Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Сыктывкарский государственный университет имени Питирима Сорокина»
(ФГБОУ ВО «СГУ им. Питирима Сорокина»)
Институт точных наук и информационных технологий
Студенческое научное объединение

СЫКТЫВКАРСКИЙ
ГОСУДАРСТВЕННЫЙ
УНИВЕРСИТЕТ
имени Питирима Сорокина

СНО

«SOROKIN STARTUP» & «SOROKIN HACK DAYS»

Региональный форум инновационных проектов (Сыктывкар, 29 ноября — 1 декабря 2022 года)

Форум практической информационной безопасности (Сыктывкар, 16 декабря 2022 года)

Сборник материалов

Сыктывкар
Издательство СГУ им. Питирима Сорокина
2022

УДК 351:35.088.7
ББК 67.401
С65

Мероприятие проведено в рамках реализации в форме субсидий из федерального бюджета образовательным организациям высшего образования на реализацию мероприятий, направленных на поддержку студенческих научных сообществ (Соглашение о предоставлении из федерального бюджета грантов в форме субсидий в соответствии с пунктом 4 статьи 78.1 Бюджетного кодекса Российской Федерации от 1 июня 2022 г. №075-15-2022-1070 — Молодежный проект «Наука молодых — устойчивое развитие Республики Коми»)

Ответственные редакторы:

Гольчевский Юрий Валентинович, канд. физ.-мат. наук, доцент, заведующий кафедрой прикладной информатики;
Устюгов Владимир Александрович, канд. физ.-мат. наук, доцент, заведующий кафедрой информационной безопасности

Редакционная коллегия:

Швецова Ирина Николаевна, канд. экон. наук, доцент, доцент кафедры финансового менеджмента;
Куликова Софья Александровна, обучающаяся группы 111а-ПИо института точных наук и информационных технологий

С65 **«SOROKIN STARTUP» & «SOROKIN HACK DAYS»**: Региональный форум инновационных проектов «Sorokin StartUP — 2022» (Сыктывкар, 29 ноября — 1 декабря 2022 года). Форум практической информационной безопасности «Sorokin Hack Days — 2022» (Сыктывкар, 16 декабря 2022 года) : сборник материалов / отв. ред.: Ю. В. Гольчевский, В.А. Устюгов. — Сыктывкар: Изд-во СГУ им. Питирима Сорокина, 2022. — 42 с.

ISBN 978-5-87661-781-1

В сборник вошли материалы Регионального форума инновационных проектов «Sorokin StartUP − 2022», а также Форума практической информационной безопасности «Sorokin Hack Days − 2022». Тематика статей охватывает актуальные вопросы развития и внедрения инноваций, развития информационных технологий и цифровой трансформации, а также разработки проектов в области информационной безопасности.

Сборник адресован студентам, аспирантам, преподавателям, а также всем интересующимся вопросами развития студенческой науки.

За достоверность сведений, изложенных в статьях, ответственность несут авторы публикаций, а также научные руководители. Мнение редакционной коллегии может не совпадать с мнением авторов.

УДК 351:35.088.7
ББК 67.401

ISBN 978-5-87661-781-1 © ФГБОУ ВО «СГУ им. Питирима Сорокина», 2022

ОГЛАВЛЕНИЕ

РАЗДЕЛ I
SOROKIN STARTUP

А. Ю. Боровлёв,
обучающийся гр. 112-ПИо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Автоматическая классификация данных дистанционного зондирования Земли для актуализации лесных потерь

Аннотация. *В статье рассматривается разработка алгоритма автоматизированной классификации данных дистанционного зондирования при мониторинге лесных экосистем на базе свободно распространяемой геоинформационной системы Quantum GIS (QGIS) и доступных пространственных данных. Введённая система оценки рисков при лесозаготовке, интегрированная в ГИС, позволяет выявлять нарушения, допущенные при лесохозяйственной деятельности, а также проводить грамотное планирование, позволяющее минимизировать воздействие на лесные экосистемы. Однако доступные данные по потерям лесного фонда (вырубки, ветровалы и лесные пожары) обновляются один раз в год, что приводит к возникновению потребности актуализировать информацию за определенные промежуточные периоды. В рамках исследования приведен алгоритм автоматизированной классификации мультиспектральной космосъемки с применением метода кластерного анализа.*

Ключевые слова: *геоинформационные системы, пространственные данные, космосъемка, геоаналитика, лесоуправление, классификация, мультиспектральные данные, лесозаготовка, лесная сертификация*

Если рассматривать лесозаготовку как фактор антропогенного преобразования ландшафта, общее негативное воздействие можно классифицировать по тем функциям, на которые оказывается влияние: средообразующая (или сохранение биоразнообразия), водорегулирующая и почвозащитная [2]. Чтобы минимизировать экологические последствия лесохозяйственной деятельности на всех этапах — начиная от планирования рубки на этапе отвода делянки и заканчивая рекультивационными работами в последующие годы после лесозаготовки — разработаны стандарты лесоуправления, которые включают в себя ряд параметров. Фундаментальной основой для критериев служат стандарты как Добровольной лесной сертификации FSC, так и введенной в 2022 году сертификации системы «Лесной эталон» [4].

Вышеуказанные системы контроля за поддержанием устойчивого лесопользования требуют проведения как внутренних аудитов со стороны предприятия, так и внешних аудитов, осуществляющихся силами контролирующих органов. В рамках этих процессов необходима организация дистанционного мониторинга за состоянием лесопользования.

Классический алгоритм как экспертного (когда подготовленный специалист проводит визуальную оценку), так и автоматизированного (посредством машинного зрения) дистанционного мониторинга базируется на использовании космической съемки. Зачастую оптимальным вариантом являются мультиспектральные данные дистанционного зондирования Земли среднего пространственного разрешения (от 10 до 30 метров на пиксель). Наличие инфракрасного спектра в изображении позволяет провести более качественное дешифрирование местности, а средняя детальность растровых данных обеспечивает их небольшой размер (до 1 Гб) и оперативную аналитику в геоинформационной системе.

Однако мультиспектральные данные позволяют усовершенствовать процесс оценки выявления лесных потерь. Вышеупомянутый инфракрасный спектр космической съемки предоставляет возможность преобразования исходного спутникового изображения в индексированный растр. Оптимальный инструмент — вегетационный индекс. В рамках данной работы применялся нормализованный относительный вегетационный индекс NDVI (Normalized Difference Vegetation Index). Это числовой показатель качества и количества растительности на исследуемом участке [3]. Он зависит от того, как растения отражают и поглощают различные световые волны разной длины. К примеру, здоровое растение активно поглощает видимую красную область спектра и отражает ближний инфракрасный диапазон. Именно за счет разности отраженной и поглощенной областей спектров можно выявить, на каких участках ландшафта процесс фотосинтетической активности соответствует здоровой зеленой биомассе, а где происходят процессы деградации. Индекс варьируется от -1 до 1, где значения до 0.15 сигнализируют об отсутствии вегетации (например, открытая почва), а после 0.15 показывают разные стадии развития или деградации экосистемы [1].

Если говорить о лесных потерях, как антропогенной (вырубки), так и естественной (пожары, ветровалы) природы, NDVI будет как количественный, так и качественный показатель трансформации ландшафта. К примеру, свежие лесозаготовки на индексированном с помощью вегетационного

индекса космоснимке можно классифицировать как объекты с открытой почвой (рис. 1).

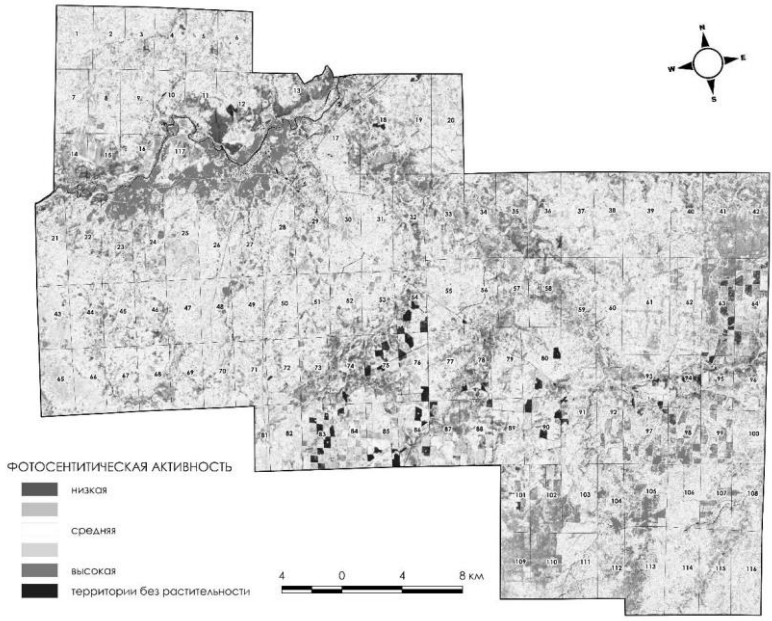

Рис. 1. Индекс NDVI, позволяющий визуализировать свежие лесозаготовки

Главное преимущество использования вегетационного индекса — это оптимизация автоматизированной классификации растрового изображения. В случае использования исходного мультиспектрального космоснимка при классифицировании можно допустить ряд ошибок, связанных с большим набором данных спектрально-яркостных характеристик пикселей. Помимо стандартных количественных значений красного, синего и зеленого цветов, в пикселе присутствуют также значения инфракрасных каналов. Индекс NDVI индексирует каждый пиксель одним значением (как говорилось выше — от -1 до 1), что позволяет избежать ошибок при классификации и не допустить появление визуальных артефактов.

В ходе данной работы классификационная обработка индексированного растрового изображения заключалась в кластеризации по спектральным признакам — методом k-средних в программе QuantumGIS с заранее предустановленным набором инструментов OrfeoToolBox. Суть метода заклю-

чается в том, что назначается определенное количество классов, на которые необходимо разбить общую совокупность всех пикселей. На первом этапе задается определенный порог разбиения точек изображения на классы (кластеры), каждый пиксель помещается в ближайший к нему кластер. Далее вычисляются центры тяжести новых кластеров и после этого алгоритмы повторяются, пока не будет найдена стабильная конфигурация классифицированного изображения [5].

