DOI 10.37882/2223–2966.2022.07–2.02

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ В СФЕРЕ НЕФТЕГАЗОВОЙ ПРОМЫШЛЕННОСТИ: УГРОЗЫ, РИСКИ, МЕРЫ ПРЕДУПРЕЖДЕНИЯ

CYBERSECURITY THREATS IN OIL AND GAS INDUSTRIAL INFORMATION SYSTEM (IIS)

A. Asfha
A. Vaish

Summary. Oil and gas operations (upstream, midstream, and downstream) — are prominent targets for cyber threats of all kinds, much like essential businesses everywhere. Criminal companies, governmental actors, and so-called hacktivists with political agendas are increasingly the sources of these risks.

As a result, the purpose of this study is to identify high-quality studies, assess their contributions, and to identify the cybersecurity threats impacts in the oil and gas industry. Therefore, the result shows that portable USB device, low employee awareness, and Outdated communication, control and monitoring system vulnerabilities and email hacks, ransomware, and phishing threats are the highest top three critical issue in oil and gas industrial information system.

Finally, cybercriminals are becoming a bigger menace to the oil and gas industry. A successful breach has a hefty cost; thus businesses industry should act quickly to create robust security practices. It can discover emerging threats and implement secure systems by using a company-wide approach that fosters security as a design principle and collaboration among facilities.

Keywords: cybersecurity threats; threats impact; cyber threat management and risk mitigation; oil and gas industrial information system.

Асфха Амануэль Эстифанос
Аспирант, Национальный исследовательский университет ИТМО
pressa@itmo.ru
Вайш Абхишек
Доктор философии в области информационной безопасности, доцент, Индийский институт информационных технологий, Аллахабад, Деогхат Джхалва
abhishek@iiita.ac.in

Аннотация. Значение топливно-энергетического комплекса (ТЭК) для мировой экономики огромно. Лидирующие позиции в международной энергетике уверенно занимают предприятия нефтегазовой отрасли, поскольку продукты их переработки применяются практически во всех отраслях промышленности. Именно поэтому предприятия разного уровня (региональные и транснациональные), занимающиеся геологоразведочными работами, добычей, транспортировкой или переработкой нефти и газа, традиционно становятся объектом преступных посягательств, зачастую связанных с использованием информационных технологий (ИТ). Источниками (субъектами) киберагрессии в отношении компаний нефтегазового сектора чаще всего выступают организованные криминальные сообщества, специальные киберподразделения военизированных структур (ориентированные на проведение прокси-военных спецопераций), а также хакеры-одиночки (активисты с радикальными социально-политическими взглядами). Целью данного исследования является анализ ситуации в сфере обеспечения информационной безопасности на предприятиях нефтегазовой отрасли, с учетом потенциальных угроз, а также мер по их нейтрализации и минимизации возможного ущерба.

Ключевые слова: кибербезопасность; противодействие преступности в сфере информационных технологий; управление рисками в ИТ-сфере; информационные системы предприятий нефтегазовой промышленности.

Введение

Изучение собранных материалов о наиболее уязвимых с точки зрения информационной безопасности элементов управляющих систем предприятий нефтегазовой отрасли позволило сформулировать следующие источники угроз:

- интенсивное применение коллективом портативных USB-устройств, что требует наличия в конструкции узловых серверов корпоративных сетей разъемов для подключения таких устройств;
- низкий уровень цифровой грамотности сотрудников компаний;
- использование устаревших протоколов передачи данных и неподдерживаемых разработчиками операционных систем;
- несовершенство систем связи, а также оборудования для контроля и мониторинга информационных потоков;
- взломы учетных записей электронной почты сотрудников компаний;
- атаки автоматизированных рабочих мест с помощью программ-вымогателей и фишинговых мошеннических процедур.

Имея дело с систематическими попытками незаконного проникновения в корпоративные информационные системы извне, нефтегазовые компании отдают себе отчет в возможных последствиях получения преступниками доступа к корпоративным базам данных или электронике, отвечающей за отслеживание технологических процессов. Ущерб в этом случае может быть колоссальным, а последствия — непредсказуемыми.

