}_1 - \bar{y}_2}{\sqrt{(n_1 - 1)\sigma_1^2 + (n_2 - 1)\sigma_2^2}} \cdot \sqrt{\frac{n_1 n_2 (n_1 + n_2 - 2)}{n_1 + n_2}} \quad (2)$$

где n_1 и n_2 – длины первой и второй частей ряда ($n_1 = n_2 = 33$); $\bar{y}_1$ и $\bar{y}_2$ – средние значения первой и второй половин ряда,; σ_1^2 и σ_2^2 – оценки дисперсий первой и второй половин ряда.

Средние значения $\bar{y}_1$, $\bar{y}_2$ и оценки дисперсий σ_1^2, σ_2^2 вычисляются по формулам [5]:

$$\bar{y}_1 = \frac{1}{n_1} \sum_{i=1}^{33} y_i \quad (3)$$

$$\bar{y}_2 = \frac{1}{n_2}\sum_{i=34}^{66} y_i \quad (4)$$

$$\sigma_1^2 = \frac{1}{n_1 - 1}\sum_{i=1}^{33}\left(y_i - \bar{y}_1\right)^2 \quad (5)$$

$$\sigma_2^2 = \frac{1}{n_2 - 1}\sum_{i=34}^{66}\left(y_i - \bar{y}_2\right)^2 \quad (6)$$

Результаты расчета числовых характеристик по формулам (3)–(6), представлены в таблице 1.

Таблица 1. Значения числовых характеристик

Часть ряда	Оценка математического ожидания	Оценка дисперсии
1	$\bar{y}_1 = 937{,}606061$	$\sigma_1^2 = 227596{,}184$
2	$\bar{y}_2 = 1926{,}54545$	$\sigma_2^2 = 98673{,}4432$

Подставляя данные из таблицы 1 в выражение (2), получаем расчетное значение критерия *t*-Стьюдента: $t_{расч}$=-9,94576.

Критическое значение распределения *t*-Стьюдента при уровне значимости α=0,05 и числа степеней свободы d_f=*n*-2=64 определяется из таблицы: $t_{кр}$=1,9977. Т.к. $|t_{расч}|$=9,94576>1,9977, то гипотеза H_0 о случайности тренда временного ряда отвергается и принимается альтернативная гипотеза H_1 о не случайности тенденции временного ряда, причем изучаемый временной ряд не стационарен.

Для устранения случайных колебаний уровней временного ряда и выделения трендовой компоненты проведем численное сглаживание ряда методом простого скользящего среднего. Сглаженные значения уровней по пяти элементам ряда определяются по формулам [7]:

$$\tilde{y}_t = \frac{1}{5}\left(y_{t-2} + y_{t-1} + y_t + y_{t+1} + y_{t+2}\right),\ \tilde{y}_t = \frac{1}{5}\left(y_{t-2} + y_{t-1} + y_t + y_{t+1} + y_{t+2}\right).$$

Графически сглаженный ряд представлен на рисунке 2. Не сложно заметить, что тенденция изменения уровней ряда носит явно нелинейный характер.

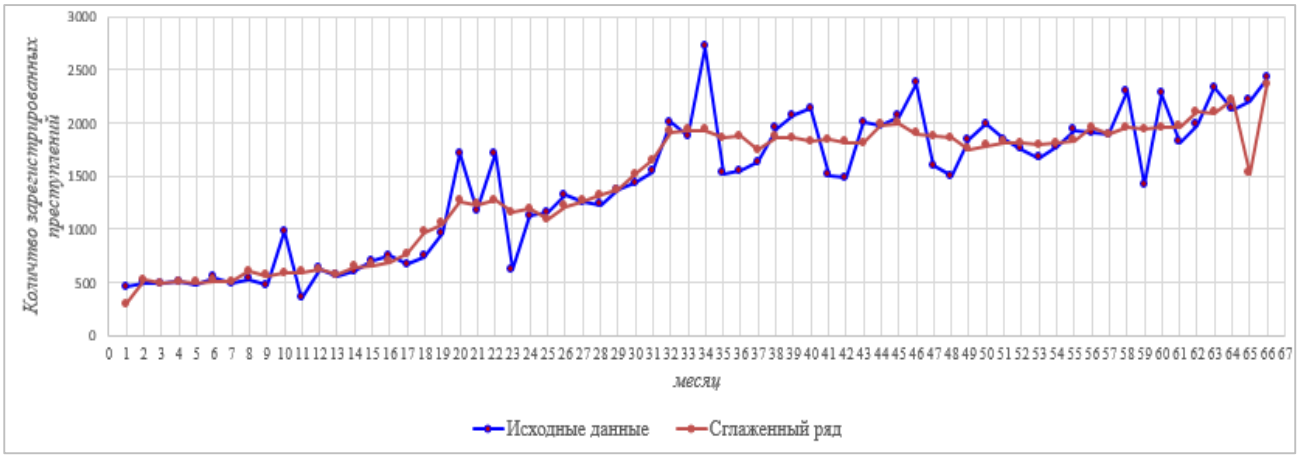


Рис. 2. Сглаживание временного ряда методом простого скользящего среднего

Установим вид тренда (линейный или нелинейный) и выявим наличие периодических компонент (сезонной и циклической) с помощью автокорреляционной функции. Коэффициенты автокорреляции вычисляются по формуле:

$$r(\tau)=\frac{\sum_{i=\tau+1}^{n}(y_i-\bar{y}_i)(y_{i-\tau}-\bar{y}_{i-\tau})}{\sqrt{\sum_{i=\tau+1}^{n}(y_i-\bar{y}_i)^2\cdot\sum_{i=\tau+1}^{n}(y_{i-\tau}-\bar{y}_{i-\tau})^2}}, \quad (7)$$