Векторизация кластеров, отвечающих за лесные потери, позволяет провести аналитическую работу по выявлению наличия, к примеру рубок, в защитных лесах, около биологически ценных экосистем, а также рассчитать количественные показатели площади лесозаготовок.

Общий алгоритм методики приведет на рис. 2.

Рис. 2. Блок-схема общего алгоритма методики автоматизированной классификации данных ДЗЗ

***

1. Biswajit Nath. Forest Cover Change using Normalized Difference Vegetation Index (NDVI): A Study of Reingkhyongkine Lake's adjoining areas, Rangamati, Bangladesh / Biswajit Nath, Shkula Acharjee // Indian Cartographer. 2013. Vol. 33. Pp. 348-353.

2. Боровлёв, А. Ю. Оценка долговременного воздействия сплошных рубок леса на водные ресурсы в средней подзоне тайги Республики Коми / А. Ю. Боровлёв, Ю. А. Паутов // Устойчивое лесопользование. 2020. № 1(80). С. 10–16.

3. Карпов, А. А. Разработка методики для перевода лесных земель в покрытые лесом земли дистанционными методами / А. А. Карпов и др. // Сибирский лесной журнал. 2019. № 6. С. 19–26.

4. Система добровольной лесной сертификации «Лесной эталон» // Собственные стандарты системы «Лесной эталон». URL: https://standart.fsc.ru/wp-content/uploads/2022/08/Лесоуправление-СТО-42952298-001-2022.pdf.

5. Тарасенко, В.В. Отработка методики дешифрирования данных дистанционного зондирования для построения карт лесного покрова карельской части Прибеломорья / В. В. Тарасенко, Б. В. Раевский // Труды Карельского научного центра РАН. 2019. № 1. С. 87–99.

***В. В. Ермаков*[1],**
обучающийся гр. 122-ПИо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Проектирование и разработка геймификацированного органайзера

Аннотация. *Описывается проект разработки и создания геймификацированного органайзера.*

Ключевые слова: *геймификация, органайзер, мобильное приложение*

В нашей жизни существует множество повседневных рутинных дел. Для того чтобы избавиться от накопленного этими делами стресса, многие люди проводят досуг за видеоиграми. В среднем по статистике каждый четвертый играет в видеоигры на разных устройствах: из 18–24-летних россиян периодически играют 56 % опрошенных, а ежедневно проводят время в виртуальном мире около 20 % [1].

Цель проекта: выполнить проектирование и разработку органайзера с использованием игровых элементов для мобильных устройств. Задачей такого проекта является ассоциация повседневных дел реальной жизни с заданиями в компьютерных играх. Все занятия, дела, обязанности, которые требуется выполнить на работе или дома, в органайзере представляются как квесты некоторой RPG-игры, успешное завершение которых развивает главного героя. Также игрок может получать задания от неигрового персонажа с последующей наградой или может делать работу, которую пользователю, как герою survival-игры, придется выполнить, чтобы «прожить» еще один день. То есть требуется внести элементы геймификации в органайзер.

[1] Научный руководитель Гольчевский Ю. В., канд. физ.-мат. наук, доцент ФГБОУ ВО «СГУ им. Питирима Сорокина», г. Сыктывкар, Российская Федерация.

Простыми словами, геймификация — это применение игровых механик для неигровых процессов [2]. В качестве примера приведем приложение для бега Zombies, Run! 11 или Zombies, Run! 5k Training 2. Часто люди говорят себе фразу: «Завтра с утра начинаю бегать». На следующий день они признают, что не могут (не хотят) сдержать свое обещание. Поэтому компания Six to Start создала приложение, повышающее мотивацию бегать. Каждый день пробежки на улице — это не просто попытка приучить себя к здоровому образу жизни, а опасная вылазка человека в постапокалиптическом мире, где игрок собирает полезные ресурсы, отстраивает свою базу, и каждый новый день приближает его к возрождению цивилизации. Это звучит как опасное, но невероятно интересное приключение, которое стимулирует пользователя по крайней мере попробовать поучаствовать в этом «эксперименте».

Термин «геймификация» был использован в 2002 г. британским разработчиком видеоигр Ником Пеллингом, запустившим стартап по применению игровых технологий в корпоративных сервисах [3]. Сейчас этот прием можно считать трендом, так как применяется во многих сферах деятельности: управление персоналом в бизнесе, повышение лояльности клиентов в маркетинге, обучении, саморазвитии [4–6]. Приемы геймификации распространились в мобильных приложениях, например:

Kahoot — проведение викторин, анкетирования, тестов и иных проверочных мероприятий;

Cake, Duolingo, Fluyo — изучение иностранного языка;

NeuroNation — образование людей на тему различных областей ментального здоровья;

Mimo: научись программировать.

Отметим, что идея создания геймифицированного органайзера не нова, и подобные приложения существуют, например приложение Do it Now. По задумке, в нем есть герой — это представление самого себя в виртуальном RPG-мире. У героя есть навыки, характеристики, опыт и золото, он может повышать свой уровень, выполняя задачи [7].

Предполагается, что предлагаемое приложение представляет собой совокупность функций типичного негеймифицированного органайзера с доработкой новых и включением игровых техник. Интерфейс состоит из семейства вкладок со своими функциями. Главной вкладкой выступает страница с перечнем задач, которые необходимо выполнить пользователю.

Также на этой странице присутствует возможность отметки выполнения задачи. Предполагается механизм создания задач со следующими параметрами:

Подпункты задач обычного органайзера (время, регулярность выполнения, к какой группе задач относится задача, наличие подзадач, тегов и т. д.)

Очки опыта, получаемые при выполнении или провале задания. Количество очков формируется из дополнительных подпунктов, каждый из которых является процентным значением: сложность, срочность, важность и прочие. Количество подпунктов пользователь может изменять.

Количество монет, наименование предметов, получаемых при выполнении задания.

Выбор навыков, на которые влияет выполнение задания. Навыки — параметры, характеризующие «героя» в органайзере. Наименование навыков также формируется самим игроком. В то же время допускается идея их установки разработчиком для большего удобства. Каждому из параметров присваивается процент от опыта, получаемого за выполнение задачи.

Штрафы за невыполнение задачи. Игрок может указать в качестве стимула, что в случае невыполнения задания он теряет некоторую долю опыта, например, назначенного за его выполнение.

Задача представляет одну из обязанностей, которую пользователь должен выполнить в реальной жизни. Рассмотрим на конкретном примере: «сделать отжимания».

Игрок указывает время, например «8:00», периодичность — каждый день, по-своему усмотрению может указать тег «спорт». Для установки опыта он выбирает следующие параметры (как пример): сложность — 90 %, срочность — 20 %, важность — 110 % (значение может быть больше 100 %). Итого, игрок получит 0.9 * 0.2 * 1.1 * k (где k — любой коэффициент, например, 1000) = 0.198 * 1000 = 198 очков опыта. Количество монет указывается произвольное, допустим, 5 монет. В качестве прокачиваемых навыков можно указать «силу», «ловкость» (если это все разные параметры) и присвоить им 70 %, 100 %, 40 %. Получив достаточное количество опыта и повысив навык, игрок получает новый уровень. После выполнения задачи игрок получает опыт и выбранную награду, которую он может потратить в «магазине».

Магазин — вкладка приложения, в которой предлагаются товары с возможностью их приобретения за монеты. Эти товары представляют собой услуги, которые пользователь может себе позволить в реальной жизни, например: разрешение съесть что-нибудь сладкое, провести дополнительное время за компьютером, посмотреть сериал и прочее. Таким образом, реализуется система дисциплинирования и поощрения пользователя.

Для создания приложения планируется использовать ряд технологий, связанных с разработкой мобильных приложений. Также необходимо обрабатывать (хранить и взаимодействовать) достаточно большой объем данных, что обусловливает потребность в СУБД, например PostgreSQL.

Данный проект для всех участников будет иметь свою особую пользу. Например, для пользователей — это выработка дисциплины, а также доступный и условно-бесплатный способ ее развития и поддержания. Такое приложение можно использовать для небольшой компании для назначения задач, с возможной оплатой выполнения по результатам «развития» героя.

***

1. ВЦИОМ посчитал геймеров в России [Электронный ресурс]. URL: https://ruposters.ru/news/20-07-2022/vtsiom-poschital-geimerov-rossii (дата обращения: 28.10.2022).

2. Геймификация в бизнесе. Основы // РБК Тренды [Электронный ресурс]. URL: https://habr.com/ru/post/511426/ (дата обращения: 30.10.2022).

3. Ветушинский, А. С. Больше, чем просто средство: новый подход к пониманию геймификации / А. С. Ветушинский [Электронный ресурс]. URL: https://socofpower.ranepa.ru/files/docs/3_2020/1.pdf (дата обращения: 01.11.2022).

4. Диева, А. А. Геймификация бизнес-процессов: социологический анализ передовых управленческих практик / А. А. Диева [Электронный ресурс]. URL: https://journals.rudn.ru/sociology/article/view/24545/ru_RU (дата обращения: 01.11.2022).

5. Making Sense of Gamification in Loyalty Programs [Электронный ресурс]. URL: https://www.oracle.com/a/ocom/docs/spark-series-making-sense-of-gamification-in-loyalty-programs.pdf (дата обращения: 01.11.2022).

6. How to use gamification to encourage participation, engagement, and customer loyalty // Modern Marketing Blog [Электронный ресурс]. URL: https://blogs.oracle.com/marketingcloud/post/gamification-encourage-participation-engagement-customer-loyalty (дата обращения: 01.11.2022).

7. Руководство приложения “Do it Now” [Электронный ресурс]. URL: https://play.google.com/store/apps/details?id=com.levor.liferpgtasks (дата обращения: 30.10.2022).