Единственный выход — создание специальных ИТ-служб безопасности, главным предназначением которых стало бы обнаружение угроз, их ликвидация, а также поддержание работоспособности систем защиты локальных вычислительных сетей (ЛВС) компании от кибератак. Причем деятельность таких ИТ-служб должна быть комплексной и постоянно развивающейся, что является необходимым условием для своевременного ответа на новые вызовы, продуцируемые киберпреступниками.

Важной составной частью комплекса обеспечения кибербезопасности является специальное программное обеспечение (ПО). Антивирусные приложения, брандмауэры и другие ИТ-системы предотвращения вторжений на сегодняшний день отражают до 50% кибератак на корпоративные серверы промышленных предприятий.

Беспрецедентное влияние компаний топливно-энергетического комплекса на состояние мирового рынка и постоянно растущая стоимость энергоресурсов привлекают к активам хозяйствующих субъектов, связанных с ТЭК, повышенное внимание криминалитета и сил, стремящихся к дестабилизации мирового порядка.

Согласно экспертным прогнозам, инвестиции в нефтедобычу в 2019 году достигли 500 млрд. долл. США, при том, что мировой спрос на нефть остается стабильным (на уровне 1 млн. баррелей в день) [1; 2]. Потребление природного газа в 2018 году превысило 140 трлн. кубических футов (Tcf) [3], а к 2040 году оно достигнет 203 трлн. кубических футов (Tcf) [1]!

Быстрыми темпами растут мощности трубопроводов — уже сегодня 97% канадской нефти и нефтепродуктов транспортируется исключительно по трубопроводам. По данным, Американского института нефти (API) в 2019 году трубопроводная система США (инфраструктура среднего потока[1] сети магистрального трубопровода) имела протяженность 2,7 млн. миль [4].

Топливная инфраструктура разных стран, а также компании нефтегазовой отрасли не раз становились мишенью для злоумышленников. Преступников не останавливает даже транснациональный статус таких предприятий. Так, огромный резонанс имела хакерская атака «высокого» уровня против американского трубопроводного оператора — компании Colonial Pipeline, случившаяся 6 мая 2021 года. Компания оказалась перед необходимостью приостановить поставки энергоносителей по трубопроводу. Положение удалось выправить, лишь перечислив киберпреступникам огромный выкуп в биткоинах.

Стоит отметить, что интенсивный процесс цифровизации экономики в целом и промышленного сектора в частности сделал предприятия нефтегазовой отрасли значительно более уязвимыми для хакерских атак. Во многом это стало следствием перехода от централизованных систем управления к распределенным сетям (когда ключевая информация хранится не только на главном сервере, но в разное время может быть локализована на одной или даже на нескольких узловых рабочих станциях корпоративной информационной сети).

Первоначально информационные системы отдельных предприятий были относительно автономны, но в контексте претворения в жизнь принципов концепции «Индустрия 4.0» стало возможным интегрировать различные промышленные объекты в общую систему обмена информацией. Теперь инженеры в состоянии удаленно манипулировать процедурами диспетчериза-

[1] Инфраструктура среднего потока соединяет нефтеперерабатывающие заводы и объекты, которые распределяют нефть и газ конечным потребителям (инфраструктура нижнего потока).

ции и сбора данных (SCADA) [5], а также контролировать все текущие технологические процессы в режиме реального времени посредством управления электроникой, мониторинга показаний датчиков и т.д.

Но одновременно с ускорением научно-технического прогресса обозначаются и новые угрозы. Наиболее опасные из них относят к классу APT (Advanced Persistent Threat) — это *сложные постоянные угрозы*, основанные на разработке программ-взломщиков. К таким угрозам причисляют:

- кибершпионаж (кражу интеллектуальной собственности);
- целенаправленную хакерскую деятельность с помощью внедрения в ИС-жертву программ-вирусов и программ-«червей» (Duqu, Flame), а также атаки типа Night Dragon и Nitro в целях кражи, удаления или искажения данных, выведения из строя системы SCADA.

Авторы вредоносного ПО пользуются уязвимостями программных сред Oracle Java, Windows (особенно серверов Microsoft Active Directory), кодов браузеров и их дополнений (расширений). География подобных ИТ-диверсий против крупных нефтегазовых компаний довольно широка — США, Саудовская Аравия, Катар, Россия, Иран, многие страны Ближнего Востока.