где $\bar{y}_i=\frac{1}{n-\tau}\sum_{i=\tau+1}^{n}y_i$ и $\bar{y}_{i-l}=\frac{1}{n-\tau}\sum_{i=\tau+1}^{n}y_{i-1}$, $\tau=1,2,3,...,33$, $n=1,2,3,...,66$.

Результаты расчетов коэффициентов автокорреляции приведены в таблице 2 и графически в виде коррелограммы изображены на рисунке 3.

Проверив найденных значения коэффициентов автокорреляции на статистическую значимость, можно сделать вывод, что величины $r(1)-r(18)$ и $r(24)$ в целом статистически значимы. Так как $r(1)$=0,81201755 и $r(12)$=0,808511, следовательно, кроме трендовой компоненты временной ряд содержит периодическую сезонную компоненту, причем тренд обладает нелинейной тенденцией. Так же следует отметить, что ряду свойственна цикличность с периодом T=12 моментов времени.

Таблица 2. Значения коэффициентов автокорреляции

τ	r(τ)	τ	r(τ)	τ	r(τ)
1	0,81201755	12	0,808511	23	0,421153
2	0,81834509	13	0,628437	24	0,577719
3	0,749446727	14	0,628437	25	0,338144
4	0,757058102	15	0,654236	26	0,425245
5	0,785036158	16	0,526854	27	0,229915
6	0,807016574	17	0,542379	28	0,27034
7	0,726392669	18	0,556938	29	0,293353
8	0,704502172	19	0,480387	30	0,307957
9	0,665687997	20	0,494151	31	0,242579
10	0,711996249	21	0,405089	32	0,25063
11	0,684143514	22	0,433721	33	0,239035

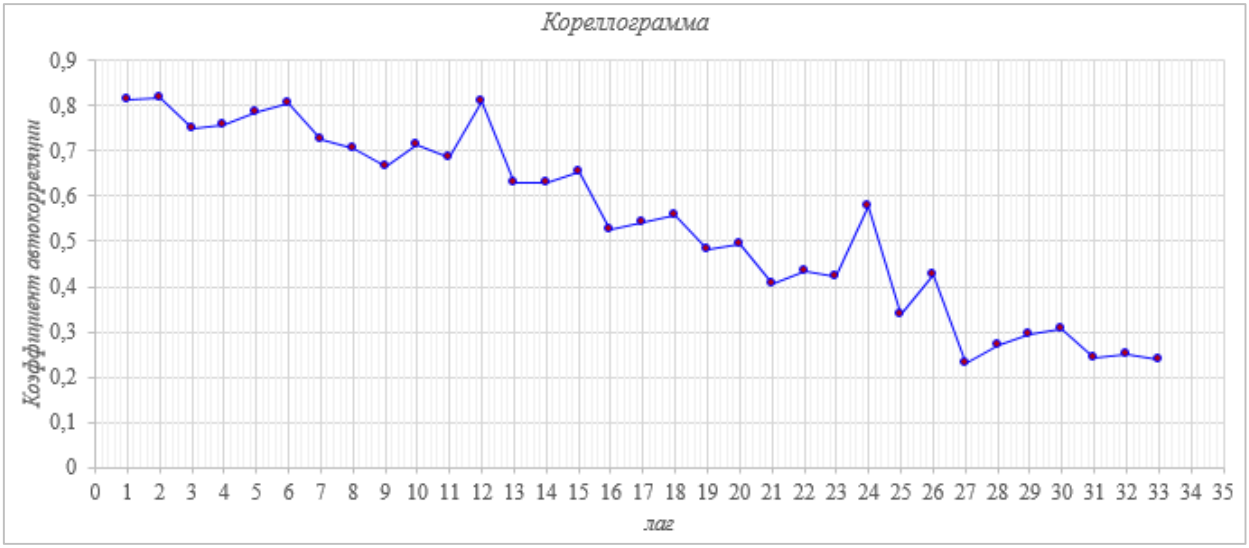


Рис. 3. Коррелограмма

Найдем трендовую компоненту изучаемого временного ряда. Для этого произведем аналитическое выравнивание статистических данных, применяя метод наименьших квадратов:

$$\sum_{i=1}^{n}\left(y_i - y(x_i)\right)^2 \to \min . \qquad (8)$$

Как было отмечено ранее, тренд носит нелинейных характер. Следовательно, для его моделирования подберем полиномиальную функцию.