М. В. Замыслов*[2]*,
обучающийся гр. 112-ПИо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Проектирование информационной системы «Чат-бот путеводитель по СГУ им. Питирима Сорокина»

Аннотация. *Современный университет представляет из себя развитый кампус, в связи с этим часто могут возникать проблемы ориентирования у студентов и гостей университета. В этой связи задача ориентирования в учебных корпусах университета с использованием современных коммуникационных средств считается актуальной. К наиболее современным средствам коммуникации относятся чат-боты, именно поэтому задача будет решаться с их помощью.*

Ключевые слова: *университет, чат-бот, «ВКонтакте», Python, автоматизация*

Достаточно часто студенты первого курса в начале обучения, а также гости (например, родители студентов, слушатели дополнительных образовательных программ) сталкиваются с проблемой ориентирования в учебных корпусах университета, что можно и нужно решать.

Например, МФ МГТУ им. Н.Э. Баумана имеет собственный веб-ресурс с интерактивной картой учебного корпуса [1], показанный на рис. 1.

Рис. 1. Интерактивная карта МФ МГТУ им. Н.Э. Баумана [1]

[2] Научный руководитель В. В. Миронов, канд. физ.-мат. наук, доцент ФГБОУ ВО «СГУ им. Питирима Сорокина» г. Сыктывкар, Российская Федерация.

Также студенты молодежной IT-лаборатории на базе СПбГЭТУ «ЛЭТИ» представили свое решение на основе трехэтапного построения интерактивной карты [2].

Решением данной проблемы может являться создание информационной системы (далее ИС), которая покажет и подскажет правильную и короткую дорогу до того или иного объекта в учебном корпусе. Данная ИС реализуется в виде чат-бота в социальной сети «ВКонтакте», которая будет выводить маршрут в виде наглядных карт и текстового описания пути. Пример работы такого чат-бота показан на рис. 2.

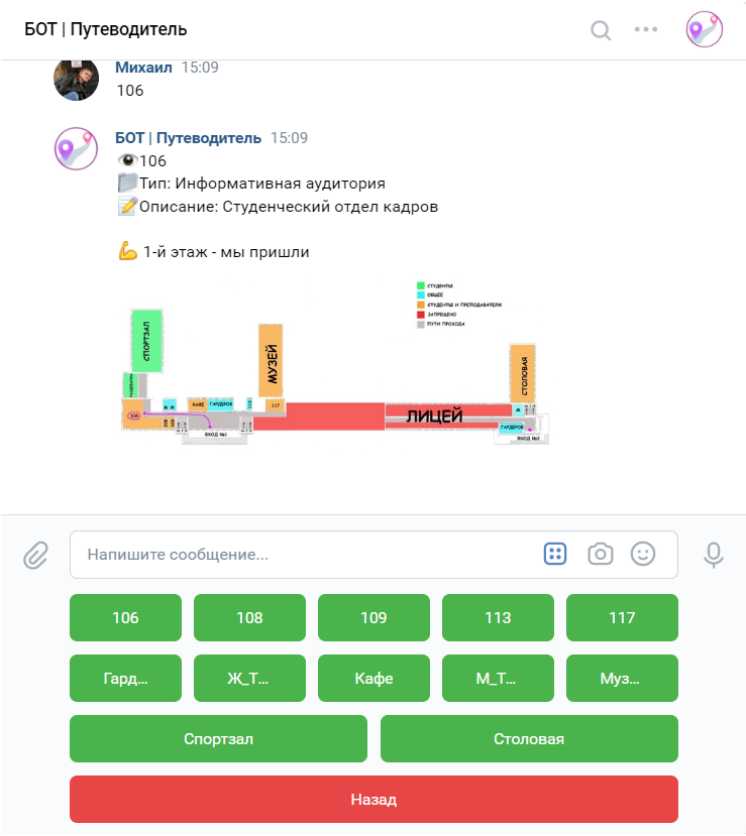

Рис. 2. Пример вывода маршрута

Чтобы студенту найти ту или иную аудиторию среди множества других, потребуется указать ее при помощи интерактивной пользовательской

клавиатуры, пример которой показан на рис. 2, в следующей последовательности: выбор учебного корпуса — выбор этажа — выбор аудитории. Также пользователю предоставляется возможность ручного поиска аудитории и в случае нахождения ее в базе данных (далее БД) получить маршрут к ней, начиная от главного входа.

Существует достаточно много способов для нахождения кратчайшего маршрута [3]: «Поиск в ширину», Алгоритм Дейкстры, «Поиск в глубину», «Лучший-первый», «Разделяй и властвуй», Алгоритм Креша, Алгоритм А. Указанные выше алгоритмы подходят для решения данной задачи, но так как в данном случае не требуется построение маршрутов в реальном времени, то можно найти более простое решение.

Для формирования маршрута предполагается применить алгоритм, основанный на нахождении минимального расстояния между двумя точками по их координатам:

программа проверяет наличие нужной пользователю аудитории и берет ее координаты на отрисованной карте из БД;

программа находит все ближайшие к искомой аудитории точки поворотов линии по стандартной формуле нахождения расстояния между двумя точками по координатам;

после нахождения всех нужных точек поворота программа начинает прорисовывать маршрут от начала пути (всегда это главный вход) до нужной аудитории, обозначая ее как конечную точку маршрута.

Пример визуализации карты и описанных элементов изображен на рис. 3. Алгоритм начинает расчет от входа (самая нижняя точка), затем находит ближайшие точки поворота, в нашем случае их 2, затем выстраивает по ним маршрут фиолетовой линией.

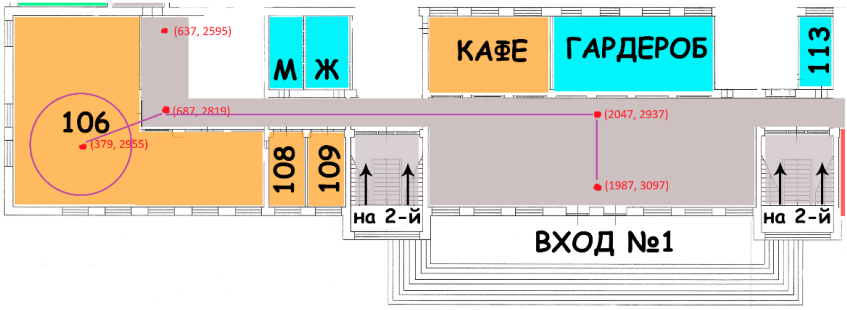

Рис. 3. Нахождение маршрута до аудитории под номером 106

Для отображения маршрутов используем заранее загруженные на сервер «ВКонтакте» карты, чтобы пользователь мог получить маршрут в кратчайшие сроки.

Выбор социальной сети «ВКонтакте» в качестве платформы обусловлен ее высокой популярностью на территории России [4]. Помимо этого, она обладает собственным API, который отличается обширным функционалом, сопоставимым с реальным функционалом самой социальной сети.

В случае успешного опыта применения такого чат-бота он может быть перенесен и в мессенджер Telegram, который также обладает большим функционалом и имеет большое количество пользователей.

Что касается ресурсов, то данный чат-бот разработан при помощи языка программирования Python с применением библиотек VK API, Pillow и реляционной СУБД MS SQL Server. При создании чат-бота для Telegram планируется использовать PyTelegramBotAPI.

Образовательная организация от внедрения данного решения получает, в первую очередь, нефинансовые выгоды, которые заключаются в повышении лояльности, развитии эффективности кампусной системы университета, уменьшении нагрузки на административный и обслуживающий персонал.

Данный проект является частью программы по ускоренной адаптации студентов первого курса в учебный процесс и программы цифровой трансформации Университета, чат-бот является частью экосистемы чат-ботов СГУ им. Питирима Сорокина [5].

***

1. МФ МГТУ им. Н.Э. Баумана [Электронный ресурс]. URL: https://map.msfu.ru (дата обращения: 08.10.2022).

2. SmartMap — электронная навигация для университета [Электронный ресурс]. URL: https://kursach37.com/oformlenie-spiska-literatury-po-gost/ (дата обращения: 08.10.2022).

3. Клочкова, Е. Н. Обоснование выбора алгоритма поиска пути решения задач построения маршрута к месту назначения / Е. Н. Клочкова // Вестник Московского университета МВД России. 2015. № 5. С. 205–209.

4. Горбатов, А. В. Социальные сети / А. В. Горбатов // Труды Института государства и права Российской академии наук. 2011. № 6. С. 182–193.

5. Замыслов, М. В. Проектирование информационной системы «Экосистема чат-ботов СГУ им. Питирима Сорокина» / М. В. Замыслов // Материалы молодежной научной конференции, посвященной памяти Н.А. Фролова. Сыктывкар: Изд-во СГУ им. Питирима Сорокина, 2022.

Е. Ю. Турышев, И. Д. Захаров[3],
обучающиеся гр. 131-ПИо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Работа с СЗИ от НСД на отечественных операционных системах

Аннотация. *В данной работе изучается возможность применения отечественных средств защиты от несанкционированного доступа (далее СЗИ от НСД) на операционных системах (далее ОС) российской разработки и оценивается степень готовности программных средств к такому варианту эксплуатации. Проводится оценка безопасности подобных решений.*

Ключевые слова: *СЗИ от НСД, защита информации, отечественные операционные системы, импортозамещение, Secret Net LSP*

В 2014 г. обострившаяся политическая ситуация и последовавшие за ней санкции западных стран привели к тому, что российское правительство стало выделять импортозамещение в качестве одного из приоритетных направлений деятельности и развития.

Отдельное обсуждение направления отечественного программного обеспечения состоялось в рамках XIII Российского инвестиционного форума. По его итогам Дмитрий Медведев дал поручения о разработке мер поддержки отечественного ПО и по формированию комплекса мер по импортозамещению ПО, используемого для государственных и муниципальных нужд [1].

29 июня 2015 г. Президент России Владимир Путин подписал разработанный Минкомсвязи федеральный закон № 188 о создании единого реестра российского программного обеспечения. Закономерным развитием событий стало вышедшее за ним постановление Правительства РФ от 16 ноября 2015 г. № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд», которое вступило в силу с 1 января 2016 г.