Методы

В этом обзоре литературы анализ данных был начат с 2018 по 2021 год. Таким образом, 50% респондентов опроса состояли из владельцев оффшорных нефтегазовых активов или сотрудников компаний, которые являются владельцами этих активов. В общей сложности 25% работников на морских нефтегазовых активах были представлены подрядчиками (личными и техническими). В общей сложности 19% участников были сторонними консультационными фирмами (консультационными и классификационными организациями). В общей сложности 6% также включали участников из академических учреждений, которые имеют опыт или знания в области морской нефтегазовой деятельности.

Из ответов участников было отмечено, что они представляли оффшорные нефтегазовые активы, из которых 35% были из различных географических регионов по всему миру. 30% респондентов были из Европы, 16% респондентов были найдены из Азиатско-Тихоокеанского региона и региона Ближнего Востока, 6% из Северной Америки. Кроме того, 5% в Центральной и Южной Америке, 5% в Африке и 3% в Восточном Средиземноморье. Очевидно, что активы широко рассредоточены, и эта выборка представляет активы и сотрудников, которые развернуты и эксплуатируются по всему миру.

Влияние фактора киберугроз на деятельность предприятий нефтегазового сектора в зависимости от их места в отраслевой инфраструктуре

Функционирование предприятий нефтегазового сектора в зависимости от места и роли, которые они занимают в рамках отраслевой инфраструктуры (под инфраструктурой нефтегазовой промышленности в данном случае мы понимаем совокупность отраслей и видов деятельности, обеспечивающих добычу, хранение, переработку и доставку потребителям углеводородов), характеризуются группами показателей (транспортной, энергетической, социальной, институциональной, информационной), определяющих эффективность деятельности этих предприятий и позволяющих оценить состояние и динамику нефтегазовой отрасли в целом и отдельных ее составляющих, в том числе в контексте ценообразования поставляемых ими продуктов (оказываемых услуг).

Нас интересуют несколько типов предприятий нефтегазовой отрасли:

1. геологоразведочные;
2. добывающие;
3. транспортные;
4. перерабатывающие (включая те структуры, которые занимаются первичной переработкой).

Вопросы обеспечения информационной безопасности для каждого из указанных типов предприятий связаны с нейтрализацией ряда потенциальных угроз и рисков, в основе которых лежат различные факторы.

Предприятия, осуществляющие проектно-изыскательские и геологоразведочные работы используют закрытые системы сбора данных, поэтому, как правило, наименее уязвимы для хакеров. Кроме того, из-за весьма условного влияния на процесс ценообразования поставляемого углеводородного сырья в текущем времени периодические сбои в функционировании таких предприятий не ведут к серьезным потерям как в финансовом плане, так и в отношении ущерба окружающей среде или здоровью персонала этих компаний. Атака на ИС предприятий, занимающихся геофизической оценкой, проектированием месторождений, буровыми работами, иногда вообще может не попасть в поле зрения персонала этих компаний. В общем случае угрозой для таких предприятий выступает утечка данных, характеризующих производительность скважин, а также технологические сведения, связанные с бурением или текущими финансовыми операциями. К нежелательным последствиям в этой связи можно отнести прямые финансовые потери и возможную утрату компанией конкурентных преимуществ на рынке.

Таблица 1. Характеристики условий и последствий потенциальной кибератаки информационной системы предприятия на аппаратном уровне

Таксономия уязвимостей	Угрозы	Последствия
Недостаточная устойчивость к несанкционированному доступу. Отсутствие условий для обеспечения физической безопасности устройств. Использование морально устаревших устройств и оборудования	Несанкционированные атаки, физические атаки и пр.	Устройства могут быть конструктивно изменены или уничтожены. Сетевая инфраструктура может быть повреждена. Может быть нанесен ущерб окружающей среде

Сектор добычи нефти и газа наименее устойчив к киберагрессии вследствие большей ориентированности на работу «в поле», где ИТ-фактор имеет второстепенное значение, а значит и контроль за состоянием обслуживающих информационных систем оказывается менее последовательным (по причине отсутствия специалистов высокой квалификации или современных инструментов мониторинга). В то же время электроника, отвечающая за отслеживание различных производственных параметров, здесь менее сложна, чем на уровне геологоразведки, и именно она чаще всего становится объектом хакерских атак. Нарушение целостности информационной системы, ее взлом могут привести к утрате контроля за ключевым оборудованием, отвечающим за технологическую безопасность процесса добычи нефти и газа, что чревато прекращением эксплуатации скважин.