В качестве нелинейных функций рассмотрим полиномы различных степеней (рис. 4-8):

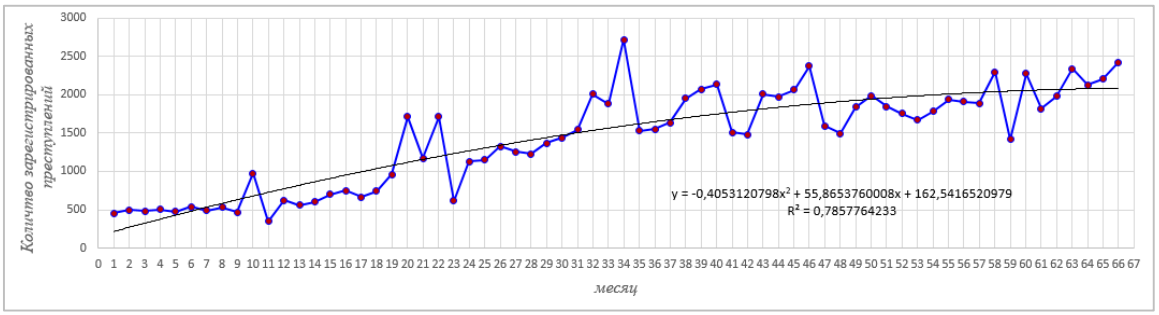


Рис. 4. Полиномиальный тренд второй степени

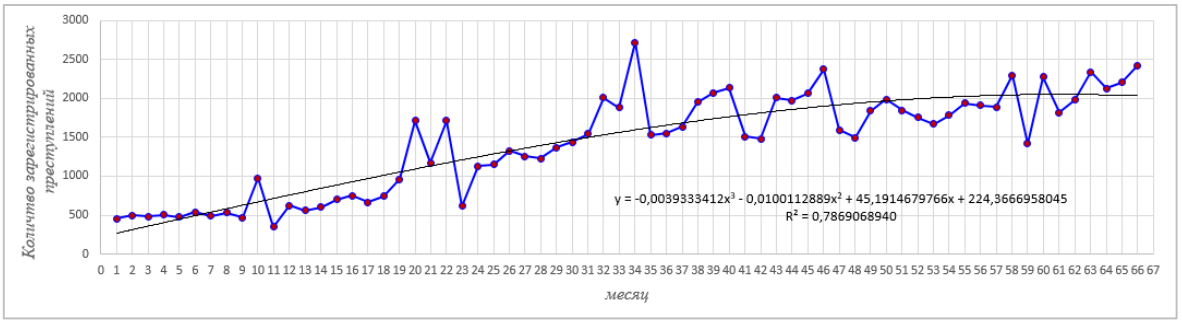


Рис. 5. Полиномиальный тренд третьей степени

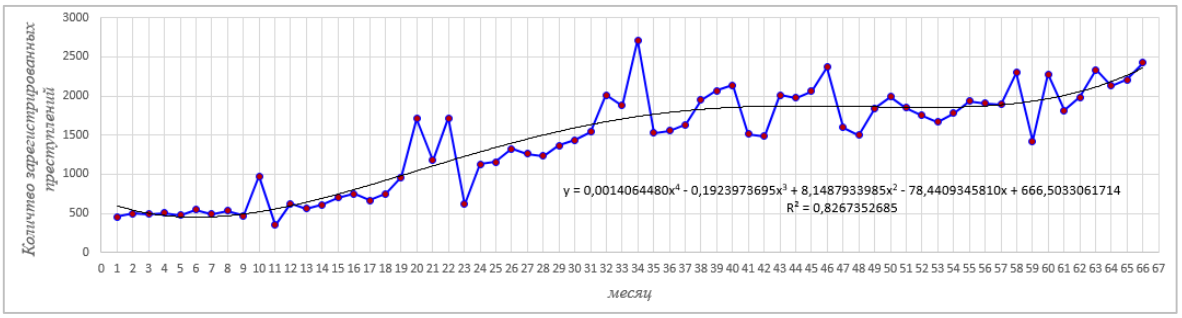


Рис. 6. Полиномиальный тренд четвертой степени

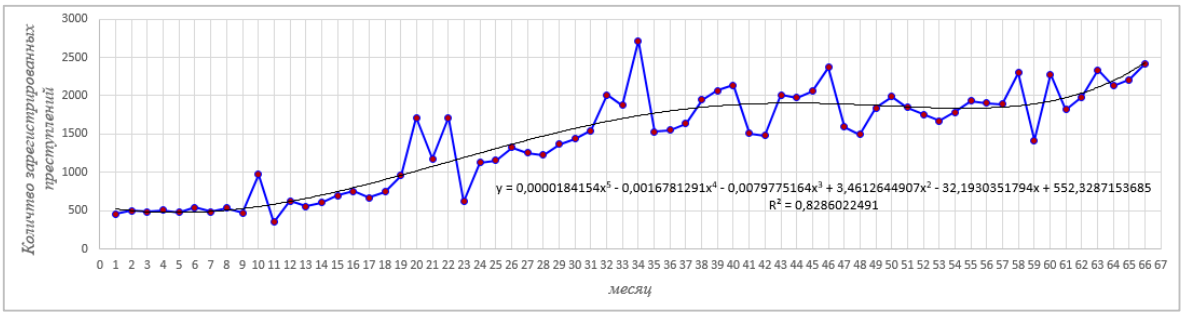


Рис. 7. Полиномиальный тренд пятой степени

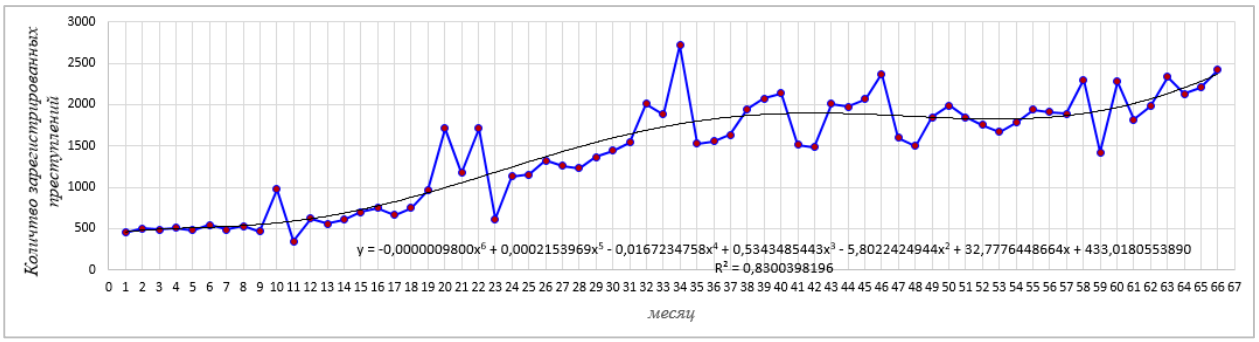


Рис. 8. Полиномиальный тренд шестой степени

Для оценки математической точности полученного уравнения тренда вычислим среднюю ошибку аппроксимации:

$$A_{cp} = \frac{1}{n}\sum_{i=1}^{n}\left|\frac{y_i - y(x_i)}{y_i}\right| \cdot 100\%. \qquad (9)$$

Вычисленные значения средней ошибки аппроксимации представлены в таблице 3.

Таблица 3. Значения средней ошибки аппроксимации и коэффициентов детерминации для различных видов полиномиальных функций

№	Вид тренда	Коэффициент детерминации, R^2	Средняя ошибка аппроксимации, A_{cp}
	полиномиальный 2 степени		
	полиномиальный 3 степени		
	полиномиальный 4 степени		
	полиномиальный 5 степени		
	полиномиальный 6 степени		

Из представленных моделей наилучшим образом аппроксимирует исходные данные полиномиальная модель шестой степени (рис. 8), т.к. имеет наибольшее значение коэффициента детерминации R^2=83% и наименьшее значение средней ошибки аппроксимации A_{cp}=13,73%. Однако следует отметить, что значение ошибки аппроксимации превышает порог в 8-10%.