В 2019 г. был утвержден федеральный проект «Информационная безопасность». Согласно его паспорту, доля российского софта, используемого госкомпаниями, в 2021 г. должна была составить от 50 %. Однако по

[3] Научный руководитель М. А. Виноградов, ФГБОУ ВО «СГУ им. Питирима Сорокина», г. Сыктывкар, Российская Федерация.

данным центра компетенций по импортозамещению в сфере ИКТ концу 2021 г. этот показатель находился на уровне 30–35 % [2].

В феврале-марте 2022 г. в результате ухода с российского рынка некоторых производителей ПО потребность перехода на отечественные аналоги возросла. Так, 4 марта компания Microsoft, производитель популярной ОС Windows, объявила об остановке продаж [3], вследствие чего работа на Windows в государственных и муниципальных организациях официально стала невозможной. Обострились угрозы информационной безопасности, участились атаки на ресурсы Российской Федерации.

Таким образом, проблема адаптации СЗИ от НСД под отечественные ОС проявляется на сегодняшний день особенно остро.

В этой работе оценим степень готовности перехода программных средств защиты информации на отечественные ОС. В рамках данного проекта исследуемым продуктом стало СЗИ от НСД Secret Net LSP (5 класс защиты СВТ, сертификация защиты АС отсутствует [4]). Это версия продукта Secret Net Studio для ОС на базе Linux. В спецификациях указано, что поддерживаются все основные отечественные разработки (Альт, РЕД ОС, Astra и Лотос) [5], правда не в последних актуальных версиях, так, версии ядра Linux, поддерживаемых ОС, достаточно сильно отстают. Отметим, что класс предоставляемой защиты не подойдет для обработки информации, содержащей служебную тайну (класс 1Г АС).

В рамках данного проекта было предложено установить и настроить Secret Net LSP на одну из ОС отечественной разработки. Все операции производились согласно официальной сопровождающей документации по развертыванию.

Кратко можно отметить, что в ходе исследования были выявлены следующие проблемы:

В случае блокировки рабочей станции этим ПО требуется физическое присутствие администратора для последующей разблокировки, что не всегда представляется возможным в больших организациях.

Были зафиксированы случаи неснимаемой блокировки, но закономерность появления такого состояния выявить не удалось, предположительно, ошибка может относиться к использованию системы виртуализации VMware ESXi.

Отсутствие серверной версии СЗИ. Решение для централизованной настройки присутствует в Secret Net Studio, но оно выпускается только под операционные системы семейства Windows.

Так, работа с СЗИ от НСД на отечественных операционных системах возможна, но на примере Secret Net LSP можно выделить ряд недостатков, касающихся как особенностей настройки ПО, так и отсутствия ряда необходимых в коммерческих и государственных сценариях использования функций. Отметим, что руководство по развертыванию рассматриваемой СЗИ на любую из отечественных ОС отсутствует, хотя качество существующих руководств находится на высоком уровне. Стоит упоминания вариант использования встроенных в сертифицированные ФСТЭК ОС модулей СЗИ от НСД, которые имеют широкое применение в области обеспечения безопасности на коммерческом и государственном уровне, но такие системы проприетарны и не позволяют поддерживать высокий уровень вариативности настройки компонентов IT-инфраструктуры предприятия.

Оценка эффективности применения подобных решений и разработка некоторых дополнительных рекомендаций будут являться предметом для изучения в дальнейшем исследовании и обсуждении.

***

1. Поручения по итогам XIII Сочинского инвестиционного форума // Правительство России [Электронный ресурс]. URL: http://government.ru/orders/selection/401/14972/ (дата обращения: 18.11.2022).

2. Доля российского софта в госкомпаниях оказалась вдвое ниже нормативов [Электронный ресурс]. URL: https://www.rbc.ru/technology_and_media/27/12/2021/61c21e289a79479e8562641b (дата обращения: 17.11.2022).

3. Microsoft suspends new sales in Russia [Электронный ресурс]. URL: https://blogs.microsoft.com/on-the-issues/2022/03/04/microsoft-suspends-russia-sales-ukraine-conflict/ (дата обращения: 18.11.2022).

4. Сертификаты соответствия ФСТЭК № 2790 [Электронный ресурс]. URL: https://www.securitycode.ru/upload/iblock/588/2790.pdf (дата обращения: 19.11.2022).

5. Системные требования Secret Net LSP 1.10.1 [Электронный ресурс]. URL: https://www.securitycode.ru/products/szi_secret_net/?tab=system (дата обращения: 19.11.2022).

6. Сертификаты соответствия ФСТЭК №3594 [Электронный ресурс]. URL: https://wikisec.ru/index.php?title=Сертификат_ФСТЭК_3594 (дата обращения: 19.11.2022).

Л. С. Шадрин*[4]*,
обучающийся гр. 112-ПИо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Проектирование системы автоматического хронометража на платформе Arduino

Аннотация. *Описывается проект разработки и создания системы автоматического хронометража на основе платформы Arduino.*

Ключевые слова: *проектирование, автоматический хронометраж, ардуино, приборостроение, автоматические системы*

Системы хронометража повсеместно используются при судействе в циклических видах спорта, когда необходимо фиксировать время прохождения дистанции каждым из участников. Для исключения человеческого фактора и повышения точности замера повсеместно используются системы автоматического хронометража. К тому же подобные системы позволяют заметно увеличить скорость работы судейской бригады и дают возможность получать результаты состязания в режиме реального времени. Ярким представителем вида спорта, в котором системы автоматического хронометража получили широкое распространение, является легкая атлетика. Правила использования подобных систем в данном виде спорта регламентируются правилами IAAF [1].

Предлагаемая система автохронометража построена на базе платы «Искра JS». Данная плата совместима по компоновке со стандартом Arduino Uno R3, что позволяет использовать модули и платы расширения Arduino. Подробное описание технических характеристик, а также возможностей платы представлено на сайте фирмы-изготовителя [2].

Использование платформы Arduino в данном проекте обладает рядом преимуществ. В частности, неоспоримым плюсом является большое сообщество и наличие документации, доступной на различных языках, что открывает большой потенциал для экспериментов, комбинаций различных модулей, а также позволяет создавать продукт, ориентированный на выполнение узкоспециализированных задач [3].

[4] Научный руководитель Ю. В. Гольчевский, канд. физ.-мат. наук, доцент ФГБОУ ВО «СГУ им. Питирима Сорокина», г. Сыктывкар, Российская Федерация.

«Искра JS» — плата со встроенным интерпретатором языка JavaScript. Написание кода на языке JavaScript заметно упрощает разработку системы в силу того, что он проще в отличие от строго-типизированных языков. Для данной платы существуют библиотеки, которые позволяют легко подключать дополнительные устройства. Для системы хронометража могут быть использованы библиотеки @amperka/rtc — драйвер для работы с часами реального времени и @amperka/light-sensor — драйвер модуля сенсора освещённости. С полным списком библиотек, а также некоторыми аспектами функционирования и программирования системы можно ознакомиться на сайте фирмы-изготовителя и в работах [4–7].

Система автоматического хронометража состоит из трех блоков: один блок для старта и два блока финиша. Устройство блока старта состоит из следующих элементов: элемент питания, кнопка включения, беспроводная связь на базе микросхемы nRF24L01+, микрофон. Первый блок финиша состоит из элемента питания, кнопки включения и лазера, а второй блок состоит из элемента питания, кнопки включения, беспроводной связи на базе микросхемы nRF24L01+, фоторезистора, дисплея и кнопки сброса. Схема системы представлена на рис.

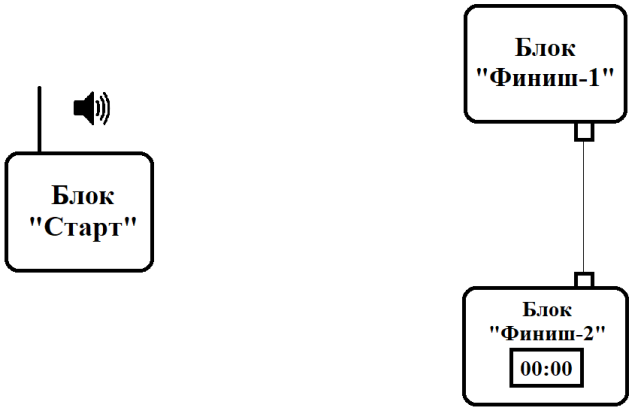

Рис. Схема системы автоматического хронометража

Передача сигнала между блоками осуществляется при помощи беспроводной связи. Для использования устройства необходимо включить первый блок финиша и навести лазер на фоторезистор второго блока финиша. Затем включается блок старта. Старт реагирует на резкий громкий звук, например хлопок или выстрел стартового пистолета, превышающий 50

условных единиц (громкость регулируется при программировании). При превышении этого порога на дисплее второго блока финиша запускается секундомер. Секундомер останавливается при пересечении лазера, когда фоторезистор регистрирует меньше 200 люкс. Когда свет лазера попадает на фоторезистор, то последний регистрирует значение в 7000 люкс. Для повторного использования необходимо произвести сброс секундомера на ноль посредством нажатия кнопки.

Таким образом, предлагаемая система не вызывает сложностей при эксплуатации. Использование платформы позволяет быстро устранять неисправности и поломки, а также дает большой потенциал к развитию данной системы. Прототип системы, разработанной в рамках проекта, протестирован в реальных условиях.

Система автохронометража, представленная в данном проекте, позволяет фиксировать время прохождения дистанции одного спортсмена. Было замечено, что систему можно усовершенствовать, например, фиксировать время прохождения какого-либо отрезка, а не всей дистанции, однако в этом случае система нуждается в доработке для фиксации времени на коротких дистанциях.