Рисками здесь выступают финансовые потери, вызванные потенциальной остановкой добычи углеводородов, а также инциденты, связанные с неисправностью оборудования, которые могут повлечь за собой системные нарушения требований охраны труда в рамках производственного процесса.

Перерабатывающие предприятия, как правило, располагают протоколами, определяющими последовательность действий для предотвращения кибератак. Речь идет о системе управления инцидентами (ICS — The Incident Command System). Она объединяет стандартные алгоритмы реагирования на чрезвычайные ситуации и распространяется на функционал сетей трубопроводов, сферу хранения нефти, нефтепродуктов и газа, а также на морские и железнодорожные перевозки углеводородов от месторождений до нефтеперерабатывающих заводов и др. перерабатывающих производств.

Наименьшее количество случаев отказа информационных систем по причине их взлома фиксируется в добывающем секторе. Вероятными целями киберпреступников здесь выступают ИС управления работой трубопроводных сетей, станций подкачки и других технических сооружений, которые непосредственно контролируют операционный поток и транспортировку.

Процессы первичной обработки, хранения и транспортировки нефтепродуктов и газа критично зависимы от целостности и бесперебойного функционирования соответствующего оборудования. В частности, в отношении трубопроводного транспорта незаконное внедрение в ответственные информационные системы управления ведет к искажению или изменению текущих рабочих показателей трубопровода, что, очевидно, ставит под угрозу его эксплуатацию. В то же время «точек входа» для хакеров здесь предостаточно — магистральный трубопровод включает в себя множество различных технологических сооружений и агрегатов. Наиболее опасными в данном случае являются риски, связанные с нарушением целостности трубопровода и последствиями подобной аварии — утечка углеводородов в окружающую среду, ущерб здоровью персонала, обслуживающего конкретный объект, или населения, живущего на прилегающих к объекту территориях. Эти неблагоприятные события могут привести к нарушению ритмичности поставок углеводородного сырья и/или его потере, что неминуемо скажется на финансовой составляющей деятельности компании.

В сфере промышленной переработки нефти и газа, и нефтехимической отрасли в целом объектами киберпреступников традиционно выступает ИТ-системы газо- и нефтехранилищ, а также нефтеперерабатывающих заводов (НПЗ). Хакеры, как правило, стремятся получить данные, касающиеся запасов сырой нефти и нефтепродуктов. Последствия в общем случае понятны — репутационные риски и связанный с ними финансовый ущерб.

И, наконец, последняя интересующая нас подгруппа предприятий — *структуры, осуществляющие реализацию сырья и продуктов его переработки* конечным пользователям. Несанкционированное вмешательство со стороны третьих лиц в оперативный контроль процессов отгрузки/поставки энергоносителей может привести ко множеству негативных последствий — к примеру, нарушению техники безопасности эксплуатации отдельных технических объектов, простоям и, как следствие, перебоям в поставках и потере доходов.

Таблица 2. Характеристики условий и последствий потенциальной кибератаки информационной системы предприятия на уровне МПО

Таксономия уязвимостей	Угрозы	Последствия
Устаревшая операионная система. Отсутствие защиты предустановленного программного обеспечения от несанкционированного доступа	Внедрение вредоносного ПО	Нарушение или выведение из строя системы ICS

Таблица 3. Характеристики условий и последствий потенциальной кибератаки информационной системы предприятия на уровне ПО

Таксономия уязвимостей	Угрозы	Последствия
Некорректный контроль вводимых входных данных. Устаревшее (необновляемое) или нестандартное программное обеспечение. Отсутствие шифрования передаваемой управляющей информации. Отсутствие надлежащей аутентификации и контроля доступа	Внедрение вредоносных SQL-запросов. Кибератаки, выполняемые программами-вирусами, в том числе на основе удаленно исполняемого кода. DDoS-атаки. XSS-атаки (Cross-Site Scripting) — внедрение вредоносных скриптов на веб-страницы). CSRF-атаки (Cross-Site Request Forgery) — подделка межсайтовых запросов и т.д.	Несанкционированный доступ к ИТ-системе предприятия. Возможность удаленно вмешиваться в работу ИТ-системы предприятия, контролировать процессы, получать доступ к данным и т.д.)