Оценим статистическую значимость построенного тренда, используя F-критерий Фишера:

$$F_{расч} = \frac{\sum_{i=1}^{n}\left(y(x_i)-\bar{y}\right)^2}{\sum_{i=1}^{n}\left(y(x_i)-y_i\right)^2} \cdot \frac{n-m-1}{m}, \qquad (10)$$

где n – количество наблюдений, m – количество объясняющих факторов модели.

Для изучаемых статистических данных: $F_{расч} = 1917{,}382$.

Критическое значение распределения Фишера, учитывая уровень значимости $\alpha = 0{,}05$ и число степеней свободы $df_1 = m$ и $df_2 = n - m - 1$, определяется по таблице: $F_{табл} = 3{,}99$.

Поскольку $F_{расч} = 1917{,}382 > F_{табл} = 3{,}99$ $F_{расч}$=1917,382>3,99, то с вероятностью ошибки 0,05 уравнение общей тенденции временного ряда в целом статистически значимо, т.е. адекватно.

Практический интерес также представляет оценка тесноты связи между уровнями ряда и моментами времени. Вычислим коэффициент парной корреляции и сравним его со значением шкалы Чеддока:

$$r_t = \frac{\sum_{i=1}^{n}\left(x-\bar{x}\right)\left(y_i-\bar{y}\right)}{\sqrt{\sum_{i=1}^{n}\left(x-\bar{x}\right)^2 \cdot \sum_{i=1}^{n}\left(y_i-\bar{y}\right)^2}}. \qquad (11)$$

Таким образом, получаем $r_t = 0{,}3719$, что свидетельствует о слабой связи между уровнями ряда и моментами времени.

Возведя в квадрат найденный коэффициент парной корреляции, вычислим коэффициент детерминации R^2: $R^2 = 0{,}13834$.

Следовательно, количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации всего на 13,8% объясняются моментом времени *t*.