Часто возникают ситуации, когда спортсмены финишируют вплотную. При этом лазер может некорректно фиксировать время. Данную проблему можно решить при помощи использования отельного лазера для каждой дорожки, однако в таком случае необходимо синхронизировать старт всех секундомеров. Другим вариантом решения является использование RFID-меток в нагрудном номере каждого спортсмена. В таком случае время будет фиксироваться не с помощью лазерного луча, а с помощью электромагнитного импульса [8].

Стоимость комплектующих спроектированной системы составляет около 7 тысяч рублей, что делает ее весьма привлекательной для потребителя. Например, стоимость базового набора системы автохронометража Limetime превышает 300 тыс. руб. [9], а стоимость аналогичной системы от MyLaps начинается от 4000 евро [10].

Подобные системы хронометража весьма востребованы в настоящее время. Например, ими могут заинтересоваться коммерческие, некоммерческие и государственные организации, которые проводят спортивные мероприятия. Кроме этого, систему можно применять в научных и медицинских исследованиях в качестве альтернативы ручным измерениям.

***

1. Book of Rules: Book C-C2.1 «Technical Rules» [Электронный ресурс]. URL: https://www.worldathletics.org/about-iaaf/documents/book-of-rules (дата обращения: 05.10.2022).

2. Iskra JS: подключение, настройка, распиновка и схемы [Электронный ресурс]. URL: http://wiki.amperka.ru/js:iskra_js (дата обращения: 05.10.2022).

3. Блум Джереми. Изучаем Arduino: инструменты и методы технического волшебства : пер. с англ. СПб.: БХВ-Петербург, 2015. 336 с.

4. Начало работы с Espruino: JavaScript в микроконтроллере [Электронный ресурс]. URL: http://wiki.amperka.ru/js:start (дата обращения: 05.10.2022).

5. Espruino Hardware Reference [Электронный ресурс]. URL: http://www.espruino.com/Reference (дата обращения: 05.10.2022).

6. GitHub — amperka / Espruino at iskrajs [Электронный ресурс]. URL: https://github.com/amperka/Espruino/tree/iskrajs (дата обращения: 05.10.2022).

7. Дэвид Фленган. JavaScript. Подробное руководство, 6-е изд. : пер. с англ. СПб: Символ-Плюс, 2012. 1080 с.

8. Хабр. Система спортивного хронометража — взгляд изнутри [Электронный ресурс]. URL: https://habr.com/ru/post/366249/ (дата обращения: 11.10.2022).

9. Limetime.IO. Система автохронометража [Электронный ресурс]. URL: https://limetime.io/buy (дата обращения: 17.10.2022).

10. MyLaps. Система автохронометража [Электронный ресурс]. URL: https://mylaps.su/run/ (дата обращения: 17.10.2022).

***И. В. Щукина*[5],**
обучающаяся гр. 112-ПИо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Проектирование и разработка системы психодиагностических тестов для профессиональной ориентации и поиска кадров

Аннотация. *В данной работе представлены проектирование и разработка системы тестирования для профессиональной ориентации.*

Ключевые слова: *профессиональная ориентация, профориентационное тестирование, автоматизация профориентационного тестирования*

[5] Научный руководитель Ю. В. Гольчевский, канд. физ.-мат. наук, доцент ФГБОУ ВО «СГУ им. Питирима Сорокина» г. Сыктывкар, Российская Федерация.

Ранее в работе [1] нами уже отмечалось, что выбор профессии является сложным и, пожалуй, самым ответственным шагом для каждого человека. Существует большое разнообразие различных тестов и методик для психодиагностического исследования личности, дающих достаточно полное представление о человеке, его характере, поведении, навыках, особенностях. В среднем в каждом подобном тесте содержится примерно от 300 до 500 вопросов. При отсутствии автоматизации такие тесты отнимают достаточно много времени как у тестируемого, так и у эксперта, оценивающего ответы.

Создание системы тестирования позволяет не только сократить время на исследование личности и составление профессионального портрета, но и осуществлять поиск и подбор кадров работодателями, собирать статистические данные и прослеживать изменения профессиональных предпочтений абитуриентов в различных срезах. При этом с подобным сервисом, спроектированным и выполненным в виде веб-приложения, пользователь может взаимодействовать с любого устройства, которое имеет выход в сеть Интернет.

Цель данного проекта — выполнить проектирование и разработку информационной системы для проведения профориентационного тестирования и помощи специалистам в расшифровке и интерпретации личностного портрета. Практическая значимость заключается в том, что он позволяет решить актуальную проблему, связанную со сложностью и длительностью обработки результатов психодиагностического тестирования в процессе изучения профессиональной ориентации людей.

В данном проекте использовалась адаптация методики многостороннего исследования личности MMPI (Minnesota Multiphasie Personality Inven), разработанная в 1971 г. Л. Н. Собчик и другими психологами в Ленинградском психоневрологическом институте имени В. М. Бехтерева, получившая название «Стандартизированное многофакторное исследование личности» (сокращенно — СМИЛ) [2].

Для того чтобы разрабатываемая система тестирования была наиболее конкурентоспособной и востребованной на рынке, необходимо устранить недостатки аналогичных продуктов, а также добавить новые возможности для веб-сервиса (например, возможность осуществлять поиск и подбор кадров работодателями, добавить модули взаимодействия между участниками профориентационного процесса, осуществлять работу с большими данными для сбора статистики и прослеживания изменений профессиональных предпочтений абитуриентов в зависимости от возраста и различ-

ных факторов социального окружения и другое). В процессе исследования существующих подобных систем тестирования были сформулированы наиболее общие их недостатки: отсутствие возможности вернуться к незавершенному тесту; отсутствие возможности просмотра результатов теста через некоторое время; отсутствие личного кабинета (для пользователя и для эксперта); отсутствие возможности получить комментарий от психолога-эксперта при неоднозначной интерпретации результатов теста; отсутствие описания профпортрета и направлений подготовки по подходящим специальностям; отсутствие возможности накапливать данные и проводить анализ в динамике.

Общая схема функциональных модулей предлагаемого веб-сервиса представлена на рис. 1. Всего выделено четыре основных функциональных модуля: регистрация и авторизация, тестирование, подбор образовательных программ и учебных заведений, администрирование.

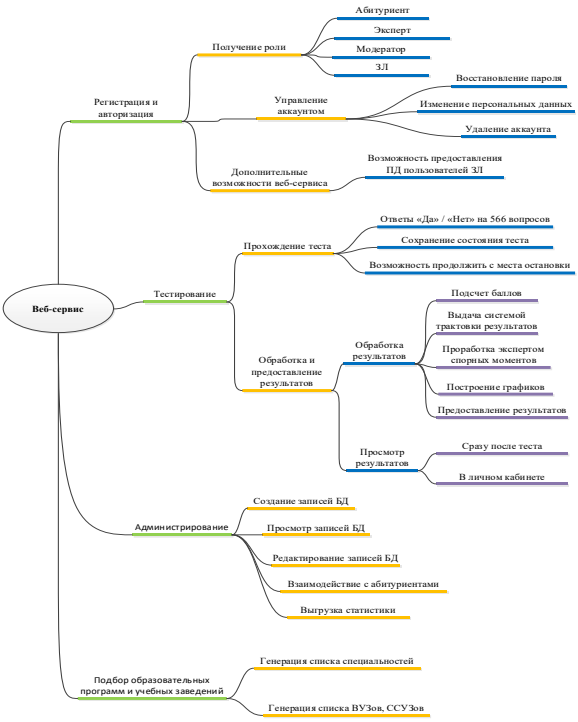

Рис. 1. Схема функциональных модулей веб-сервиса

Все работы по проекту можно условно разделить на четыре значимых группы, что показано на рис. 2.

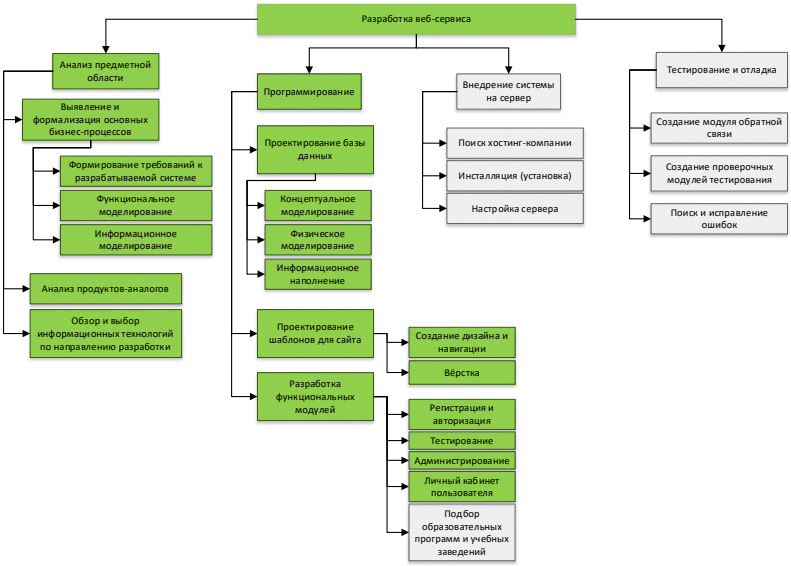

Рис. 2. Структура работ по проекту

При анализе необходимых для работы данных были выявлены основные сущности и построена концептуальная модель данных (см. рис. 3).

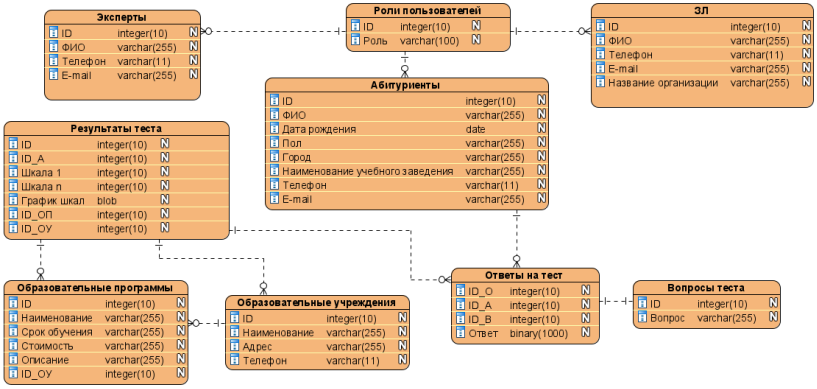

Рис. 3. Концептуальная модель базы данных

Реализованы прототип базы данных и наиболее важные интерфейсы, дающие возможность регистрации, пробного тестирования, получения итоговых баллов, включая пересчет баллов по методике СМИЛ, построена стратегическая карта BSC. Примеры интерфейсов показаны на рис. 4.

