

Заключение. Внедрение разработанной методики и программного обеспечения в практику сельскохозяйственных предприятий позволит не только повысить точность и достоверность кормового анализа, но и создать научную базу для разработки новых нормативных документов в области кормопроизводства, соответствующих требованиям международных стандартов. Это будет способствовать повышению конкурентоспособности аграрного сектора на внутреннем и международном рынках, а также укреплению позиций Республики Беларусь в области аграрной науки и технологии.

Интегрированная методика комплексного анализа кормов с учетом неопределенности измерений обладает широким спектром практических применений, которые охватывают как сельскохозяйственные предприятия, так и научные исследования. Методика может быть использована в аналитических лабораториях, в производстве кормов, в научных исследованиях и разработке стандартов, в образовании, при экспорте и сертификации кормов.

Предлагаемая методика и программное обеспечение способствуют повышению экономической эффективности сельского хозяйства, соответствию международным стандартам и внедрению инновационных технологий в аграрный сектор. Результаты исследования могут стать основой для дальнейших исследований в области метрологии и кормопроизводства, а также служить инструментом для решения актуальных проблем аграрной отрасли.

1. Буювич, А. Э. Методика определения содержания нейтрально-детергентной клетчатки в кормах с применением амилазы с учетом неопределенности измерений / А. Э. Буювич, Т. В. Буювич // Наука - образованию, производству, экономике [Электронный ресурс] : материалы 76-й Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов, Витебск, 1 марта 2024 г. – Витебск : ВГУ имени П. М. Машерова, 2024. – С. 21–24.

2. Буювич, А. Э. Разработка программ для автоматизации расчетов содержания веществ с учетом неопределенности измерений / А. Э. Буювич, Т. В. Буювич // Материалы докладов 57-й Международной научно-технической конференции преподавателей и студентов : в 2 т. / УО «ВГТУ». – Витебск, 2024. – Т. 2. – С. 364–367.

3. Буювич, А. Э. Алгоритм определения массовой доли сырой клетчатки с учетом неопределенности измерений / А. Э. Буювич, Т. В. Буювич // Наука - образованию, производству, экономике : материалы 77-й Региональной научно-практической конференции преподавателей, научных сотрудников и аспирантов, Витебск, 28 февраля 2025 г. – Витебск : ВГУ имени П. М. Машерова, 2025. – С. 15–18. – Библиогр.: с. 18 (4 назв.).

СОВРЕМЕННАЯ СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ: ВИДЫ АТАК И МЕТОДЫ ИХ ПРЕДОТВРАЩЕНИЯ

Зарудный В.В.,

*магистрант ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Кашевич И.Ф., канд. физ.-мат. наук, доцент*

Ключевые слова. Социальная инженерия, фишинг, вишинг, смишинг, кибератака, спам рассылка, информационная безопасность.

Keywords. Social engineering, phishing, vishing, smishing, cyberattack, spam mailing, information security.

В настоящем цифровом мире информация – один из наиболее ценных ресурсов для любой организации. В связи с этим как можно больше киберпреступников хотят завладеть этой информацией, поэтому придумывают всё более продуманные и эффективные методы атак [1, 2]. К этим методам относится целая глава – социальная инженерия, которая представляет собой серьёзную и часто недооцениваемую угрозу.

Социальная инженерия – это психологическое манипулирование людьми с целью совершения ими определённых действий, выгодных злоумышленнику, или разглашения конфиденциальной информации.

Такой вид атак включает множество различных подходов. Но главное, их задача – завоевать доверие пользователя, ослабить его бдительность, убедить в чём-либо, запугать и так далее. Конечная цель – побудить человека к действиям.

Очень важно, чтобы каждый сотрудник умел своевременно выявлять попытки атак, к примеру фишинговые рассылки электронных писем [3]. Поэтому данная работа будет посвящена созданию методики по работе с практическими инструментами по укреплению безопасности и сокращению числа успешных атак социальной инженерии.

Цель работы – разработка тренировочного стенда для проведения тестирования на осведомлённость сотрудников для предотвращения атак в области социальной инженерии.

Материал и методы. Материалом исследования в данной работе являются объекты информационной системы: почтовые сервера и почтовый агент, web-сервис *GoPhish* и учебная тренировочная локальная сеть. В работе применяются аналитические и сравнительно-сопоставительные методы исследования.

Результаты и их обсуждение. При подробном анализе методов атак социальной инженерии была составлена сравнительная таблица, включающая в себя названия методов и основные каналы для осуществления атаки.

Таблица – Анализ методов атак по каналам осуществления атак

Название метода	Требуется подготовка	Сбор информации	Каналы осуществления атаки					
			Телефонная связь	Соц. сети	Мессенджеры	E-mail	SMS	Съёмные накопители
Фишинг				+	+	+	+	
Претекстинг	+	+	+	+	+	+	+	+
Услуга за услугу			+					
Приманка			+	+	+	+	+	+
Обратная социальная инженерия	+							

Отличным подходом для повышения уровня осведомлённости сотрудников в любой организации будет проведение отделом информационной безопасности учебных фишинговых атак. Это отличная методика для того, чтобы определить текущий уровень познаний сотрудников, определить проблемы, которые нужно проработать более конкретно и усердно, найти пути решения для достижения желаемого результата, провести сравнительный анализ после повторного теста и подвести итоги в отчёте.