Ранее было отмечено, что временный ряд содержит повторяющиеся во времени колебания. Для нахождения значений сезонной компоненты

необходимо (табл. 3): 1) найти разность между значениями уровней ряда и их сглаженными значениями, т.е. вычислить $y_t - \tilde{y}_t$; 2) сгруппировать полученные разности по каждому месяцу (январь, февраль, март и т.д.) и найти их средние арифметические; 3) скорректировать сезонные компоненты так, чтобы их сумма равнялась нулю [7].

Для построения модели временного ряда с учетом сезонности прибавим соответствующую скорректированную сезонную компоненту $s_t^{ск}$ к значению тренда:

$$\hat{y}_t^{мод} = \hat{y}_t - s_t^{ск}. \quad (12)$$

Таблица 4. Значения сезонной компоненты

№	Месяц	Сезонная компонента, S_t
1	январь	-6,38667
2	февраль	+19,14667
3	март	+72,88
4	апрель	+10,24667
5	май	+3,746667
6	июнь	-108,953
7	июль	+5,113333
8	август	+69,63333
9	сентябрь	-42,6867
10	октябрь	+470,4333
11	ноябрь	-396,127
12	декабрь	-97,0467
Сумма		0

Значения уровней временного ряда для исследуемой модели, вычисленные по формуле (12), представлены на рисунке 5.

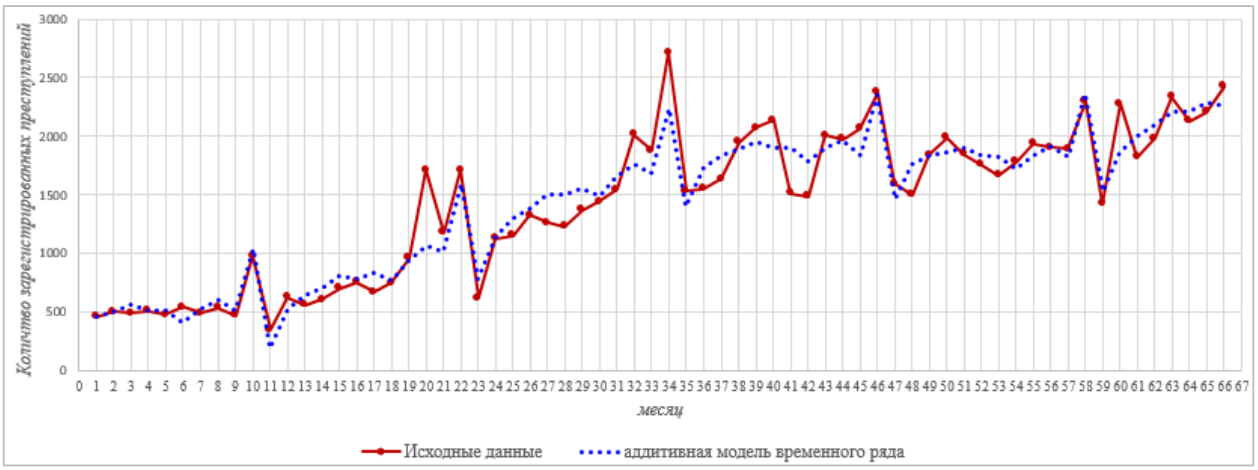


Рис. 9. Аддитивная модель временного ряда с учетом периодической компоненты

Точность полученной аддитивной модели можно определить с помощью средней ошибкой аппроксимации, в нашем случае она составила: $A_{cp} = 10{,}3\%$.

Используя построенную аддитивную модель временного ряда, можно вычислить прогнозное значение количества преступлений на июль 2023 года, которое составит 2456 преступлений.

В заключении следует отметить, что обработка статистического материала, характеризующего количество IT-преступлений, совершенных в Краснодарском крае с января 2018 года по июнь 2023 года, обеспечила формирование аддитивной модели временного ряда, включающей в себя трендовую и сезонную компоненты. Уравнение тренда представляет собой полиномиальную функцию шестой степени: $y = -0{,}0000009800x^6 + 0{,}0002153969x^5 - 0{,}0167234758x^4 + 0{,}5343485443x^3 - 5{,}8022424944x^2 + 32{,}7776448664x + 433{,}0180553890$. Сезонная компонента имеет цикличность с периодом $T = 12$. Ее максимальное отклонение наблюдается в октябре (+470,4333), а минимальное – в ноябре (-396,127). Теснота связи между уровнями ряда и моментами времени t практически отсутствует ($r_t = 0{,}3719$). Количество преступлений, совершенных с использованием информационно-телекоммуникационных технологий или в сфере компьютерной информации, в месяц на 13,8% объясняются моментом времени. Построенная аддитивная

модель временного ряда имеет не плохую точность $A_{ср} = 10{,}3\%$ и достаточно высокую тесноту связи $R^2 = 83\%$, что свидетельствует о статистически значимой модели в целом.