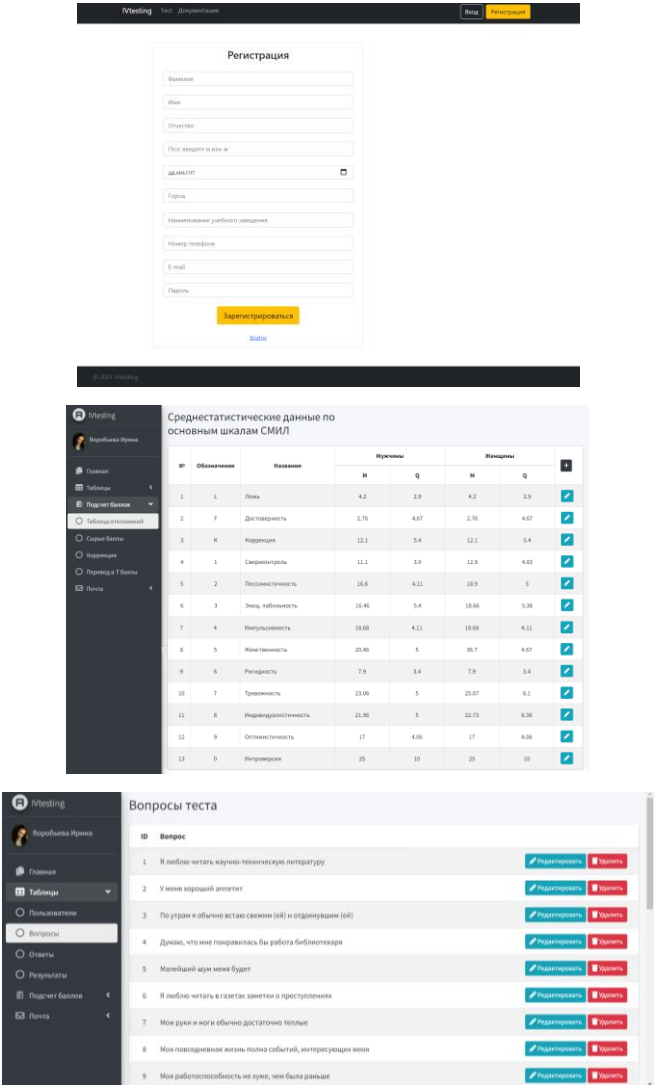

Рис. 4. Примеры разработанных в проекте интерфейсов

***

1. Воробьева, И. В. Проблема автоматизации психодиагностических тестов для профессиональной ориентации и поиска кадров / И. В. Воробьева // Наука молодых — устойчивое развитие Республики Коми : сборник научных трудов студентов и магистрантов. Сыктывкар: Изд-во СГУ им. Питирима Сорокина, 2022. С. 225– 230. DOI: 10.34130/9785876617361_224.

2. Собчик, Л. Н. Стандартизированный многофакторный метод исследования личности / Л. Н. Собчик / Методика. Миннесотский многоаспектный личностный опросник [Электронный ресурс]. URL: https://psycabi.net/testy/472-smil-566-mmpi-test-metodika-minnesotskij-mnogoaspektnyj-lichnostnyj-oprosnik-standartizirovannyj-mnogofaktornyj-metod-issledovaniya-lichnosti-sobchik-l-n (дата обращения: 11.11.2022).

РАЗДЕЛ II
SOROKIN HACK DAYS

Д. В. Суздалов, Н. А. Потехин,
обучающиеся гр.141-Ибо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Методологии проведения тестирования на проникновение в России и в зарубежных странах

Аннотация. *В современном и быстро развивающемся мире информационных технологий всё острее возникает необходимость в разработке и совершенствовании методов выполнения высококачественных тестирований систем на безопасность, которые охватывают весь спектр потенциально возможных угроз, при этом не усложняя процесс их проведения. В данной статье будут представлены некоторые из существующих методологий и стандартов по проведению тестирования на проникновение.*

Ключевые слова*: тестирование на проникновение, сети, защита, безопасность, пентест, аудит информационной безопасности*

Быстрые темпы цифровизации приводят к увеличению числа инцидентов в области кибербезопасности. Множество компаний подвергается атакам со стороны злоумышленников, и большинство таких попыток оказываются успешными. В связи с этим каждая организация старается построить себе надежную, как крепость, систему, которая будет способна уменьшить количество таких инцидентов. Самые распространенные способы решения поставленной задачи у большинства компаний — покупка специализированных программных продуктов и комплексов, но есть и те, кто считает, что их организация вполне может справиться штатными силами. Единственная точка соприкосновения взглядов выражается в предварительном проведении AAA-испытаний:

1. Аналитическая оценка построенной системы.
2. Аудит системы на наличие уязвимостей.
3. Анализ эксплуатационных последствий.

Такой подход к оценке безопасности получил броское и яркое жаргонное название «Пентест». В переводе с английского языка сокращение Pentest означает «Тестирование на проникновение».

Процесс тестирования на проникновение характеризуется активным анализом системы на наличие уязвимостей, а конечной его целью является выявление возможных уязвимостей и недостатков, способных привести не только к нарушению триады КДЦ (конфиденциальность, доступность, целостность) и прочим неблагоприятным последствиям, но и к ненужным для организации финансовым потерям. Стоит отметить, что тестирование может затрагивать как виртуальный уровень, так и физический.

Задача тестирования заключается в составлении подробного отчета заказчику. Отчет содержит не только найденные уязвимости, но и последствия их эксплуатации, а также рекомендации по устранению выявленных недостатков. Такой подход очень удобен следующим **категориям заказчиков**:

организациям, которым важно знать текущее состояние защищенности их систем и предотвратить возможное прерывание бизнес-процессов;

разработчикам, которые заботятся о пользователях и хотят обеспечить безопасный UX (User Experience).

В настоящее время благодаря быстрому развитию данного направления разработано и используется множество методологий, стандартов, а также сформировались лучшие мировые практики по проведению тестирования на проникновение. Большинство из методик признаны специалистами, но, что важнее всего, они упрощают проведение мероприятий по тестированию. Чтобы понять разницу между существующими методологиями, необходимо провести их сравнительный анализ (табл. 1).

Наиболее популярные из существующих зарубежных методик:

Web Security Testing Guide (WSTG) [8]:

Предоставляет пошаговую инструкцию для анализа защищенности веб-приложений.

Open Web Application Security Project (OWASP) [5]:

Методика ориентирована на тестирование веб-приложений. Имеет подробное описание тестирования веб-приложений и фактически является единственной подобной методикой, узко ориентированной именно на веб-приложения.

Open Source Security Testing Methodology Manual (OSSTMM) [4]:

Методология проверки операционной безопасности физических расположений технических устройств, человеческого взаимодействия и всех видов связи. Полезна для быстрого старта в данном направлении.

Information Systems Security Assessment Framework (ISSAF) [1]:

Методика разработана консорциумом OISSG (Open Information Systems Security Group) в качестве стандарта внутреннего аудита организаций этого консорциума, является наиболее подробной и применительна как на этапе предварительной оценки защищенности объектов сети в интересах проверки возможности их использования в составе какой-либо информационной системы, так и на этапе разработки объектов для проверки отдельных возможностей и функций ИБ.

Methodology of Information Systems Security Penetration Testing (PETA) [2]:

Методика является достаточно обзорной и определяет только самые общие подходы к проведению тестирования на проникновение, оставляя выбор конкретных целей тестирования, используемых тестовых ИТВ, и прочие параметры тестирования на усмотрение заказчика и аудитора.

Отечественная методика:

Методика Positive Technologies [10]:

Данную методику рекомендуется использовать для тестирования конечного продукта, уже введенного в эксплуатацию.

Стандарты, которые используются при проведении тестирований на проникновение за рубежом:

NIST SP 800-115 Technical Guide to Information Security Testing and Assessment [3]:

Стандарт можно использовать как на этапе предварительной оценки защищенности объектов, так и на этапе разработки объектов для проверки отдельных возможностей и функций ИБ. Также этот стандарт можно использовать как шаблон для разработки — какие стандартные функции обеспечения ИБ должны присутствовать в разрабатываемом объекте.

Penetration Testing Execution Standard (PTES) [6]:

Этот стандарт можно использовать как на этапе предварительной оценки защищенности объектов в интересах проверки возможности их использования в составе какой-либо информационной системы, так и на этапе разработки объектов для проверки отдельных их возможностей и функций ИБ.

Отечественный стандарт, который используется при проведении тестирований на проникновение:

ГОСТ Р 58143-2018. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соот-

ветствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения [9].

ГОСТ приводит рекомендации по стадиям тестирования на проникновение (планирование, разработка тестов, проведение тестирования, разработка отчетности).

Также представлен порядок действий по тестированию на проникновение в соответствии с различными потенциалами атакующего.

Таблица

Результаты сравнительного анализа отечественных и зарубежных методик тестирования на проникновение

Характеристика	*OSSTMM*	*ISSAF*	*OWASP*	*PETA*	*Postive Technologies*
1	*2*	*3*	*4*	*5*	*6*
Рекомендации по обсуждению с заказчиком целей и задач тестирования	+	+	+	-	-
Рекомендации по подготовке договора на тестирование	+	+	-	-	-
Законодательные аспекты тестирования	±	+	-	-	-
Рекомендации по сборе информации об объекте тестирования	+	+	+	±	+
Подробные рекомендации по анализу и оценке уязвимостей	±	+	+	-	±
Рекомендации по этапам тестирования и их содержанию	+	+	+	+	+
Отдельные рекомендации по тестированию телекоммуникационных сетей	+	+	±	-	+
Отдельные рекомендации по тестированию беспроводных сетей	+	+	-	-	+
Отдельные рекомендации по проверке безопасности физической инфраструктуры	+	+	+	-	-
Отдельные рекомендации по проверке безопасности баз данных	-	+	±	-	-
Рекомендации по конкретному ПО, используемому для тестирования	-	+	±	-	-

Окончание табл.