В данной работе представлен тренировочный стенд, который достаточно быстро можно развернуть в любой системе. Фишинговая атака будет проводиться посредством электронных писем. Поэтому лучше всего для такой цели подойдёт сервис *GoPhish*, он позволяет проводить детальную настройку атаки, включая редактирование шаблона сообщения, страницы на которую будет переходить пользователь после нажатия на ссылку в сообщении, пользователя откуда будет приходить письмо и пользователей кому будет приходить письмо. Для отправки сообщений будут использоваться собственные почтовые сервера *Postfix* и *Dovecot*, которые будут развёрнуты на виртуальной машине с операционной системой *Ubuntu* на базе ядра *Linux*. Сервис *GoPhish* представляет собой отдельный сервер, поэтому также будет развёрнут на второй виртуальной машине с операционной системой *Windows 10*.

Для полноценной работы стенда необходимо 2 виртуальных машины с операционными системами *Windows 10* и *Linux*, 2 почтовых сервера *SMTP*, выполняющий роль *MTA* (агент передачи почты) и *POP3*, выполняющий роль *MDA* (агент доставки почты),

а также основной сервер *GoPhish* и почтовый клиент *Thunderbird*. Для запуска индивидуально настраивается фишинговая компания в сервисе *GoPhish*, добавляются группы пользователей и соответственно заполняются пользователи, редактируется шаблон сообщения в зависимости от потребностей пользователя. Также имеется возможность просматривать в результатах компании рассылки открывал пользователь письмо или нет, путём добавления специального трекера в письмо. Ещё одним пунктом настраивается страница перенаправления пользователя по ссылке в письме и указываются данные отправителя. Остаётся только запустить компанию из раздела «*Campaigns*». Заполняем созданными данными каждое поле. В поле «*URL*» указывается IP-адрес и порт IIS сервера, который был также развёрнут на виртуальной машине рядом с *GoPhish* сервером. Нужен он для того, чтобы *html*-файл веб-страницы, на которую будет перенаправлен пользователь по ссылке из письма был доступен во всей локальной сети. Выбираем также дату и время отправки и запускаем кампанию. При переходе по ссылке из письма пользователь увидит специальное сообщение.

Заключение. В работе подробно изучена современная социальная инженерия, проанализированы основные типы атак и способы их реализации, составлена сравнительная таблица атак. Был разработан тренировочный стенд для проверки уровня осведомлённости сотрудников и предотвращения атак, связанных с социальной инженерией. Все разработанные материалы были реализованы в организации РУП «Витебскэнерго» и результаты показали, что разработанная методика действительно является эффективной для повышения уровня осведомлённости сотрудников организации.

1. Нестеров, С. А. Информационная безопасность: учебник и практикум для акад.бакалавриата / С. А. Нестеров. – Санкт-Петербургский политехнический университет Петра Великого. – Москва : Юрайт, 2018. – 321 с.

2. Зарудный, В. В. Организация системы удалённого доступа / В. В. Зарудный ; науч. рук. Кашевич И. Ф. // XVIII Машеровские чтения: материалы междунар. научн.-практ. конф. студентов, аспирантов и молодых ученых, Витебск, 25 октября 2024 г. : в 2 т. – Витебск : ВГУ имени П.М.Машерова, 2024. – Т. 1. – С. 28–30. – URL: <https://rep.vsu.by/handle/123456789/44682> (дата обращения: 15.09.2025).

3. Васильева, Н. А. Методы защиты сотрудников от фишинговых атак: роль тренингов и образования / Н. А. Васильева. – М. : РУДН, 2020. – 220 с.

О ПРОИЗВЕДЕНИИ σ -МНОЖЕСТВА ФИШЕРА И σ -КЛАССА ФИШЕРА

Китаров Д.А.,

*магистрант ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Воробьёв Н.Т., доктор физ.-мат. наук, профессор*

Ключевые слова. Класс Фиттинга, класс Фишера, множество Фишера, σ -класс Фишера, σ -множество Фишера, произведение классов и множеств.

Keywords. Fitting class, Fisher class, Fisher set, σ -Fisher class, σ -Fisher set, product Fisher classes and Fisher sets.

Все рассматриваемые группы конечны. В терминологии и обозначениях следуем [1]. Классом Фиттинга называют класс групп $\mathfrak{F}$, замкнутый относительно нормальных подгрупп и произведений нормальных $\mathfrak{F}$ -подгрупп. Классом Фишера называется класс Фиттинга $\mathfrak{F}$ конечных групп G , который удовлетворяет условию: если $G \in \mathfrak{F}$ и H – подгруппа группы G , которая содержит нормальную подгруппу K группы G такую, что H/K является p -группой для некоторого простого числа p , то $H \in \mathfrak{F}$. Известно, что произведение множества Фиттинга и класса Фиттинга даёт множество Фиттинга [2], а произведение множества Фишера и класса Фишера – множество Фишера [3]. В связи с этим актуальна задача о том, является ли произведение σ -множества Фишера $\mathcal{F}$ группы G и σ -класса Фишера $\mathfrak{F}$ – σ -множеством Фишера группы G . Решение указанной задачи – основная цель настоящей работы.

Материал и методы. Мы будем использовать σ -метод предложенный А. Н. Скибой [4] для построения σ -множества Фишера и σ -класса Фишера суть которого заключается в следующем. Напомним, что σ – некоторое разбиение множества всех простых чисел $\mathbb{P}$, т.е. $\sigma = \{\sigma_i; i \in I\}$, где $\mathbb{P} = \bigcup_{i \in I} \sigma_i$, $\sigma_i \cap \sigma_j = \emptyset$, для всех