Литература

1. ЕМИСС Государственная статистика https://fedstat.ru/

2. Кайбичев И.А. Математическое моделирование временного ряда количества преступлений в России / И.А. Кайбичев, Е.И. Кайбичева // Вестник экономики, управления и права. 2019. №4 (49). URL: https://cyberleninka.ru/article/n/matematicheskoe-modelirovanie-vremennogo-ryada-kolichestva-prestupleniy-v-rossii (дата обращения: 05.10.2023).

3. Официальный сайт Министерства внутренних дел Российской Федерации https://мвд.рф/dejatelnost/statistics.

4. Портал правовой статистики Генеральной прокуратуры Российской Федерации http://crimestat.ru/.

5. Старостенко, И. Н. Элементы статистической обработки данных: учеб. пособие / И. Н. Старостенко, А. А. Хромых. – Краснодар: Краснодарский университет МВД России, 2020. – 74 с. – ISBN-978-5-9266-1613-9. – Текст: непосредственный + Текст: электронный. – http://ebs.libkrumvd.ru/elib/470/, требуется авторизация.

6. Федеральная служба государственной статистики https://rosstat.gov.ru/

7. Черевастов, М. Г. Получение аддитивной модели временного ряда, характеризующего дорожно-транспортную аварийность на примере Нижегородской области / М. Г. Черевастов, Ю. И. Молев // Транспортные системы. – 2020. – № 1(15). – С. 4-12. – DOI 10.46960/62045_2020_1_4. – EDN URWXIT.

Сведения об авторе

Хромых Анна Алексеевна, кандидат физико-математических наук, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: AnnXA@mail.ru.

Шарпан Мария Владимировна

РЕКОМЕНДАЦИИ ПО АДМИНИСТРИРОВАНИЮ ПОДСИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА

В рамках национальной программы импортозамещения МВД России переводит свою ИТ-инфраструктуру на российские решения. С 2020 года ведомство осуществляет комплексную замену зарубежных технологий отечественными и проводит пилотные проекты по ее реализации.

В качестве инфраструктурной платформы МВД России выбрана Astra Linux Special Edition, зарекомендовавшая себя как надежно защищенная отказоустойчивая ОС, которая позволяет выполнять все основные задачи ведомства.

Но, не всегда сотрудники органов внутренних дел при работе с операционной системой Astra Linux понимают, как настроить ту или иную подсистему по обеспечению защиты информации, как ее администрировать.

Рассмотри ручную настройку одной из подсистем защиты информации.

По умолчанию, в ОС Astra Linux используется дискреционное разграничение доступа, реализуется механизм, который обеспечивает наличие для каждой пары субъект-объект явное недвусмысленное перечисление разрешенных вариантом доступа. То есть, пользователь сам решает, кому предоставить доступ к файлу, владельцем которого он является. И, конечно, в таком способе разграничения доступа присутствуют свои недостатки, а именно то, что не предоставляется возможным управление информационными потоками, которые содержат информацию разных уровней конфиденциальности, то есть администратор не может проконтролировать утечку данных, доступных пользователю. А мандатный способ разграничения доступа способен решить подобного рода проблемы.

Мандатное разграничение доступа основано на подсистеме безопасности Parsec, самостоятельно разработанной и включающей в себя соответствующий программный интерфейс и модуль расширения ядра, поддерживающий виртуальную файловую систему parsec fs и набор системных вызовов,

позволяющих уполномоченным пользователям управлять политикой безопасности Astra Linux. Другими словами, Parsec это такой монитор обращений, который контролирует и определяет какой из категорий можно получить доступ к какому-то файлу, и, поскольку, решение предоставлять доступ принимает именно parsec, а не пользователь, как в случае с дискреционным доступом, то этот вид доступа еще также называют принудительным контролем доступа.

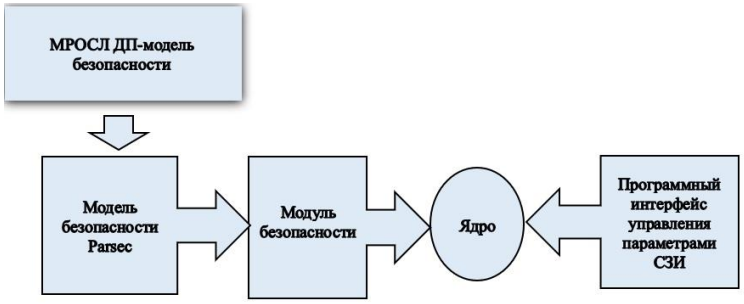


Рис.1. Схема мандатного разграничения доступа

Настройка режима мандатного контроля целостности производится в политике безопасности (Пуск – Панель управления – Безопасность – Политика безопасности – Мандатный контроль целостности).