1	*2*	*3*	*4*	*5*	*6*
Рекомендации по формированию отчета о тестировании	+	+	+	-	-
Анализ и рекомендации по устранению найденных уязвимостей	-	+	-	-	-

Примечание: «+» — имеется в полном объеме; «±» — имеется в кратком изложении или упоминается; «–» — данный материал отсутствует либо изложен таким образом, что не представляет ценности для аудитора.

Пентест является неотъемлемой частью обеспечения безопасности, с его помощью заказчики могут не только выявить недостатки и уязвимости своих систем, но и в дальнейшем предотвратить возможные прерывания в бизнес-процессах, сохранить репутацию и не понести финансовые потери. Множественные вариации методологий и стандартов, разработанные для данного направления, а также их постоянное развитие и совершенствование облегчают процесс тестирования специалистам. Проведенный сравнительный анализ наглядно показывает, в чём заключается разница между существующими методологиями.

***

1. ISSAF — Information System Security Assessment Framework. 2006. 1264 с. [Электронный ресурс] // oissg.org URL: http://www.oissg.org/issaf02/issaf0.1-5.pdf (дата обращения: 09.09.2022).

2. Klíma, T. PETA: Methodology of information systems security penetration testing / T. Klíma // Acta Informatica Pragensia. 2016. Т. 5. № 2. С. 98–117.

3. NIST Special Publications 800-115. Technical Guide to Information Security Testing and Assessment. USA, Gaithersburg: 2008. 80 с. [Электронный ресурс] // nvlpubs.nist.gov URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата обращения: 09.09.2022).

4. OSSTMM 3 [Электронный ресурс] // isecom.org. URL: https://www.isecom.org/OSSTMM.3.pdf (дата обращения: 06.09.2022).

5. OWASP Testing Guide. Version 4. 2014 [Электронный ресурс] // owasp.org URL: https://www.owasp.org/index.php/OWASP_Testing_Project (дата обращения: 09.09.2022).

6. PTES — The Penetration Testing Execution Standard // Penetration Testing Execution Standard 30.04.2012 [Электронный ресурс] // pentest-standard.org. URL: http://www.pentest-standard.org/index.php/PTES_Technical_Guidelines (дата обращения: 09.09.2022).

7. Technical guide to information security testing and assessment [Электронный ресурс] // nvlpubs.nist.gov. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf (дата обращения 08.09.2022).

8. WSTG — v4.2 | OWASP Foundation [Электронный ресурс] // owasp.org. URL: https://owasp.org/www-project-web-security-testing-guide/v42/ (дата обращения: 06.09.2022).

9. ГОСТ Р 58143-2018. Национальный стандарт Российской Федерации. Информационная технология. Методы и средства обеспечения безопасности. Детализация анализа уязвимостей программного обеспечения в соответствии с ГОСТ Р ИСО/МЭК 15408 и ГОСТ Р ИСО/МЭК 18045. Часть 2. Тестирование проникновения (утв. и введен в действие Приказом Росстандарта от 24.05.2018 N 274-ст) [Электронный ресурс] // СПС «КонсультантПлюс» (дата обращения: 08.09.2022).

10. Тесты на проникновение // Positive Technologies [Электронный ресурс]. 2018 // ptsecurity.com. URL: https://www.ptsecurity.com/ru-ru/services/pentest/ (дата обращения: 09.09.2022).

***К. О. Акчурин*[6],**
обучающийся гр. 121-Ибо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Угрозы фишинга и методы противодействия

Аннотация. *Ошибки действий пользователей корпоративной сети зачастую имеют неблагоприятные последствия в отношении безопасности информации для компаний. В последнее время число удачных атак на корпоративные ресурсы компании растет за счет распространения злоумышленниками именно фишинговых ссылок. Поэтому одной из приоритетных задач компаний, направленных на противодействие угрозам безопасности информации, является организация процесса обучения пользователей методам распознавания фишинговых атак.*

Ключевые слова: *информационная безопасность, обучающий процесс, фишинг, персонал, угрозы информации*

В результате совершения фишинговой атаки на компьютеры сотрудников компании злоумышленники пытаются получить какую-либо конфиденциальную информацию и/или доступ к охраняемым корпоративным ресурсам. Атакующий, маскируясь под видом доверительного субъекта

[6] Научный руководитель Н. Р. Оленева, ст. преподаватель ФГБОУ ВО «СГУ им. Питирима Сорокина», г. Сыктывкар, Российская Федерация.

(письмо, сообщение, сайт), манипулируя психологией человека, заставляет его пройти по поддельной ссылке, ввести данные своей учетной записи для входа в систему или загрузить вредоносные файлы. В результате необдуманных действий ничего не подозревающий пользователь сам предоставляет доступ злоумышленнику к интересующей его конфиденциальной информации, которую он будет использовать для дальнейших мошеннических действий.

По данным отчёта от PhishMe следует, что 91 % всех кибератак приходится на фишинговые рассылки. 70 % кибератак используют комбинации фишинга и взлома.

Согласно исследованию Proofpoint, 75 % организаций по всему миру подверглись фишинговой атаке в 2020 г. Почти каждое пятое предприятие пострадало из-за кражи учетных данных.

Результаты исследования, проводимые «Лабораторией Касперского» за 2021 г., показывают, что наиболее «удачными» комбинациями психологических факторов для проведения успешной фишинг-атаки стали «любопытство+жадность» и «любопытство+страх» [1].

Согласно аналитике от Positive Technologies за IV квартал 2021 — I квартал 2022, 67 % атак носили целенаправленный характер: 16 % атак были совершены на госучреждения, 11 % на медицинские учреждения, 8 % на промышленные предприятия. Круговая диаграмма представлена на рис. 1.

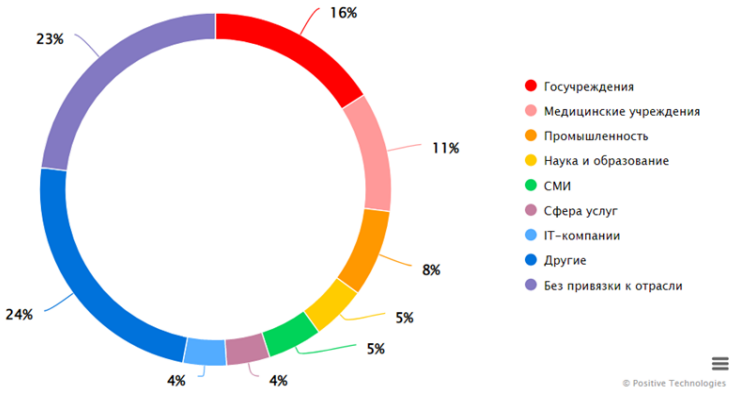

Рис. 1. Категории «жертв» среди организаций

В I квартале 2022 г. действия злоумышленников были преимущественно направлены на кражу конфиденциальной информации: для организаций это в первую очередь персональные данные (34 %) и сведения, составляющие коммерческую тайну (19 %). Также пользовались популярностью медицинская информация (14 %) и учетные данные (12 %). В атаках на частных лиц были украдены учетные данные (46 %), персональные данные (19 %) и данные платежных карт (21 %) [2].

На основании выше представленной статистики любая компания должна быть заинтересована в обучении пользователей методам распознавания фишинговых атак. Подобный процесс обучения пользователя можно представить в виде схемы, представленной на рис. 2.

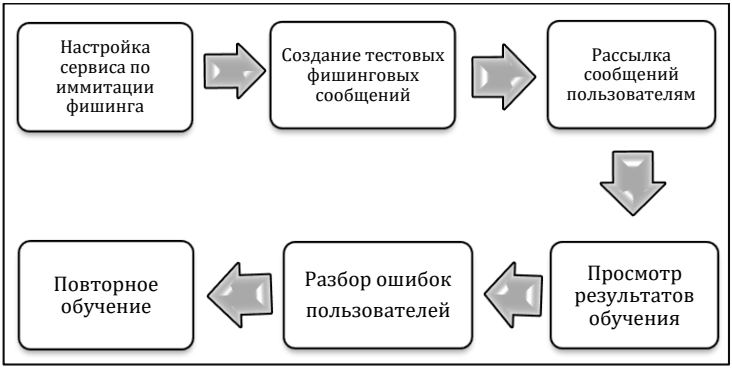

Рис. 2. Процесс обучения пользователя

Для моделирования обучающей фишинговой атаки компании могут воспользоваться бесплатным сервисом GoPhish [3]. Он позволит настроить воспроизведение действий потенциального злоумышленника и быстро выяснить реакцию сотрудников на фишинговые письма. Gophish осуществляет рассылку писем по заранее заданным шаблонам и спискам адресов электронной почты. Также данный сервис использует встроенный веб-сервер для отображения фишинговых страниц. Ссылки для перехода на данные страницы находятся в тексте писем. Для контроля за процессом фишинг-теста используется «компания» — она объединяет шаблон письма, список адресов пользователей, фишинговую страницу и набор параметров SMTP. После того как «компания» запущена, в интерфейсе можно просмотреть, кто из пользователей перешел по ссылке на фишинговую страницу, а кто нет.

После запуска консольная программа автоматически создает два сервера: фишинговый и админский. Создадим профиль, от имени которого будут рассылаться фишинговые письма. В компании в качестве отправителя можно использовать, например, имя и адрес электронной почты системного администратора.

Затем создадим тестовую группу пользователей-целей с указанием их электронных адресов и фишинговое письмо содержащим ссылку «ловушку». Далее создадим фишинговую страницу, которая будет собирать логины и пароли пользователей, произведем дополнительные настройки и запустим процесс имитации фишинговых атак для пользователей нашей компании.