Таблица 4. Характеристики условий и последствий потенциальной кибератаки информационной системы предприятия на уровне сетевой архитектуры

Таксономия уязвимостей	Угрозы	Последствия
Уязвимый протокол связи. Отсутствие шифрования и аутентификации. Недостатки сетевого дизайна. Недостатки способа подключения устройств в рамках реализации проекта архитектуры интернета вещей на конкретном предприятии	Перехват управления DNS-сервером (Domain Name System — системы доменных имен) и выполнение атак на основе подмены серверных запросов	Кража корпоративных паролей. Перехват сообщений электронной почты. Получение доступа к корпоративной ЛВС и VPN-сетям (посредством изменения доменных имен серверов)

Дифференциация угроз безопасности информационных систем предприятий нефтегазовой промышленности

С точки зрения архитектуры ICS (системы управления инцидентами) угрозы в отношении управляющих информационных систем принято подразделять на категории, которые описываются в специальной литературе (фреймворках, словарях) и обеспечивают стандартизацию создания и развертывания прикладного программного обеспечения, лежащего в основе этих информационных систем [6; 7; 8; 9].

В отношении нефтегазовой инфраструктуры в качестве существенных характеристик ICS выделяют:

1. Аппаратный уровень. Он включает в себя весь комплекс физического оборудования: программируемые логические контроллеры, датчики, процессоры, энергонезависимые модули памяти, удаленные оконечные устройства, оборудование для контроля доступа (смарт-карты, RFID-датчики, обеспечивающие автоматическую радиочастотную идентификацию объектов и т.д.), реле и иные устройства. К аппаратному обеспечению, кроме того, относят также маршрутизаторы и сеть кабелей, формирующих ЛВС, а также серверы, рабочие станции, ноутбуки и прочую периферийную электронику.

2. Уровень микропрограммного обеспечения (МПО) — машинно-ориентированные программные мо-

Таблица 5. Характеристики условий и последствий потенциальной кибератаки информационной системы предприятия на уровне бизнес-процессов

Таксономия уязвимостей	Угрозы	Последствия
Недостаточная квалификация персонала предприятия. Ошибки (дефекты), заложенные в просчетах бизнес-логики	Кибератаки на основе подмены действий квалифицированного пользователя	Финансовые потери в долгосрочном аспекте

Таблица 6. Удельный вес различных типов уязвимостей, использованных при кибератаках информационных систем предприятий нефтегазовой отрасли,%

Код	Наименование уязвимости	%
V1	Портативное USB-устройство	24,81
V2	Низкая осведомленность сотрудников	21,85
V3	Устаревшая система связи, управления и мониторинга	19,63
V4	Количество устройств, имеющих доступ к критически важным данным	15,19
V5	Сеть Wi-Fi	14,45
V6	Другие	4,07

Код	Наименование уязвимости	%
T1	Взломы электронной почты	16,75
T2	Вирус-вымогатель	14
T3	Фишинг	13,75
T4	Вредоносные инсайдерские угрозы	11,25
T5	Дистанционное управление системой	11
T6	Утечки данных	10,5
T7	Кибершпионаж	9,75
T8	Отказ в обслуживании	9,5
T9	Другие	3,5

дули низкого уровня, транспонирующие команды операционной системы на уровень управляющего машинного кода (такая информация обычно хранится в энергонезависимой памяти).

В настоящее время практически все электронные устройства содержат встроенное программное обеспечение, предустановленное их производителем (различные операционные системы, инструкции для управления оборудованием, а также набор команд базовой системы ввода-вывода).

3. Уровень прикладного программного обеспечения (ПО). Этот уровень описывает программное обеспечение, необходимое для мониторинга и управления оборудованием, то есть программные модули и приложения, которые позволяют пользователям взаимодействовать с устройствами и серверами (человеко-машинные интерфейсы (HMI), интерфейсы прикладного программирования (API), проприетарные программные пакеты и пр.).