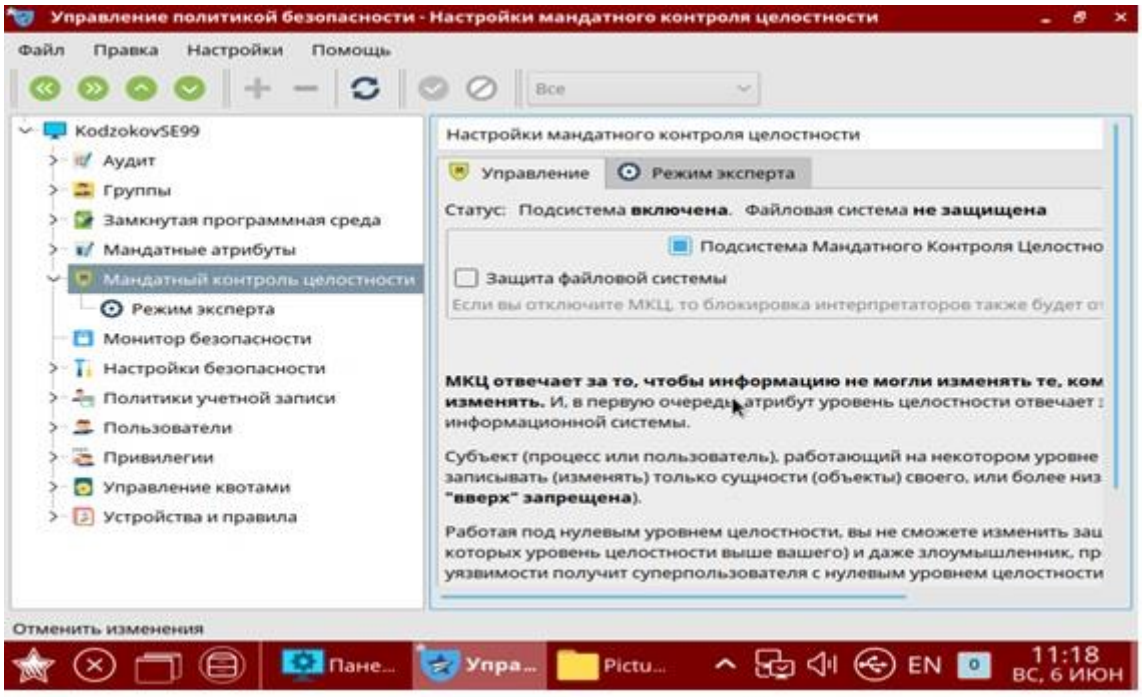


Рис.2. Мандатный контроль целостности

По умолчанию, при установке ОС Astra Linux, мандатный контроль

целостности включается сам, но контролирует только процессы. Файловая система не защищается. Это можно увидеть в мониторе безопасности:

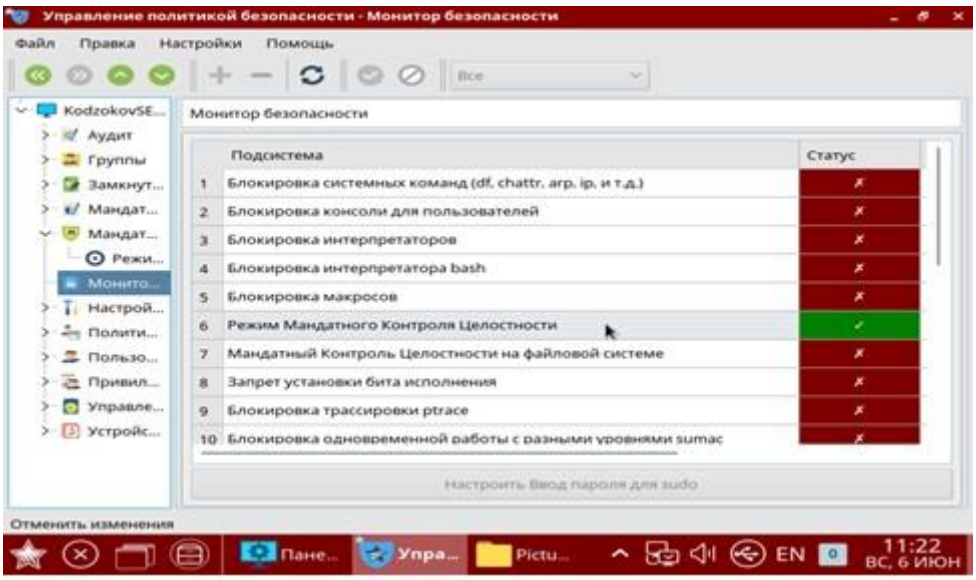


Рис.3. Монитор безопасности

На рисунке 3 видно, что мандатный контроль целостности файловой системы не включен. Для обеспечения должной безопасности это необходимо исправить. Настройка осуществляется в разделе «мандатный контроль целостности»:

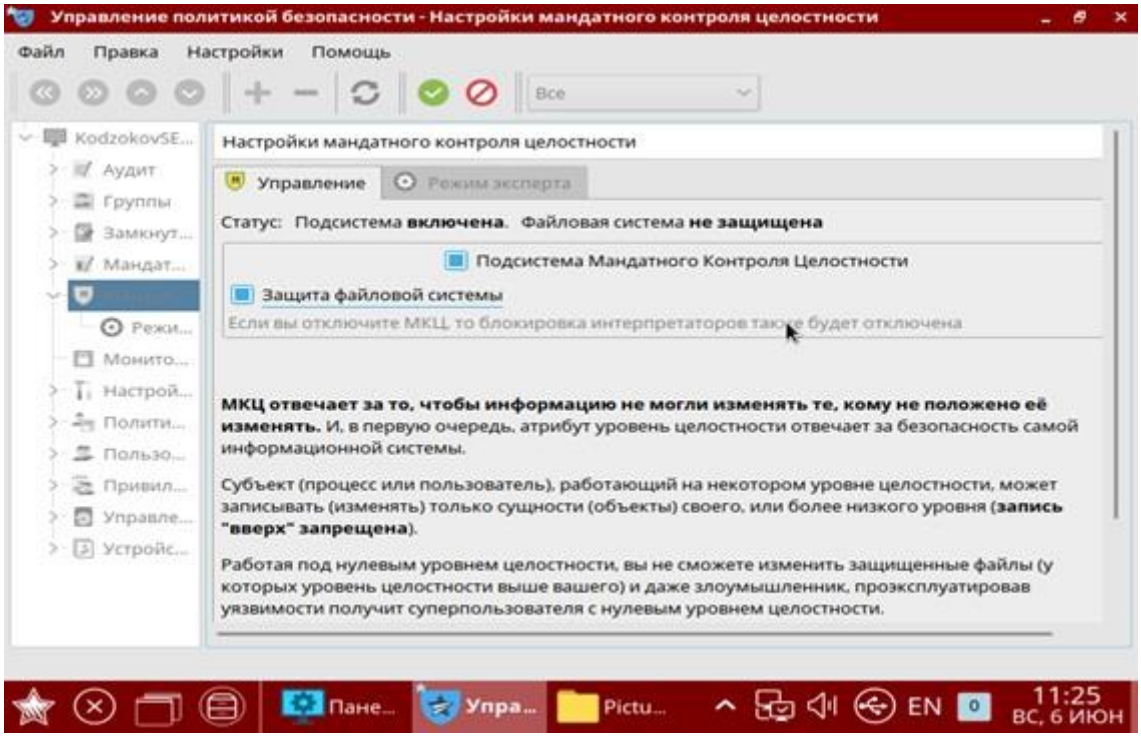


Рис.4. Настройки мандатного контроля целостности

Принимаем изменения, система при этом потребует перезагрузки. Теперь видны изменения в мониторе безопасности, а именно то, что в графе «мандатный контроль целостности файловой системы» стоит знак галочки. Это означает, что пользователь с уровнем целостности ниже уровня целостности файла не сможет произвести в нем какие-либо изменения. Parsec будет блокировать действия такого пользователя, потому что пользователь запустил процесс, который выше его прав, даже если пользователь зашел как root. Иными словами, Parsec мониторит систему и видит, что в системе находятся пользователи, которые зашли с низким уровнем контроля целостности; он мониторит их действия, и если в контексте какого-нибудь пользователя, возможно, из-за применения какого-то эксплойта или других причин, создался или запустился новый процесс под высоким уровнем целостности, хоть пользователь заходил под низким, то parsec сразу блокирует данное действие.

Литература

1. Девянин, П. Н. Основы безопасности операционной системы Astra Linux Special Edition. Управление доступом: учебное пособие / П.Н. Девянин, В.Ю. Тележников, С.В. Третьяков. – Москва: Горячая линия-Телеком, 2022. – 148 с. – ISBN 978-5-9912-0996-0: Б. ц. – Текст: непосредственный.

2. Одиноков, В. В. Операционные системы и сети: учебное пособие / Одиноков В.В., Коцубинский В.П. – Томск: Томский государственный университет систем управления и радиоэлектроники, 2007. – 391 с. – ISBN 978-5-86889-374-2. – Текст: электронный // IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/13951.html, требуется авторизация.

3. Филиппов, А.А. Операционные системы: учебное пособие / Филиппов А.А. – Ульяновск: Ульяновский государственный технический университет, 2021. – 100 с. – ISBN 978-5-9795-2129-9. – Текст: электронный // IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/121273.html, требуется авторизация.

4. Широков, А.И. Операционные системы и среды: основные понятия теории: учебник / Широков А.И., Кирдяшов Ф.Г., Мурадханов С.Э. – Москва: Издательский Дом МИСиС, 2018. – 192 с. – ISBN 978-5-906953-49-0. – Текст: электронный // IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/117318.html, требуется авторизация.

Сведения об авторе

Шарпан Мария Владимировна, кандидат физико-математических наук, доцент кафедры информатики и математики Краснодарского университета МВД России; e-mail: marusi2000@mail.ru.

Научное издание

МАТЕМАТИЧЕСКИЕ МЕТОДЫ
И ИНФОРМАЦИОННО-ТЕХНИЧЕСКИЕ СРЕДСТВА

Материалы
XIX Международной научно-практической конференции
(22 июня 2023 г.)

В авторской редакции
Компьютерная верстка *А. А. Хромых*

ISBN 978-5-9266-1914-7

Подписано в печать 02.11.2023.
Авт. л. 11,6. Заказ 201.

Краснодарский университет МВД России.
350005, г. Краснодар, ул. Ярославская, 128.