Если пользователи перейдут по поддельным ссылкам «ловушкам», GoPhish запишет эти данные. Статистику пользователей, проваливших обучение, можно просмотреть на странице результатов данного сервиса.

***

1. Куликова, Т. Спам и фишинг в 2021 г. / Т. Куликова, Т. Щербакова // securelist.ru. URL: https://securelist.ru/spam-and-phishing-in-2021/104407/ (дата обращения: 01.10.2022).

2. Исследование Positive Technologies. Актуальные киберугрозы: I квартал 2022 г. / Исследование Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2022-q1/ (дата обращения: 01.10.2022).

3. Царёв, Е. GoPhish: Бесплатная фишинг-платформа для обучения сотрудников / Е. Царёв. URL: https://tsarev.biz/news/gophish-besplatnaya-fishing-platforma-dlya-obucheniya-sotrudnikov/ (дата обращения: 04.10.2022).

В. В. Стрекалова,
обучающаяся гр. 111-Ибо
А. Н. Некрасов,
старший преподаватель
кафедры информационной безопасности
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Подделка межсайтовых запросов веб-сайта

Аннотация. *В статье рассмотрены вопросы подделки межстайтовых запросов в программном обеспечении.*

Ключевые слова: *межсайтовые запросы, веб-сайты, CSRF в платежной системе, кибербезопасность*

Одной из самых распространенных атак уязвимости является обход каталога — заменяя запрос к веб-серверу, злоумышленник может получить доступ к конфиденциальным данным. Такое возможно при отсутствии контроля доступа к объектам.

Чтобы решить проблему с обходом каталогов, необходимо четко «прописать», к каким файлам может получить доступ пользователь. В примере необходимо предоставить пользователю доступ к папке documents с файлами. Чтобы пользователь не смог выйти за пределы данной папки, необходимо ввести проверку. Указываем базовый каталог, проверяем на соответствие и предоставляем пользователю доступ только после проверки.

Для защиты от включения файла и подделки запросов на стороне сервера необходимо ограничить пользователя от других функций. Например, для выбора языка страницы ограничим пользователя тем, что веб-приложение не сможет загружать ничего другого, кроме трех веб-страниц с разными языками.

Таким образом пользователь получит доступ только к тем страницам, к которым должен получить доступ, а к другим функциям у него доступа не будет.

В рамках данного исследования были рассмотрены отсутствие контроля доступа к функциональному уровню, подделка межсайтовых запросов: обход каталога, включение локального файла, подделка запросов на стороне веб-сервера, CSRF в платежной системе, CSRF при смене пароля и способы их защиты.

***

1. OWASP Top 10 [Электронный ресурс]. URL: https://owasp.org/Top10/ (дата обращения: 10.09.2022)

2. Введение в безопасность Web-приложений [Электронный ресурс]. URL: https://clck.ru/qFXWF (дата обращения: 15.09.2022)

А. И. Терновецкий[7]
обучающийся гр. 121-Ибо
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Исследование радиоэфира с использованием технологии SDR

Аннотация. *Статья посвящена вопросам построения и практического использования программируемых цифровых радиоприемников SDR на примере известного устройства HackRF One.*

Ключевые слова: *программируемые цифровые радиоприемники*

Сегодня в среде технических энтузиастов и инженеров-специалистов различных профилей (в том числе по информационной безопасности) набирают популярность программируемые цифровые радиоприемники (SDR, Software Defined Radio, в русскоязычном интернете часто переводится как «программно-определяемое радио»).

SDR – это радиокоммуникационная система, где компоненты, реализующиеся обычно «в железе», реализованы по средствам программного обеспечения, работающего на персональном компьютере или встраиваемой системе.

Существуют программные конструкторы, такие как GnuRadio Companion, позволяющие формировать тракты (приемные и передающие) обработки сигналов в виде графических схем, в которых за различные стадии преобразований отвечают стандартные блоки с настраиваемыми параметрами, а также существует возможность соединения блоков в единый конвейер обработки.

Технология SDR традиционно используется в специальных областях телекоммуникаций (например, для создания систем связи специального назначения). Однако ее с успехом можно применять для весьма широкого круга задач, в том числе — для создания высокочастотного контрольно-измерительного оборудования, а также для следующих целей:

- приема, обработки и анализа аналоговых и цифровых радиосигналов с различными видами модуляций;
- отслеживания местоположения воздушного и водного транспорта;

[7] Научный руководитель В. А. Устюгов, канд. физ.-мат. наук, доцент, зав. кафедрой информационной безопасности ФГБОУ ВО «СГУ им. Питирима Сорокина», г. Сыктывкар, Российская Федерация.

- приема данных с различных датчиков и беспроводных устройств;
- использования в качестве GPS-приемника;
- использования в качестве анализатора спектра;
- в радиоастрономии;
- получения генератора случайных чисел с высокой энтропией;
- исследования неизвестных протоколов связи.

В настоящем проекте применен радиоприемник HackRF One. Его основной разработчик Майкл Оссманн инициировал разработку в начале 2012 г. (согласно истории проекта на официальном репозитории на https://github.com/greatscottgadgets/hackrf), проект развивается до сих пор (последний коммит датирован 07 ноября 2022 г.).

Цифровой радиоприемник HackRF One, внешний вид платы которого показан на рисунке, использован нами как средство обнаружения радиосигналов и мониторинга состояния радиоэфира, что продиктовано целями обеспечения информационной безопасности и устойчивости работы систем связи.

Так, путем ручного поиска сигналов с помощью программного обеспечения GQRX и SDRSharp были выявлены и идентифицированы с помощью программного обеспечения Artemis 3 ряд сигналов.

Рис. Внешний вид платы программируемого радиоприемника HackRF One в металлическом корпусе

Отметим в заключение, что наличие свободных библиотек для работы с приемниками SDR позволяет разрабатывать инструменты для автоматического обнаружения радиосигналов, в том числе паразитных или несанкционированных.

***

1. Tripathi, N., Reed J. H. Cellular Communications: A Comprehensive and Practical Guide / N. Tripathi, J. H. Reed. Wiley-IEEE Press, 2014. С. 1036.

2. Valdar, A. Understanding Telecommunications Networks. 2nd edition. The Institution of Engineering, Technology, 2017. С. 383.

3. Биккенин, Р. Р. Теория электрической связи / Р. Р. Биккенин, М. Н. Чесноков. М.: Издательский центр «Академия», 2010. С. 336.

4. Гепко, И. А. Современные беспроводные сети: состояние и перспективы развития / И. А. Гепко. К.: ЭКМО, 2009. С. 672.

Е. С. Шестакова,
обучающаяся гр. 111-ИБо
А. Н. Некрасов,
старший преподаватель
кафедры информационной безопасности
ФГБОУ ВО «СГУ им. Питирима Сорокина»,
г. Сыктывкар, Российская Федерация

Тестирование веб-сайтов на наличие уязвимостей путём проведения инъекций

Аннотация. *В статье рассмотрены вопросы тестирования на наличие уязвимостей в программном обеспечении и использованием инъекций.*

Ключевые слова*: тестирование на наличие уязвимостей, HTML инъекция, iFrame*

HTML-инъекция — тип уязвимости, атака которой позволяет злоумышленнику встроить в веб-приложение собственный HTML-код. Если отправить ссылку на такую модифицированную веб-страницу другому пользователю, который доверяет этому веб-приложению и перейдет по указанной ссылке, то он попадет на вредоносный сайт злоумышленника.

HTML-инъекция позволяет злоумышленнику создать на доверенном сайте собственную форму авторизации, которая позволит получить идентификационные данные пользователей.

iFrame — это технология, которая в определенном месте веб-страницы предусматривает изображение или содержимое другой веб-страницы, документа. Как правило, iFrame-инъекции используются для загрузки вредоносного кода: при посещении веб-страницы с таким iFrame без ведома пользователя начинается загрузка вредоносного файла.

Инъекция почтовых заголовков эксплуатируется злоумышленниками в целях отправки большому числу адресатов почтовых писем (спам). Идея в том, что при отправке сообщения веб-сервером почтовому серверу к этому сообщению добавляется заголовок (в данном примере заголовок bcc), в котором указаны адреса других пользователей.

Инъекция команд операционной системы — такая уязвимость, с помощью использования которой возможно выполнение произвольных команд в операционной системе веб-сервера.

***

1. A1. Injection. OWASP TOP 10 [Электронный ресурс]. URL: https://it-systems.su/a1-injection-owasp-top-10/ (дата обращения: 01.09.2022).

2. OWASP Top 10 [Электронный ресурс]. URL: https://owasp.org/Top10/ (дата обращения: 10.09.2022).

3. Введение в безопасность Web-приложений [Электронный ресурс]. URL: https://clck.ru/qFXWF (дата обращения: 15.09.2022).

Научное издание

«SOROKIN STARTUP» & «SOROKIN HACK DAYS»

Региональный форум инновационных проектов
(Сыктывкар, 29 ноября — 1 декабря 2022 года)

Форум практической информационной безопасности
(Сыктывкар, 16 декабря 2022 года)

Сборник материалов

Ответственные редакторы Ю.В. Гольчевский, В. А. Устюгов

Редактор *Л. Н. Руденко*
Верстка и компьютерный макет *А. А. Ергакова*
Выпускающий редактор *Л. В. Гудырева*

Подписано в печать 12.12.2022. Дата выхода в свет 23.12.2022.
Усл. п. л. 2,4. Заказ № 114.
Тираж 50 экз. (1-й завод 10 экз.)

Издательский центр СГУ им. Питирима Сорокина
167982. Сыктывкар, ул. Коммунистическая, 23Б
Тел. (8212)390-472, 390-473.
E-mail: ipo@syktsu.ru
http://www.syktsu.ru/

Отпечатано в соответствии с предоставленными материалами
в ООО "Типография "Центральная",
167000, Республика Коми, г. Сыктывкар, ул. Интернациональная, 157