4. Уровень сетевой архитектуры. К данному ровню относят все элементы, сопрягающие отдельные устройства управляющей ИС в единое информационное пространство — корпоративную вычислительную сеть**:** коммутаторы, протоколы сетевых соединений, роутеры (модемы-маршрутизаторы) и прочее оборудование, включая радио-, беспроводные и аналоговые антенны.

5. Уровень бизнес-процессов. Под бизнесс-процессами понимается весь комплекс управляющих и контрольных процедур, реализуемый в рамках информационной системы предприятия применительно к его организационно-технологическим потребностям. Он включает в себя систему принятия решений, логистику, технологические карты производственных процессов и т.д. (т.н. бизнес-логику).

Заключение

Нефтегазовые компании всё масштабнее используют ИТ-технологии для управления организационно-тех-

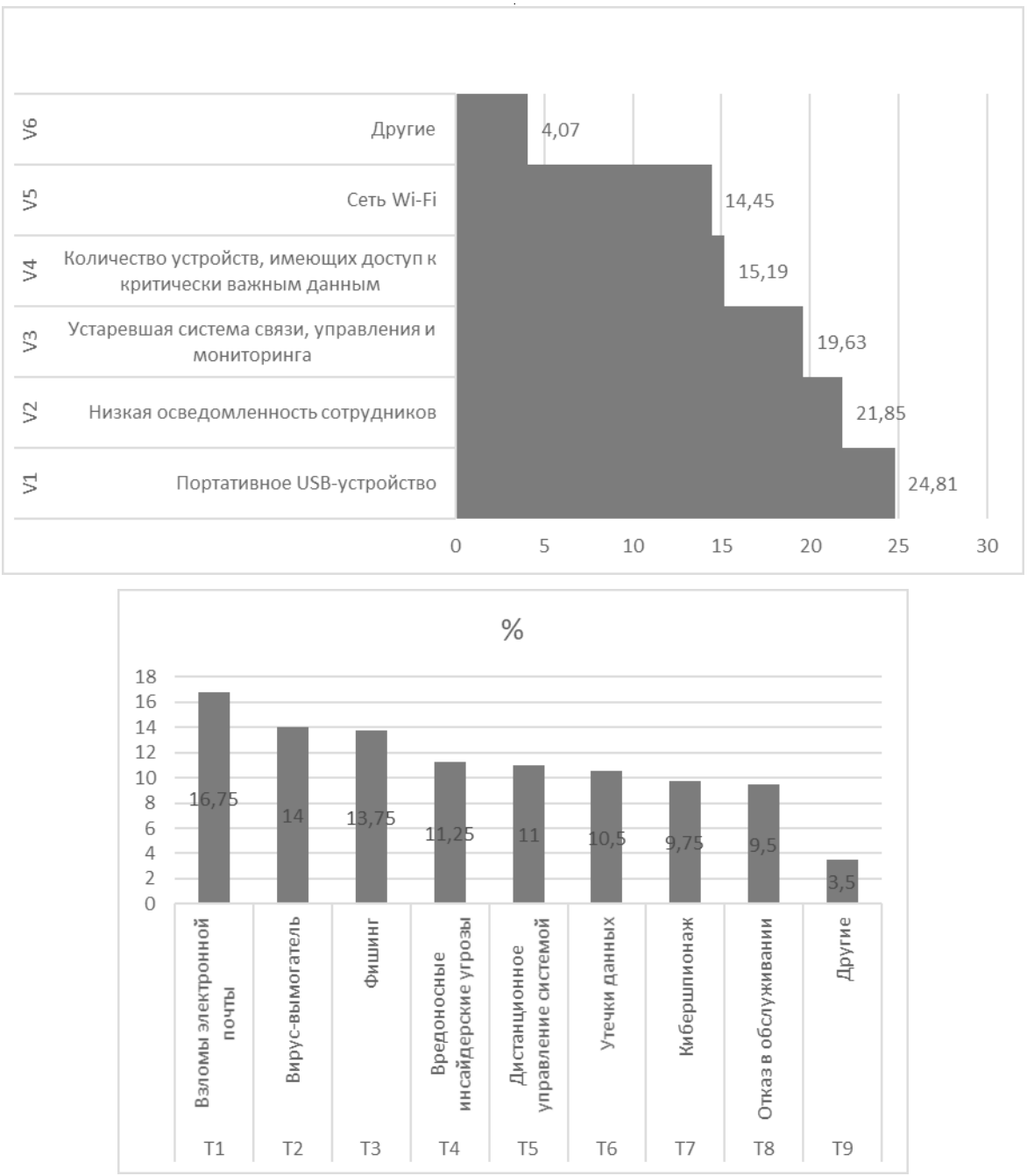

Рис. 1, 2. Графическое представление результатов исследования различных типов уязвимостей при кибератаках ИС предприятий нефтегазовой отрасли

нологическими процессами. Большая номенклатура объектов производственной инфраструктуры (скважины, вышки, станции подкачки, хранилища, распределительные сети) и управленческих центров, построенных на принципе распределенных сетей, предоставляют в этом смысле немало возможностей для кибератак. Поэтому в целях обеспечения информационной безопасности необходимо создать и интегрировать в ИС нефтегазовых компаний комплексные решения, которые позволят управлять рисками и своевременное реагировать на возникающие киберугрозы. Причем универсального решения здесь нет — каждая компания должна на основании собственного опыта определять приоритеты, бюджет и структуру финансирования работ по выстраиванию эффективной корпоративной ИТ-защиты.

Данные наших исследований указывают на тот факт, что наибольшую опасность с точки зрения потенциальной киберагрессии представляет собой использование портативных USB-устройств, низкая цифровая культура

персонала компаний (отсюда частые взломы учетных записей сотрудников, случайная активация программ-вымогателей и фишинговых процедур), а также использование устаревшего оборудования и программного обеспечения. Именно эти угрозы требуют, на наш взгляд, первоочередного внимания и адекватного ответа в части обеспечения информационной безопасности информационных систем предприятий нефтегазовой отрасли.

ЛИТЕРАТУРА

1. Анализ и прогнозы — Управление энергетической информации США. Анализ и прогнозы — Управление энергетической информации США // Доступ: https://www.eia.gov/outlooks (дата обращения: 21.12.2019).
2. Серия отчетов о рынке «Нефть 2019 — Анализ». Международное энергетическое агентство (МЭА), март 2019 года. [Онлайн]. Доступ: URL: https://www.iea.org/reports/oil-2019 (дата обращения: 21.12.2019).
3. Гарсайд М. Глобальное потребление природного газа в 2018 году // Statista, 09 августа 2019 года. [Онлайн]. Доступ: https://www.statista.com/statistics/282717/global-natural-gasconsumption (дата обращения: 21.12.2019).
4. Генерация энергии в Америке: состояние американской энергетики в 2019 году // Американский институт нефти, 2019 год. [Онлайн]. Доступно: https://www.api.org/~/media/Files/Policy/SOAE2019/SOAE2019_Report.pdf (дата обращения: 03.01.2020 г.).
5. Алькарас С. и Зеадалли С. Защита критических систем управления в XXI веке // Компьютер.— Т. 46. № 10. стр. 74–83, 2013.
6. Стауффер К., Пиллиттери В., Лайтман С., Абрамс М., Хан А. // NIST SP 800–82 rev. 2: Руководство по безопасности промышленных систем управления (ICS): Системы диспетчерского управления и сбора данных (SCADA), Распределенные системы управления (DCS) и другие конфигурации систем управления, такие как Программируемые логические контроллеры (PLC). Министерство торговли США, NIST, 2015.
7. Маклафлин С., Константину К., Ван Х., Дэви Л., Садеги А., Маньятакос М., Карри Р. Ландшафт кибербезопасности в промышленных системах управления // Труды IEEE. Т. 104. № 5. С. 1039–1057, 2016.
8. Стром Б., Эпплбаум А., Миллер Д., Никелс К., Пеннингтон А., Томас К. Mitre attack: дизайн и философия, MITRE, 2018.
9. Келирис.А., Константину К., Цоутсос Н.Г., Байад Р., Маньятакос М., Обеспечение многоуровневой оценки кибербезопасности промышленных систем управления с помощью тестовых стендов аппаратного обеспечения в цикле, 21-я конференция по автоматизации проектирования в Азии и Южной части Тихого океана. С. 511–518, 2016.

Журнал «Современная наука: актуальные проблемы теории и практики»